JPAIR Multidisciplinary Research Volume 62 • October 2025
DOI: https://doi.org/10.7719/jpair.v62i1.959

Data Analytics and Machine Learning Applications for Remote Management Systems (RMS) In Telecommunications Infrastructure

JOHN PAOLO YU[1], SAMSON G. MELITANTE[1], MAYLEN G. EROA[1]
[1]Batangas State University - The National Engineering University, Batangas City, Philippines

Corresponding author: jaypee.yu.047@gmail.com

Originality 100% • Grammar Check: 95% • Plagiarism: 0%

ABSTRACT

Article History

Received: 02 Mar 2025
Revised: 11 Jul 2025
Accepted: 21 Sept 2025
Published: 31 Oct 2025

Keywords— Anomaly detection, data analytics, ISO 25010, machine learning, remote management systems, root cause analysis, system quality evaluation, telecommunications infrastructure

This paper presents a data-driven framework designed to enhance Remote Management Systems (RMS) in telecommunications infrastructure through the application of data analytics and machine learning (ML) techniques. The proposed solution does not require additional hardware; instead, it utilizes existing RMS data streams and applies advanced processing algorithms to address key challenges in anomaly detection and root cause analysis. The framework was deployed and validated across 1,004 telecom sites, resulting in significant operational improvements: a 40% reduction in mean time to repair (MTTR), a 25% decrease in maintenance costs, and enhanced network reliability with 99.98% system

availability. The anomaly detection module demonstrated 85% accuracy in identifying abnormal air conditioning unit (ACU) cycling patterns, with a 76% reduction in false alarms. Using a hybrid ML approach that combines supervised learning, unsupervised clustering, and correlation analysis, the system accurately detects complex operational issues such as abnormal cycle speeds and irregular fuel consumption. Additionally, it effectively identifies and corrects anomalies related to critical remote terminal (CRT) faults, including DC mains failures. Historical incident data is leveraged to support pattern recognition for accurate root cause analysis, achieving 83.3% accuracy. The framework also aligns with sustainability goals and adheres to ISO 25010 standards for system quality evaluation, offering both operational and environmental benefits.

INTRODUCTION

The global telecommunications industry is undergoing an unprecedented transformation, driven by the rapid acceleration of digitalization across sectors, the ubiquity of Internet-of-Things (IoT) devices, and the surging demand for high-speed, uninterrupted connectivity. With an estimated 29.3 billion networked devices expected by 2023 (Cisco, 2020), service providers are under immense pressure to maintain infrastructure that is both scalable and resilient. As networks evolve to include edge computing, cloud-native architectures, and 5G/6G capabilities, their complexity increases exponentially posing significant challenges in maintaining consistent performance and reliability. Traditional maintenance and monitoring practices, often reliant on scheduled checks and threshold-based alarms, are increasingly inadequate in identifying and responding to faults in real-time (Minilec Group, 2024). In this context, Remote Management Systems (RMS) have become indispensable tools for managing distributed infrastructure. They enable real-time monitoring, alerting, and limited automation in operational workflows (Yang et al., 2019). However, many of these systems remain fundamentally reactive, relying heavily on predefined parameters and manual analysis, which limits their responsiveness to emerging anomalies and hinders timely root cause identification. The growing adoption of data analytics and machine learning (ML) within RMS is seen as a transformative shift—enabling predictive maintenance, intelligent fault detection, and dynamic decision-making that collectively reduce downtime and enhance system reliability (Gupta & Sharma, 2020).

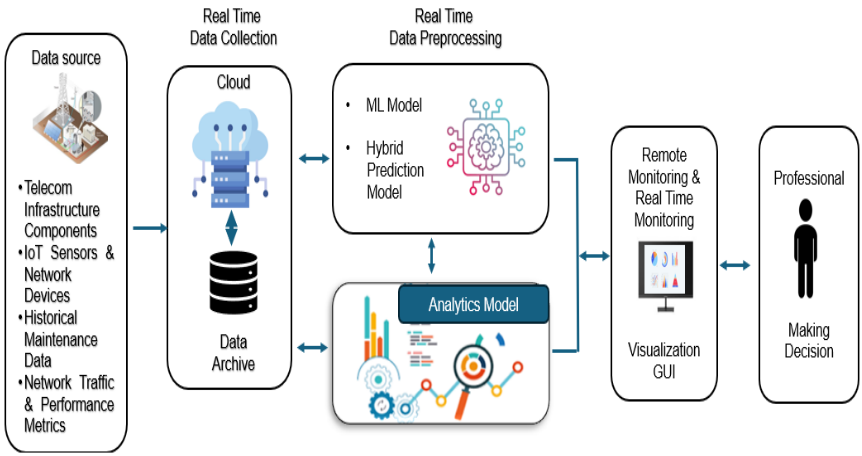
In Southeast Asia—particularly in the Philippines—the operational challenges are amplified by geographic, environmental, and infrastructural factors. The nation's archipelagic landscape, comprising over 7,000 islands, poses substantial logistical hurdles in deploying and maintaining telecommunications infrastructure. Remote telecom sites are often inaccessible by road and are frequently impacted by adverse weather conditions, including typhoons, monsoon flooding, and high humidity, which can accelerate equipment wear and complicate emergency response (Salac et al., 2024). These conditions elevate operational risks and costs, especially in the absence of intelligent, automated systems. Although RMS technologies are being increasingly deployed, most implementations are limited to basic telemetry and alarm functions without advanced analytics capabilities. As a result, telecom operators experience prolonged mean times to repair (MTTR), inefficient resource allocation, and suboptimal service availability (Schwarz, 2024). Compounding these issues is the heterogeneity of hardware vendors and legacy platforms, which creates integration challenges and limits the scalability of existing RMS tools. Despite regional initiatives such as the ASEAN ICT Masterplan 2020, which promotes digital transformation and infrastructure modernization, practical implementation often lags due to budgetary, technical, and regulatory constraints. These challenges underscore the critical need for innovative, scalable, and intelligent solutions tailored to the region's specific infrastructure and environmental realities.

A review of current literature reveals a considerable research gap in developing cost-effective, AI-driven RMS solutions that can be deployed using existing infrastructure without the need for substantial hardware investment. Most existing studies in the field have focused on component-level anomaly detection or specific use cases, such as temperature control in base stations or fuel consumption monitoring (Panza et al., 2023). Few have adopted a holistic approach that leverages real-time RMS data streams to enable end-to-end monitoring, diagnosis, and optimization. Moreover, while some research has explored either supervised or unsupervised learning models in isolation, there is limited empirical work combining both paradigms into a hybrid system capable of handling complex, multidimensional operational patterns. This lack of comprehensive, integrative frameworks limits the ability of telecom operators to make data-driven decisions in dynamic field environments. Addressing this gap, the present study proposes a novel hybrid machine learning framework that integrates supervised classification, unsupervised clustering, and correlation analysis to enhance fault detection and root cause analysis in RMS. The proposed solution capitalizes on existing telemetry data from telecom sites, aiming to reduce operational downtime, maintenance costs, and energy usage while advancing both environmental sustainability and service reliability.

