Engineering Applications of Artificial Intelligence 163 (2026) 113138

Contents lists available at ScienceDirect

Engineering Applications of Artificial Intelligence

journal homepage: www.elsevier.com/locate/engappai

Research paper

Applied artificial intelligence-based equipment condition monitoring in manufacturing industry

Tariq Ahamed Ahanger [a,*,1], Munish Bhatia [b], Abdulrahman Alabduljabbar [a], Abdullah Albanyan [a]

[a] College of Computer Engineering and Sciences Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia
[b] Department of Computer Applications National Institute of Technology Kurukshetra, Haryana, India

ARTICLE INFO

Keywords:
Convolutional neural network
Smart manufacturing
Blockchain
Artificial intelligence

ABSTRACT

Advancements in the smart manufacturing sector have significantly increased the adoption of real-time equipment health monitoring systems. Digital twin technology has the potential to reduce rework costs, enhance machine tool uptime, and improve the dimensional accuracy of manufactured products. By utilizing digital twin technology, machining processes can now be monitored in real-time with operational and environmental variations. Digital twins provide a comprehensive view of equipment health, enabling more effective anomaly detection and fault diagnostics. The proposed study introduces an anomaly detection framework for machining, leveraging digital twin technology to facilitate real-time equipment health monitoring. The proposed framework integrates secure monitoring through blockchain technology combined with the Internet of Things to analyze production trends. Furthermore, it employs a dual-directional convolutional neural network approach to enable real-time vulnerability detection and optimize decision-making processes. Experimental simulations were performed to determine the validation of the presented approach. Based on experimental simulations, enhanced performance was registered in terms of Delay Efficiency (5.21 ms), Prediction Performance (Accuracy (92.25%), Sensitivity (93.25%), (Specificity (94.25%)), F-Measure (95.15%)), Energy Efficacy Analysis (1.18 mJ), Model Reliability (95.24%), and Stability Analysis (79%).

1. Introduction

Smart manufacturing represents a comprehensive discipline for integrating computer-aided design, manufacturing and advance technology (Chen, 2020). This transformative notion will continue to play a crucial role in revolutionizing industrial procedures. Fig. 1 depicts the key elements of smart manufacturing in Industry 4.0. However, modern tools and technologies used for operations such as cutting, shaping, and polishing in production are prone to higher failure rates under extreme conditions of heat, pressure, and force (Li et al., 2024). These failures can lead to significant economic losses, not only due to material damage but also from production disruptions. Empirical data highlights the critical need for robust Equipment Health Monitoring (EHM) systems. A recent study estimates that unplanned downtime costs industrial manufacturers approximately $50 billion annually, with equipment failure being the primary cause in 42% of cases (Shekari and Ray, 2024). In the automotive sector, for instance, a single minute of production downtime can result in losses of up to $22,000 (Pallisco, 2023). Moreover, failures in high-precision tools used in aerospace manufacturing can lead to losses exceeding $1 million per incident, factoring in material damage, production delays, and potential safety risks (Peng et al., 2024). Conspicuously, EHM has become essential for ensuring production efficiency and minimizing machine failure. A thorough review of the literature has identified two main categories of EHM strategies:

1. *Direct Approaches:* These involve assessing tools using optical instruments or other physical measurements. While accurate, such methods often require halting operations, leading to extended equipment downtime and reduced productivity.
2. *Indirect Approaches:* These rely on experimentally validated correlations between measurable parameters (e.g., vibration, temperature, acoustic signals) and tool wear. Indirect methods are more suitable for real-time EHM applications as they can be implemented without interrupting production processes.

* Corresponding author.
E-mail addresses: t.ahanger@psau.edu.sa (T.A. Ahanger), munish.bhatia@nitkkr.ac.in (M. Bhatia), a.alabduljabbar@psau.edu.sa (A. Alabduljabbar), a.albanyan@psau.edu.sa (A. Albanyan).
[1] Associate Professor.

https://doi.org/10.1016/j.engappai.2025.113138
Received 19 September 2024; Received in revised form 13 September 2025; Accepted 8 November 2025
Available online 10 November 2025

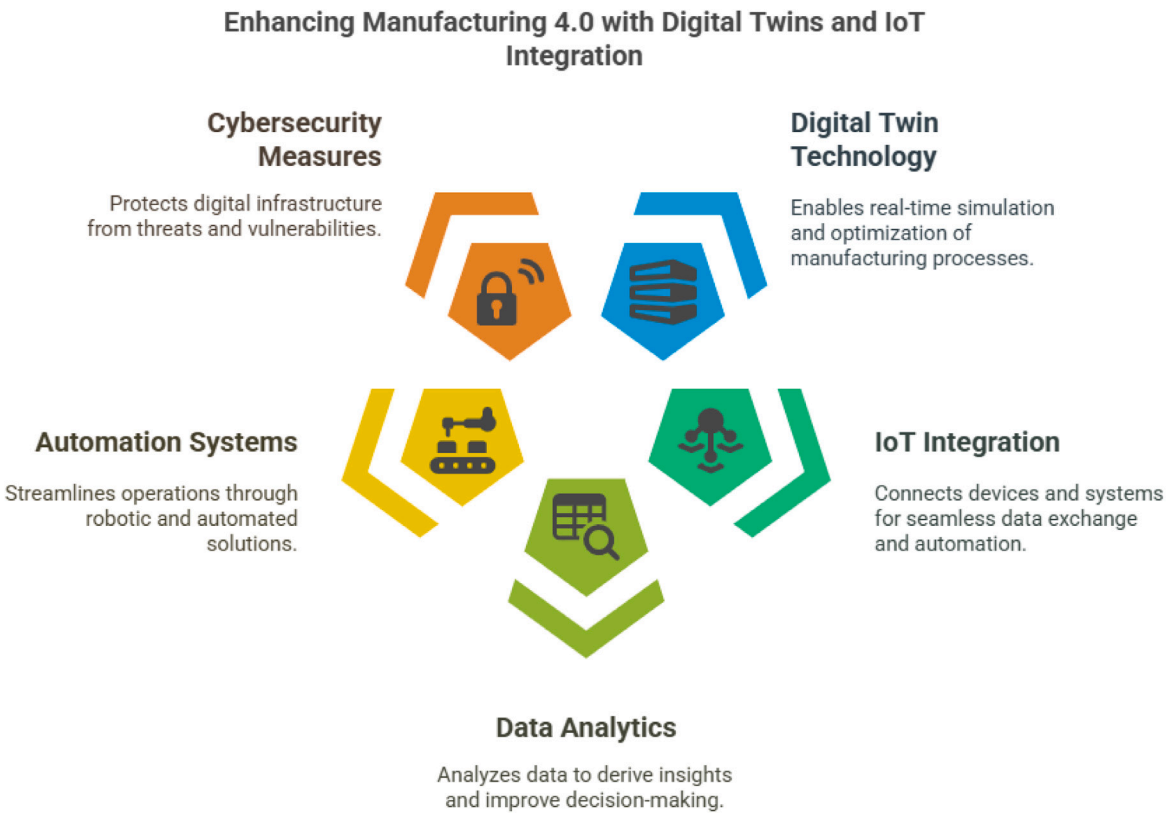


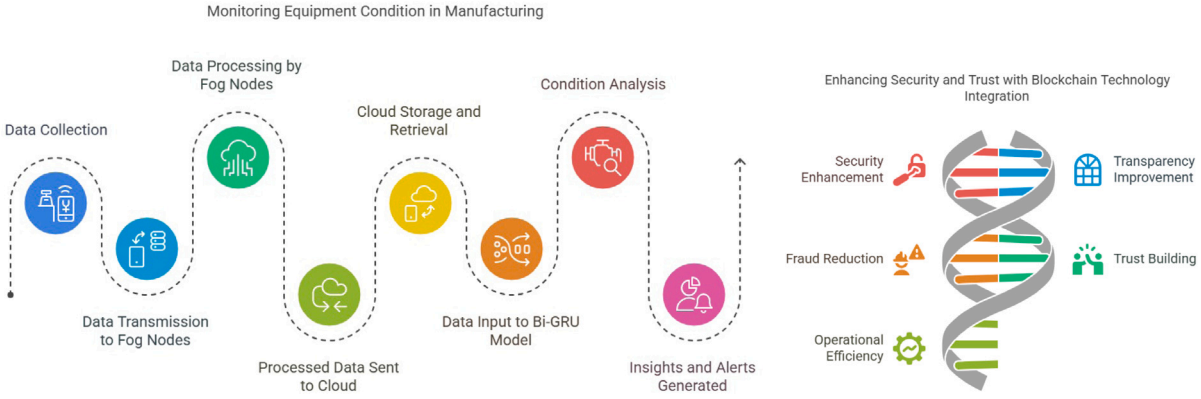
Fig. 1. Key elements for smart manufacturing 4.0 ecosystem.

1.1. Research domain

There has been significant research in analyzing indirect methods for the continuous monitoring of cutting tool health. These methods extract critical signal features from various sensing devices, such as acoustic emission, vibration, sound, and power (Soori et al., 2023). Numerous studies have explored techniques for signal feature extraction, including wavelet packet decomposition, time-domain and frequency-domain analysis, and AI-driven methods. However, despite extensive research, only a limited number of these techniques have been implemented in practical applications (Jagtap et al., 2021). The low adoption rate can be attributed to two primary challenges: the difficulty in selecting relevant signal features from a large pool of options and the inherent inflexibility of signal features in adapting to varying operating conditions (Liu et al., 2023). To address these challenges, model feature-based techniques have been proposed. Instead of directly using sensor data, these approaches construct a process model that integrates sensor information indirectly. Features are extracted based on the model's frequency response characteristics (Yu et al., 2021). Prior research has predominantly focused on simpler machining operations, leaving limited advancements in addressing the complexities of dynamic machining environments (Yang et al., 2020). For intricate and dynamic machining tasks, there are currently no established aspects for real-time EHM. This highlights the need for further development and standardization in the current domain of study.

