

AI Powered IT Networks and the Implementation of Advanced Sustainable Infrastructure Solutions to Enterprise Systems Globally

Shruti Singh

Information Technology

National Digital Library Of India

Abstract:

The contemporary business demands a smart system that will be capable of making the use of cybersecurity as well as sustainable energy optimized. This paper presents a Smart Enterprise AI Framework, which combines network intrusion detection and renewable energy forecasting to facilitate real-time decision-making. This framework is a multi-class classification and regression machine learning algorithm that is used to analyse network traffic, predict the solar power generation, and predict the wind energy production. An end-to-end preprocessing pipeline, consisting of data cleaning, encoding, scaling, and model training, was adopted. The created models were well-predicted and could be effectively incorporated into a single system that could produce concurrent insights in various areas of the enterprise. The findings underscore the promise of multi-domain AI solutions as a means to improve enterprise reliability, better sustainability planning, and assist with intelligent monitoring. The suggested framework offers an expandable basis to future real-time AI systems to make quicker decisions based on data and close the divide between cybersecurity and sustainability in intelligent enterprise settings.

Keywords: Smart Enterprise AI, Intrusion Detection, Renewable Energy Forecasting, Machine Learning, Solar Energy Prediction, Wind Energy Forecasting, Decision Support Systems

1. Introduction

Smart enterprise ecosystems that operate on Artificial Intelligence (AI), cloud computing and analytics have emerged due to the rapid digitalization of the industries. With the trend of interconnected IT infrastructures, organizations are progressively engaging in mission-critical operations, heavy data processing, and real-time decision-making that have amplified challenges of managing secure, efficient, and sustainable digital infrastructure ((Mahmood, H. S., Abdulqader, D. M., Abdullah, R. M., Rasheed, H., Ismael, Z. N. R., & Sami, 2024). As a result, companies currently have to have combined technological systems, which will respond to cybersecurity risks and energy sustainability issues at the same time (Baruwa, 2023).

The increased reliance on digital services has led to a rise in cyber-attacks against enterprise networks, cloud services, and critical infrastructure like this unprecedented scale. Simultaneously, the global sustainability programs and climate change issues have made organizations cut down on carbon emission and shift towards renewable energy sources (Issa, J., Abdulrahman, L. M., Abdullah, R. M., Sami, T. M. G., & Wasfi, 2024). Historically cybersecurity management and energy optimization have been considered as separate realms. Nevertheless, the notion of intelligent enterprises requires a coordinated strategy where AI technologies will be able to track, predict, and optimize network security as well as energy consumption in one intelligent ecosystem (Omar, H. Y., Abdulqader, D. M., Abdullah, R. M., Ismael, H. R., Rashid, Z. N., & Sami, 2024)v.

This study suggests an AI-based business model combining intrusion detection and renewable energy prediction to enable safe and sustainable business activities (Balasubramanian, 2024). The study combines machine learning methods with real-world data to show how AI can improve the resiliency of cybersecurity and provide additional data-based approaches to managing energy at the same time (Petrovsky, 2024).

1.1 AI-Powered IT Networks

IT networks supporting enterprise have become very complex, distributed, and data-intensive networks that facilitate cloud computing, remote work, IoT devices, and real-time business processes (Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, 2022). With the increasing size of such networks, manual monitoring and rule-based approaches to management are proving to be inadequate. The challenges faced by organizations are on the rise, including cyber threats, network congestion, system failures, and downtime, which may all have a significant impact on productivity and business continuity. In order to address these obstacles, companies are resorting to Artificial Intelligence (AI) to automate their network management and improve decision-making (Shaban, A. A., & Zeebaree, 2025).

Machine learning and deep learning methods are used in AI-driven IT networks to scan network behavior continuously, identify abnormalities and can predict future failures before they happen. This facilitates proactive cybersecurity like real-time threat detection, automated response mechanisms, and predictive maintenance of network elements. Moreover, AI can be used to optimize the network by performing intelligent bandwidth allocation, load balancing, and intelligent traffic routing (Vimal, 2025). Consequently, AI enhances security in addition to increasing the reliability, scalability, and operational efficiency of enterprise networks, making them more robust and future-proof.

