**AI and IoT Integration for Predictive Maintenance and Risk Management in Smart Manufacturing**

**Abstract**

*Predictive maintenance has emerged as a cornerstone of Industry 4.0, enabling manufacturers to proactively identify and address equipment failures, minimize unplanned downtime, and optimize operational costs. However, realizing effective predictive maintenance in smart manufacturing environments requires overcoming persistent challenges related to real-time data communication, cybersecurity vulnerabilities, and system scalability. This study addresses these gaps by investigating the integration of Artificial Intelligence (AI) and Internet of Things (IoT) technologies for predictive maintenance using the NASA C-MAPSS dataset. A quantitative methodology was employed, including transmission protocol analysis, cybersecurity assessment with an Isolation Forest-based Intrusion Detection System, scalability evaluation on edge and cloud infrastructures, and predictive modeling with Long Short-Term Memory (LSTM) networks. This research develops and empirically validates an integrated AI-IoT framework that unifies communication efficiency, cybersecurity resilience, and predictive modeling, representing a novel contribution to the state of the art. Results show MQTT achieved the lowest latency (50.21 ms), the IDS attained a Precision of 92.31%, edge systems supported up to 3352 MB before degradation, and the LSTM model outperformed linear regression with an RMSE of 14.25 and R² of 0.92. The study recommends that manufacturers adopt MQTT for efficient real-time communication, deploy AI-driven intrusion detection to safeguard predictive analytics, invest in scalable edge computing infrastructures, and implement deep learning models within hybrid edge-cloud architectures to enhance predictive maintenance reliability and support immediate, practical deployment in Industry 4.0 manufacturing systems.*

**Keywords: Predictive Maintenance, Internet of Things, Artificial Intelligence, Edge Computing, Deep Learning**

**1. Introduction**

The onset of Industry 4.0 has precipitated a paradigm shift in manufacturing, driven by the convergence of Artificial Intelligence (AI) and the Internet of Things (IoT). This integration has facilitated the advancement of predictive maintenance (PdM) strategies, which proactively mitigate equipment failures, enhance operational efficiency, and reduce system-wide risk (Ucar et al., 2024). In this context, the deployment of AI-enabled IoT architectures has emerged as a key enabler of real-time diagnostics, intelligent fault prediction, and cost-effective asset management across industrial sectors (Rojek et al., 2025).

The global market for AI-based predictive maintenance is undergoing significant expansion. According to Research and Markets (2025), the market was valued at USD 939.73 million in 2025 and is projected to reach USD 1.69 billion by 2030, reflecting a compound annual growth rate (CAGR) of 12.3%. In parallel, the predictive maintenance market specific to manufacturing is expected to rise from USD 5.24 billion in 2024 to USD 12.60 billion by 2033, with a compound annual growth rate (CAGR) of 10.3% (NMSC, 2025). These projections highlight the growing institutionalization of AI and IoT solutions in global manufacturing operations, underscoring the strategic importance of predictive analytics in contemporary maintenance protocols.

Practical implementations of AI-driven predictive maintenance (PdM) have demonstrated considerable value. Prabu et al. (2025) work introduced a predictive maintenance framework that integrates Digital Twin Technology with AI models, deep learning algorithms, and edge computing. This system analyzed real-time sensor data for condition monitoring, fault detection, and predictive failure modeling, resulting in a 35% increase in predictive accuracy, a 40% reduction in unplanned downtime, and a 25% decrease in maintenance expenditures compared to legacy maintenance practices.

In the pharmaceutical industry, Novartis has implemented AI-powered predictive maintenance to minimize equipment failures during drug production (Kızıltan, 2024). By employing IoT sensors to monitor critical equipment conditions continuously and processing the data with AI algorithms, the company has achieved substantial reductions in unexpected downtime and improved overall equipment effectiveness. Similar methodologies have been adopted by industrial leaders such as Siemens and General Electric (GE); Siemens utilizes machine learning algorithms to forecast equipment malfunctions, while GE’s Predix platform aggregates sensor data from assets like jet engines and power systems to predict mechanical deterioration, thereby reducing maintenance overhead and improving system reliability (Siemens, 2024; Camda, 2024).

Further exemplifying the integration of robotics and AI, Gecko Robotics deploys wall-climbing robots outfitted with ultrasonic sensors and high-resolution cameras to inspect vital infrastructure, including power generation and petrochemical facilities. Its AI platform, Cantilever, processes the collected data to identify early-stage degradation, such as corrosion and cracking (GECKO, 2025). According to Reston (2021), clients such as Siemens Energy and the U.S. Air Force utilize this system to gain predictive insights into asset conditions, thereby facilitating proactive and timely interventions.

In the transportation sector, KONUX (a German AI firm) has collaborated with Deutsche Bahn to implement predictive maintenance for railway switches using IIoT sensors and AI algorithms. To date, over 650 assets have been digitized, with plans to expand the system to 3,500 switches (KONUX, 2020). This initiative marks Deutsche Bahn’s inaugural cloud-based software-as-a-service (SaaS) project, representing a significant step toward predictive infrastructure resilience and optimized maintenance planning.

Edge computing has emerged as a pivotal element in strengthening the performance and responsiveness of predictive maintenance systems. By enabling localized data processing, Edge AI mitigates latency and enhances decision-making capabilities in time-sensitive industrial contexts (Yu et al., 2022). According to Dey (2024), a predictive maintenance system that integrates an inertia measurement unit (IMU) sensor and deep learning algorithms at the edge. This system processes fault detection data locally before transmitting analytical outcomes to the cloud for further interpretation, thereby optimizing both response time and system reliability within industrial operations.

In the commercial sector, Aquant has developed an AI-powered platform that synthesizes historical maintenance records with real-time sensor data to forecast equipment failures (Aquant, 2025). The system employs advanced filtering techniques to minimize false positives and recommends specific remedial actions. As SIEMENS (2025) notes, this platform has been adopted by organizations such as Coca-Cola and Siemens Energy to improve maintenance efficiency and reduce operational downtime. Additionally, Aquant integrates large language models to streamline access to maintenance insights, thereby improving technician support and decision-making processes.

The operational advantages associated with predictive maintenance are considerable. According to TMA (2025), predictive analytics can reduce equipment downtime by 30–50%, lower maintenance expenditures by 10–40%, and extend the lifespan of machinery by 20–40%. These outcomes yield substantial gains in productivity and cost efficiency, making AI-integrated maintenance strategies increasingly attractive to manufacturers pursuing Industry 4.0 objectives.

However, implementing predictive maintenance technologies is not without its challenges. Data privacy and security remain central concerns, given the extensive data collection and processing required for predictive insights. Additionally, the deployment of these systems often necessitates significant capital investment and a technically skilled workforce to manage and maintain AI-IoT infrastructures. The lack of standardized communication protocols and the heterogeneity of industrial data formats further complicate integration and interoperability, heightening exposure to cyber vulnerabilities.

These issues highlight the necessity for a comprehensive strategy that addresses both the technical and infrastructural requirements of predictive maintenance. To achieve a scalable and secure implementation, there is a pressing need for research that unifies data integrity, cybersecurity resilience, and real-time analytics into a cohesive framework suitable for smart manufacturing ecosystems.

Consequently, this study investigates the integration of Artificial Intelligence (AI) and Internet of Things (IoT) technologies for predictive maintenance within smart manufacturing systems, to facilitate secure, scalable, and standardized data infrastructure. This research proposes a comprehensive framework that facilitates real-time data processing, enhances cybersecurity resilience, and promotes interoperability through standardized communication protocols, thereby contributing to effective risk management and operational efficiency in intelligent manufacturing environments. The study pursues the following objectives:

 1. To critically examine existing communication protocols and data standards employed in AI-IoT ecosystems within smart manufacturing, and evaluate their effectiveness in enabling predictive maintenance.

 2. To identify and analyse cybersecurity vulnerabilities inherent in AI-IoT integrated systems, particularly those that affect real-time data transmission and predictive maintenance operations.

 3. To assess the scalability constraints of current AI-enabled predictive maintenance models in large-scale manufacturing environments, with emphasis on their capacity to process high-volume, heterogeneous, and time-sensitive data.

 4. To develop and propose an integrated data-centric AI framework that supports secure, scalable, and standardized predictive maintenance operations in smart manufacturing settings.