1.2. Research motivation

The challenges in modern manufacturing present not only hurdles but also opportunities to drive innovation and create more resilient systems. One of the most promising solutions lies in the application of digital twins, a transformative technology that has the potential to revolutionize equipment health monitoring and overall manufacturing processes (Rath et al., 2024). The term digital twin was first introduced in 2003 during a course on product lifecycle management at the University of Michigan, describing a visionary concept that integrates physical products with their virtual counterparts through data-driven connections (Ayvaz and Alpay, 2021). Since then, digital twins have evolved from a theoretical framework to a practical and indispensable tool in modern industries. The renewed attention to digital twins in 2012, propelled by initiatives from the Air Force and NASA, demonstrated their immense potential to enhance equipment health monitoring. These initiatives combined ultra-high-fidelity simulations with physical models, real-time sensor data, and historical datasets, enabling unprecedented insights into equipment performance and reliability. While earlier progress in this domain was hindered by technological limitations, the relentless pursuit of innovation has led to remarkable breakthroughs, opening doors to more sophisticated applications. Digital twins have emerged as a game-changing technology in equipment health monitoring, driven by advancements in sensor technology, big data analytics, the Internet of Things (IoT), and deep learning (Ihekoronye et al., 2021). This convergence of technologies enables manufacturers to monitor equipment conditions in real time, predict failures before they occur, and optimize maintenance schedules. By providing detailed insights into the health and performance of machinery, digital twins empower organizations to reduce downtime, minimize costs, and ensure operational efficiency. Studies have highlighted the adaptability and effectiveness of digital twins in applications such as condition monitoring and fault detection, including autoclave defect prediction and equipment fault diagnostics (Khang et al., 2023). These successes underscore the transformative impact of digital twins in safeguarding equipment health and enhancing productivity. For manufacturers, the ability to proactively address equipment issues represents not just a technical achievement but a motivational leap toward building smarter, more sustainable systems. The use of digital twins in equipment health monitoring exemplifies the power of technology to turn challenges into opportunities. By leveraging this innovative



(a) Conceptual Data Flow (b) Blockchain Integration

Fig. 2. Conceptual vision of secure monitoring in manufacturing industry.

approach, manufacturers can achieve unprecedented levels of reliability and efficiency, fostering a culture of continuous improvement and resilience. Digital twins serve as an inspiring reminder that with the right tools and vision, even the most complex challenges can be overcome, paving the way for a brighter and more sustainable future in manufacturing.

1.3. Major contribution

The current study introduces a novel approach for real-time EHM assessment aimed at anomaly detection, addressing challenges related to complexity, flexibility, and time-sensitive deployment. The proposed methodology synergistically culminates the transformative capabilities of digital twins with an innovative model to achieve its objectives. Specifically, the model is designed to achieve the following key goals:

1. **IoT-Driven Anomaly Detection**: IoT devices and smart sensors are employed to identify unexpected patterns in comprehensive data collection for EHM in manufacturing.
2. **Data Integration and Standardization**: A central module, powered by digital twin technology, is developed to integrate and standardize sensor data from multiple users while creating virtual models of the production network.
3. **Deep Learning-Based Analysis**: A cloud-based deep learning technique, utilizing a bidirectional convolutional neural network (BCNN), is implemented to analyze EHM data and detect anomalies.
4. **Secure Data Management**: Blockchain technology is employed to ensure secure, immutable data storage while enabling continuous monitoring of the manufacturing process.

Fig. 2 illustrates the theoretical data flow of the proposed solution. The integration of IoT technology ensures the secure and permanent preservation of EHM data. By leveraging the reliable and unalterable data management features of blockchain, the framework supports long-term monitoring and tracking of EHM performance. Moreover, BCNNs are highly effective for anomaly detection in equipment health monitoring in manufacturing due to the ability to analyze spatial and temporal data. By processing data in forward and backward directions, BCNNs capture complex patterns and subtle deviations in sensor signals, which are critical for identifying early-stage faults. Their robustness to noise ensures reliable performance in real-world manufacturing environments, where sensor data is often noisy. BCNNs excel at integrating multi-dimensional data, such as vibration signals and thermal imaging, enabling comprehensive monitoring and precise fault localization. Additionally, they handle sequential dependencies in equipment behavior, making them particularly suited for processes with repetitive cycles. With scalability, adaptability, and real-time processing capabilities, BCNNs empower manufacturers to detect anomalies proactively, reduce downtime, and enhance operational efficiency, making them a valuable tool for predictive maintenance. In summary, the key features include

- Real-time anomaly detection using IoT devices and smart sensors.
- Centralized data integration and virtual modeling via digital twin technology.
- Advanced anomaly analysis through a bidirectional convolutional neural network.
- Secure, immutable data storage and monitoring enabled by blockchain technology.

Paper organization. Section 2 explores the significant advancements in monitoring enabled by the IoT and Digital Twin technologies. Section 3 outlines the methodology employed to analyze EHM within production processes. Section 4 delves into the implementation details of the proposed approach for performance assessment. Finally, conclusion is presented in Section 5 with future research directions.

2. Literature review

This section examines various initiatives related to smart manufacturing monitoring, along with research in the industrial sector that utilizes digital twin technology.

2.1. Digital twin-based equipment monitoring in industry

Digital twins have recently gained significant traction as a powerful tool for equipment monitoring and fault identification, though each approach comes with its limitations. Haghshenas et al. (2023) developed a digital twin tailored to the drivetrain systems of offshore wind turbines by integrating a torsional dynamic model, online measurements, and fatigue damage estimation, enabling predictions of the drivetrain's remaining lifespan. However, the proposed method is highly specific to drivetrain systems and may not generalize well to other components or industries. Jwo et al. (2022) proposed a digital twin model for autoclave defect prediction that incorporates four interconnected models: geometric, physical, behavioral, and rule-based. While comprehensive, the complexity of integrating these models may lead to high computational costs and challenges in real-time implementation. To improve forecast accuracy, Wu et al. (2021) introduced a five-dimensional digital twin model for wind turbines. Despite its advanced structure, the presented model's scalability to other systems or environments remains unclear, and its reliance on extensive data may limit its applicability in data-scarce scenarios. Sayed et al. (2024) validated

the digital twin architecture through a case study on triplex pump fault diagnostics, demonstrating its ability to use real-time physical asset data to continuously update a simulation model for equipment failure diagnosis. However, the approach may struggle with high levels of noise in sensor data or unforeseen fault modes that deviate from the training data. In machining applications, Ren et al. (2022) created a data-driven digital twin integrated with a deep learning model for equipment monitoring. While effective, its reliance on data-driven methods introduces potential issues related to overfitting, data quality, and interpretability of results. Additionally, Bariah and Debbah (2024) proposed a hybrid digital twin architecture combining model-based and data-driven approaches to enhance reliability while accounting for environmental factors throughout a tool's lifecycle. Although promising, the hybrid approach may face challenges in balancing the trade-offs between computational efficiency and accuracy, especially in dynamic environments. These studies collectively highlight the potential of digital twins to enable efficient real-time execution of EHM, marking a significant advancement in the real-time management of complex operations. However, the limitations in scalability, computational requirements, data dependency, and generalizability underline the need for further research.

2.2. Industrial digital twin

Leng et al. (2021) proposed a semi-physical commissioning technique that integrates digital twin concepts into an open manufacturing framework, enabling efficient system integration and testing. However, its reliance on semi-physical methods may limit scalability and adaptability when applied to complex systems with high variability. Huang et al. (2024) improved the reconfiguration process of automated manufacturing systems by leveraging data mapping within a digital twin-enabled environment. Despite its effectiveness, the proposed approach may face challenges in handling large-scale systems or environments with incomplete or inconsistent data mapping. Thamotharan et al. (2023) introduced a digital twin-based model for continuous healthcare monitoring and forecasting, focusing on unforeseen complications related to diabetes. While promising, the model's predictive accuracy may be constrained by the quality and availability of patient-specific data, making it less effective in data-scarce or diverse healthcare settings. Xu et al. (2021) proposed a reference framework combining digital twin concepts with cloud computing to enhance data evaluation and service management. Although the proposed framework improves efficiency, its dependence on cloud infrastructure may introduce latency and security concerns, particularly in sensitive or real-time applications. Rahim et al. (2024) explored digital twin-based strategies for clinical crisis management by integrating predictive models, machine learning, and discrete event simulation frameworks. While these methods enable operational improvements with minimal disruption, the reliance on complex simulations and predictive algorithms may hinder real-time adaptability in rapidly evolving crises. Singh et al. (2023) developed a digital twin-powered warehouse product-service approach, allowing real-time data collection and display from the physical warehouse. However, its effectiveness may be limited by the accuracy and reliability of sensor data, as well as the computational demands of real-time processing.

2.3. Blockchain-based intelligent solutions

Digital twins and blockchain have been extensively studied as standalone technologies, but recent research has increasingly focused on integration to enhance storage, monitoring, security, and operational efficiency across various domains. Khan et al. (2023) presented an architecture that utilizes blockchain to enable flexible and real-time allocation of power. The proposed approach also incorporated a smart contract-based mechanism to improve coordination and task assignment in multi-agent models, with the model validated through testing in diverse production environments. Similarly, Guo et al. (2021) developed a blockchain-powered multi-agent system aimed at improving work coordination. The proposed approach collected data on operational events and peripheral control decisions, which were used to construct a cloud-based deep learning prediction engine for task rescheduling. In the healthcare sector, Amofa et al. (2024) explored the use of blockchain in combination with digital twins to improve patient data security and interoperability in digital health systems. The presented framework demonstrated how blockchain could ensure the integrity of patient records while enabling real-time monitoring through digital twins. Similarly, Akash and Ferdous (2022) proposed a blockchain-integrated digital twin model for personalized medicine, allowing secure data sharing and predictive analytics for treatment optimization. In manufacturing, Roumeliotis et al. (2024) introduced a blockchain-enabled digital twin framework for smart factories, focusing on improving transparency and traceability in supply chain management. The proposed model utilized blockchain to securely store production data while digital twins provided real-time monitoring and optimization of manufacturing processes. Similarly, Suhail et al. (2021) explored the integration of blockchain and digital twins for predictive maintenance in industrial systems, enabling secure data exchange between machines and predictive models to reduce downtime and improve efficiency. In the energy sector, Borowski (2021) proposed a blockchain-based digital twin model for decentralized energy trading, where digital twins represented physical energy assets, and blockchain ensured secure transactions between stakeholders. This approach facilitated real-time monitoring of energy usage and optimized energy distribution through smart contracts. Thakur et al. (2023) and Son et al. (2022) emphasized the critical role of blockchain technology in enhancing security within digital twin ecosystems. Thakur et al. (2023) highlighted its effectiveness in protecting sensitive industrial data, while Son et al. (2022) explored its role in safeguarding IoT-based digital twin systems from cyberattacks.