1.2 Sustainable Infrastructure in Enterprise Systems

The high pace of digital transformation has greatly augmented the energy requirement of enterprise IT infrastructure, especially data center and cloud platforms. These buildings need to be powered continuously to perform computing, cooling and storage which makes them very expensive to operate and have environmental impact (Khan, M. W., Saad, S., Ammad, S., Rasheed, K., & Jamal, 2024). Due to the growing recognition of climate change and sustainability issues by organizations, there has been a growing demand to develop enterprise systems that are energy-efficient, environmentally friendly and economically viable. This has brought about the use of green computing and renewable energy solutions in enterprise ecosystem (Belgaum, M. R., Alansari, Z., Musa, S., Alam, M. M., & Mazliham, 2021).

Sustainable infrastructure aims at minimizing energy usage and carbon emissions and ensuring high-system performance. Companies are moving towards the use of renewable energy sources in their businesses including solar power, wind power, and energy-saving hardware and intelligent cooling systems. AI is critical in streamlining energy consumption through prediction of power demand, resource utilization, and efficiency of the entire system. Through integrating AI with sustainable infrastructure approaches, organizations can achieve a balance between technological advancement and environmental responsibility, ensuring long-term growth and sustainability (Prabu, 2024).

2. Literature Review

(Masud, S. B., Chowdhury, S. A., Abubakkar, M., Sozib, H. M., Bellal, R. B., Hoque, A., & Shafi, 2025) elaborated the transformative potential of Artificial Intelligence in infrastructure and facilities management, and how AI technologies can facilitate predictive maintenance, resource optimization, and intelligent decision-making. In their research, they highlighted that AI-based automation saves money, increases efficiency, and enhances sustainability of infrastructure systems. The authors concluded that AI incorporation is turning into an essential demand of contemporary enterprise infrastructure.

(Karamchand, 2025) proposed to use AI models as green models to secure data center infrastructure and introduced the idea of sustainable cybersecurity. The study noted the increasing energy demands of cybersecurity activities and proposed energy-efficient AI algorithms to achieve smaller carbon footprints without compromising the quality of security. The research showed that green AI could facilitate sustainability of the environment as well as enhanced protection of threats.

(Okem, E. S., Iluyomade, T. D., & Akande, 2024) delved into the concept of AI and nanotechnology integration to enhance the sustainability and resilience of pavement infrastructure. Their study revealed the application of AI-based

predictive analytics in optimization of maintenance schedules, the extension of infrastructure life and environmental impact. The research mentioned the significance of integrating emerging technologies to develop infrastructure systems that are future-ready and resilient.

(Augoye, O., Adewoyin, A., Adediwin, O., & Audu, 2025) conducted a review of the place of AI in energy financing and sustainable infrastructure investments. The authors explained how AI-driven financial models help predict energy demand, assess risks, and optimize investment decisions for renewable energy projects. Their results showed that AI is an important factor in speeding up the implementation of sustainable infrastructure solutions globally.

(Bharati, 2021) suggested AI-enabled agile enterprise systems to manage industrial wastewater in secure cloud systems. The study revealed how AI could help to monitor the environment, enhance the efficiency of waste water treatment, and secure data management. The paper has highlighted the need to incorporate sustainability practices in the enterprise IT systems.

(Ahmad, N., & Mehmood, 2015) explored the preparedness of enterprise systems towards future sustainable cities. Their work outlined the difficulties of achieving sustainability within enterprise architectures and the necessity of smart, scalable and ecologically sound enterprise systems. The authors have come to the conclusion that sustainable enterprise systems are needed to contribute to the development of smart cities.

(Okereke, M., Isi, L. R., Ogunwale, B., Gobile, S., Oboyi, N., & Sofoluwe, 2025) conducted a comparative study of the trends in worldwide investments in sustainable data center infrastructure. Their research was dedicated to the use of renewable energy, energy-saving cooling systems, and AI-powered resource optimization. The study highlighted the increased significance of green data centers in aiding the global change to the digital front.