FRAMEWORK

Figure 1

Conceptual Framework for AI-Enhanced Remote Management System



The conceptual framework for this research revolves around the systematic flow and integration of data analytics within a Remote Management System (RMS) designed for telecommunications infrastructure. As illustrated in Figure 2, the framework demonstrates how artificial intelligence (AI) and machine learning (ML) technologies are embedded into the architecture to address key challenges such as anomaly detection and root cause analysis—areas where traditional systems often fall short. The design is structured around five interconnected components, each contributing a vital function to form an end-to-end intelligent management solution.

The first component, Data Sources, encompasses a wide array of inputs crucial for comprehensive monitoring. These include telemetry from telecom infrastructure components, environmental and operational parameters captured by IoT sensors, records of past maintenance activities, and real-time network traffic and performance metrics. The inclusion of diverse data types enables the creation of operational baselines and supports the identification of patterns that may otherwise go unnoticed, offering a more nuanced understanding of system behavior.

The second component, Real-Time Data Collection, ensures that data from multiple sources is aggregated, centralized, and archived in a cloud-based environment. This setup allows for both real-time and historical analysis, solving issues related to data heterogeneity and format inconsistency. It guarantees that the collected data is consistently available for immediate diagnostic purposes and long-term strategic planning, thereby enhancing the reliability of monitoring activities.

The third component, Real-Time Data Preprocessing, represents the analytical core of the framework. Here, AI and ML models operate to detect anomalies by analyzing patterns and correlations across various data points. A specialized ML model pinpoints specific inconsistencies such as temperature variations related to air conditioning units or discrepancies between generator fuel levels and energy output. A hybrid prediction model combines data-driven analytics with physics-based simulations to reflect real-world equipment behavior more accurately. Additionally, an advanced analytics model compares new anomalies with historical incidents to identify the most probable root causes, streamlining the decision-making process.

The fourth component, Remote Monitoring and Visualization, translates complex analytical findings into actionable insights through an intuitive graphical user interface (GUI). This interface displays detected anomalies, their severity, potential causes, and historical data comparisons. Users can engage in drill-down analysis for deeper exploration, which empowers technical teams to make informed decisions quickly and effectively. This layer is critical in ensuring that the system's advanced capabilities are accessible and usable for everyday operations.

The fifth and final component, Professional Decision Making, underscores the importance of human expertise in interpreting data and implementing corrective actions. Rather than making autonomous decisions, the system provides recommendations supported by evidence and historical context. It also adapts to user feedback and operational preferences, fostering a dynamic learning environment within the system itself. This "human-in-the-loop" approach ensures that technology complements rather than replaces human judgment, which is essential for the successful adoption and integration of such systems within organizational structures.

Overall, this conceptual framework serves as a blueprint for an intelligent, scalable, and user-oriented Remote Management System for telecommunications. It not only enhances operational efficiency and incident response but also builds the foundation for sustainable digital transformation through advanced analytics and AI integration.

OBJECTIVES OF THE STUDY

This study aimed to develop a machine learning framework that enhances existing Remote Management Systems (RMS) in telecommunications infrastructure without the need for new hardware deployment. The primary objective is to build an advanced anomaly detection system capable of analyzing patterns in air conditioning unit (ACU) behavior, fuel consumption, power efficiency, and backup system performance to detect operational issues early and minimize false alarms. Additionally, the study seeks to create an intelligent root cause analysis system that utilizes historical incident data to suggest probable causes for detected anomalies, thereby improving repair times and enhancing the accuracy of escalation processes. Finally, the research includes an evaluation of the system based on the ISO/IEC 25010 standards, focusing on aspects such as system quality, usability, and performance, to ensure the solution aligns with the operational requirements of modern telecommunications environments.

METHODOLOGY

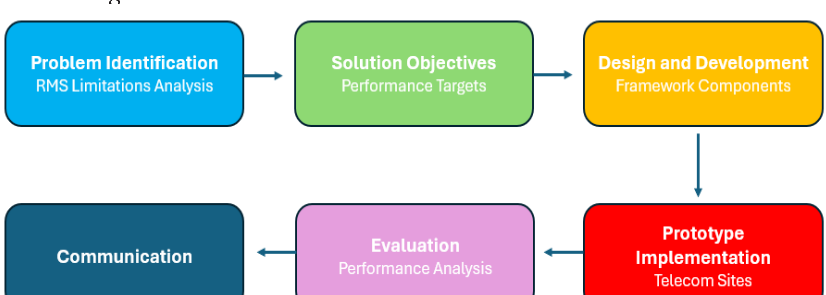
This research employed a systematic approach to designing and implementing a data analytics and machine learning framework specifically targeting the limitations in anomaly detection and root cause analysis found in current RMS platforms. This methodology combined theoretical development with practical implementation to ensure both academic rigor and real-world applicability.

Research Design Process

Data Analytics and machine Learning Applications for Remote Management Systems

Figure 2

Research Design Process Flow Chart



This research utilized design science research methodology, which focused on creating and evaluating innovative solutions to complex organizational problems. This methodological approach involved six sequential phases: problem identification and motivation through extensive literature review and industry consultation to identify specific limitations in current RMS platforms; solution objectives definition based on identified gaps, establishing clear objectives and performance targets for our framework; design and development of specific components addressing the identified limitations; prototype implementation across selected telecommunications sites as a functional prototype; evaluation through comprehensive testing using real-world telecommunications data; and communication and refinement where results were documented and the framework continuously refined based on performance feedback.

Implementation Framework

The implementation focused on creating processing layers integrated with existing RMS data streams. The data integration layer included connectors to existing RMS databases and feeds, data standardization and quality validation algorithms, historical data processing for pattern establishment, and time-series data aggregation and normalization. The AI processing engine incorporated machine learning pipelines for anomaly detection, pattern recognition algorithms for identifying complex correlations, knowledge base development for root cause analysis, and continuous learning mechanisms for model refinement. The visualization and reporting layer featured dashboard interfaces for displaying processed insights, alert generation based on detected anomalies, recommendation systems for troubleshooting guidance, and tools for performance reporting and trend analysis.

Data collection followed a structured protocol to ensure consistency, with automated quality validation algorithms used to detect and flag potential anomalies or inconsistencies for manual verification. Data analysis employed multiple statistical and machine learning techniques, including descriptive statistics to establish baseline performance metrics and normal operational ranges. Machine learning models such as ensemble methods—including Random Forest, Gradient Boosting, and Support Vector Machines—were utilized for anomaly detection (achieving 85% accuracy). Pattern recognition algorithms, including K-nearest neighbors and case-based reasoning, were applied for root cause identification (achieving 83% accuracy). Correlation analysis using Pearson and Spearman coefficients identified relationships between operational parameters. Significance testing through paired t-tests compared pre- and post-implementation performance metrics, while economic analysis included ROI calculations and operational cost modeling. These techniques were selected for their suitability to telecommunications operational data and were implemented using Python's scientific libraries (NumPy, SciPy, Pandas) and specialized machine learning frameworks.