2.4. Research challenges

The current section highlights the critical challenges that are vital for advancing the state-of-the-art in the field.

1. *Leveraging expert knowledge*: Modern frameworks heavily rely on expert insights and domain knowledge to effectively guide the modeling process.
2. *Incorporating diverse modeling assumptions*: Accurate representation of machine tools requires adopting various assumptions about system behavior and characteristics, particularly concerning their physical and geometric properties.
3. *Complexity of machine tools*: The intricate and sophisticated nature of machine tools poses significant challenges in accurately modeling their behavior and interactions.
4. *Reduced understanding of tool degradation*: A lack of comprehensive knowledge about the processes of tool wear and temporal degradation complicates the effective application of EHM systems.
5. *Focus on severe tool damage in digital twin models*: Digital twin models based on physical and geometric parameters are primarily effective at detecting major issues, such as broken tools, but struggle to identify more subtle forms of wear and degradation.
6. *Challenges in tracking gradual tool wear*: Traditional digital twin approaches are not well-suited for monitoring the progressive wear and tear of tools, limiting the effectiveness in predictive maintenance.
7. *Ineffectiveness in heterogeneous environments*: The ability of traditional digital twin methodologies to monitor tool conditions is further hindered in demanding operational environments characterized by varying conditions and high stress.

Table 1
Comparative analysis (1 Yes, 0 No).

Parameters	Haghshenas et al. (2023)	Jwo et al. (2022)	Wu et al. (2021)	Sayed et al. (2024)	Ren et al. (2022)	Proposed model
Data Mining	0	1	1	0	0	1
Feature Extraction	0	0	0	0	0	1
Decision Making	0	1	0	0	0	1
Heterogeneous Data	1	0	1	0	0	1
Baseline Sensing Technology Used	1	1	1	1	1	1
Classification Model used	0	0	0	0	0	1
Fog Computing Layer	0	0	0	0	1	1
Security	1	0	1	1	0	1
Numerical Quantification	0	0	0	0	0	1
Remote Data Storage	1	1	0	0	1	1

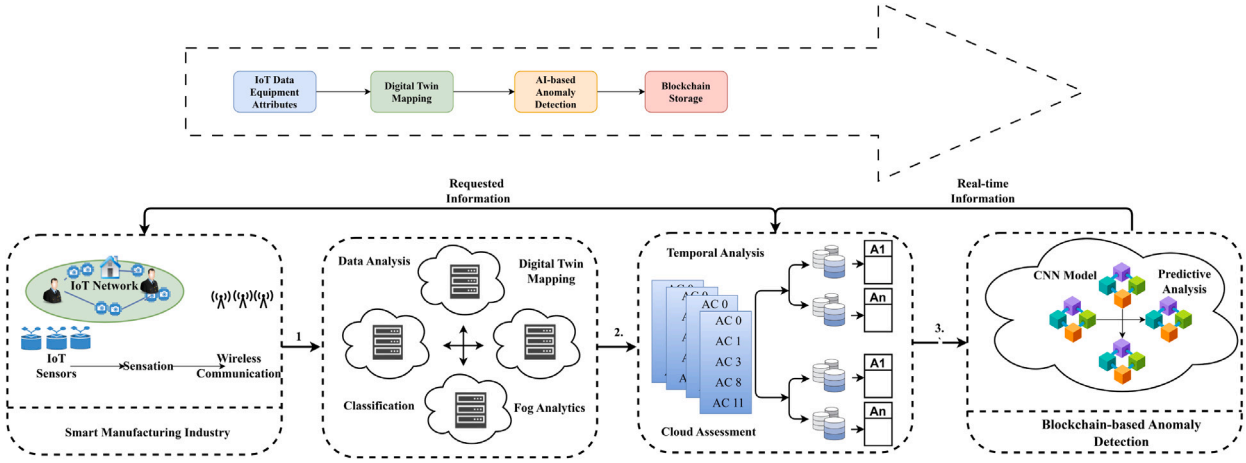


Fig. 3. Proposed model.

Additionally, Table 1 presents a comparative assessment of state-of-the-art research works, providing a comprehensive overview of the current methodologies. This analysis emphasizes the need for innovative approaches to overcome these challenges and improve the efficiency of digital twin technologies in real-world applications.

3. Proposed model

The smart technology architecture for equipment health monitoring in the manufacturing is illustrated in Fig. 3. The proposed approach enables continuous tracking and monitoring of vulnerabilities by representing physical devices as digital twins. This system presents secure surveillance by seamlessly integrating physical objects used in production through a blockchain-based architecture built on digital twin principles, eliminating the need for direct physical interaction. By combining IoT sensors, digital twin technologies, and blockchain-enabled data management, the design addresses the critical need for better security within the industrial sector. The proposed framework integrates key functionalities such as secure data analysis, and real-time monitoring, creating an effective solution for equipment health management. Several essential components form the foundation of this proposed system, ensuring its effectiveness and adaptability to the dynamic demands of modern manufacturing environments.

1. **IoT Devices**: Deployed across numerous industrial machinery to collect temporal data for equipment health.
2. **Digital twin-based Vulnerability Mapping**: Digital twin entities enable the identification of vulnerabilities and facilitate real-time monitoring of physical equipment through their virtual counterparts.
3. **Blockchain Technology**: Enables secure data storage and management of industrial data, safeguarding it against tampering or unauthorized access. This technology provides a reliable foundation for maintaining data integrity within the system.
4. **Predictive Analytics**: Utilizes data from IoT sensors, and blockchain systems to perform advanced analytics. This includes analyzing consumption patterns, forecasting potential equipment health risks, and enabling proactive maintenance strategies.

3.1. IoT-based data acquisition

The proposed architecture designates the IoT-based data sensation for collecting and processing data related to equipment health. By leveraging IoT sensors embedded in various components, the module gathers diverse data types, including numerical and non-numerical text data, equipment-specific information (such as operating frequency and rates), and time-related data. The acquired information is categorized in sets, which include critical parameters like operating duration, frequency, wear and tear, and delays. To effectively manage and analyze these varied input types, the model employs multiple feature extraction techniques, ensuring accurate and comprehensive data processing.

1. **Cross-Modality Search via Hashing**: This approach is applied to textual data to enable efficient retrieval and analysis.
2. **Symbolic Aggregate Approximation (SAX)**: GPS data is approximated using the SAX method, ensuring accurate representation and simplification of spatial information.
3. **HCRF Model Analysis**: The dataset, which includes equipment health data, is assessed using the Hidden Conditional Random Field technique to uncover patterns and relationships.

the extracted attributes are classified into three distinct types: static, stochastic, and dynamic. Once the data is collected, it is sequentially transmitted to the fog–cloud layer, where a comprehensive analysis of health-related vulnerabilities is performed. To enable effective categorization and forecasting, continuous data is segmented into fixed time intervals. This approach allows for the classification of anomalies and

facilitates predictive analysis, enabling the identification of trends and the forecasting of potential issues over specific periods. The presented approach incorporates several essential processes:

1. **Data Collection and Feature Extraction**: The process begins with gathering data from Internet of Things (IoT) sensors and extracting relevant features.
2. **Event Association**: The collected data is mapped to the corresponding event sets for further analysis.
3. **Attribute Categorization**: Extracted features are classified into three groups: static, dynamic, or stochastic, based on their characteristics.
4. **Sequential Edge–Cloud Processing**: The data is forwarded in sequential manner to the fog–cloud storage for comprehensive processing.
5. **Signal Segmentation for Event Classification and Prediction**: Continuous signals are divided into discrete segments, enabling event classification and predictive analysis.

The presented approach involves data collection, feature abstraction, and assessment on-premises and in the cloud, offering a comprehensive solution to address EHM anomalies within the industrial sector. The proposed model is built upon the following key steps:

1. *Temporal Block Analysis*: The first step involves the formulation of the temporal window block. This block is defined by several characteristics that describe an event, whether it is normal or anomalous. These characteristics include:
   - Q_u: Identifies the sensor type that recorded the event-related signal.
   - Q_n: Represents the measurement captured by the sensor concerning the event.
   - Q_t: Specifies the initializing time of the event.
   - Q_f: Depicts the ending time of the event.

   The event duration, ΔT, is calculated as follows:

   $$\Delta T = Q_f - Q_t \tag{1}$$

   The presented model effectively captures sensor-specific data along with the temporal context associated with manufacturing EHM vulnerabilities by utilizing a block representation tied to specific events.
2. *Data Forwarding*: Signals from IoT sensors installed in industrial units are transmitted to external systems through gateways and other adapters. The data is relayed to cloud-based systems using multiple communication channels, including wireless, wired, and ZigBee networks. Data collection and transfer are facilitated by the Transfer Control Protocol (TCP) and WiFi modules. This multi-channel transmission approach ensures the efficient transfer of sensor readings from the physical layer to edge and cloud devices for analysis and processing. By leveraging a diverse range of communication technologies and protocols, the system accommodates various deployment scenarios and ensures a reliable flow of data from IoT sensors to the advanced processing layers of the framework. This adaptable, multi-channel strategy provides a robust and flexible data transmission process.
3. *Middleware* : The middleware module serves as a critical component in the system, responsible for processing and analyzing incoming data to extract meaningful insights. It manages various operational tasks, including the coordination of data flow between different layers and ensuring efficient communication within the framework. Additionally, the module enables remote assessments, allowing for the evaluation of system performance and equipment health from a distance. It also supports wireless monitoring, providing real-time tracking and oversight of connected devices and sensors. This comprehensive functionality ensures seamless integration and management of data across all system components.