(Mille, 2026) explored autonomous AI-driven enterprise cloud security and digital health, financial systems, and smart infrastructure. The paper has emphasized the importance of AI in automating business processes, increasing cybersecurity, and improving resilience of systems. The author found that self-sovereign AI platforms are the future of intelligent and sustainable enterprise ecosystems.

3. METHODOLOGY

This paper will introduce a proposal of a Smart Enterprise AI System, which combines three AI modules, which are Network Intrusion Detection, Solar Power Prediction, and Wind Energy Forecasting. The methodology will include data acquisition, preprocessing, model development, evaluation and system integration.

3.1 Proposed Smart Enterprise AI Framework

This study introduces a hybrid AI system to deploy cybersecurity surveillance and renewable energy prediction to assist in intelligent enterprise decision-making.

The suggested model is structured into four layers:

- **Data Layer:** Multi-domain sets of data on cybersecurity and renewable energy industries.
- **Preprocessing Layer:** The data can be cleaned, transformed, encoded and scaled to be ready to be modeled.
- **AI Modeling Layer:** Three independent machine learning models are trained to do classification and regression.
- **Integration Layer:** Single prediction engine and dash board visualization of real-time enterprise insights.

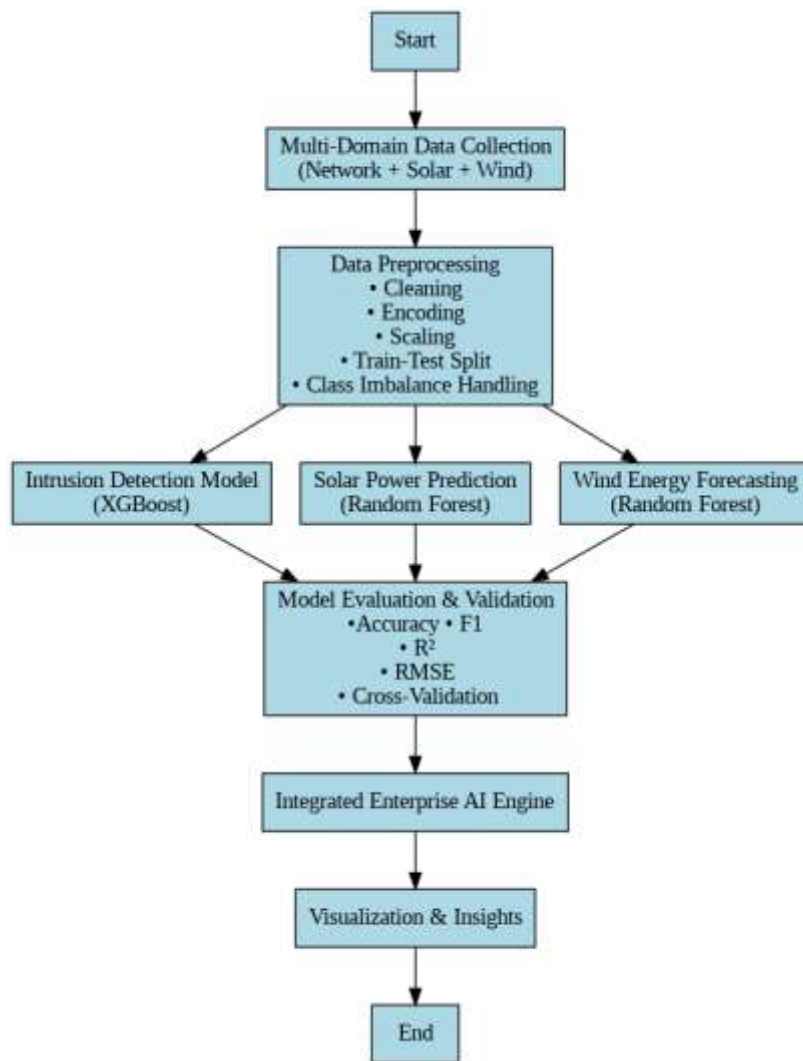


Figure 1: Workflow of the Proposed Smart Enterprise AI Framework

3.2 Dataset Description

In this work, three data sets in the areas of cybersecurity and renewable energy will be utilized to create the proposed Smart Enterprise AI System.