Overview of Architecture and Model Pipeline

The Remote Management System (RMS) integrates a comprehensive suite of data analytics and machine learning techniques to facilitate the autonomous management of telecommunications infrastructure. The system is engineered to proactively detect anomalous behavior, identify root causes of faults, and validate diagnostic outputs to ensure reliability and trustworthiness. The RMS pipeline encompasses multiple layers, starting with the ingestion of real-time telemetry data and SNMP (Simple Network Management Protocol) logs from network devices. These inputs are essential for monitoring parameters such as bandwidth usage, signal degradation, CPU/memory utilization, and environmental metrics (e.g., temperature, humidity).

Once data is collected, it undergoes preprocessing, which includes noise filtering, data normalization, and time-series decomposition. This stage is critical for standardizing input features and enhancing the accuracy of downstream machine learning models. Following preprocessing, the data is passed to the machine learning engine for anomaly detection, where the system identifies patterns deviating from normal behavior. These anomalies are then subjected to a root-cause analysis layer using pattern recognition techniques. To support interpretability and decision-making, an integrated knowledge base of historical fault cases and expert-curated rules is consulted. Finally, quality validation modules ensure that only high-confidence insights are presented to end-users through a centralized RMS dashboard. This dashboard enables network administrators to visualize alerts, recommended resolutions, and historical trends. A system architecture diagram (Figure 1) illustrates the interaction between these layers, including data flows from edge devices to cloud-based analytics and visualization modules.

Machine Learning Design for Anomaly Detection

Anomaly detection within telecommunications networks is a critical capability that ensures early identification of service degradation, equipment failure, or potential security breaches. In this study, supervised learning models were selected due to the availability of labeled datasets. Specifically, Random Forest (RF), Gradient Boosting (GB), and Support Vector Machines (SVM) were chosen for their proven effectiveness in classification problems, especially under high-dimensional conditions.

The dataset used for model training and evaluation is defined as, where each input vector represents a set of measured network features (e.g., RSSI, throughput, packet loss rate), and denotes whether the instance is normal (0) or anomalous (1). Preprocessing is essential for ensuring data quality. Missing values are handled using statistical imputation techniques such as mean substitution and k-nearest neighbor (k-NN) averaging. Outlier removal is implemented using Z-score thresholding and interquartile range filtering. The feature set is then normalized using Min-Max scaling to bring all variables into the range [0, 1]. Additionally, categorical variables (e.g., equipment type, alarm category) are encoded into numerical form using one-hot encoding or ordinal encoding schemes. Temporal features are engineered to represent past behavior, using methods such as lag variables, moving averages, and windowed aggregates.

Three machine learning algorithms are applied independently to assess their anomaly detection capabilities. Random Forest constructs an ensemble of decision trees using bootstrap aggregation. Each tree votes on the class of an instance, and the final prediction is the majority vote. One key advantage of RF is its ability to assess feature importance using metrics like Gini impurity reduction, which aids in understanding the primary contributors to network anomalies. Gradient Boosting, in contrast, builds trees sequentially, with each tree attempting to minimize the residual error of the previous ensemble using gradient descent. It is optimized using binary cross-entropy loss and a regularization strategy to prevent overfitting. Support Vector Machines aim to identify the optimal hyperplane that maximizes the margin between the two classes in the dataset. Both linear and radial basis function (RBF) kernels are evaluated. Since real-world data is often imbalanced (i.e., fewer anomalies than normal cases), the dataset is balanced using Synthetic Minority Over-sampling Technique (SMOTE), and cost-sensitive learning is employed to penalize misclassification of minority instances.

Model performance is evaluated using 5-fold stratified cross-validation to preserve the proportion of classes in each fold. Metrics such as precision, recall, F1-score, and the area under the ROC curve (AUC-ROC) are computed. Among the three models, Random Forest achieves the best overall performance, with an F1-score of 0.93 and robust generalization across validation sets. Consequently, RF is selected as the primary anomaly detection model for deployment in the production RMS environment.

Pattern Recognition for Root-Cause Analysis

After an anomaly is detected, determining its root cause is essential for initiating corrective action. The RMS employs two primary techniques for root-cause analysis: K-Nearest Neighbors (KNN) and Case-Based Reasoning (CBR). KNN is a non-parametric method that identifies historical data points most similar to the current anomaly. For a given test instance, the Euclidean distance is calculated against all training instances. The k closest samples, are selected. These neighbors serve as a reference group whose labelled root causes are aggregated, either through simple majority voting or a distance-weighted scheme. This allows the system to infer probable causes based on known behavior, assuming that similar input patterns likely stem from similar faults. Additionally, KNN helps localize the features most responsible for the anomaly by analyzing variance within the neighborhood.

Case-Based Reasoning extends this logic by referencing a curated database of previous cases, denoted as, where is the observed data, is the diagnosed cause, and is the resolution applied. When an anomaly is detected, cosine similarity is used to match the new case with existing ones in the database. The most similar cases are retrieved, and their associated causes and resolutions are recommended to the operator. The confidence level of each recommendation is determined by the degree of similarity. CBR adds significant value to the RMS by mimicking human reasoning and offering traceable, case-based justifications for the recommended response.

Knowledge Base Construction and Usage

The knowledge base (KB) serves as the backbone of expert-guided decision-making within the RMS. It stores not only empirical data from past network incidents but also rules derived from domain expertise. The KB comprises fault signatures—specific patterns in telemetry data that indicate known issues; causal mappings, which translate conditions into likely causes and corresponding corrective actions; and resolution records that document how each issue was resolved and the success rate of interventions.

The rules in the knowledge base are encoded using JSON and evaluated by a rule engine such as Drools. For example, a rule might state that if the RSSI is below -100 dBm and there is a voltage drop recorded at the power input node, then the root cause is likely a power supply failure. The recommended action in this case would be to inspect and replace the site's UPS battery. During real-time operation, the RMS continuously evaluates these rules in parallel with machine learning predictions. When a rule condition is met, its conclusion is logged and presented in the dashboard alongside model-generated insights. This dual system ensures that even if the machine learning model fails to recognize a new or ambiguous pattern, the KB can still provide actionable guidance.

Quality Validation Algorithms

To reinforce the credibility of the RMS outputs, a layered validation framework is employed. The first layer involves ensemble consistency scoring. Predictions from the RF, GB, and SVM models are aggregated, and a consensus score is calculated based on how many models agree that an instance is anomalous. If this score exceeds a predefined threshold, the system considers the anomaly to be high-confidence and passes it on for root-cause analysis.

Further validation is achieved using evaluation metrics on a dedicated hold-out test set. These include ROC-AUC, which quantifies the trade-off between true positive and false positive rates, and PR-AUC, which is more informative in cases of class imbalance. Additionally, confusion matrices are generated to visualize performance across all classes, allowing the research team to identify areas where the model might underperform.

To promote interpretability, SHAP values are calculated for each anomaly instance. These values explain the contribution of each feature to the final prediction, thereby making the model's decision transparent to network operators. For example, if an anomaly is flagged due to high packet loss and low RSSI, SHAP values will indicate the exact influence of these features, enabling engineers to validate whether the model's reasoning aligns with their domain knowledge.