Algorithm 1 Pattern Transformation

Require: Two event sets, G_m and G_n, with corresponding event collection cycles L_m and L_n.
Ensure: A transformed event pattern G'_m that aligns G_m within the unified database.

Initialize $G'_m = \emptyset$ (an empty set for the transformed pattern)
for each event G_{1n} in G_1 **do**
  Compute the corresponding time instance on G_2: $L_{2n} = L_2 \times n$
  Identify the neighboring events G_{1r} and G_{1s} in G_1 such that:
  $L_{1r} = \max\{L_{1m} \mid L_{1m} < L_{2n}\}$
  $L_{1s} = \min\{L_{1m} \mid L_{1m} > L_{2n}\}$
  Compute the weights for linear interpolation:
  $w_r = \frac{k_{1s} - L_{2n}}{L_{1s} - L_{1r}}, \quad w_s = \frac{L_{2n} - L_{1r}}{L_{1s} - L_{1r}}$
  Calculate the interpolated value for G_{1n}:
  $G'_{1n} = w_r \cdot G_{1r} + w_s \cdot G_{1s}$
  Append G'_{1n} to G'_m
end for
Return the transformed event pattern G'_m

3.2. Digital twin modeling

The proposed approach leverages a machine learning framework to mathematically model the concept of digital twins. EHM event data is gathered from physical and digital sources and integrated within the digital twin paradigm. To effectively utilize raw data collected from IoT devices, the digital twin requires pre-processed data. A key function within the proposed framework is referred to as *Pattern Transformation*, which plays a critical role in ensuring data uniformity. Given that IoT sensors often collect data at varying intervals, Pattern Transformation is essential for standardizing signals. This can be achieved by either increasing the data volume or reducing its frequency to a common lower level. Deep learning algorithms are employed to standardize the frequency of time series data and consolidate patterns. Synchronizing data frequencies is vital for enabling the digital twin model to accurately capture and represent EHM patterns, as well as to manage vulnerabilities effectively. By standardizing data frequencies, the proposed method ensures more precise and consistent representations of real-world events, allowing the digital twin model to train on a harmonized dataset. Pattern Transformation is indispensable for successfully integrating the digital twin concept into the broader monitoring framework, as it guarantees the accuracy and consistency of data used for training and simulation. This harmonization process is critical for the effective implementation of a digital twin-based EHM system, enabling the model to accurately represent and analyze health risks in real-world scenarios.

Definition 1. Let G_1 and G_2 represent two groups of event patterns that are enhanced at L_1 and L_2 cycles, respectively. The *Pattern Transformation* process aligns these patterns by using the event dimension G_1 as a reference to construct the next data dimension, G_2

Specifically, the data points in G_1 are either adjusted or stretched to ensure their frequency and temporal alignment match the event patterns in G_2. It is crucial to harmonize these two sets of event data into a unified dataset, G_{unified}, to train the digital twin model effectively. By aligning event patterns with varying frequencies, the *Pattern Transformation* phase improves the dataset's ability to depict real-world patterns accurately. This ensures that the digital twin model is trained on a cohesive and realistic dataset, enhancing its overall performance and reliability. Fig. 5 depicts the overall data flow procedure.

$$G'_{1m} = G'_{1r} + \frac{L_2 \times n - L_1 \times r}{L_1}(G_{1(r+1)} - G_{1r}) \tag{2}$$

Where G_r represent the baseline time series data pattern, while G_{1r} and $G_{1(r+1)}$ denote the reference points located along the G_1 curve. After

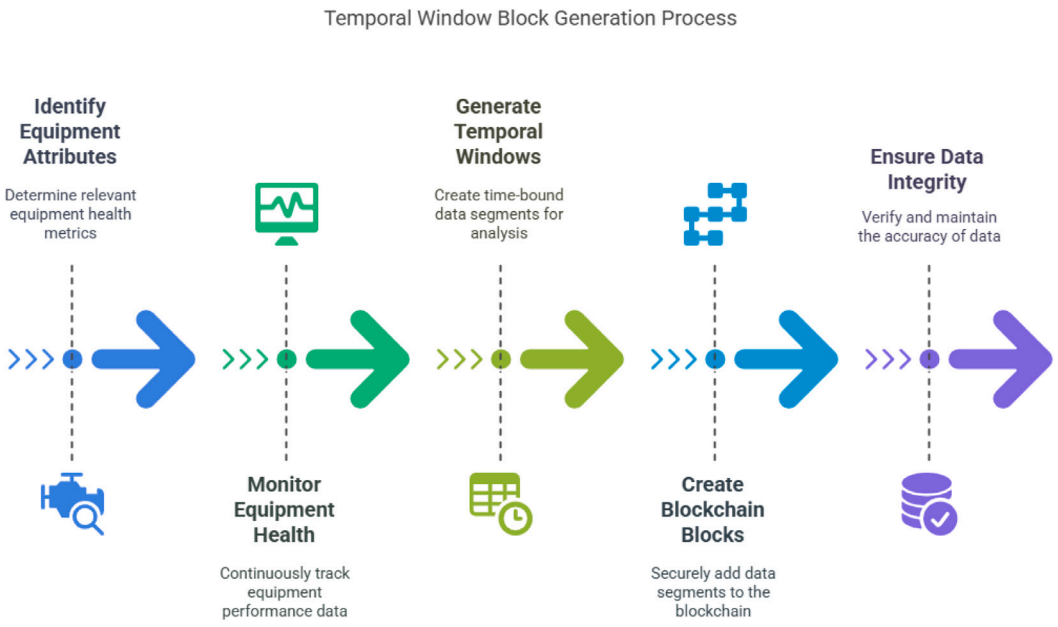


Fig. 4. Blockchain-based temporal data management.

identifying these reference values, the weighted mean method is applied to calculate the distance ratio across the temporal scale between G_{1r}, G_{1n}, and $G_{1(r+1)}$. This approach ensures an accurate measurement of the temporal relationships within the data.

$$r = \lfloor \frac{L_2 \times n}{L_1} \rfloor \tag{3}$$

If G_1 and G_2 differ, the frequency ratio $\frac{L_1}{L_2}$ serves as a critical reference for determining the next reference point on the original G_1 curve. The complete procedure for this estimation is outlined in Algorithm 1.

3.3. Blockchain data assessment

To enable efficient data management in a dynamic, real-time environment, the proposed approach leverages blockchain technology. A key focus of the system is predicting critical events, achieved through an anomaly detection mechanism that provides real-time alerts to monitoring organizations. The detailed procedure for conducting the analysis and generating alerts is outlined in Algorithm 2. At its core, the system integrates blockchain-based data management with anomaly detection to facilitate real-time EHM. This integrated approach addresses the need for continuous oversight while ensuring timely notifications, ultimately enhancing the effectiveness of smart monitoring systems.

3.3.1. Data block generation

The proposed method leverages blockchain technology to enhance the management and utilization of EHM-related event data, particularly for health monitoring and instant user notifications. When a potential vulnerability or relevant event is detected, the system promptly updates the blockchain with the associated details. To optimize efficiency, the method employs data aggregation to consolidate multiple transactions into a single block. By utilizing a consortium blockchain, the approach eliminates the need for a traditional verification stage, streamlining the process. The primary goal of integrating blockchain technology is to accurately detect abnormal events through monitoring services based on equipment conditions. Blockchain records are openly accessible to multiple stakeholders, ensuring transparency and collaboration. Reliable and precise data processing is critical for effective intelligent monitoring services, and the proposed method generates blocks at random intervals to enhance system performance. As illustrated in Fig. 4, the evolution of blockchain in manufacturing over time demonstrates data management. By incorporating blockchain, the proposed solution effectively addresses the demand for secure and trustworthy data management. It simplifies real-time anomaly detection and alert generation while significantly enhancing the overall capabilities of intelligent monitoring systems.

Algorithm 2 Alert Generation Procedure

Require: CurrentEvent: The event currently being evaluated.
Threshold: The critical threshold value.
EventList $= \{\text{NextEvent}_1, \text{NextEvent}_2, \ldots, \text{NextEvent}_m\}$: A list of subsequent events.
Ensure: Alert: The generated notification status.
Initialize $\Delta = \emptyset$ ▷ Prepare a set to store differences.
if CurrentEvent ≤ Threshold **then** ▷ Check if the current event is at or below the threshold.
    Alert ← Critical ▷ Set the alert status to "Critical".
else
    for $i = 1$ to m **do** ▷ Iterate through the list of subsequent events.
        Compute $\Delta_i = |\text{CurrentEvent} - \text{NextEvent}_i|$ ▷ Calculate the absolute difference.
        Add Δ_i to Δ ▷ Store the computed difference.
    end for
    if $\exists \Delta_i \in \Delta$ such that $\Delta_i \leq$ Threshold **then** ▷ Check if any difference is below or equal to the threshold.
        Alert ← Critical ▷ Set the alert status to "Critical".
    else
        Alert ← Normal ▷ Set the alert status to "Normal".
    end if
end if
Return Alert ▷ Output the generated alert status.

3.3.2. Consensus blockchain

The proposed design employs a **Reputation-based Byzantine Fault Tolerant (RBFT)** method to establish the consortium blockchain network. RBFT provides several key benefits, including:

Fig. 5. Pattern transformation data flow.

1. **Decentralized Processing**: Ensures that no single entity controls the network.
2. **Enhanced Speed**: Improves the efficiency of data processing and consensus.
3. **Robust Security**: Protects against malicious attacks and unauthorized access.
4. **High Reliability**: Guarantees consistent and accurate operation.
5. **Low Latency**: Reduces the time required for transaction validation.
6. **Transaction Finality**: Ensures that once a transaction is confirmed, it cannot be reversed or modified.