- CICIDS2017 Intrusion Detection Dataset:** The CICIDS2017 dataset is a realistic network traffic that includes network traffic that models normal behavior and various cyberattacks, including DoS, DDoS, brute force, botnet, and web attacks. Every network flow has a lot of traffic-based features. Attack Type is the target variable, which is multi-class.
- Solar Power Generation Dataset:** This dataset of solar power generation was based on weather-based solar energy prediction. It contains meteorological conditions like temperature, humidity, solar radiation, speed of winds and pressure. This is a regression task since the target variable is Power Generated.
- Global Wind Energy Dataset:** A global energy dataset (1965-2023) comprising of country-based annual energy production was utilized in wind energy forecasting. The data were converted into long format where Country, Year and Energy Production were the variables.

3.3 Data Preprocessing

All data sets were ready to guarantee the quality of data and model stability. Non-numeric symbols, multiple records and missing values were eliminated prior to model training. The most important preprocessing steps were:

- Handling infinite and missing values
- Label encoding of categorical variables (attack types and countries)
- Feature scaling using StandardScaler
- Stratified train–test split (80:20)
- Class imbalance handling using class weights

3.4 Model Architecture

Three machine learning models were developed for different enterprise domains.

Module	Algorithm	Task
Intrusion Detection	XGBoost	Multi-class Classification
Solar Forecasting	Random Forest	Regression
Wind Forecasting	Random Forest	Regression

All trained models were integrated into a **unified enterprise AI system** capable of providing real-time cybersecurity monitoring and renewable energy forecasting.

3.5 Evaluation Metrics

Classification and regression tasks were evaluated using different metrics that could be used to guarantee reliable performance measurement of all modules.

Classification Metrics

Standard multi-class performance measures were used to evaluate the classification model:

- **Accuracy:** Proportion of correct instances.
- **Precision:** The number of positive cases predicted that are really positive.
- **Recall:** Measures the model to correctly identify actual positive cases.
- **F1-Score:** Harmonic mean of precision and recall, offers balanced scores.
- **Confusion Matrix:** Graphical display of the correct and incorrect predictions per class.

Regression Metrics

The regression models were tested based on the popular error and goodness-of-fit metrics:

- **R² Score (Coefficient of Determination):** This is used to indicate the extent to which the model accounts of the variation in the variable of interest.
- **Root Mean Square Error (RMSE):** This is used to measure the error of prediction and the accuracy of the model used.

These evaluation metrics are used to give a comprehensive evaluation of model performance in the classification and regression tasks.

4. Results

This section will give the results of the experiment of the proposed Smart Enterprise AI Framework. Evaluation of the classification and regression models performance was done through the use of proper metrics and visual analysis.

4.1 Intrusion Detection Performance

The classification model proved to have a high ability to classify and differentiate various classes of network traffic. The overall accuracy of the model as well as the balance between precision and recall was high, which shows that the model is effective in identifying malicious activities and reducing false alarms.

The confusion matrix analysis indicates that most of the traffic categories were accurately identified with only a few misclassifications between similar patterns. This validates the strength of the model to deal with complex and high-dimensional traffic data.