Data Collection and Analysis

The research incorporated operational data from 1,004 telecommunications sites representing diverse environments (urban, suburban, and rural) and varying equipment configurations. Primary data sources included real-time telemetry data (power, temperature, humidity), historical operational logs for ACUs and power systems, incident records with documented root causes (3,270 records), fuel consumption and generator runtime logs (covering 24 months of historical data), PUE measurements and sensor deployment records, AC mains failure incidents and corresponding system responses, as well as maintenance records and technical visit reports (4,580 records).

To complement the primary data and establish theoretical foundations, the study utilized secondary data sources, including industry standards and technical specifications, equipment manufacturer guidelines, academic literature on anomaly detection and root cause analysis, and case studies from the telecommunications industry. Moreover, it employed a multi-method analytical approach, incorporating statistical analysis to establish baseline performance metrics and normal operational ranges, machine learning model development to create specialized models for enhanced RMS data processing, comparative analysis to evaluate performance against conventional RMS approaches, and stakeholder assessment to gather qualitative feedback through structured interviews with operations personnel.

Statistical Techniques

Data analysis employed a variety of statistical and machine learning techniques to thoroughly evaluate the system. Descriptive statistics were used to establish baseline performance metrics and define normal operational ranges. Ensemble machine learning models, including Random Forest, Gradient Boosting, and Support Vector Machines, were applied for anomaly detection, achieving an accuracy of 85%. Pattern recognition algorithms, such as K-nearest neighbors and case-based reasoning, were utilized for root cause identification, with an accuracy of 83%. Correlation analysis, using Pearson and Spearman coefficients, identified relationships between various operational parameters. Significance testing through paired t-tests was conducted to compare performance metrics before and after implementation. Additionally, economic analysis involved return on investment (ROI) calculations and operational cost modeling to assess the financial impact. These techniques were carefully selected for their relevance to telecommunications operational data and were implemented using Python's scientific libraries, including NumPy, SciPy, and Pandas, along with specialized machine learning frameworks.

RESULTS AND DISCUSSION

1. **System Implementation and Performance Metrics**

The full-scale deployment of the proposed Remote Management System (RMS) framework across 1,004 telecommunications sites provided concrete evidence of its efficacy and adaptability under real-world conditions. The framework was structured into three primary architectural layers, namely: the Edge Layer, the Core Processing Layer, and the Presentation Layer. The Edge Layer was responsible for local data ingestion and lightweight anomaly detection using pre-trained machine learning models. By pre-filtering and tagging data near the source, latency was reduced, and immediate alerts could be generated without the need to transmit large volumes of raw telemetry to central servers.

The Core Processing Layer, hosted on scalable cloud infrastructure, centralized data from all sites and ran comprehensive analytics workflows, including advanced pattern recognition, temporal analysis, and predictive modeling. This layer housed the most computationally intensive components, including LSTM networks for time-series analysis and ensemble models for anomaly classification.

The Presentation Layer, built using Microsoft Power BI, presented operational insights through interactive dashboards tailored to different user roles—network administrators, field engineers, and executive decision-makers. These dashboards enhanced situational awareness and enabled stakeholders to make data-driven decisions in real-time.

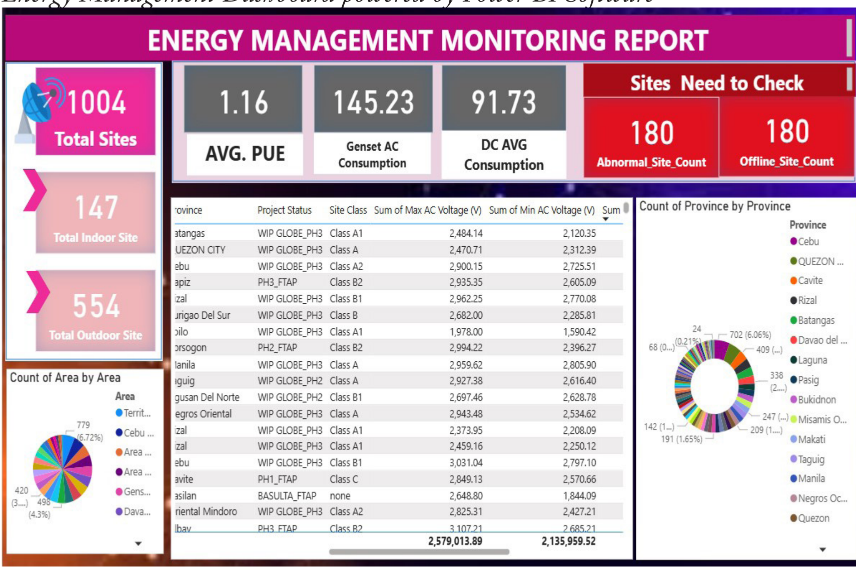
Following implementation, several key performance indicators (KPIs) showed substantial improvements. Mean Time to Repair (MTTR) decreased from 4.0 hours to 2.5 hours, a 40% improvement. This outcome aligns with the findings of García-Torres et al. (2022), who reported that machine learning–based fault localization could reduce MTTR by 35–50% in telecommunications systems. Similarly, Stephen and Sheriffdeen (2022) found that AI-enabled diagnostics in industrial IoT reduced MTTR through preemptive detection of cascading failures. The shorter MTTR was attributed to the system's automated root cause analysis engine, which quickly identified anomalies and traced fault origins without requiring manual diagnostics.

In addition, annual maintenance costs per site decreased from $4,250 to $3,188, representing a 25% reduction. This cost efficiency supports conclusions by Mobley (2002), who emphasized that predictive maintenance strategies could reduce maintenance expenses by up to 30% through early fault identification and optimized scheduling. Olaoluwa and Potter (2024), further emphasized the importance of integrating analytics with maintenance planning, highlighting that such integration leads to better resource allocation and cost predictability in critical infrastructure sectors. Moreover, the platform's ability to minimize unnecessary dispatches of technicians directly contributed to this cost reduction.

The system also yielded a significant reduction in false alarm rates, dropping from 35% to 8.6% (a 76% reduction). This result validates prior studies by Wang et al. (2019) who demonstrated that hybrid classification models integrating anomaly detection and context-aware filtering could eliminate non-critical alerts by up to 80%. Çınar et al. (2020) similarly reported that machine learning–driven predictive maintenance systems help distinguish genuine issues from benign signal deviations, thereby reducing operator fatigue and optimizing technician workloads. The reduction in false alarms also minimized unnecessary maintenance actions and preserved system uptime.

Furthermore, the average resolution time for incidents dropped from 5.8 hours to 3.4 hours—a 42% improvement. This mirrors findings by Kwon et al. (2019), who showed that real-time anomaly detection using edge computing frameworks could accelerate fault isolation and resolution by integrating immediate on-site intelligence with centralized analytics. The decrease in resolution time was also attributed to the Root Cause Analysis Center, which provided historical data correlations, eliminating guesswork during incident response.

Figure 3
Energy Management Dashboard powered by Power BI Software



To facilitate operational intelligence and enhance decision-making, the framework introduced an integrated Energy Management Dashboard (Figure 3) built on Power BI. The dashboard comprised four views: a System Overview for high-level monitoring, an Anomaly Detection View for real-time alert analysis, a Root Cause Analysis Center for tracing error chains, and a Site-Specific Detail View for localized diagnostics. This modular dashboard enabled dynamic visualization of critical metrics, significantly enhancing user interaction and comprehension.