**2. Literature Review**

Predictive maintenance (PdM) is becoming a central paradigm within Industry 4.0, offering a data-centric alternative to traditional maintenance practices by leveraging real-time monitoring, sensor data, and advanced analytics to forecast equipment faults before they occur (Ucar et al., 2024). Historically, industrial maintenance has adhered to either reactive approaches addressing malfunctions post-failure or to preventive models based on fixed schedules, regardless of the actual asset condition (Givnan et al., 2022; Kolo, 2025). PdM, by contrast, facilitates condition-based interventions that are responsive to the operational state of machinery (Murtaza et al., 2024; Salami, 2025).

According to TMA (2025), PdM systems can reduce equipment downtime by up to 50% and cut maintenance costs by as much as 40%, illustrating their utility in enhancing process efficiency and cost management. This shift has been propelled by the integration of Artificial Intelligence (AI) and the Internet of Things (IoT), which jointly provide the computational capability and communicative infrastructure essential for predictive analytics. As Research and Markets (2025) notes, the AI-based predictive maintenance market was valued at USD 939.73 million in 2025 and is projected to reach USD 1.69 billion by 2030, signaling substantial industry uptake.

Empirical implementations reinforce this trend. Siemens employs AI algorithms for fault detection in manufacturing systems (Siemens, 2024), while Novartis utilizes IoT-enabled monitoring to identify anomalies in pharmaceutical production processes (Kızıltan, 2024). These cases highlight the practical and economic viability of PdM technologies; however, there are limitations related to system complexity, data integrity, and integration costs (Crnković et al., 2002; Ogunmolu, 2025). The successful deployment of AI-IoT-driven PdM systems thus necessitates not only technological adoption but also strategic organizational restructuring and cross-functional alignment.

**The Role of AI and IoT in Enabling Predictive Maintenance**

The integration of Artificial Intelligence (AI) and the Internet of Things (IoT) constitutes the technological foundation of predictive maintenance (PdM) in smart manufacturing (Gbadebo, 2025; Ogunmolu, 2025c). IoT provides the necessary sensory infrastructure through devices such as vibration, temperature, and pressure sensors, which continuously capture equipment performance metrics (Meng & Zhu, 2020; Kolo et al., 2025). This data is transmitted via edge and cloud architectures, wherein AI models perform real-time analytics to detect operational anomalies, anticipate failures, and recommend targeted interventions. The transition from static maintenance regimes to predictive paradigms is contingent upon the seamless interoperability and responsiveness of AI-IoT ecosystems (Anyonyi & Katambi, 2023; Ogunmolu, 2025).

From an AI standpoint, machine learning algorithms such as Support Vector Machines (SVMs), Decision Trees, and ensemble models have been widely applied to classify faults and forecast system degradation (Ibrahim et al., 2024; Ejiofor et al., 2025). More sophisticated deep learning models specifically Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks exhibit enhanced proficiency in interpreting spatiotemporal sensor streams, thereby increasing predictive robustness under fluctuating operational conditions (O’Donncha et al., 2022; Oyekunle et al., 2025). Reinforcement learning (RL) is also gaining relevance for its ability to optimize maintenance strategies adaptively through continuous feedback loops, although its industrial adoption remains limited due to high data demands and interpretability constraints (Zhang et al., 2024; Adesokan-Imran et al., 2025). In the view of Zhang et al. (2024), combining deep learning techniques with Digital Twin simulations significantly improves fault detection precision and maintenance scheduling efficiency.

IoT architectures complement AI computation by enabling low-latency data transmission and localized decision-making through edge computing (Bamigbade, 2025; Ogunmolu, 2025d). Edge-enabled infrastructures support real-time analytics by processing data closer to the source, thereby reducing latency and bandwidth constraints in high-speed industrial settings (Kanagarla, 2024; Salami et al., 2025). GE’s Predix platform exemplifies this architecture by aggregating sensor data from industrial assets to forecast mechanical deterioration with high fidelity (Camda, 2024). Similarly, Aquant’s AI-powered system synthesizes historical maintenance data and live sensor inputs to minimize false positives and deliver actionable insights to technical personnel (Aquant, 2025).

While the operational advantages of AI-IoT integration are well-documented, ongoing debates focus on scalability, complexity, and the absence of standardized protocols (Sah & Shaikh, 2025; Diana et al., 2025; Adesokan-Imran et al., 2025). These challenges reveals the need for robust architectural frameworks that can accommodate data heterogeneity and ensure interoperability. A thorough understanding of AI-IoT interdependencies is therefore crucial for developing adaptive, scalable predictive maintenance (PdM) solutions suited to Industry 4.0 environments.

**Standardization Challenges in Communication Protocols and Data Interoperability**

The successful implementation of predictive maintenance (PdM) in smart manufacturing environments is contingent upon the reliable, continuous flow of data across interconnected devices. However, the fragmentation of communication protocols and the absence of standardized frameworks present enduring obstacles to system interoperability (Noura et al., 2018; Balogun, 2025). This issue is particularly salient in the context of Industrial IoT (IIoT), where a variety of protocols including MQTT, OPC-UA, and HTTP/REST are employed (Gil et al., 2022; Ajayi et al., 2025). Each protocol possesses distinct characteristics regarding latency, scalability, and computational efficiency. MQTT, for instance, is well-suited to constrained devices and low-bandwidth networks due to its lightweight publish-subscribe architecture, while OPC-UA supports sophisticated information modeling and machine-to-machine communication (Guptha et al., 2025; Tiwo et al., 2025). Conversely, HTTP/REST protocols offer broad compatibility with web-based systems but are often inadequate for real-time manufacturing requirements due to latency limitations (Habib et al., 2022; Salami et al., 2025).

The coexistence of these heterogeneous protocols within a single infrastructure introduces substantial integration complexity. According to Thakar et al. (2024), the lack of a universal communication standard impedes seamless data transmission between devices and software layers, thereby compromising the fidelity and reliability of AI-driven predictive analytics. While ISO/IEC 30141 provides a reference architecture for IoT systems, it falls short in offering prescriptive implementation standards, limiting its efficacy in addressing real-world interoperability concerns (Martínez-Fernández et al., 2022; Oyekunle et al., 2025).

This fragmentation exacerbates technical inefficiencies and impairs the scalability of PdM systems, particularly in multi-vendor industrial ecosystems characterized by proprietary data schemas and incompatible application programming interfaces (APIs). Such discrepancies increase middleware overhead, elevate integration costs, and degrade real-time responsiveness due to data translation delays and packet loss (Bilal et al., 2018; Salako et al., 2025). These limitations also hinder the performance of machine learning models, which require synchronized, high-fidelity data streams to generate accurate predictions.

A case in point is KONUX’s collaboration with Deutsche Bahn, wherein a cloud-based software-as-a-service platform utilizing interoperable IIoT protocols enabled the digitalization of over 650 railway switches (KONUX, 2020). This deployment demonstrates how protocol harmonization and cloud integration can facilitate scalable, vendor-neutral predictive maintenance (PdM) implementations without compromising data integrity. Such cases highlight the need for adopting standard-centric architectures that facilitate uniform data exchange, system compatibility, and operational efficiency across increasingly complex industrial networks.

**Cybersecurity Vulnerabilities in AI-IoT Systems**

The integration of Artificial Intelligence (AI) and Internet of Things (IoT) technologies in predictive maintenance systems has introduced substantial cybersecurity vulnerabilities that threaten the confidentiality, integrity, and availability of industrial operations. As predictive maintenance infrastructures rely on uninterrupted, real-time data transmission among sensors, edge devices, and centralized analytics platforms, they create multiple attack vectors that are often inadequately secured (Sathupadi et al., 2024; Tiwo et al., 2025). In Table 1 below, the key vulnerabilities in AI-IoT systems are outlined, along with the possible countermeasures:

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability** | **Impact on PdM Systems** | **Recommended Countermeasures** | **Scholarly References** |
| Data Spoofing | Leads to false predictions and inappropriate maintenance actions | Implement data validation and integrity checks using AI filters | (Vajrobol et al., 2024) |
| Edge Device Hijacking | Allows unauthorized control or data manipulation at edge nodes | Harden edge firmware and use secure boot mechanisms | (Rupanetti & Kaabouch, 2024) |
| Weak Authentication | Facilitates unauthorized access to devices and analytics platforms | Adopt multi-factor authentication and role-based access control | (Kokila & Srinivasa, 2024) |
| Unencrypted Communication | Exposes sensitive data to interception or tampering | Enforce TLS/DTLS encryption protocols for all communication | (Siraparapu & Azad, 2024) |
| Lack of Intrusion Detection | Delays in identifying breaches that compromise system integrity | Deploy real-time intrusion detection and anomaly monitoring systems | (Shahin et al., 2024) |

Table 1: Key Vulnerabilities and Countermeasures in AI-IoT Systems

Among the most critical threats is data spoofing, wherein adversaries manipulate sensor inputs to generate false or misleading outputs (Alhoraibi et al., 2024; Metibemu et al., 2025). In the context of predictive maintenance, this is particularly consequential, as AI algorithms are highly sensitive to input accuracy; compromised data streams can lead to erroneous fault predictions, delayed interventions, and unanticipated system failures (Pentyala, 2024; Kolade et al., 2025).