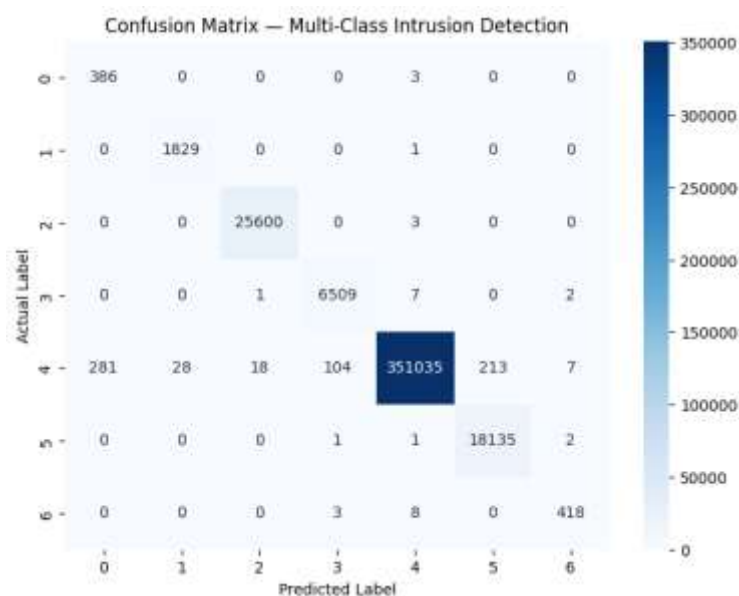


Figure 2: Confusion matrix illustrating the classification performance across multiple traffic classes.

Analysis of feature importance indicated that input features were only a small subset that was important in detection of attacks. This demonstrates the fact that the model could discover meaningful patterns, and eliminate noise due to irrelevant variables.

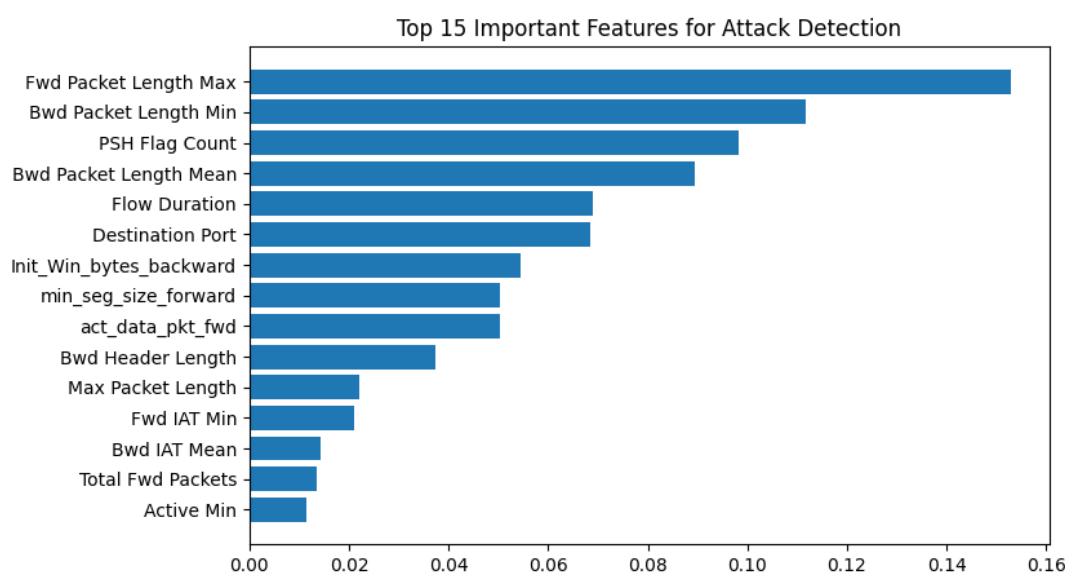


Figure 3: Feature importance ranking showing the most influential features for attack detection.

In general, the results of the classification indicate that the model can be successfully used to facilitate the real-time monitoring of cybersecurity in an enterprise setting.

4.2 Renewable Energy Forecasting Performance

The regression models had good predictive power of energy generation. The high R^2 scores show that the models were able to capture the relationship between the input variables and energy output.

The Actual vs Predicted plots indicate that the majority of predictions are near the ideal diagonal line, which proves that there is low prediction error and the model behaviour is stable.