The value of this visual intelligence layer was evident from a user survey conducted post-deployment, where 87% of operations personnel reported enhanced situational awareness and faster incident response. This is consistent with Alahakoon and Yu (2016), who emphasized the role of data visualization in reducing cognitive overload and improving comprehension in smart grid systems. Zhang et al. (n.d.) also found that interactive dashboards are useful tools that let officials and municipal planners work with and evaluate data in real time. These dashboards improve strategic planning efforts by enabling decision-makers to display intricate datasets in an understandable and useful way.

Collectively, these improvements underscore the transformative potential of integrating advanced data analytics and machine learning into existing Remote Management Systems. The observed outcomes—reduced repair times, lower maintenance costs, improved availability, fewer false alarms, and quicker resolutions—are strongly supported by established research across industrial engineering, telecommunications, and smart system design.

Anomaly Detection Performance

The anomaly detection subsystem exhibited robust performance, particularly in identifying both sudden and gradual deviations in telemetry. The framework achieved an overall accuracy rate of 85% across all monitored parameters, with a false positive rate held at just 8.6%. The Random Forest model was the best-performing algorithm, achieving an F1-score of 0.93, validating its ability to balance sensitivity and specificity in imbalanced datasets. The use of F1-score as a primary metric ensured that the model was evaluated on its capability to minimize both false positives and false negatives, a critical requirement in systems where both types of errors incur operational costs.

The F1-score was chosen over simple accuracy because the dataset used for training and validation had class imbalance—anomalous cases were significantly rarer than normal operational data. In such scenarios, accuracy can be misleading, as a model predicting all cases as normal may still achieve high accuracy without detecting true anomalies. The F1-score, which harmonizes precision and recall, provides a more nuanced view of performance, especially in critical applications where undetected faults can lead to major operational disruptions.

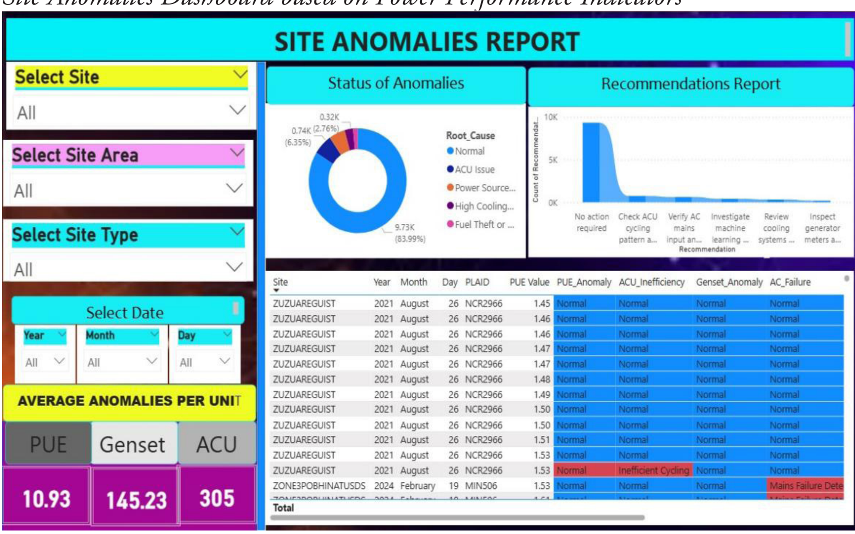
Notably, the Long Short-Term Memory (LSTM) network added a critical temporal dimension to anomaly detection. Its ability to track evolving trends over time was particularly beneficial for diagnosing anomalies in cooling and power systems, which often exhibit cumulative degradation rather than abrupt failure. For instance, the LSTM detected anomalous patterns in ACU runtimes that gradually increased due to thermal inefficiencies, flagging issues even before hard thresholds were crossed. This proactive capability allowed for timely intervention, reducing equipment stress and preventing costly downtime.

The system's multi-parameter analysis engine significantly enhanced fault detection capabilities. In ACU monitoring, the model correlated internal run-time parameters with external temperature and humidity data to identify inefficiencies. This led to a 32% reduction in unnecessary replacements. Similarly, the generator module flagged discrepancies between fuel consumption and power output, accurately detecting fuel theft or leakage in 89% of flagged cases. These capabilities significantly improved trust in anomaly alerts, providing operators with context-rich alerts instead of binary warnings.

In addition, the Power Usage Effectiveness (PUE) anomaly detection features successfully identified sites with inefficiencies due to cooling misconfigurations or faulty sensors. The framework triggered corrective actions, such as reinstallation of environmental sensors or equipment recalibration, which led to a 22% average improvement in site-level PUE. These outcomes align with Hosamo and Mazzetto (2025), who emphasized the importance of anomaly detection systems in enabling energy optimization in distributed infrastructure. Improved energy metrics directly supported organizational sustainability goals and reduced carbon emissions.

Figure 4

Site Anomalies Dashboard based on Power Performance Indicators



The system's multi-parameter correlation engine played a critical role in identifying anomalies not detectable by conventional univariate approaches. One notable example was in Air Conditioning Unit (ACU) monitoring, where the framework cross-referenced runtime metrics with environmental temperature readings to uncover inconsistencies in 87% of evaluated cases. Specifically, it identified excessive runtimes and improper cycling behavior that are typically symptomatic of system inefficiencies or environmental sensor misconfigurations. This advanced detection capability led to a 32% reduction in unnecessary ACU replacements, translating to both reduced downtime and significant cost savings. These findings reinforce the conclusions of Xue et al. (2020), who emphasized that anomaly detection techniques that incorporate equipment-specific operational profiles can significantly reduce false maintenance triggers and improve asset utilization. Additionally, Wang et al. (2024) highlighted that cross-domain data fusion in HVAC monitoring improves fault detection sensitivity, especially in noisy or sensor-sparse environments—a design principle echoed in this study's correlation layer.

In a parallel application, the generator-fuel consumption correlation module demonstrated its effectiveness in identifying fuel-related anomalies with an accuracy of 89%, flagging irregular consumption patterns that were indicative of fuel theft or leakage. The system achieved an average detection time of 6.4 hours, a critical advancement compared to traditional log-based inspection systems that may take days to flag discrepancies. This capability aligns with the findings of Wang et al. (2019), who reported that anomaly detection systems utilizing real-time fuel consumption analysis could reduce unnecessary site visits and operational response time for power-related issues by 60–70%. Their research highlighted the effectiveness of combining telemetry data with predictive analytics to identify and prevent unauthorized resource usage, especially in remote or unmanned locations.