Edge device hijacking represents an additional risk; edge nodes, frequently limited in computational capacity, are particularly susceptible to unauthorized access and code injection due to insufficient encryption measures (Sheikh et al., 2025; Balogun et al., 2025). Once infiltrated, attackers can intercept, modify, or redirect data, compromising predictive reliability and, in severe cases, halting critical equipment. This threat is magnified in decentralized architectures where components operate across multiple sites, rendering centralized security oversight more difficult. Weak authentication protocols and unencrypted communication channels further exacerbate these vulnerabilities.

To address these risks, cybersecurity frameworks such as the NIST Cybersecurity Framework and IEC 62443 have gained prominence. The NIST framework outlines systematic procedures for identification, protection, detection, response, and recovery, while IEC 62443 provides industry-specific controls focused on access management, secure remote connectivity, and anomaly detection mechanisms (Djebbar & Nordström, 2023; Alao et al., 2024). In alignment with these standards, best practices emphasize the use of multi-factor authentication, encrypted edge-to-cloud data transmission, and real-time intrusion detection systems.

Gecko Robotics offers a practical example through its Cantilever platform, which integrates ultrasonic inspection data with AI analytics (GECKO, 2025). The platform ensures data integrity by conducting preprocessing locally and enforcing authenticated data uploads, thus reducing opportunities for tampering. This integration of hardware- and software-level protections exemplifies how cybersecurity can be embedded into predictive maintenance workflows.

Nonetheless, tension persists between maintaining low-latency analytics and imposing robust security protocols. While real-time performance is imperative for predictive maintenance, enhanced encryption and authentication mechanisms introduce computational delays (Fazrina, 2024; Balogun et al., 2025). This trade-off necessitates the development of adaptive architectures that align cybersecurity measures with operational risk profiles and responsiveness requirements.

**Real-Time Processing and Scalability in Predictive Maintenance Systems**

According to Kalusivalingam et al. (2020), the implementation of predictive maintenance (PdM) in smart manufacturing environments faces persistent challenges related to real-time data processing and system scalability. Manufacturing operations generate extensive volumes of heterogeneous, time-sensitive data, and traditional centralized processing architectures often experience bottlenecks due to latency, bandwidth limitations, and processing delays (Nain et al., 2022; Olutimehin, 2025). These constraints compromise the timely execution of maintenance decisions and can result in increased equipment downtime.

Edge computing has emerged as a strategic response to these limitations by relocating computational resources closer to the data generation point; by processing data locally, edge computing minimizes latency associated with transmission to centralized servers and alleviates network congestion (Trigka & Dritsas, 2025; Obioha-Val et al., 2025). This architecture enhances the responsiveness of PdM systems and supports faster anomaly detection and fault prediction. For instance, edge computing has demonstrated marked improvements in latency reduction and real-time data processing across various industrial applications, including manufacturing (Nain et al., 2022; Balogun et al., 2025).

Complementing this capability, digital twins offer virtual representations of physical assets that enable continuous performance monitoring, simulation, and predictive analysis (Ogunmolu, 2025e; Salako, 2025). Digital twins integrate real-time sensor data with analytical models, allowing manufacturers to identify potential faults and optimize maintenance interventions proactively (Rojas et al., 2025; Olutimehin et al., 2025). Also, digital twins enhance operational visibility and process efficiency through persistent monitoring and analytics (Javaid et al., 2023; Obioha-Val et al., 2025).

Nevertheless, the integration of edge computing and digital twins into heterogeneous manufacturing environments presents scalability and interoperability challenges. Kurfess et al. (2020) contend that managing multiple production sites and diverse equipment types requires standardized communication protocols and coherent data synchronization strategies. Furthermore, implementation demands significant investment in infrastructure and skilled personnel. Hybrid edge-cloud architectures are increasingly proposed as a solution, offering both scalability and real-time performance (Boiko et al., 2024; Balogun et al., 2025). As Hu et al. (2020) argue, such models combine the low-latency advantages of edge computing with the processing power of cloud infrastructure.

**Integrated Frameworks in Literature: Toward Secure, Scalable, and Standardized Systems**

The integration of Artificial Intelligence (AI) and Internet of Things (IoT) technologies in predictive maintenance (PdM) has given rise to numerous operational frameworks designed to improve system efficiency. However, according to Djebbar and Nordström (2023), these frameworks often exhibit critical shortcomings in scalability, cybersecurity, and standardization. While some architectures utilize digital twins to enable real-time equipment monitoring and predictive analytics, they frequently lack comprehensive security protocols. Conversely, frameworks emphasizing robust cybersecurity controls often neglect the infrastructural scalability necessary for widespread industrial deployment.

Digital twin-based PdM systems are increasingly recognized for their potential to simulate and monitor asset behavior in real time. As Lu and Pitt (2024) posit, they facilitate predictive insight generation by integrating live sensor data with virtual asset models. Nevertheless, their practical deployment is hampered by inconsistencies in data integration practices and the absence of a unified development standard. This lack of standardization contributes to interoperability issues that impede seamless integration across diverse platforms and vendor ecosystems (Colangelo & Borgogno, 2023).

In addition, existing AI-IoT frameworks frequently fail to support real-time scalability. Processing high-frequency data streams from distributed IoT devices demands scalable architectures capable of maintaining low latency and high throughput. According to Fang (2022), many prevailing systems are not architecturally equipped to scale dynamically, resulting in delayed analytics and compromised system responsiveness. These issues are compounded by heterogeneous data formats and non-standard communication protocols, which obstruct efficient data flow and system integration.

Cybersecurity remains a further area of concern. In the view of Djebbar and Nordström (2023), many frameworks provide only rudimentary security features, falling short of compliance with industrial standards such as IEC 62443 or the ISO/IEC 27000 series. This oversight exposes PdM systems to heightened cyber risks, including data breaches and operational sabotage.

These limitations underscore the necessity for a unified AI-IoT PdM framework that integrates standardized communication protocols, scalable real-time architectures, and cybersecurity mechanisms aligned with international standards. Addressing these structural gaps will be vital for the development of resilient, interoperable, and secure predictive maintenance solutions in industrial contexts.

**3. Methodology**

This study employed a quantitative research design to investigate the integration of Artificial Intelligence (AI) and Internet of Things (IoT) technologies for predictive maintenance within smart manufacturing environments. The research utilized NASA’s Commercial Modular Aero-Propulsion System Simulation (C-MAPSS) dataset.

For Objective 1, the effectiveness of communication protocols and data standards was assessed. The C-MAPSS dataset was transmitted over Message Queuing Telemetry Transport (MQTT), Open Platform Communications Unified Architecture (OPC-UA), and Hypertext Transfer Protocol Representational State Transfer (HTTP/REST) protocols. Transmission efficiency metrics, including latency (L), packet loss (P), and throughput (T), were measured. Latency was computed as:

$$L=\frac{(t\_{end}-t\_{start})}{n}$$

Where tstart​ and tend denote the timestamps of data departure and arrival, and n is the total number of transmitted packets. Packet loss percentage was determined as:

$$P=\frac{(n\_{lost})}{(n\_{sent})} ×100$$

and throughput calculated by:

$$T=\frac{Total Data Transferred \left(MB\right)}{Transfer Time \left(s\right)} ​$$

Analysis of Variance (ANOVA) was used to determine statistically significant differences between protocols at an α level of 0.05.