The key steps are as follows;

1. **Consensus Mechanism**: The system uses a modified RBFT methodology to achieve a consensus-driven outcome efficiently.
2. **Block Creation**: After the validator completes the creation of block BC_j, the blockchain is updated by disseminating the newly created block throughout the network.
3. **Block Validation**:
   - Only **authorized nodes** within the blockchain network are allowed to sign the block header, which validates the transaction.
   - The signatures, often referred to as **votes**, are generated using the identities of network participants and are recorded on the blocks.
4. **Vote-Based Security**:
   - The vote-based mechanism, combined with the consortium blockchain structure, significantly reduces the risk of **attacks**.
   - This approach ensures **low latency** and **high throughput**.

The overall consensus procedure is detailed as Algorithm 3. The enhanced RBFT-based blockchain integration algorithm ensures secure and efficient consensus for adding new blocks to a consortium blockchain. It begins by initializing variables such as the signature count, consensus status, and retry attempts. Each peer in the network generates a signature for the new block, and valid signatures are counted. If the total valid signatures meet or exceed the predefined

threshold, the system synchronizes with an NTP server for accurate timestamping, hashes the block, and appends it to the blockchain, updating the consensus status to true. If the threshold is not met, the algorithm retries the process after a designated time interval, up to a maximum number of retries. Invalid signatures and failed attempts are logged for auditing purposes. The algorithm ensures fault tolerance, reliability, and traceability, while gracefully handling consensus failures and retrying within defined limits. The proposed method ensures **secure, decentralized, and reliable data management** by leveraging an RBFT-based consortium blockchain. Based on the **reliability, scalability, and speed** of the blockchain-based design, **real-time monitoring** becomes the backbone of the equipment monitoring system, ensuring efficient and intelligent operation.

Algorithm 3 Enhanced RBFT-Based Blockchain Integration with Missing Aspects

Require: $NewBlock$ ▷ The newly created block to be validated
Ensure: $ConsensusStatus$ ▷ Final status of the consensus process: True or False
Initialize Variables:
$SignatureCount \leftarrow 0$ ▷ Set initial signature count to zero
$ConsensusStatus \leftarrow$ False ▷ Default consensus status is False
$BlockchainUpdated \leftarrow$ False ▷ Indicates if the blockchain is updated
$RetryAttempts \leftarrow 0$ ▷ Initialize retry attempts counter
$MaxRetries \leftarrow$ Predefined Limit ▷ Set maximum allowed retries
Start transaction verification process
for $Node \leftarrow 1$ to $TotalPeers$ **do** ▷ Iterate through all peers in the network
  Compute $Signature_{Node}$ ▷ Generate a signature for the block by each peer
  if $Signature_{Node}$ is valid **then** ▷ Check if the signature is valid
    Increment $SignatureCount$ ▷ Update the count of valid signatures
  else
    Log error for $Node$ ▷ Record invalid signature for auditing purposes
  end if
end for
if $SignatureCount \geq Threshold$ **then** ▷ Verify if the required number of signatures is met
  Synchronize with NTP server for accurate timestamping ▷ Ensure time consistency
  Perform hashing of $NewBlock$ ▷ Generate cryptographic hash for the block
  Append $NewBlock$ to the blockchain ▷ Finalize and add the block to the chain
  Set $ConsensusStatus \leftarrow$ True ▷ Consensus successfully achieved
  Set $BlockchainUpdated \leftarrow$ True ▷ Mark the blockchain as updated
else
  Increment $RetryAttempts$ ▷ Track the number of retries
  if $RetryAttempts < MaxRetries$ **then** ▷ Check if retries are within the allowed limit
    Wait for the predefined interval $TimeInterval$ ▷ Pause before retrying
    Restart the verification process ▷ Retry consensus process
  else
    Log failure ▷ Record failure after exceeding retry attempts
    Set $ConsensusStatus \leftarrow$ False ▷ Consensus failed after retries
  end if
end if
return $ConsensusStatus$ ▷ Output the final consensus result (True or False)

3.4. Decision-making services

The proposed model employs a unique hybrid approach that integrates deep learning techniques to detect potential EHM-related anomalies in the manufacturing sector. Its primary objective is to identify instances where EHM variations occur at abnormal rates during the transmission process.

3.4.1. Anomaly assessment

The proposed approach introduces an innovative event assessment model aimed at improving the accuracy of detecting equipment health vulnerabilities. This model is built on a combination of key components, with its architecture designed to maximize efficiency and accuracy. At its core, the model utilizes a **1D Convolutional Neural Network (1D CNN)**, which serves as the foundation for event prediction by extracting critical features from input data. The architecture of the 1D CNN includes the following:

1. **Convolutional Layers**:
   - These layers analyze local patterns in the input data by adjusting filter quantities.
   - They are responsible for detecting event-specific properties and extracting meaningful features.
2. **Pooling Layers**:
   - These layers efficiently represent event patterns by reducing the dimensionality of the data while preserving essential features.
   - They help in summarizing the extracted features for further analysis.
3. **Feature Extraction and Real-Time Analysis**:
   - The 1D CNN leverages its feature extraction capabilities to analyze raw data in real time, enabling quick detection of key patterns.

Despite its strengths, traditional 1D CNN algorithms face challenges in capturing short-lived temporal patterns associated with specific events. To address this limitation, the proposed approach integrates **Gated Recurrent Units (GRUs)** into the 1D CNN architecture. GRUs enhance the model's ability to:

- Detect and interpret long-term temporal dependencies.
- Analyze underlying patterns across multiple events.

This integration allows the system to overcome the limitations of standard CNNs and significantly improve event detection accuracy. The hybrid approach, combining the strengths of 1D CNNs and GRUs, forms the backbone of the system. This synergy enables:

- Precise detection of vulnerabilities.
- Comprehensive characterization of conditional events in industrial equipment.

By integrating these components, the proposed method delivers a robust solution for real-time monitoring and analysis of equipment health, effectively capturing short-term and long-term temporal patterns.

3.4.2. Dynamic attribute modulation

To improve the accuracy and stability of condition analysis with limited training data, the hybrid CNN-GRU model leverages the complementary strengths of convolutional and recurrent architectures. This approach is particularly advantageous in equipment health monitoring (EHM), where the collection of large annotated datasets is often challenging. The proposed model employs a CNN-BiGRU (Bidirectional Gated Recurrent Unit) design, enabling it to effectively identify consecutive actions. By utilizing bidirectional recurrent units, the model

captures interdependencies between data samples and learns forward and backward temporal relationships. This bidirectional capability, combined with the CNN's spatial feature extraction, allows the architecture to efficiently recover spatial information while preserving critical temporal components. The inclusion of additional architectural elements further enhances the model's ability to detect and analyze consecutive events, resulting in a more reliable and robust solution. A key advantage of this hybrid design is its ability to capture spatial correlations and long-term temporal dependencies in the data, enabling precise detection and analysis of complex event patterns in industrial settings. By integrating GRUs with bidirectional recurrent units, the model improves its understanding of the sequential and interdependent structure of the data, enhancing its capacity to identify vulnerabilities in EHM. To address the challenge of limited labeled data, the proposed model incorporates **Self-Supervised Learning (SSL)** techniques. SSL enables the model to learn useful representations from unlabeled data by solving pretext tasks, such as predicting temporal orders, reconstructing input sequences, or contrastive learning. By pretraining the CNN-BiGRU model with SSL, the architecture can extract meaningful spatial and temporal features from raw data, significantly reducing the reliance on large annotated datasets. This pretraining step enhances the model's ability to generalize and improves its performance on downstream tasks, such as anomaly detection and pattern recognition in EHM. Furthermore, the model leverages **Federated Learning (FL)** to facilitate collaborative training across multiple decentralized data sources, such as industrial equipment in different locations. FL ensures that sensitive data remains on local devices, addressing privacy and security concerns while enabling the model to benefit from diverse and distributed datasets. In the federated setting, each local device trains a copy of the CNN-BiGRU model on its data and shares only the updated model parameters with a central server. The server aggregates these updates to produce a global model, which is then redistributed to local devices for further training. This iterative process allows the model to learn from diverse data distributions without compromising data privacy, making it particularly suitable for real-world industrial applications. To streamline sequential feature modeling, the parameter matrix

$$\mathbf{T} = [t_1, t_2, \ldots, t_r]$$

is transferred from the CNN to the GRU model. Here, $\mathbf{T}$ represents the parametric matrix, while the current event state is denoted as t_l. The GRU network analyzes r attribute matrices for each occurrence t_k within a given time interval ΔU. The reset gate of the GRU cell, denoted as s_u, is computed as follows:

$$s_u = \sigma(\mathbf{W}_s \cdot \mathbf{T} + \mathbf{U}_s \cdot \mathbf{h}_{t-1} + \mathbf{b}_s),$$

Where:

- σ is the sigmoid activation function,
- $\mathbf{W}_s$ and $\mathbf{U}_s$ are weight matrices,
- $\mathbf{b}_s$ is the bias term, and
- $\mathbf{h}_{t-1}$ is the hidden state from the previous time step.

This hybrid CNN-BiGRU architecture provides a robust and reliable method for detecting and analyzing complex event patterns by capturing spatial and temporal dependencies in the data. The alternate cell state, denoted as d_u, is computed by integrating the reset gate s_u with the previous cell state l_{u-1} and the input state q_u. This process is mathematically expressed as:

$$d_u = \tanh(\mathbf{N}q_u + (\mathbf{P}(s_u \circ l_{u-1}) + g)),$$

Where:

- $\tanh(q) = \frac{e^q - e^{-q}}{e^q + e^{-q}}$ is the hyperbolic tangent activation function, and
- $\circ$ represents element-wise multiplication.

The update gate, v_u, is calculated as:

$$v_u = \sigma(\mathbf{N}_v q_u + \mathbf{P}_v l_{u-1} + k_v),$$

where σ is the sigmoid activation function.

Using these components, the current state l_u is updated by blending the alternate state d_u with the previous state l_{u-1} based on the update gate v_u:

$$l_u = v_u \circ l_{u-1} + (1 - v_u) \circ d_u.$$

The final output of the BiGRU network, l_u, is passed through fully connected layers corresponding to the number of event classes being analyzed. To generate the classification outcomes, the Softmax function is applied as follows:

$$\mathbf{S}_u = \text{softmax}(\mathbf{N}_s l_u),$$

where $\mathbf{N}_s$ represents the weight matrix of the fully connected layers.