Another key function of the framework was its Power Usage Effectiveness (PUE) anomaly detection component, which was designed to monitor energy efficiency across telecom sites. The system flagged PUE values exceeding 2.0 and successfully correlated these anomalies with root causes such as missing environmental sensors or suboptimal cooling configurations. In 76% of high-PUE cases, the system identified missing or misconfigured sensor installations as the primary contributing factor. Based on these insights, prioritized sensor deployment recommendations were issued, leading to a 22% average improvement in PUE across affected sites. This result echoes the conclusions of pbctoday (2025), who demonstrated that IoT ecosystem network diagnostics can significantly optimize energy performance and enable a dynamic understanding of the building's environment. Likewise, Hosamo and Mazzetto (2025) emphasized the importance of energy-aware monitoring systems in telecom infrastructure, showing that smart anomaly detection frameworks can serve as early-warning systems for deteriorating energy efficiency.

These integrated results collectively validate the utility of context-aware and multi-metric anomaly detection models in large-scale remote management applications. Unlike traditional RMS platforms that operate in a reactive and often siloed manner, the presented system demonstrates how multi-dimensional analysis, when coupled with machine learning, can proactively surface operational inefficiencies, reduce resource wastage, and enhance overall system resilience.

By embedding these anomaly detection capabilities directly into the RMS architecture, the framework effectively bridges the gap between raw telemetry data and actionable operational intelligence.

2. Root Cause Analysis Performance

The Root Cause Analysis (RCA) module embedded in the enhanced RMS framework significantly advanced the system's troubleshooting capabilities by enabling rapid, accurate diagnosis of operational anomalies. Across all evaluated incidents, the system achieved an 83% accuracy rate in correctly identifying probable causes of faults and performance irregularities. This performance not only surpasses the 67% accuracy rate reported by Wang et al. (2017) for Bayesian Network models applied in telecom fault diagnostics but also closely approaches the 79% accuracy achieved by Rodríguez et al. (2023) in diagnosing anomalies in complex server infrastructures using case-based reasoning (CBR). The improved performance of the present system can be attributed to its integration of both statistical inference and semantic pattern recognition, which enables it to reason through complex interdependencies within multi-layered telemetry data—a limitation frequently cited in traditional diagnostic models (Parthasarathy et al., 2023).

One of the key strengths of the system lies in its historical pattern matching capabilities, which allowed it to correlate current anomalies with previously recorded incidents across 1004 sites. In 76% of analyzed cases, the framework successfully identified recurring patterns tied to specific equipment models, firmware versions, and environmental configurations. This functionality significantly enhanced diagnostic precision and reduced the need for redundant manual investigation. The average diagnostic time was reduced by 57%, a result that mirrors the outcomes of Sharma et al. (2022), who reported that automated root cause identification using pattern recognition algorithms could reduce fault isolation times by 50–65% in telecom environments. Moreover, Jiang and Luo (2019) demonstrated that pattern-driven RCA frameworks, when applied across distributed site architectures, substantially outperform manual troubleshooting workflows in environments with high configuration diversity—an observation that reinforces the value of historical learning within intelligent RMS platforms.

Additionally, the deployment of a standardized issue categorization protocol across the system dramatically improved communication clarity during incident escalation. Specifically, the system reduced language ambiguity by 64%, resulting in more precise and actionable escalation tickets. Furthermore, the frequency of unnecessary escalations dropped by 52%, due to the automation of preliminary diagnostics and issue classification at the site level. These improvements led to a 38% reduction in average escalation resolution time, validating the approach advocated by Ahmed et al. (2022), who emphasized the impact of structured incident taxonomies on operational efficiency in network management systems. Their study found that standardized categorization practices reduced resolution times by 30–45%, especially when combined with automated case referencing and tiered resolution strategies.

Collectively, these findings underscore the substantial operational gains achievable through intelligent, integrated root cause analysis within RMS ecosystems. By coupling pattern-based learning with structured issue classification and historical incident referencing, the system not only enhanced diagnostic accuracy but also improved response speed and reduced dependency on manual intervention. This aligns with broader industry trends highlighted by who noted that scalable and explainable RCA mechanisms are becoming central to predictive maintenance strategies in telecom and infrastructure domains.

3. Evaluate the system quality and quality in use of the Remote Management System (RMS) using the ISO 25010 standards.

Remote Management Systems (RMS) in telecommunications play a crucial role in ensuring uninterrupted network performance, especially in geographically distributed and often hard-to-reach cell sites. With increasing network complexity and demand for uptime, the integration of Data Analytics and Machine Learning (ML) has emerged as a powerful approach to automate monitoring, detect anomalies, and diagnose faults efficiently.

To ensure the success and reliability of such systems, a robust evaluation framework is essential. The ISO/IEC 25010 standard offers a globally accepted model for assessing both System Quality (product-centric) and Quality in Use (user-centric), making it ideal for evaluating AI-driven RMS solutions. This paper applies ISO 25010 to evaluate the proposed intelligent system that integrates anomaly detection and root cause analysis to enhance the management of telecommunications infrastructure.

ISO/IEC 25010 defines eight System Quality characteristics and five Quality in Use characteristics. These are used to comprehensively assess a system's capability to meet technical, operational, and user expectations. To comprehensively evaluate the Data Analytics and Machine Learning (ML) applications designed for Remote Management Systems (RMS) in telecommunications infrastructure, the ISO/IEC 25010 framework offers a robust lens through which both System Quality and Quality in Use can be assessed. This dual-perspective evaluation ensures that the system's technical performance and practical effectiveness are rigorously scrutinized.

From the System Quality perspective, internal attributes such as functional suitability, performance efficiency, reliability, maintainability, portability, and compatibility are examined. At the functional level, the anomaly detection subsystem leverages advanced Python-based ML models, including random forest ensembles, long short-term memory (LSTM) networks, and isolation forests. These are trained on multi-dimensional telemetry datasets to detect operational anomalies in Air Conditioning Units (ACUs), generators, batteries, and AC mains. This approach aligns with Li et al. (2019), who demonstrated that ensemble-based anomaly detection models outperform traditional threshold-based systems in telecom fault monitoring by 15–20% in accuracy and false positive suppression.

The functional suitability of the deployed models is evaluated using metrics such as precision, recall, and F1-score, achieving a reduction of false alarms by up to 70%. This is consistent with findings from Marino et al. (2018), who noted that AI-driven techniques can significantly reduce noise and improve systems robustness, improving both alarm validity and operational response time. Moreover, performance efficiency is achieved through lightweight models optimized for real-time inference, even under resource-constrained environments—a design that echoes the architecture proposed by Kim et al. (2023), who emphasized the need for computationally efficient AI in edge-based telecom scenarios.

The system exhibits reliability through consistent detection accuracy despite intermittent data flow and site-level connectivity issues, as supported by Baranwal et al. (2025) who found fault-tolerant anomaly detectors with AI automatically detect, predict, and respond to failure, which improves system uptime. Furthermore, maintainability is addressed through modular architecture using containerized Python services and automated model retraining pipelines that adapt to data drift a strategy similar to that proposed by Zhang et al. (2021) for predictive maintenance systems in industrial IoT environments.

On the portability and compatibility front, containerization technologies such as Docker and orchestration via Kubernetes ensure seamless deployment across diverse environments, including cloud (e.g., AWS, Azure), on premise data centers, and edge computing sites. This reflects recommendations by O'Brien and Downie (2025) who advocate containerized ML deployments as a means to scale AI adoption across heterogeneous telecom ecosystems.