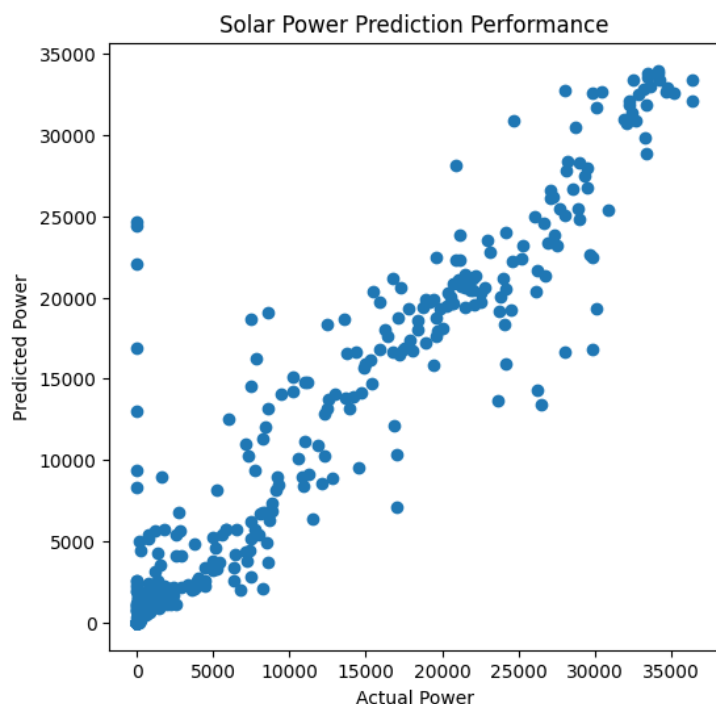


Figure 4: Actual vs predicted values plot showing the accuracy of the renewable energy forecasting model.

The findings of the feature importance suggest that the importance of environmental and temporal variables is significant in predicting renewable energy. This confirms the appropriateness of ensemble learning methods to energy forecasting tasks.

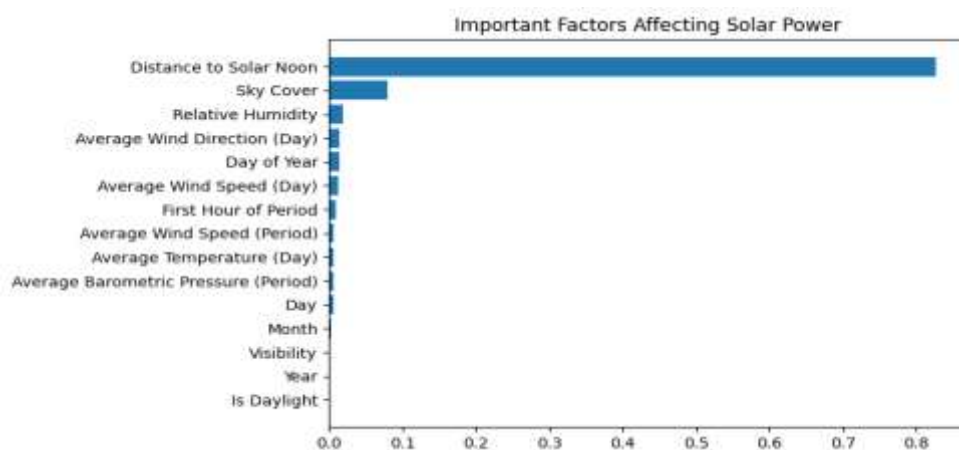


Figure 5: Feature importance analysis highlighting key environmental and temporal variables influencing energy prediction.

These results indicate that machine learning models can be effectively utilized in the process of sustainability-oriented decision making of an enterprise.

4.3 Integrated Enterprise AI System Performance

The holistic architecture was able to produce predictions in real-time that were both related to the status of enterprise security and production of renewable energy. The system output revealed the capability to integrate multi-domain intelligence in one platform to support real time monitoring and decision making.