The model's loss is computed using the cross-entropy error function, defined as:

$$\lambda\langle \mathbf{S}_u, \mathbf{T}_u \rangle = -\sum_{l=1}^{q} \mathbf{T}_u \log(\mathbf{S}_u),$$

where $\mathbf{T}_u$ is the ground-truth label vector. The hybrid model's weights are optimized using Backpropagation Through Time (BPTT) in conjunction with the ADAM stochastic optimizer, ensuring effective training and convergence toward optimal performance. This integrated approach, enhanced by SSL and FL, provides a robust and efficient solution for detecting and analyzing consecutive events indicative of anomalous conditions. Key components of the optimization process include:

1. **Self-Supervised Learning (SSL):** By retraining the model on unlabeled data with pretext tasks, SSL enables the extraction of meaningful spatial and temporal features, reducing the need for large labeled datasets and improving generalization.
2. **Federated Learning (FL):** FL allows collaborative training across decentralized data sources while maintaining data privacy, enabling the model to learn from diverse datasets without compromising security.
3. **Backpropagation Through Time (BPTT):** A specialized training method for recurrent neural networks, BPTT propagates error gradients backward through the unrolled network, allowing the model to capture temporal dependencies in the data.
4. **ADAM Stochastic Optimizer:** ADAM (Adaptive Moment Estimation) combines momentum and adaptive learning rates to ensure efficient and reliable convergence during training, enhancing the overall performance of the model.

The hybrid CNN-GRU model excels at identifying correlations and uncovering patterns within equipment data, making it highly effective in recognizing and analyzing vulnerability trends. Leveraging optimization strategies such as BPTT and the ADAM optimizer, the model enhances its ability to process sequential data and detect anomalous occurrences. This combination facilitates efficient training and enables the model to converge toward an optimal parameter set, significantly improving its performance in analyzing complex event sequences.

4. Experimental validation

The proposed framework for equipment health monitoring and anomaly detection in the manufacturing industry is designed as a multi-stage process. It begins with the collection of operational data from machinery and concludes with comprehensive risk assessment and decision-making. The framework undergoes a series of systematic validation steps to ensure its reliability and effectiveness in identifying potential anomalies and predicting equipment vulnerabilities. To evaluate the performance of the proposed mechanism in detecting and addressing issues within manufacturing systems, six critical metrics are utilized:

1. **Detection Efficiency**: Measures the timeliness and responsiveness of the anomaly detection process.
2. **Prediction Performance**: Evaluates the capability of the framework to predict potential equipment failures.
3. **Energy Efficacy Analysis**: Estimate the energy utilization for low power devices.
4. **Model Reliability**: Examines the robustness and stability of the framework under various operational conditions.
5. **Stability Analysis**: Ensures the mechanism is stable over large data instances.
6. **Cost Complexity Analysis**: Determines the cost complexity for the proposed model.

Each of these metrics plays a pivotal role in refining and improving the overall efficiency and effectiveness of the proposed equipment health monitoring and anomaly detection framework, ensuring it provides actionable insights for maintaining operational reliability and minimizing downtime in manufacturing processes.

4.1. Simulation environment

The model's specifications are divided into implicit and explicit components, each outlining essential features and capabilities.

4.1.1. Implicit specifications

The system is built with advanced hardware and software configurations to ensure optimal performance. Key details include:

- **Storage and Processing:** A 4TB Read-Only Memory (ROM), an Intel Core i7 processor (11th generation), and 32 GB of RAM.
- **Operating System and Tools:** Ubuntu Linux 12.02 LPS serves as the operating system, with Docker Engine version 16.4 managing containerization. Development tools include Node Package Manager (NPM) version 4.0, Docker Compose version 2.0, Node.js version 8.0, and Git version 2.4, supporting programming in version 2.6x.

4.1.2. Explicit specifications

The explicit specifications focus on the system's protocols, hardware setup, and overall architecture:

- **Consensus Protocol:** A customized Reliable Byzantine Fault Tolerance (RBFT) protocol ensures secure and efficient consensus.
- **Hardware Configuration:** The system features a processing speed of 2.26 GHz, 64 GB of RAM, a quad-core architecture, and a 4TB hard disk drive.
- **Perception Nodes:** Two categories of nodes are defined:
  - **Category 1:** IoT sensors.
  - **Category 2:** Node MCUs.
- **Node Management and Database:** Nodes are distributed via the Ethereum network, with MongoDB employed as the database solution.

4.1.3. Blockchain and testing framework

- **Performance Testing:** Hyperledger Caliper is used to evaluate and benchmark the system's performance.
- **Network Setup:** The blockchain infrastructure includes one server acting as the CoVEn (Coordinator Validator Node) and 30 peers operating within a peer-to-peer (P2P) network.

These detailed specifications provide a comprehensive overview of the model's technical foundation, emphasizing its capacity for secure, scalable, and efficient operation. The integration of advanced hardware, software, and blockchain technologies ensures the system's reliability and effectiveness. For validation, the online challenging dataset from the UCI repository is acquired comprising 80222 data instances.

4.2. Delay efficacy

To ensure the equipment health monitoring and anomaly detection system in the manufacturing industry operates at peak efficiency with minimal latency, it is essential to strategically allocate anomaly detection resources. Sensor nodes embedded in the equipment transmit data, which is then processed and analyzed at the central monitoring station. The temporal efficiency of the proposed anomaly detection mechanism was evaluated using the total execution time as a key performance indicator (KPI). The delay in the system, incorporating blockchain latency, can be mathematically represented as:

$$Delay = Delay^{Anomaly} + Delay^{Mapping} + Delay^{Decision} + Delay^{Blockchain}$$

Here, $Delay^{Blockchain}$ depends on the number of peers in the blockchain network, as the consensus mechanism and data propagation times are influenced by network size. Larger peer networks typically introduce additional latency due to increased communication overhead and validation times. The study measured blockchain latency by calculating the average of three rates — minimum, average, and maximum — of timed events associated with the creation of nodes and blocks. The number of detected anomalies varied across different simulation scenarios. Each simulation was conducted five times, and the results were averaged to ensure accuracy and consistency. Fig. 6 illustrates the detailed execution results, including anomaly detection delay, risk mapping time, response latency, and blockchain latency for different peer configurations.

4.2.1. Results

The findings of the proposed equipment health monitoring and anomaly detection mechanism in the manufacturing industry are demonstrated in Fig. 6. The system achieved an average anomaly detection latency of 5.22 s, while the average risk mapping time was 8.35 s, and the response delay was 12.64 s. When incorporating blockchain technology, the latency introduced by the blockchain varied based on the number of peers in the network. For a network with 10 peers, the blockchain latency was 3.50 s, which increased to 4.85 s with 20 peers and 6.10 s with 30 peers. Consequently, the total delay for the mechanism, including blockchain latency with 30 peers, amounted to 32.31 s. Despite the additional latency from blockchain integration, the overall latency per anomaly detection was measured at 5.21 ms, indicating that the mechanism remains efficient and responsive. These results highlight the system's ability to combine low-latency anomaly detection with the security and transparency benefits of blockchain technology, ensuring reliability, scalability, and operational efficiency in the manufacturing industry.

4.2.2. Results discussion

The results show that blockchain latency rises from 3.50 s (10 peers) to 6.10 s (30 peers), reflecting a near-logarithmic growth trend with network size. Despite this increase, the system maintains real-time anomaly detection because:

1. *Separation of Critical Processing Stages*: The core anomaly detection pipeline (sensor data acquisition, feature extraction, and CNN-BiGRU-based decision-making) operates independently of blockchain verification. This ensures that anomaly detection latency itself remains very low (average of 5.22 s, translating to 5.21 ms per anomaly event) even when blockchain peers scale up.
2. *Blockchain as a Post-Processing Layer*: Blockchain is primarily used for recording and securing results, not for direct anomaly detection. This means anomalies are detected and acted upon in real time, while blockchain confirmation occurs in parallel, introducing overhead only in terms of logging and auditability.

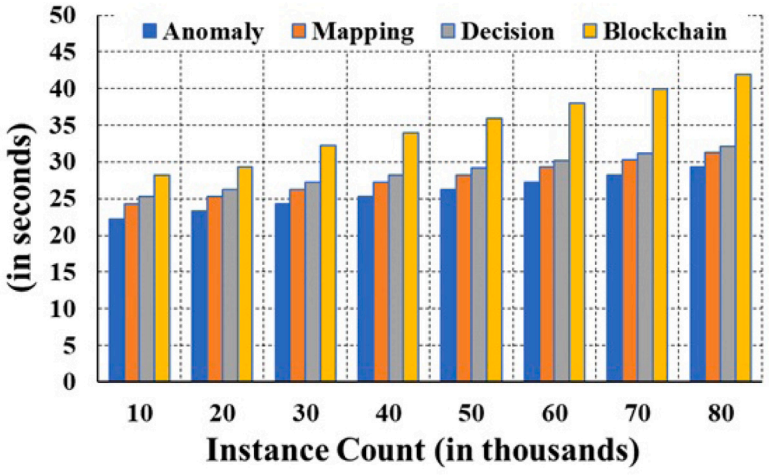


Fig. 6. Delay efficacy.

3. *Logarithmic Latency Growth*: Since the increase in blockchain latency is logarithmic rather than linear, the overall delay remains bounded within acceptable limits for industrial real-time systems. Even with 30 peers, the total delay of 32.31 s (including mapping and decision-making) does not critically impair anomaly response mechanisms.
4. *Mitigation Strategies*: Moreover, several standard mitigation approaches can be used for deployment:
   (a) *Sharding or Peer Grouping*: Partitioning peers into subnetworks for localized validation can minimize communication overhead.
   (b) *Asynchronous Logging*: Anomalies can be acted upon immediately, while blockchain updates occur asynchronously in the background.
   (c) *Edge Computing Integration*: Partial anomaly verification can be offloaded to edge nodes, reducing the volume of data transmitted to blockchain peers.