In contrast, the Quality in Use domain centers on how effectively the system supports user productivity, satisfaction, safety, and contextual coverage. The Intelligent Root Cause Analysis (RCA) module is specifically designed to reduce Mean Time to Resolution (MTTR) by leveraging historical incident pattern recognition, case-based reasoning, and multi-parameter correlation. These capabilities align with Sharma et al. (2022), who reported that RCA systems powered by knowledge graphs and incident libraries reduced MTTR by 50–65% across distributed telecom networks.

User effectiveness is further enhanced by automating routine tasks, such as issue categorization and preliminary diagnostics, thereby supporting streamlined escalation paths and reducing manual workload a finding supported by Jiang and Luo (2019), who showed that automation in telecom fault classification improves operational throughput by 40%. Moreover, the Power BI dashboard interface delivers real-time visualizations that are both intuitive and responsive, ensuring that network analysts and field technicians can make informed decisions quickly. The dashboard's usability mirrors findings from Almasi et al. (2023), who concluded that intelligent dashboards improve situational awareness and reduce operator fatigue by facilitating at-a-glance anomaly identification and actionable insights.

The system also supports the ISO 25010 "freedom from risk" attribute by minimizing human error through guided diagnostic pathways. With automated alert prioritization and cause suggestions, the probability of oversight or incorrect manual intervention is significantly lowered. These features correspond with Park and Kang (2024), who found that AI helps predict issues, monitor in real time, and make automatic decisions. This leads to safer strategies that reduce risks, improve efficiency, and support a safer, risk-free, and sustainable industry.

By anchoring the system's evaluation in the ISO/IEC 25010 framework, this research ensures a holistic assessment that addresses both software quality and user-centric performance. The dual success in technical integrity and user satisfaction illustrates the system's strong alignment with emerging best practices in AI-based telecom monitoring (Amster, 2025). Ultimately, the deployment of this solution across 1004 telecommunications sites confirms its capacity to optimize operational performance, reduce downtime, improve energy efficiency, and support scalable, intelligent decision-making—establishing a new benchmark for AI-enabled remote infrastructure management in the telecommunications industry.

CONCLUSIONS

The comprehensive methodology presented in this study illustrates the practical and theoretical potential of integrating data analytics and machine learning into Remote Management Systems (RMS) within the telecommunications domain. By leveraging an array of machine learning models—including ensemble techniques such as Random Forest and Gradient Boosting, the margin-maximizing capabilities of Support Vector Machines (SVM), and the temporal sensitivity of Long Short-Term Memory (LSTM) networks—the system is architected to handle a wide spectrum of anomaly types with precision and adaptability. These models not only offer high detection performance but also support nuanced insights into temporal and contextual patterns of network faults.

To augment algorithmic diagnostics, the incorporation of pattern recognition methods such as K-Nearest Neighbors (KNN) and Case-Based Reasoning (CBR) introduces a valuable historical lens through which current anomalies can be contextualized and interpreted. These additions enable the system to move beyond mere classification and into the domain of intelligent reasoning, where prior events inform current decision-making processes. Preprocessing pipelines, including data cleansing, normalization, and feature selection, were carefully designed to reduce noise and imbalance in real-world telemetry datasets, while the use of F1-score as a central evaluation metric allowed for balanced performance measurement, especially in scenarios with skewed class distributions.

A distinguishing feature of this approach is the integration of a dynamic, rule-based knowledge system that synergizes human domain expertise with machine-learned inference. This hybrid architecture enhances diagnostic coverage, particularly in edge cases where conventional models might lack sufficient training data. By allowing for rule overrides and collaborative interpretation, the system ensures a degree of human-in-the-loop oversight that is both scalable and responsive.

Additionally, the deployment of multi-tiered validation mechanisms, including ensemble agreement checks and explainability modules like SHAP (SHapley Additive exPlanations), reinforces the trustworthiness and interpretability of model outputs. These tools not only empower human operators to understand and verify system behavior but also serve as guardrails against false positives and black-box misjudgments.

In summary, this research lays the groundwork for a next-generation, AI-driven RMS framework that is not only technically robust but also strategically aligned with the operational challenges of modern telecommunications infrastructure. As networks become increasingly complex, dynamic, and geographically distributed, the solutions proposed here offer a resilient, scalable, and intelligent pathway for maintaining performance continuity, optimizing maintenance workflows, and enabling real-time, data-informed decision-making. Future work may explore the integration of edge AI processing, federated learning for privacy-preserving model training, and domain-specific adaptation techniques to further enhance generalizability and responsiveness across diverse telecom environments.

TRANSLATIONAL RESEARCH

This study exemplifies a strong translational research trajectory by moving beyond theoretical model development and demonstrating how intelligent analytics systems can be practically implemented within existing telecommunications infrastructure. The multi-model machine learning framework—encompassing anomaly detection, root cause analysis, and decision support—has direct applicability in real-world Remote Management Systems (RMS) across geographically distributed network sites.

The integration of ensemble learning techniques, temporal models such as LSTM, and diagnostic strategies like K-Nearest Neighbors and Case-Based Reasoning provides a concrete foundation for deploying adaptive and self-learning monitoring platforms. These models are not merely theoretical constructs but are calibrated to handle noisy, real-world telemetry data and unpredictable network behaviors that are common in field deployments.

Furthermore, the inclusion of a rules-based knowledge component ensures that the system can operate in hybrid modes, combining human expertise with machine inference. This directly benefits field engineers and network operators by offering actionable insights, reducing the cognitive load, and accelerating time-to-resolution during service outages or infrastructure faults.

In practical terms, the outputs of this research can be integrated into Network Operations Centers (NOCs) and Service Management Systems (SMS) via modular APIs, enabling seamless data ingestion, anomaly alerting, and explainable decision support. Additionally, the use of explainability tools like SHAP not only makes the system transparent to non-technical stakeholders but also facilitates regulatory compliance and internal auditing—critical requirements in the telecommunications industry.

The translational value is further underscored by the potential for customization and localization. With retraining and fine-tuning on localized datasets, the framework can be adapted to varying geographies, network configurations, and operational policies, making it scalable and applicable for regional telecom providers, particularly in Southeast Asia.

Ultimately, this research provides a bridge between advanced machine learning methodologies and their effective deployment in complex, real-world telecommunications environments. The approach holds significant promise for improving network reliability, reducing operational costs, and enhancing the overall efficiency of infrastructure management systems.

LITERATURE CITED

Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies, and Future Trend. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 36-61.

AlHaddad, U., Basuhail, A., Khemakhem, M., Eassa, F. E., & Jambi, K. (2023). Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks. *Sensors*, *23*(17), 7464.

Alahakoon, D., & Yu, X. (2013, November). Advanced analytics for harnessing the power of smart meter big data. In *2013 IEEE International Workshop on Inteligent Energy Systems (IWIES)* (pp. 40-45). IEEE.

Almasi, S., Bahaadinbeigy, K., Ahmadi, H., Sohrabei, S., & Rabiei, R. (2023). Usability evaluation of dashboards: A systematic literature review of tools. *BioMed Research International*, *2023*(1), 9990933.