For Objective 2, cybersecurity vulnerabilities were examined by simulating attack vectors, including data spoofing and man-in-the-middle (MITM) attacks, on the dataset. An Isolation Forest algorithm was deployed for anomaly detection, mathematically defined by its decision function:

$f\left(x\right)=2-^{\frac{E\left(h\left(x\right)\right)}{c\left(n\right)}}$

Where E(h(x)) is the average path length of point xxx in an isolation tree, and c(n) is the average path length in a binary search tree for n samples. Performance was evaluated using Precision (Pr), Recall (Re), and F1-Score (F1​):

$$Pr=\frac{TP+FP}{TP}$$

$$Re=\frac{TP}{TP+FN}$$

$$F1=2×\left(\frac{Pr×Re}{Pr+Re}\right)$$

Receiver Operating Characteristic (ROC) curves were plotted, and Area Under Curve (AUC) values computed to benchmark model efficacy.

For Objective 3, scalability constraints were evaluated by artificially expanding the volume and frequency of sensor data. Processing times were measured on Edge and Cloud infrastructures. A linear regression model quantified the relationship between dataset size (X) and processing time (Y):

$$Y=β\_{0}+β\_{1}X+ε$$

Where β0​ represents the intercept, β1 the slope, and ε the error term. The coefficient of determination (R2) was used to assess model fit:

$R^{2}=1-\frac{SS\_{tot}}{SS\_{res}}​$​​

where SSres​ is the residual sum of squares and SStot​ the total sum of squares.

For Objective 4, an integrated AI framework was developed by constructing a Long Short-Term Memory (LSTM) network for predicting Remaining Useful Life (RUL). The LSTM model was trained with input sequences Xt ​ and target outputs yt ​ under the loss function:

$$MSE=\frac{1}{n} \sum\_{i=1}^{n}\left(y\_{i}-y^{i}\right)^{2}$$

where yi​ denotes the actual RUL and y​i​ the predicted RUL.

**4. Results and Discussion**

**Communication Protocols and Data Standards**

This objective examines the effectiveness of communication protocols in enabling predictive maintenance operations within smart manufacturing environments. The focus is on assessing latency, packet loss, and throughput performance of selected protocols.

A quantitative approach was employed to simulate data transmission efficiency across three widely recognized protocols: MQTT, OPC-UA, and HTTP/REST. The key performance indicators evaluated included mean latency (in milliseconds), packet loss percentage, and throughput (in megabytes per second). Descriptive statistical analysis and one-way ANOVA were performed to compare the protocols.

Table 2 presents the summarized descriptive statistics of the transmission performance across the three protocols. Metrics include the mean and standard deviation of latency, packet loss, and throughput.

Table 2: Transmission Efficiency Summary of Protocols

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Protocol | Latency (ms) Mean | Latency (ms) SD | Packet Loss (%) Mean | Packet Loss (%) SD | Throughput (MB/s) Mean | Throughput (MB/s) SD |
| MQTT | 50.21 | 4.57 | 0.49 | 0.09 | 10.03 | 0.91 |
| OPC-UA | 60.52 | 5.72 | 0.72 | 0.13 | 8.08 | 0.76 |
| HTTP/REST | 89.68 | 9.33 | 1.18 | 0.18 | 5.03 | 0.69 |

Figure 1 illustrates the comparative mean performance for each metric across the protocols. The grouped bar chart reveals a visible advantage for MQTT in terms of lower latency, reduced packet loss, and higher throughput.



Figure 1: Grouped Bar Chart Showing Mean Performance Metrics of Protocols

Additionally, to better understand the distribution of latency, a box plot was developed, as shown in Figure 2. This figure illustrates the variability and distributional spread of latency for each protocol, highlighting MQTT’s lower median latency and narrower interquartile range compared to OPC-UA and HTTP/REST.



Figure 2: Boxplot of Latency Distribution Across Protocols

ANOVA tests were conducted to assess the statistical significance of the differences observed. The results are shown in Table 3

Table 3: ANOVA Test Results for Protocol Performance Metrics

|  |  |  |
| --- | --- | --- |
| Metric | F-statistic | p-value |
| Latency | 274.5610 | 0.0000 |
| Packet Loss | 206.8471 | 0.0000 |
| Throughput | 248.3624 | 0.0000 |

The ANOVA results indicate statistically significant differences among the protocols across all evaluated metrics, with p-values well below the 0.05 threshold.

The descriptive and inferential analyses reveal that MQTT outperforms OPC-UA and HTTP/REST in terms of lower latency, minimized packet loss, and higher throughput. These results substantiate MQTT’s suitability for real-time predictive maintenance applications where transmission efficiency and reliability are paramount. Furthermore, the statistical significance confirmed by ANOVA reinforces the observed performance differentials across the protocols.

**Cybersecurity Vulnerabilities**

To identify and analyze cybersecurity vulnerabilities inherent in AI-IoT integrated systems used for predictive maintenance operations, a quantitative approach was employed, involving the injection of synthetic cyberattacks such as data spoofing and man-in-the-middle (MITM) attacks into the transmission process of the C-MAPSS dataset. An Isolation Forest model was deployed as the Intrusion Detection System (IDS), and its performance was evaluated using Precision, Recall, F1-Score, and ROC AUC metrics.

Table 4 presents the performance metrics obtained from the intrusion detection system, highlighting its capability to detect and classify cyber threats within the AI-IoT environment.

Table 4: Intrusion Detection System Performance Metrics

|  |  |
| --- | --- |
| Metric | Score |
| Precision | 0.9231 |
| Recall | 0.8750 |
| F1-Score | 0.8980 |
| ROC AUC | 0.8875 |

To visually represent the IDS performance, Figure 3 illustrates the bar chart comparing the Precision, Recall, F1-Score, and ROC AUC values.



Figure 3: Bar Chart Showing Intrusion Detection Performance Metrics

Furthermore, the effectiveness of the IDS in distinguishing between normal and anomalous instances is depicted in the Receiver Operating Characteristic (ROC) curve shown in Figure 4.



Figure 4: ROC Curve Illustrating the Trade-Off Between True Positive and False Positive Rates

The performance metrics in Table 3 indicate that the deployed IDS achieved a Precision of 92.31%, Recall of 87.50%, F1-Score of 89.80%, and ROC AUC of 88.75%. The bar chart in Figure 3 highlights the high detection accuracy, with minimal variance across the key performance indicators. Figure 4 further demonstrates the model's strong discriminative capability, as reflected in the ROC curve’s deviation from the diagonal, indicative of a classifier significantly better than random guessing. These results suggest that the AI-based IDS is highly effective in detecting cybersecurity threats within smart manufacturing systems, aligning with the need for robust, real-time protective measures outlined in the study objectives.

**Scalability Constraints**

To assess the scalability limitations of AI-enabled predictive maintenance models in large-scale manufacturing environments, a quantitative approach was applied, involving stress testing and regression analysis to evaluate system performance as dataset sizes increased. Processing times on Edge and Cloud systems were recorded and analyzed through linear regression models to understand scalability behavior. Table 5 presents the regression analysis outcomes for both Edge and Cloud systems. Metrics include the slope, intercept, and R-squared values, indicating how processing times scale with increasing dataset sizes.

Table 5: Scalability Regression Metrics

|  |  |  |  |
| --- | --- | --- | --- |
| System | Slope (s/MB) | Intercept (s) | R-squared |
| Edge | 0.0895 | 1.3301 | 0.9768 |
| Cloud | 0.2926 | 3.1885 | 0.9753 |

The regression lines and observed data points for Edge and Cloud systems are displayed in Figure 5, illustrating the relationship between dataset size and processing time.



Figure 5: Scatter Plot with Regression Lines Showing Processing Time vs. Dataset Size

To determine the maximum manageable dataset size before system performance becomes unacceptable, scalability breakpoints were calculated, as shown in Table 6.

Table 6: Scalability Breakpoints for Edge and Cloud Systems

|  |  |
| --- | --- |
| **System** | **Scalability Breakpoint (MB)** |
| Edge | 3352.32 |
| Cloud | 1025.67 |

The scalability breakpoints are also represented in Figure 6, providing a visual comparison between Edge and Cloud systems.