According to the performance visualization, the security module has received the best system score, which is the high level of ability to detect abnormal traffic on the network. Wind energy forecasting was also able to give meaningful output, and this validates the usefulness of the energy prediction models. The score of solar prediction is relatively lower, which means that there could be more optimization of the model and enrichment of data.

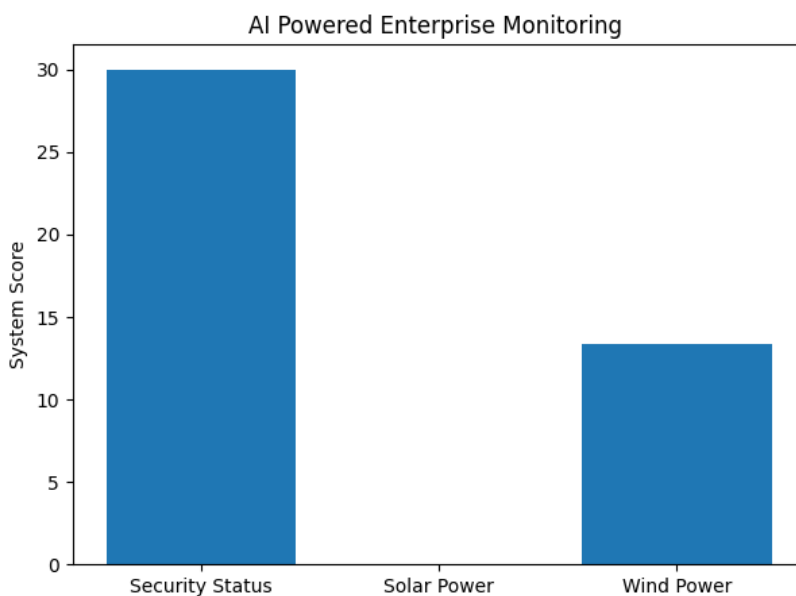


Figure 6: AI-based enterprise monitoring results showing comparative system scores for security status, solar power, and wind power predictions.

4.4 Cross-Validation Results

The generalization ability of the models was tested through cross-validation. The outcomes revealed a stable and reliable performance of the proposed system, as the results reflected the consistency of the performance in several folds.

The high consistency of the validation scores imply that the models are not overfitting and can be applied reliably on unknown data.

5. Conclusion

This paper suggested a Smart Enterprise AI Framework, which combines cybersecurity monitoring with renewable energy prediction to aid intelligent enterprise operations. Several machine learning systems were designed and integrated into a single system that is able to produce real-time insights in both security and sustainability realms. The intrusion detection model was found to be highly effective in detecting abnormal network behavior, revealing that machine learning is an effective tool in proactive cyber defense.

The ensemble learning methods were suitable to model the complex patterns of the environment and time as the renewable energy forecasting models generated reliable predictions. The hybrid system was able to produce concurrent results on both security conditions and energy generation, which indicates the possibility of multi-domain AI to contribute to data-driven decision-making in the contemporary business.

In general, the findings demonstrate that the framework in question has the potential to improve reliability, security, and sustainability of enterprises. Further developments in future work may be directed towards the addition of real-time streaming data, deep learning methods, and IoT-based monitoring to enhance the system scalability, prediction accuracy, and ability to be deployed in the real world.

References:

1. Ahmad, N., & Mehmood, R. (2015). Enterprise systems: Are we ready for future sustainable cities. *Supply Chain Management: An International Journal*, 20(3), 264-283.
2. Augoye, O., Adewoyin, A., Adediwin, O., & Audu, A. J. (2025). The role of artificial intelligence in energy financing: A review of sustainable infrastructure investment strategies. *International Journal of Multidisciplinary Research and Growth Evaluation*, 6(2), 277-283.
3. Balasubramanian, S. (2024). AI-driven solutions for sustainable infrastructure development and management. *Journal ID*, 8291, 5184.
4. Baruwa, A. (2023). AI powered infrastructure efficiency: enhancing US transportation networks for a sustainable future. *International Journal of Engineering Technology Research & Management (IJETRM)*. 2023Dec21, 7(12), 329-50.
5. Belgaum, M. R., Alansari, Z., Musa, S., Alam, M. M., & Mazliham, M. S. (2021). Impact of artificial intelligence-enabled software-defined networks in infrastructure and operations: Trends and challenges. *International Journal of Advanced Computer Science and Applications*, 12(1).
6. Bharati, S. (2021). AI Driven Agile Enterprise Systems for Industrial Wastewater Management in Secure Software Defined Cloud Environments. *International Journal of Research and Applied Innovations*, 4(6), 6208-6215.
7. Issa, J., Abdulrahman, L. M., Abdullah, R. M., Sami, T. M. G., & Wasfi, B. (2024). AI-powered sustainability management in enterprise systems based on cloud and web technology: Integrating IoT data for environmental impact reduction. *Journal of Information Technology and Informatics*, 3(1), 154.
8. Karamchand, G. (2025). Sustainable cybersecurity: Green AI models for securing data center infrastructure. *International Journal of Humanities and Information Technology*, 7(02), 06-16.
9. Khan, M. W., Saad, S., Ammad, S., Rasheed, K., & Jamal, Q. (2024). Smart infrastructure and AI. In *AI in Material Science* (pp. 193-215). CRC Press.
10. Mahmood, H. S., Abdulqader, D. M., Abdullah, R. M., Rasheed, H., Ismael, Z. N. R., & Sami, T. M. G. (2024). Conducting in-depth analysis of AI, IoT, web technology, cloud computing, and enterprise systems integration for enhancing data security and governance to promote sustainable business practices.
11. Masud, S. B., Chowdhury, S. A., Abubakkar, M., Sozib, H. M., Bellal, R. B., Hoque, A., & Shafi, S. B. (2025). The revolution of AI in enhancing infrastructure and facilities management.
12. Mille, J. (2026). Autonomous AI Driven Enterprise Platforms for Cloud Security Digital Health Financial Systems and Smart Infrastructure. *International Journal of Science, Research and Technology*, 9(2), 413-422.
13. Okem, E. S., Iluyomade, T. D., & Akande, D. O. (2024). Revolutionizing US Pavement Infrastructure: A pathway to sustainability and resilience through nanotechnology and AI Innovations. *World Journal of Advanced Engineering Technology and Sciences*, 11(2), 411-428.
14. Okereke, M., Isi, L. R., Ogunwale, B., Gobile, S., Oboyi, N., & Sofoluwe, O. (2025). Data Centres: An In-Depth Comparative Analysis of Global Trends in Sustainable Infrastructure Investment.
15. Omar, H. Y., Abdulqader, D. M., Abdullah, R. M., Ismael, H. R., Rashid, Z. N., & Sami, T. M. G. (2024). A Review on Upshots of Cloud Computing and Web Technology on the Future Green Transformation: AI, IoT, and Secure Enterprise Systems in Fostering Sustainable Work Practices. *Journal of Information Technology and Informatics*, 3(2).

16. Petrovsky, N. I. (2024). AI-Powered Smart Connect Ecosystems with BERT, NLP, WSN, and SDN for Sustainable IT Infrastructure Modernization. *International Journal of Research and Applied Innovations*, 7(6), 11666-11671.
17. Prabu, R. (2024). Advanced AI Driven Cloud Systems for Secure Scalable and Intelligent Enterprise Operations with Autonomous Decision Making. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, 7(5), 11001-11009.
18. Shaban, A. A., & Zeebaree, S. R. (2025). Building scalable enterprise systems: The intersection of web technology, cloud computing, and AI marketing. *Polaris Global Journal of Scholarly Research and Trends*, 4(1).
19. Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2022). AI-powered operational resilience: Building secure, scalable, and intelligent enterprises. *Artificial Intelligence and Machine Learning Review*, 3(1), 1-10.
20. Vimal, V. R. (2025). Next Generation Enterprise Architecture for SAP Cloud Systems Leveraging AI Driven Analytics and Hybrid Infrastructure. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 7(6), 11174-11182.