4.3. Prediction estimation

The proposed strategy demonstrates effective prediction of equipment vulnerabilities in the manufacturing industry through rigorous statistical analysis. To evaluate the performance of the equipment health monitoring system, key metrics such as accuracy, sensitivity, specificity, and F-measure are calculated. These metrics are defined as follows:

- **Accuracy**:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

- **Sensitivity (Recall)**:

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

- **Specificity**:

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}}$$

- **F-measure**:

$$\text{F-measure} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

where $\text{Precision} = \frac{\text{TP}}{\text{TP+FP}}$

4.3.1. Result analysis

For performance enhancement, benchmarking is performed against state-of-the-art research studies including Haghshenas et al. (2023), Wu et al. (2021), and Jwo et al. (2022). Detailed results are presented in Fig. 7. To ensure a fair comparison, the monitoring method is fine-tuned while preserving its foundational structure. Performance metrics are aggregated across heterogeneous datasets to deliver comprehensive insights into the robustness and effectiveness of the equipment health monitoring system.

1. Fig. 7(a) demonstrates that the proposed method excels in predicting equipment vulnerabilities in manufacturing, achieving an average accuracy of 92.25%, outperforming Haghshenas et al. (2023) with 90.25%, Wu et al. (2021) (with 89.95%), and Jwo et al. (2022) (with 88.02%).
2. Fig. 7(b) shows that the method attains an average sensitivity of 93.25%, exceeding the capabilities of Haghshenas et al. (2023) with 89.35%, Wu et al. (2021) (with 87.75%), and Jwo et al. (2022) (with 85.52%) in detecting equipment vulnerabilities.
3. As depicted in Fig. 7(c), the method achieves a mean specificity of 94.25%, surpassing Haghshenas et al. (2023) with 91.21%, Wu et al. (2021) (with 89.43%), and Jwo et al. (2022) (with 87.07%).
4. Fig. 7(d) highlights the method's significant advantage in F-Measure, with a value of 95.15%, enhancing equipment vulnerability prediction.

These results demonstrate that the proposed method is a more effective solution for predicting equipment vulnerabilities in manufacturing compared to other decision-making mechanisms. A key reason for the model's superiority is its utilization of a bi-directional Convolutional Neural Network (bi-CNN) architecture. This approach enhances feature extraction by capturing spatial hierarchies in both forward and backward directions, allowing for a more comprehensive analysis of equipment health data.

4.4. Energy efficiency analysis

This section estimates the energy consumption for the proposed model over a variable number of data instances. Fig. 8 depicts the overall results for the proposed model. It can be seen that the proposed model consumes 95.25 mJ of energy over 80,000 data instances, averaging 1.18 mJ per computation.

The energy efficiency of the proposed model is achieved through several technical optimizations:

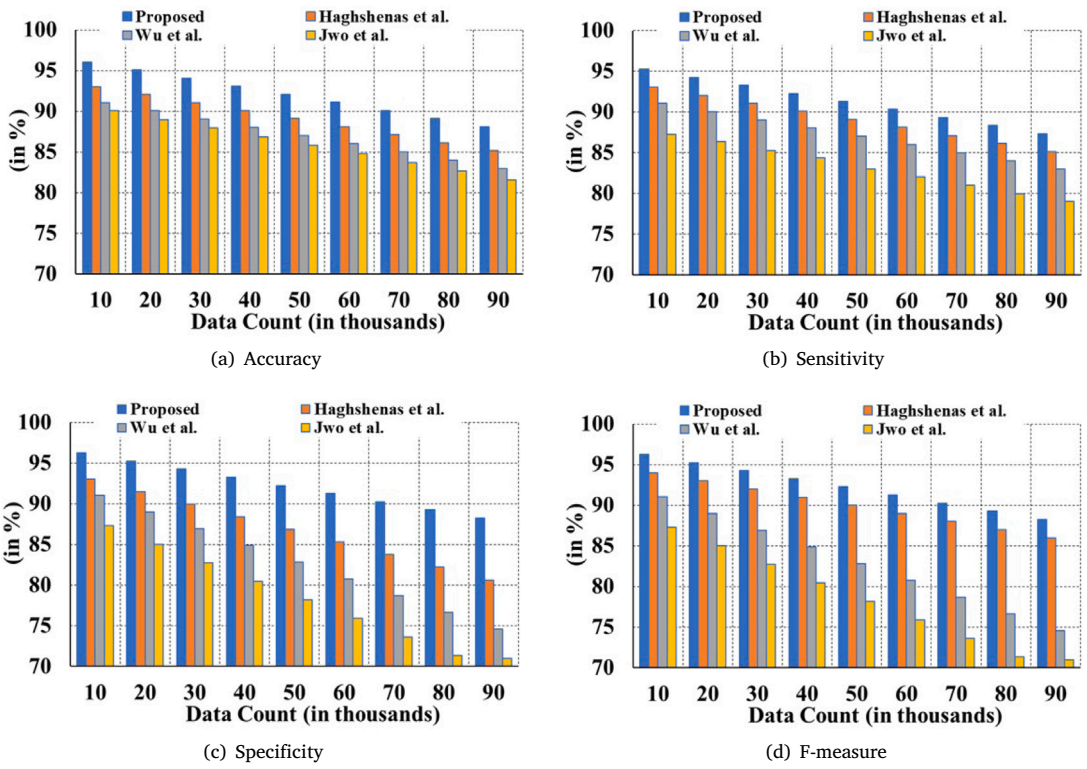


Fig. 7. Decision-modeling efficacy.

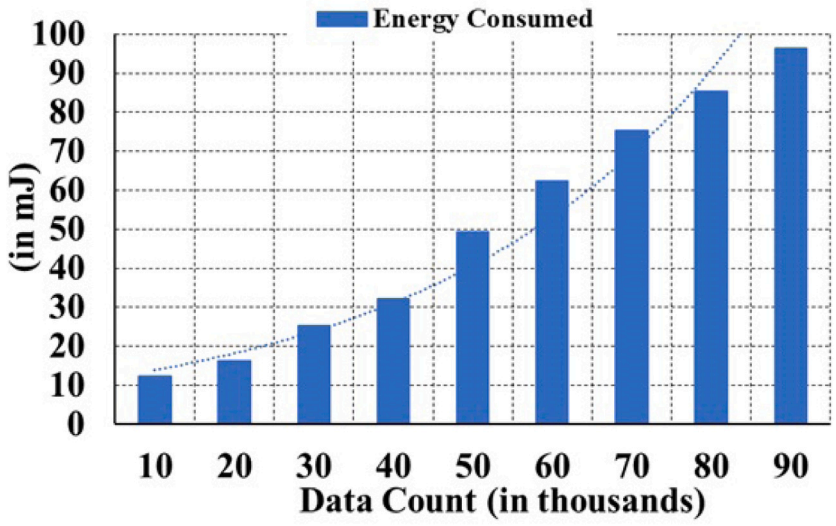


Fig. 8. Energy efficiency analysis.

- **Optimized BCNN Architecture:** The bi-directional Convolutional Neural Network (bi-CNN) is designed to efficiently process data by leveraging parallel computation paths. This reduces redundant operations and minimizes computational overhead, contributing to lower energy consumption.
- **Efficient Data Handling:** The model employs advanced data preprocessing techniques that streamline the input data, reducing the amount of unnecessary information processed. This ensures that only relevant features are extracted and analyzed, decreasing the overall energy required for computation.
- **Adaptive Algorithm Design:** The algorithm dynamically adjusts its complexity based on the input data characteristics. By scaling computational resources according to the demand, the model maintains high performance while conserving energy.

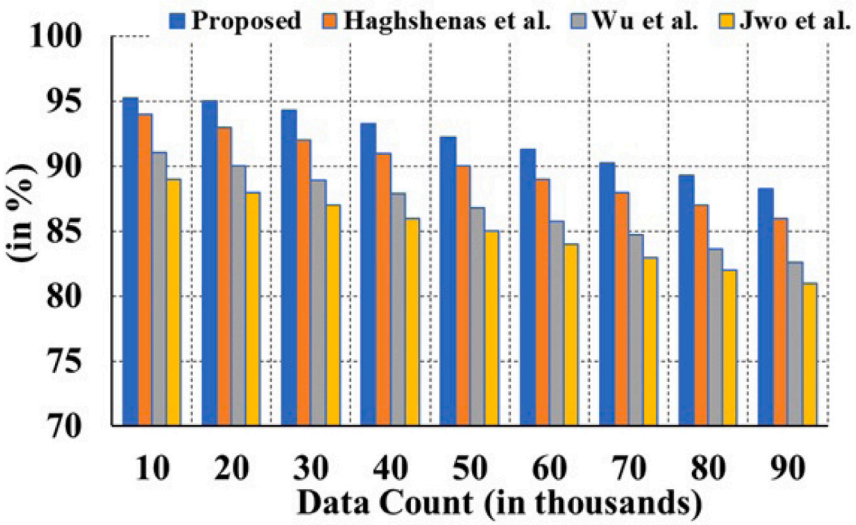


Fig. 9. Reliability analysis.

– **Hardware Utilization:** The model is optimized for execution on energy-efficient hardware platforms. By aligning software design with hardware capabilities, the model achieves significant reductions in energy usage during data processing tasks.

These technical strategies ensure that the proposed model not only excels in predictive accuracy but also maintains a low energy footprint, making it suitable for deployment in resource-constrained environments.