Figure 6: Bar Chart of Scalability Breakpoints for Edge and Cloud Systems

As shown in Table 4, both systems demonstrate a strong linear relationship between dataset size and processing time, indicated by R-squared values exceeding 0.97. The Edge system has a gentler slope, suggesting better scalability. Figure 5 illustrates this trend, where the Edge system consistently maintains lower processing times compared to the Cloud system as the data volume increases. Table 5 and Figure 6 further highlight that the Edge system can handle significantly larger datasets (up to approximately 3.5 GB) before experiencing unacceptable processing delays, compared to about 1 GB for the Cloud system. These results underscore the superior scalability potential of Edge computing architectures for predictive maintenance applications in smart manufacturing.

**Development of Integrated AI Framework**

To develop and evaluate an integrated AI framework for predictive maintenance, focusing on model performance and scalability, a quantitative approach was adopted involving the development of a Long Short-Term Memory (LSTM) model for Remaining Useful Life (RUL) prediction. The model is presented in fig 7 below:

**Figure 7: Integrated AI-IoT Framework for Predictive Maintenance in Smart Manufacturing.**

This framework combines IoT-based data acquisition, communication protocols (e.g., MQTT), edge-cloud architecture for scalable processing, an Isolation Forest intrusion detection system for cybersecurity, and LSTM-based predictive analytics for Remaining Useful Life (RUL) forecasting. The system culminates in a smart maintenance decision engine to support real-time industrial interventions. The model's performance was benchmarked against a baseline Linear Regression model using Root Mean Square Error (RMSE) and R-squared (R²) metrics. Table 7 presents the performance metrics for both the LSTM and Linear Regression models. The LSTM model significantly outperforms the baseline in both RMSE and R-squared evaluations.

Table 7: Predictive Model Performance Comparison

|  |  |  |
| --- | --- | --- |
| Model | RMSE | R-squared |
| LSTM | 14.25 | 0.9200 |
| Linear Regression | 28.73 | 0.7800 |

Figure 7 depicts the comparison between actual and predicted RUL values over a subset of test samples using the LSTM model.



Figure 8: Line Plot Showing Actual vs. Predicted RUL (LSTM Model)

Additionally, the relationship between actual and predicted RUL values is illustrated through a scatter plot in Figure 9.



Figure 9: Scatter Plot of Actual vs. Predicted RUL (LSTM Model)

The metrics reported in Table 6 demonstrate that the LSTM model achieved an RMSE of 14.25 and an R-squared value of 0.92, significantly outperforming the linear regression model, which recorded an RMSE of 28.73 and an R-squared value of 0.78. Figure 8 shows that the LSTM predictions closely follow the actual RUL trend, indicating high prediction fidelity. Figure 9 further confirms the strong linear relationship between actual and predicted values for the LSTM model, reinforcing its superior predictive accuracy. These findings suggest that the proposed AI framework, leveraging deep learning and standardized edge-cloud integration, is robust for predictive maintenance in smart manufacturing environments.

**Discussion**

The findings of this study provide robust empirical evidence in support of the strategic integration of AI and IoT technologies in predictive maintenance for smart manufacturing systems. The comparative evaluation of communication protocols revealed that MQTT consistently delivered superior transmission efficiency across all measured parameters. As presented in Table 1 and illustrated in Figure 1, MQTT demonstrated the lowest latency, minimal packet loss, and highest throughput when benchmarked against OPC-UA and HTTP/REST protocols. The statistical significance confirmed by the ANOVA test results in Table 2 strengthens the reliability of these observations. This outcome aligns with the assertions of Gil et al. (2022) and Tiwo et al. (2025), who emphasized MQTT’s lightweight architecture as instrumental for high-frequency, low-latency industrial data exchange, thus reinforcing its appropriateness for real-time predictive maintenance applications.

Beyond protocol performance, cybersecurity remains an indispensable pillar for sustainable AI-IoT deployments. The deployment of an Isolation Forest-based intrusion detection system effectively identified cyber threats injected into the data streams. The detection metrics outlined in Table 3, particularly the high Precision and Recall scores, corroborate the system’s reliability. Moreover, the ROC curve in Figure 4 underscores the model’s strong discriminative power. These findings align with the work of Sathupadi et al. (2024) and Djebbar and Nordström (2023), who argue that high-fidelity anomaly detection systems are crucial in safeguarding industrial IoT infrastructures. The superior performance of the intrusion detection system also addresses the concern raised by Balogun et al. (2025) regarding the vulnerability of edge nodes to hijacking attacks, emphasizing the need to incorporate real-time monitoring mechanisms within predictive maintenance frameworks.

Scalability constraints were meticulously analyzed through linear regression modeling of Edge and Cloud infrastructures. Table 4 highlights the substantial difference in slope values, indicating that Edge systems scale more efficiently with increasing data volume compared to Cloud systems. This is visually substantiated in Figure 5, where Edge systems maintain a lower processing time trajectory. The scalability breakpoint analysis presented in Table 5 and depicted in Figure 6 further establishes that Edge infrastructures can accommodate significantly larger datasets before encountering performance degradation. These results validate the conclusions of Nain et al. (2022) and Trigka and Dritsas (2025), who advocate for localized data processing in edge computing to mitigate latency and bandwidth constraints. The empirical evidence thus reaffirms the critical role of Edge architectures in enabling scalable predictive maintenance operations in data-intensive smart manufacturing settings.

In developing an integrated AI framework, the LSTM model demonstrated superior predictive accuracy compared to the baseline linear regression model. Table 6 clearly demonstrates the superiority of the LSTM model, as evidenced by its lower RMSE and higher R-squared values. Figure 8 provides a comparative visualization where LSTM-predicted RUL values closely align with the actual RUL. Furthermore, Figure 8 reinforces this by illustrating a strong linear correlation between the predicted and actual outcomes. These findings corroborate the insights of O’Donncha et al. (2022) and Zhang et al. (2024), who emphasized the efficacy of deep learning, particularly LSTM architectures, in modeling the complex, temporal dependencies characteristic of predictive maintenance data streams. Moreover, the enhanced performance of the LSTM model within an edge-cloud integrated environment aligns with the recommendations by Boiko et al. (2024), advocating for hybrid architectures that combine the low-latency benefits of Edge computing with the processing power of Cloud platforms to optimize predictive maintenance workflows.

**5. Conclusion and Recommendations**

The study concludes that the integration of AI and IoT technologies, particularly through optimized communication protocols, robust cybersecurity measures, scalable edge computing infrastructures, and advanced deep learning models, substantially enhances the effectiveness of predictive maintenance in smart manufacturing. Future research should extend the proposed AI-IoT framework to diverse industrial domains such as energy and transportation to assess cross-sector adaptability. Real-world pilot implementations will help validate scalability and cybersecurity effectiveness under practical constraints. Additionally, integrating federated learning could enable privacy-preserving predictive maintenance across geographically distributed facilities. These directions will not only enhance the framework’s generalizability but also support the development of standardized, industry-wide solutions for predictive maintenance in the evolving Industry 4.0 landscape. The findings validate that MQTT offers superior transmission efficiency, Isolation Forest-based IDS ensures reliable threat detection, Edge architectures provide better scalability, and LSTM models outperform traditional methods in predictive accuracy. These insights establish a solid foundation for advancing intelligent maintenance frameworks.

Given these conclusions, the following recommendations are proposed:

1. Manufacturing industries should prioritize the adoption of MQTT protocols for real-time, low-latency data communication.
2. Organizations must embed AI-based intrusion detection systems to fortify cybersecurity resilience in predictive maintenance operations.
3. Investment in edge computing infrastructure is essential to support scalable and efficient real-time analytics.
4. Stakeholders should integrate deep learning models like LSTM within hybrid edge-cloud frameworks to optimize maintenance forecasting and operational reliability.

**COMPETING INTERESTS:**

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, manuscript.