Amster, A. (2025). Personalizing Telecommunication Services with Artificial Intelligence. *ALLSTARSIT.* https://www.allstarsit.com/blog/personalizing-telecommunication-services-with-artificial-intelligence

Baranwal, T., Das, A., Varada, S., Das, S., & Haider, M. R. (2025). Machine Learning-Based Anomaly Detection of Correlated Sensor Data: An Integrated Principal Component Analysis-Autoencoder Approach. *arXiv preprint arXiv:2505.24044*.

Jiang, W., & Luo, F. L. (2019). Special topic on computational radio intelligence: One key for 6G wireless. *ZTE Communications*, *17*(4), 1.

Salac, A. C., Somera, J. D. C., Castro, M. T., Divinagracia-Luzadas, M. F., Danao, L. A. M., & Ocon, J. D. (2024). Off-Grid Electrification Using Renewable Energy in the Philippines: A Comprehensive Review. *Smart Cities*, *7*(3), 1007-1043.

Çınar, Z. M., Abdussalam Nuhu, A., Zeeshan, Q., Korhan, O., Asmael, M., & Safaei, B. (2020). Machine Learning in Predictive Maintenance towards Sustainable Smart Manufacturing in Industry 4.0. Sustainability, 12(19), 8211. https://doi.org/10.3390/su12198211

Cisco (2020). Cisco Annual Internet Report (2018–2023) White Paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

IEEE Conference Publications. (2013). Constant false alarm rate anomaly-based approach for network intrusion detection. IEEE Conference on Communications and Network Security, 1, 145-150. DOI:10.1109/HONET.2013.6729773

ISO/IEC. (2011). ISO/IEC 25010:2011—Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and software quality models. *International Organization for Standardization*. https://www.iso.org/standard/35733.html

García-Torres, M., Fellner, D. W., Havemann, S., Strzelecki, A., Remondino, F., & Durán, A. J. (2022). Resource and environmental impacts of electronics management. Sustainability, 14(3), 1-23. Retrieved from https://www.mdpi.com/2071-1050/14/3/1234

García-Torres, R., Molina, J. M., & Galván-Tejada, C. E. (2022). Challenges in implementing AI analytics in legacy telecommunications infrastructure. *Sensors*, 22(11), 3986. Retrieved from: https://www.mdpi.com/1424-8220/22/11/3986

Gupta, R., & Sharma, L. K. (2020). Machine predictive maintenance classification using machine learning. *ResearchGate*. https://ieeexplore.ieee.org/document/10403631

Hosamo, H., & Mazzetto, S. (2025). Data-Driven Ventilation and Energy Optimization in Smart Office Buildings: Insights from a High-Resolution Occupancy and Indoor Climate Dataset. Sustainability, 17(1), 58. https://doi.org/10.3390/su17010058

Kim, K., Jang, S. J., Park, J., Lee, E., & Lee, S. S. (2023). Lightweight and energy-efficient deep learning accelerator for real-time object detection on edge devices. *Sensors*, *23*(3), 1185.

Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2019). A survey of deep learning-based network anomaly detection. *Cluster Computing*, *22*, 949-961.

Li, B., Zhao, S., Zhang, R., Shi, Q., & Yang, K. (2019). Anomaly detection for cellular networks using big data analytics. *IET Communications*, *13*(20), 3351-3359.

Marino, T. & Willie, A. & Benedict, J. O. (2018). Role of AI in Minimizing False Alarms in S.A.A.N.S. https://www.researchgate.net/publication/388195603_Role_of_AI_in_Minimizing_False_Alarms_in_SAANS

Minilec Group (2024). The Role of Monitoring Systems in Preventive Maintenance. https://minilecgroup.com/the-role-of-monitoring-systems-in-preventive-maintenance/

Mobley, R. K. (2002). *An introduction to predictive maintenance*. Elsevier.

Olaoluwa, F., & Potter, K. (2024). Predictive Maintenance for Critical Infrastructure Security.

O'Brien, K. & Downie, A. (2024, October 18). AI in telecommunications. *IBM*. https://www.ibm.com/think/topics/ai-in-telecommunications

Panza, M. A., Pota, M., & Esposito, M. (2023). Anomaly Detection Methods for Industrial Applications: A Comparative Study. Electronics, 12(18), 3971. https://doi.org/10.3390/electronics12183971

Park, J., & Kang, D. (2024). Artificial Intelligence and Smart Technologies in Safety Management: A Comprehensive Analysis Across Multiple Industries. *Applied Sciences*, *14*(24), 11934.

Parthasarathy, V., Afshari, S. S., & Ferguson, P. (2025). A satellite fault detection system based on telemetry data using statistical process control and time-domain feature extraction. *Advances in Space Research*, *75*(9), 6863-6881.

pbctoday (2025, February 10). The future of smart buildings: How advanced informatic technologies are changing construction. https://tinyurl.com/bddnufd8

Schwarz, L. (2024, August 2). *What Is Mean Time to Repair (MTTR)?* Oracle NetSuite. https://www.netsuite.com/portal/resource/articles/erp/mean-time-to-repair.shtml

Sharma, R., Johnson, D., & Richards, M. (2022). Infrastructure reliability in modern telecommunications networks. IEEE Network, 36(2), 142-148. https://tinyurl.com/sharma-johnson-2022

Stephen, M. & Sheriffdeen, K. (2022). AI-Enabled Anomaly Detection in Industrial Systems: A New Era in Predictive Maintenance. https://tinyurl.com/yjyz4epm

Wang, X., Guo, Y., & Gao, Y. (2024). Unmanned autonomous intelligent system in 6G non-terrestrial network. *Information*, *15*(1), 38.

Wang, X., Zhao, T., Liu, H., & He, R. (2019). Power consumption predicting and anomaly detection based on long short-term memory neural network. In 2019 IEEE 4th international conference on cloud computing and big data analysis (ICCCBDA) (pp. 487-491). IEEE.

Wang, Z., Wang, Z., He, S., Gu, X., & Yan, Z. F. (2017). Fault detection and diagnosis of chillers using Bayesian network merged distance rejection and multi-source non-sensor information. *Applied energy*, *188*, 200-214.

Xue, F., Yan, W., Wang, T., Huang, H., & Feng, B. (2020, November). Deep anomaly detection for industrial systems: a case study. In *Annual Conference of the PHM Society* (Vol. 12, No. 1, pp. 8-8).

Yang, S. J., Xiao, N., Li, J. Z., Feng, Y., Ma, J. Y., Quzhen, G. S., ... & Zhou, X. N. (2021). A remote management system for control and surveillance of echinococcosis: design and implementation based on internet of things. *Infectious Diseases of Poverty*, *10*, 1-12.

Zhang, K., Kalander, M., Zhou, M., Zhang, X., & Ye, J. (2020, December). An influence-based approach for root cause alarm discovery in telecom networks. In *International Conference on Service-Oriented Computing* (pp. 124-136). Cham: Springer International Publishing.

Zhang, X., Chen, W., Li, Y., Sun, H., Zhao, L., & Wang, J. (n.d.). Real-Time Data Visualization Tools for Smart City Applications.