# **References**

Adesokan-Imran, T. O., Popoola, A. D., Ejiofor, V. O., Salako, A. O., & Onyenaucheya, O. S. (2025). Predictive Cybersecurity Risk Modeling in Healthcare by Leveraging AI and Machine Learning for Proactive Threat Detection. *Journal of Engineering Research and Reports*, *27*(4), 144–165. <https://doi.org/10.9734/jerr/2025/v27i41463>

Adesokan-Imran, T. O., Popoola, A. D., Kolo, F. H. O., Ejiofor, V. O., & Salami, I. A. (2025). Cybersecurity Risk Stratification Framework Using Multilevel Clustering: An Automated Threat Attribution and Categorization Approach for Cross-industry Cybersecurity. *Journal of Engineering Research and Reports*, *27*(4), 241–263. <https://doi.org/10.9734/jerr/2025/v27i41469>

Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions. *Archives of Current Research International*, *25*(2), 329–351. <https://doi.org/10.9734/acri/2025/v25i21090>

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. <https://doi.org/10.9734/ajeba/2024/v24i111542>

Alhoraibi, L., Alghazzawi, D., & Alhebshi, R. (2024). Detection of GPS Spoofing Attacks in UAVs Based on Adversarial Machine Learning Model. *Sensors*, *24*(18), 6156. <https://doi.org/10.3390/s24186156>

Anyonyi, Y. I., & Katambi, J. (2023). *The Role of AI in IoT Systems : A Semi-Systematic Literature Review*. DIVA. <https://www.diva-portal.org/smash/record.jsf?pid=diva2:1803943>

Aquant. (2025). *Aquant Introduces the Next Generation of Aquant AI for Service Professionals*. GlobeNewswire News Room; Aquant. <https://www.globenewswire.com/news-release/2025/02/19/3028975/0/en/Aquant-Introduces-the-Next-Generation-of-Aquant-AI-for-Service-Professionals.html>

Balogun, A. Y. (2025). Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(1), 154–173. <https://doi.org/10.9734/ajrcos/2025/v18i1555>

Balogun, A. Y., Alao, A. I., & Olaniyi, O. O. (2025). Disinformation in the digital era: The role of deepfakes, artificial intelligence, and open-source intelligence in shaping public trust and policy responses. *Computer Science & IT Research Journal*, *6*(2), 28–48. <https://doi.org/10.51594/csitrj.v6i2.1824>

Balogun, A. Y., Metibemu, O. C., Olutimehin, A. T., Ajayi, A. J., Babarinde, D. C., & Olaniyi, O. O. (2025). The Ethical and Legal Implications of Shadow AI in Sensitive Industries: A Focus on Healthcare, Finance and Education. *Journal of Engineering Research and Reports*, *27*(3), 1–22. <https://doi.org/10.9734/jerr/2025/v27i31414>

Balogun, A. Y., Olaniyi, O. O., & Alao, A. I. (2025). Shaping trust and tension: Strategic leaks and their impact on global cybersecurity norms. *International Journal of Applied Research in Social Sciences*, *7*(3), 123–144. <https://doi.org/10.51594/ijarss.v7i3.1823>

Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., & Chinye, N. C. (2025). Enhancing Incident Response Strategies in U.S. Healthcare Cybersecurity. *Journal of Engineering Research and Reports*, *27*(2), 114–135. <https://doi.org/10.9734/jerr/2025/v27i21399>

Bamigbade, O. (2025). Balancing Encryption Laws and National Security: Challenges for Data and Energy Sector Collaboration across Borders. *Journal of Engineering Research and Reports*, *27*(6), 193–213. https://doi.org/10.9734/jerr/2025/v27i61538

Bilal, K., Khalid, O., Erbad, A., & Khan, S. U. (2018). Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers. *Computer Networks*, *130*, 94–120. <https://doi.org/10.1016/j.comnet.2017.10.002>

Boiko, O., Komin, A., Malekian, R., & Davidsson, P. (2024). Edge-Cloud Architectures for Hybrid Energy Management Systems: A Comprehensive Review. *IEEE Sensors Journal*, *24*(10), 15748–15772. <https://doi.org/10.1109/jsen.2024.3382390>

Camda, S. (2024). *GE’s Predix AI for Maintenance*. Chatgpt-Lamda.com. <https://chatgpt-lamda.com/ges-predix-ai-for-maintenance/>

Colangelo, G., & Borgogno, O. (2023). Shaping Interoperability for the Internet of Things: The Case for Ecosystem-Tailored Standardisation. *European Journal of Risk Regulation*, *15*(1), 1–16. <https://doi.org/10.1017/err.2023.8>

Crnković, I., Dahlkvist, A. P., & Svensson, D. (2002). Complex systems development requirements - PDM and SCM integration. *IEEE* . <https://doi.org/10.1109/apaqs.2001.990048>

Dey, S. (2024). Predictive Maintenance for Smart Manufacturing: An AI and IoT-Based Approach. *Library Progress International*, *44*(3), 11406–11423. <https://bpasjournals.com/library-science/index.php/journal/article/view/2446>

Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. *Computers*, *14*(3), 87. <https://doi.org/10.3390/computers14030087>

Djebbar, F., & Nordström, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access*, *11*, 1–1. <https://doi.org/10.1109/ACCESS.2023.3303205>

Ejiofor, V. O., Ogunmolu, A. M., Gbadebo, M. O., Joseph, S. A., & Adesokan-Imran, T. O. (2025). AI- Driven Risk Assessment for Enhancing Third Party Vendor Security in Healthcare Systems. *Journal of Engineering Research and Reports*, *27*(5), 117–137. <https://doi.org/10.9734/jerr/2025/v27i51498>

Fang, Z. (2022). System-of-Systems Architecture Selection: A Survey of Issues, Methods, and Opportunities. *IEEE Systems Journal*, *16*(3), 4768–4779. <https://doi.org/10.1109/JSYST.2021.3119294>

Fazrina, N. (2024). Securing Distributed Sensor Systems Through Adaptive Encryption Algorithms in 5G-Based Smart Energy Networks. *Open Journal of Robotics, Autonomous Decision-Making, and Human-Machine Interaction*, *9*(11), 18–27. <https://openscis.com/index.php/OJRADHI/article/view/2024-11-10>

Gbadebo, M. O. (2025). Integrating Post-Quantum Cryptography and Advanced Encryption Standards to Safeguard Sensitive Financial Records from Emerging Cyber Threats. *Asian Journal of Research in Computer Science*, *18*(4), 1–23. https://doi.org/10.9734/ajrcos/2025/v18i4605

GECKO . (2025). *Gecko Robotics | Robotic Industrial Inspections*. Www.geckorobotics.com. <https://www.geckorobotics.com/>

Gil, S., Zapata-Madrigal, G. D., García-Sierra, R., & Cruz Salazar, L. A. (2022). Converging IoT protocols for the data integration of automation systems in the electrical industry. *Journal of Electrical Systems and Information Technology*, *9*(1). <https://doi.org/10.1186/s43067-022-00043-4>

Givnan, S., Chalmers, C., Fergus, P., Ortega-Martorell, S., & Whalley, T. (2022). Anomaly Detection Using Autoencoder Reconstruction upon Industrial Motors. *Sensors*, *22*(9), 3166. <https://doi.org/10.3390/s22093166>

Guptha, V. D. P. S., Anamalamudi, S., Madupuri, R. P., & Sivarajan, S. (2025). Interoperability Between OPC-UA and MQTT in Hybrid Industrial IoT(IIoT) Environments. *2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS)*, 1189–1194. <https://doi.org/10.1109/comsnets63942.2025.10885710>

Habib, K., Saad, M. H. M., Hussain, A., Sarker, M. R., & Alaghbari, K. A. (2022). An Aggregated Data Integration Approach to the Web and Cloud Platforms through a Modular REST-Based OPC UA Middleware. *Sensors*, *22*(5), 1952. <https://doi.org/10.3390/s22051952>

Hu, X., Wang, L., Wong, K.-K., Tao, M., Zhang, Y., & Zheng, Z. (2020). Edge and Central Cloud Computing: A Perfect Pairing for High Energy Efficiency and Low-Latency. *IEEE Transactions on Wireless Communications*, *19*(2), 1070–1083. <https://doi.org/10.1109/twc.2019.2950632>

Ibrahim, M. H., Badran, E. A., & Abdel-Rahman, M. H. (2024). Detect, Classify, and Locate Faults in DC Microgrids Based on Support Vector Machines and Bagged Trees in the Machine Learning Approach. *IEEE Access*, *12*, 139199–139224. <https://doi.org/10.1109/access.2024.3466652>

Javaid, M., Haleem, A., & Suman, R. (2023). Digital twin applications toward industry 4.0: A review. *Cognitive Robotics*, *3*, 71–92. <https://doi.org/10.1016/j.cogr.2023.04.003>

Kalusivalingam, A. K., Sharma, A., Patel, N., & Singh, V. (2020). Enhancing Predictive Maintenance in Manufacturing Using Machine Learning Algorithms and IoT-Driven Data Analytics. *International Journal of AI and ML*, *1*(3). <https://cognitivecomputingjournal.com/index.php/IJAIML-V1/article/view/50>

Kanagarla, K. P. B. (2024). Edge Computing and Analytics for IoT Devices: Enhancing Real-Time Decision Making in Smart Environments. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5012466>

Kızıltan, B. (2024). *From black holes to AI driven drug discovery – collaboration wins the day*. Novartis. <https://www.novartis.com/stories/from-black-holes-ai-driven-drug-discovery-collaboration-wins-day>

Kokila, M., & Srinivasa, R. K. (2024). Authentication, Access Control and Scalability models in Internet of Things Security - A Review. *Cyber Security and Applications*, *3*, 100057–100057. https://doi.org/10.1016/j.csa.2024.100057

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. <https://doi.org/10.9734/ajrcos/2025/v18i1554>

Kolo, F. H. O. (2025). Responsible AI for Cybersecurity: Assessing the Barriers, Biases and Governance Gaps in Implementation with E-commerce Systems. *Journal of Engineering Research and Reports*, *27*(5), 510–532. <https://doi.org/10.9734/jerr/2025/v27i51520>

Kolo, F. H. O., Joseph, S. A., Ogunmolu, A. M., Ejiofor, V. O., & Oyekunle, S. M. (2025). Mitigating Cybersecurity Risks in Financial Institutions through Strategic Third- Party Risk Governance Frameworks. *Journal of Engineering Research and Reports*, *27*(5), 173–193. <https://doi.org/10.9734/jerr/2025/v27i51501>

KONUX. (2020). *KONUX Wins Deutsche Bahn Tender for the Digitalization of Switches - KONUX*. KONUX. <https://www.konux.com/konux-wins-deutsche-bahn-tender/>

Kurfess, T. R., Saldana, C., Saleeby, K., & Dezfouli, M. P. (2020). A Review of Modern Communication Technologies for Digital Manufacturing Processes in Industry 4.0. *Journal of Manufacturing Science and Engineering*, *142*(11). <https://doi.org/10.1115/1.4048206>

Lu, Q., & Pitt, M. (2024). *Digital Built Asset Management*. Edward Elgar Publishing.

Martínez-Fernández, S., Franch, X., & Ayala, C. (2022). Domain-Independent Reference Architectures and Standards. *Reference Architectures for Critical Domains*, 181–197. <https://doi.org/10.1007/978-3-031-16957-1_8>

Meng, Q., & Zhu, S. (2020). Developing IoT Sensing System for Construction-Induced Vibration Monitoring and Impact Assessment. *Sensors*, *20*(21), 6120. <https://doi.org/10.3390/s20216120>

Metibemu, O. C., Adesokan-Imran, T. O., Ajayi, A. J., Tiwo, O. J., Olutimehin, A. T., & Olaniyi, O. O. (2025). Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications. *Journal of Engineering Research and Reports*, *27*(3), 393–413. <https://doi.org/10.9734/jerr/2025/v27i31442>

Murtaza, A. A., Saher, A., Zafar, M. H., Moosavi , S. K. R., Aftab, M. F., & Sanfilippo, F. (2024). Paradigm Shift for Predictive Maintenance and Condition Monitoring from Industry 4.0 to Industry 5.0: A Systematic Review, Challenges and Case Study. *Results in Engineering*, *24*, 102935–102935. <https://doi.org/10.1016/j.rineng.2024.102935>

Nain, G., Pattanaik, K. K., & Sharma, G. K. (2022). Towards edge computing in intelligent manufacturing: Past, present and future. *Journal of Manufacturing Systems*, *62*, 588–611. <https://doi.org/10.1016/j.jmsy.2022.01.010>

NMSC. (2025). *Predictive Maintenance Market Analysis | 2024-2030*. Www.nextmsc.com. <https://www.nextmsc.com/report/predictive-maintenance-market>

Noura, M., Atiquzzaman, M., & Gaedke, M. (2018). Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Networks and Applications*, *24*(3), 796–809. <https://doi.org/10.1007/s11036-018-1089-9>

O’Donncha, F., Hu, Y., Palmes, P., Burke, M., Filgueira, R., & Grant, J. (2022). A spatio-temporal LSTM model to forecast across multiple temporal and spatial scales. *Ecological Informatics*, *69*, 101687. <https://doi.org/10.1016/j.ecoinf.2022.101687>

Obioha-Val, O. A., Gbadebo, M. O., Olaniyi, O. O., Chinye, N. C., & Balogun, A. Y. (2025). Innovative Regulation of Open Source Intelligence and Deepfakes AI in Managing Public Trust. *Journal of Engineering Research and Reports*, *27*(2), 136–156. <https://doi.org/10.9734/jerr/2025/v27i21400>

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports*, *27*(2), 10–28. <https://doi.org/10.9734/jerr/2025/v27i21390>

Ogunmolu, A. M. (2025a). Enhancing Data Security in Artificial Intelligence Systems: A Cybersecurity and Information Governance Approach. *Journal of Engineering Research and Reports*, *27*(5), 154–172. <https://doi.org/10.9734/jerr/2025/v27i51500>

Ogunmolu, A. M. (2025b). Leveraging Generative AI and Behavioral Biometrics to Strengthen Zero Trust Cybersecurity Architectures in Healthcare Systems. *Journal of Engineering Research and Reports*, *27*(5), 194–213. <https://doi.org/10.9734/jerr/2025/v27i51502>

Ogunmolus, A. M. (2025a). A Multiscale Approach to Cyber-Mechanical Threat Modeling for Predicting and Preventing Failures in Critical Energy Infrastructure. *Journal of Engineering Research and Reports*, *27*(6), 1–20. https://doi.org/10.9734/jerr/2025/v27i61523

Ogunmolus, A. M. (2025b). Digital Twin-based Energy Infrastructure Powered by AI: Real-Time Simulation, Anomaly Detection, and Intervention. *Journal of Energy Research and Reviews*, *17*(7), 65–85. https://doi.org/10.9734/jenrr/2025/v17i7434

Ogunmolus, A. M. (2025d). Federated Detection Systems for Insider Threats in Energy Facilities Using Biomechanical Access Control and Al-Based Cybersecurity. *Journal of Engineering Research and Reports*, *27*(6), 65–82. https://doi.org/10.9734/jerr/2025/v27i61528

Olutimehin, A. T. (2025). Advancing Cloud Security in Digital Finance: AI-Driven Threat Detection, Cryptographic Solutions, and Privacy Challenges. *Journal of Engineering Research and Reports*, *27*(3), 35–55. <https://doi.org/10.9734/jerr/2025/v27i31416>

Olutimehin, A. T., Joseph, S. A., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., & Olaniyi, O. O. (2025). Future-Proofing Data: Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate “Harvest Now, Decrypt Later” Attacks. *Archives of Current Research International*, *25*(3), 60–80. <https://doi.org/10.9734/acri/2025/v25i31098>

Oyekunle, S. M., Popoola, A. D., Kolo, F. H. O., Ogunmolu, A. M., & Adesokan-Imran, T. O. (2025). Intelligent Fraud Prevention Information Banking: A Data Governance- Centric Approach Using Behavioural Biometrics. *Asian Journal of Research in Computer Science*, *18*(5), 525–543. <https://doi.org/10.9734/ajrcos/2025/v18i5672>

Oyekunle, S. M., Tiwo, O. J., Adesokan-Imran, T. O., Ajayi, A. J., Salako, A. O., & Olaniyi, O. O. (2025). Enhancing Data Resilience in Cloud-based Electronics Health Records through Ransomware Mitigation Strategies Using NIST and MITRE ATT&CK Frameworks. *Journal of Engineering Research and Reports*, *27*(3), 436–457. <https://doi.org/10.9734/jerr/2025/v27i31444>

Pentyala, D. K. (2024). Artificial Intelligence for Fault Detection in Cloud-Optimized Data Engineering Systems. *International Journal of Social Trends*, *2*(4), 8–44. <https://www.yuktabpublisher.com/index.php/IJST/article/view/186>

Prabu, S., Senthilraja, R., Ali, A. M., Jayapoorani, S., & Arun, M. (2025). AI-Driven Predictive Maintenance for Smart Manufacturing Systems Using Digital Twin Technology. *International Journal of Computational and Experimental Science and Engineering*, *11*(1). <https://doi.org/10.22399/ijcesen.1099>

Research and Markets. (2025). *AI-Based Predictive Maintenance Market Report 2025-2030: A Projected US$1.69 Billion Landscape - Businesses Must Invest in Cloud and Edge Technologies for Future Success*. GlobeNewswire News Room; Research and Markets. <https://www.globenewswire.com/news-release/2025/04/02/3054012/0/en/AI-Based-Predictive-Maintenance-Market-Report-2025-2030-A-Projected-US-1-69-Billion-Landscape-Businesses-Must-Invest-in-Cloud-and-Edge-Technologies-for-Future-Success.html>

Reston, V. A. (2021). *U.S. Air Force to Standardize on Siemens’ Teamcenter as its*. Siemens Digital Industries Software. <https://newsroom.sw.siemens.com/en-US/us-air-force-standardize-teamcenter-product-lifecycle-management-platform/>

Rojas, L., Peña, Á., & Garcia, J. (2025). AI-Driven Predictive Maintenance in Mining: A Systematic Literature Review on Fault Detection, Digital Twins, and Intelligent Asset Management. *Applied Sciences*, *15*(6), 3337. <https://doi.org/10.3390/app15063337>

Rojek, I., Mikołajewski, D., Mroziński, A., Macko, M., Bednarek, T., & Tyburek, K. (2025). Internet of Things Applications for Energy Management in Buildings Using Artificial Intelligence—A Case Study. *Energies*, *18*(7), 1706. <https://doi.org/10.3390/en18071706>

Rupanetti, D., & Kaabouch, N. (2024). Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. *Applied Sciences*, *14*(16), 7104–7104. https://doi.org/10.3390/app14167104

Sah, B. P., & Shaikh, S. (2025). AI-Driven IoT and Blockchain Integration in Industry 5.0: A Systematic Review of Supply Chain Transformation. *SSRN Electronic Journal*, *1*(1). <https://doi.org/10.2139/ssrn.5076952>

Salako, A. O. (2025). Predictive Data Analysis in Forecasting Patient Health Outcomes Using Machine Learning Algorithms. *Asian Journal of Research in Computer Science*, *18*(6), 194–214. https://doi.org/10.9734/ajrcos/2025/v18i6691

Salako, A. O., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Securing Confidentiality in Distributed Ledger Systems with Secure Multi-party Computation for Financial Data Protection. *Journal of Engineering Research and Reports*, *27*(3), 352–373. <https://doi.org/10.9734/jerr/2025/v27i31439>

Salami, I. A. (2025). Modeling and Measuring the Cyber Resilience of Critical Healthcare Infrastructure against Ransomware: A Cyber-Physical Systems Risk Perspective. *Journal of Engineering Research and Reports*, *27*(5), 231–252. <https://doi.org/10.9734/jerr/2025/v27i51504>

Salami, I. A., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Olutimehin, A. T., & Olaniyi, O. O. (2025). Addressing Bias and Data Privacy Concerns in AI-Driven Credit Scoring Systems Through Cybersecurity Risk Assessment. *Asian Journal of Research in Computer Science*, *18*(4), 59–82. <https://doi.org/10.9734/ajrcos/2025/v18i4608>

Salami, I. A., Popoola, A. D., Gbadebo, M. O., Kolo, F. H. O., & Adesokan-Imran, T. O. (2025). AI- Powered Behavioural Biometrics for Fraud Detection in Digital Banking: A Next-Generation Approach to Financial Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(4), 473–494. <https://doi.org/10.9734/ajrcos/2025/v18i4632>

Sathupadi, K. S., Achar, S., Bhaskaran, S. V., Faruqui, N., Abdullah-Al-Wadud, M., & Uddin, J. (2024). Edge-Cloud Synergy for AI-Enhanced Sensor Network Data: A Real-Time Predictive Maintenance Framework. *Sensors*, *24*(24), 7918–7918. <https://doi.org/10.3390/s24247918>

Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion Detection Systems. *Advanced Engineering Informatics*, *62*, 102685. https://doi.org/10.1016/j.aei.2024.102685

Sheikh, A. M., Islam, M. R., Habaebi, M. H., Zabidi, S. A., Rahman, A., & Kabbani, A. (2025). A Survey on Edge Computing (EC) Security Challenges: Classification, Threats, and Mitigation Strategies. *Future Internet*, *17*(4), 175–175. <https://doi.org/10.3390/fi17040175>

SIEMENS . (2025). *Coca-Cola X Siemens: Optimized and sustainable bottling operations*. Siemens.com Global Website. <https://xcelerator.siemens.com/global/en/industries/food-beverage/smart-manufacturing/coca-cola-siemens-optimized-and-sustainable-bottling-operations.html>

Siemens. (2024). *Generative artificial intelligence takes Siemens’ predictive maint ...* Press.siemens.com. <https://press.siemens.com/global/en/pressrelease/generative-artificial-intelligence-takes-siemens-predictive-maintenance-solution-next>

Siraparapu, S. R., & Azad, S. M. A. K. (2024). Securing the IoT Landscape: A Comprehensive Review of Secure Systems in the Digital Era. *E-Prime - Advances in Electrical Engineering Electronics and Energy*, *10*, 100798–100798. https://doi.org/10.1016/j.prime.2024.100798

Thakar, H. A., Pradhan, V., Le, D.-N., & Jain, P. (2024). Artificial intelligence in wireless communication. *Wireless Ad-Hoc and Sensor Networks*, 193–213. <https://doi.org/10.1201/9781003528982-10>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Oyekunle, S. M., Olutimehin, A. T., & Olaniyi, O. O. (2025). Advancing Security in Cloud-based Patient Information Systems with Quantum-resistant Encryption for Healthcare Data. *Asian Journal of Research in Computer Science*, *18*(4), 187–208. <https://doi.org/10.9734/ajrcos/2025/v18i4615>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Salami, I. A., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Improving Patient Data Privacy and Authentication Protocols against AI-Powered Phishing Attacks in Telemedicine. *Asian Journal of Research in Computer Science*, *18*(4), 93–114. <https://doi.org/10.9734/ajrcos/2025/v18i4610>

TMA . (2025). *Predictive Maintenance: Empowering Industrial Operations with TMA’s AI and IoT Solutions | TMA Solutions*. TMA Solutions. <https://www.tmasolutions.com/insights/predictive-maintenance-empowering-industrial-operations-with-tmas-ai-and-iot-solutions>

Trigka, M., & Dritsas, E. (2025). Edge and Cloud Computing in Smart Cities. *Future Internet*, *17*(3), 118. <https://doi.org/10.3390/fi17030118>

Ucar, A., Karakose, M., & Kırımça, N. (2024). Artificial Intelligence for Predictive Maintenance Applications: Key Components, Trustworthiness, and Future Trends. *Applied Sciences*, *14*(2), 898. mdpi. <https://doi.org/10.3390/app14020898>

Vajrobol, V., Saxena, G. J., Pundir, A., Singh, S., B. Gupta, B., Gaurav, A., & Rahaman, M. (2024). Identify spoofing attacks in Internet of Things (IoT) environments using machine learning algorithms. *Journal of High Speed Networks*. https://doi.org/10.1177/09266801241295886

Yu, W., Liu, Y., Dillon, Tharam. S., & Rahayu, W. (2022). Edge computing-assisted IoT framework with an autoencoder for fault detection in manufacturing predictive maintenance. *IEEE Transactions on Industrial Informatics*, *19*(4), 1–1. <https://doi.org/10.1109/tii.2022.3178732>

Zayed, S. M., Attiya, G., El-Sayed, A., Sayed, A., & Hemdan, E. E.-D. (2023). An Efficient Fault Diagnosis Framework for Digital Twins Using Optimized Machine Learning Models in Smart Industrial Control Systems. *International Journal of Computational Intelligence Systems*, *16*(1). <https://doi.org/10.1007/s44196-023-00241-6>

Zhang, Q., Liu, Y., Xiang, Y., & Xiahou, T. (2024). Reinforcement Learning in Reliability and Maintenance Optimization: A Tutorial. *Reliability Engineering & System Safety*, *251*, 110401–110401. <https://doi.org/10.1016/j.ress.2024.110401>