4.5. Reliability analysis

The study assessed the effectiveness of an equipment health monitoring model in manufacturing by making minor adjustments to its architecture while retaining the core concept. Fig. 9 presents the comprehensive results of the Reliability (fault tolerance) analysis. A subset of the dataset, composed of synthetically generated data, was utilized to evaluate the fault tolerance of advanced prediction models such as Haghshenas et al. (2023), Wu et al. (2021), and Jwo et al. (2022). The findings indicate that incorporating additional data instances improved fault tolerance. The proposed decision-making model demonstrated superior performance, achieving an average fault tolerance of 95.24%, surpassing Haghshenas et al. (2023), Wu et al. (2021), and Jwo et al. (2022), which showed fault tolerance estimates ranging from 89.51% to 92.92%. The fault tolerance (R) for each model is calculated using the formula:

$$R = 1 - \frac{\text{Number of Faults}}{\text{Total Operations}}$$

Additionally, the study highlighted the importance of model adaptability and scalability in handling large datasets, as well as the robustness of the proposed model in various operational conditions. These results emphasize that the proposed model not only outperforms state-of-the-art prediction algorithms but also provides enhanced reliability and efficiency in equipment health monitoring.

4.5.1. Robustness to noisy and missing data

While fault tolerance analysis validates the resilience of the proposed framework under operational failures, real-world manufacturing environments also introduce challenges such as noisy sensor measurements and missing data streams. To ensure robust anomaly detection and prediction, the proposed model integrates several mechanisms for data preprocessing and adaptive handling:

1. **Noise Filtering and Smoothing:** Sensor data is pre-processed using statistical smoothing techniques to eliminate transient spikes and measurement noise, ensuring that only stable signals are passed into the CNN-BiGRU pipeline.
2. **Anomaly-Aware Preprocessing:** Outlier detection methods, based on interquartile range (IQR) and Z-score thresholds, are applied to flag irregular sensor readings. Instead of discarding them outright, flagged values are cross-validated with temporal sensor history to differentiate between genuine anomalies and spurious noise.
3. **Data Imputation for Missing Streams:** Missing sensor values are addressed using temporal and spatial imputation methods. For short-term gaps, linear interpolation is used, while for longer gaps, model-driven imputation via autoencoders reconstructs missing values by exploiting correlations across multi-sensor data streams.
4. **Redundancy Through Multimodal Sensors:** The system leverages heterogeneous sensing units (IoT sensors, Node MCUs, EO/IR sensors) to provide redundancy. If one data stream is unavailable, correlated modalities supplement missing inputs to maintain decision accuracy.
5. **Adaptive Learning Integration:** The CNN-BiGRU architecture incorporates dropout regularization and robust training on corrupted datasets. This enhances its resilience to noisy or incomplete sensor inputs during real-world deployment.

These preprocessing and adaptive strategies ensure that the proposed model not only withstands hardware-level faults but also maintains reliable performance under imperfect sensing conditions. By combining filtering, imputation, redundancy, and robust learning, the framework achieves high stability and predictive accuracy, even in environments with inconsistent or degraded sensor data streams.

4.6. Stability assessment

Using Overall System Stability (OSS), the study evaluated the stability of the proposed model for monitoring equipment health in manufacturing across various datasets. OSS was calculated using the Mean Absolute Shift (MAS), where a value of 0 represents the least stable framework and 1 represents the most stable, based on a specific number of occurrences. The OSS values for the advanced decision-making models are illustrated in Fig. 10. The Mean Absolute Shift (MAS) is calculated using the formula:

$$MAS = \frac{1}{n}\sum_{i=1}^{n} |x_i - \bar{x}|$$

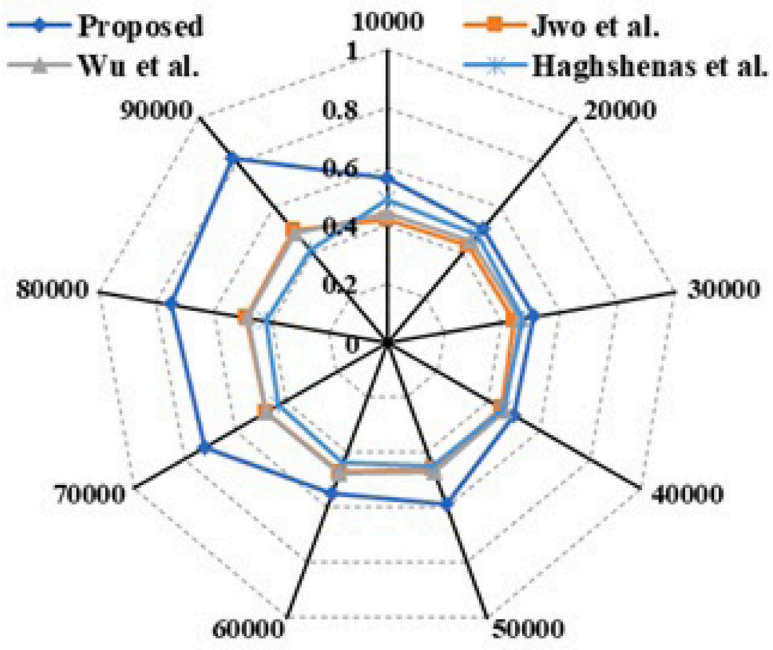


Fig. 10. Stability analysis.

where (x_i) represents individual measurements and $\bar{x}$ is the mean of the measurements. The analysis of datasets related to equipment health monitoring revealed that the proposed framework consistently outperformed existing approaches, achieving average MAS values between 0.71 and 0.79. Comparatively, Haghshenas et al. (2023) recorded a MAS value of 0.55, Wu et al. (2021) achieved a value of 0.49, and Jwo et al. (2022) reported a value of 0.41. These results demonstrate that the proposed method delivered significantly more stable and consistent outcomes in equipment health monitoring when applied to structured and coherent datasets.

4.7. Cost complexity estimation

Evaluating the computational and transactional costs is crucial for assessing the viability of an equipment health monitoring system in manufacturing. This analysis provides insights into the efficiency and feasibility of deploying the system in its intended environment. Table 2 highlights the complexity of the system's operations.

4.7.1. Computing cost ($\theta(p \log p)$)

It reflects the complexity involved in processing sensor data and making maintenance decisions.

- **Components:**
  - Data Collection: Gathering data from various sensors installed on manufacturing equipment.
  - Data Analysis: Cleaning, formatting, and analyzing data to detect anomalies or patterns indicating equipment health.
  - Event Determination: Identifying and categorizing maintenance events using predictive algorithms.

4.7.2. Transacting cost ($\theta((p-1)\log p)$)

It captures expenses related to executing maintenance transactions, including communication and coordination.

- **Components:**
  - Consensus and Coordination Fees: Costs associated with reaching agreement among stakeholders on maintenance actions.
  - Secure Data Transmission: Ensures data integrity and confidentiality through encryption, signatures, and keys during communication of maintenance alerts.

Table 2
Cost-estimation value.

Sr. no.	Type	Cost
1	Computing cost	θ(plogp)
2	Transacting cost	θ((p-1) logp)

4.7.3. Impact analysis

The computational and transactional costs have a significant impact on the system's efficiency in equipment health monitoring within manufacturing:

Computing cost

- **Processing Speed:** High computing costs can slow down data processing, affecting the system's ability to quickly analyze sensor data and make timely maintenance decisions.
- **Resource Utilization:** Efficient algorithms and data handling can reduce computing costs, leading to better utilization of computational resources and faster response times.

Transacting cost

- **Communication Delays:** High transactional costs can lead to delays in transmitting maintenance alerts and coordinating actions, impacting the system's responsiveness.
- **Scalability:** As the number of transactions increases, efficiently managing these costs becomes crucial for scaling the system without degrading performance.

Overall effects

- **Operational Efficiency:** Lower costs enhance the system's ability to operate smoothly, ensuring quick detection and response to equipment health issues.

Table 3
Ablation study results for SSL and FL.

Configuration	Accuracy (%)	F1-score	Privacy level
Baseline (CNN-BiGRU)	87.4	0.83	Low
+ SSL	91.2	0.87	Low
+ FL	89.8	0.85	High
+ SSL + FL	93.6	0.90	High

- **Cost-Effectiveness:** Reducing unnecessary expenses allows for more efficient allocation of resources, improving the economic viability of the system.
- **Reliability:** Efficient handling of computational and transactional processes contributes to the system's reliability, ensuring consistent performance and accurate monitoring.

By optimizing both computational and transactional costs, the system can achieve better efficiency, leading to improved equipment health monitoring and maintenance outcomes.

4.8. Ablation study analysis

To evaluate the contribution of individual components in the proposed hybrid CNN-BiGRU framework, ablation studies were conducted with a specific focus on **SSL** and **FL**. These experiments assess how each element impacts model accuracy, generalization, and privacy preservation in equipment health monitoring.

4.8.1. Effect of self-supervised learning (SSL)

The role of SSL was examined by comparing two experimental configurations:

1. **Baseline Model:** CNN-BiGRU trained only on labeled data.
2. **SSL-Enhanced Model:** CNN-BiGRU pretrained on unlabeled data using SSL pretext tasks, followed by supervised fine-tuning.

Results indicate that SSL substantially improves the model's feature extraction ability by leveraging unlabeled datasets. This enhancement reduces the dependency on large annotated datasets and improves anomaly detection accuracy, particularly in scenarios with limited labeled data.

4.8.2. Effect of federated learning (FL)

The impact of FL was studied by comparing:

1. **Centralized Model:** CNN-BiGRU trained on aggregated global datasets.
2. **Federated Model:** CNN-BiGRU trained locally on decentralized devices, where only model parameters are shared for aggregation.

FL preserves sensitive operational data by ensuring that raw inputs remain on local devices. Experimental results confirm that FL achieves accuracy comparable to centralized training while providing high privacy guarantees.

4.8.3. Combined SSL and FL

When both SSL and FL are integrated, the hybrid CNN-BiGRU framework demonstrates:

- Improved anomaly detection accuracy due to SSL-pretrained feature representations.
- Strong privacy preservation through FL's decentralized training paradigm.
- Robustness against heterogeneous and imbalanced datasets across distributed industrial environments.

Table 3 summarizes the experimental findings, highlighting the performance impact of SSL and FL.

The ablation studies confirm that SSL enhances feature generalization under data-scarce conditions, while FL ensures privacy preservation and robustness in decentralized environments. Their integration yields the best trade-off between performance and security, validating the design of the proposed hybrid model.

4.9. Discussions

The proposed model highlights the significant impact of digital twin technology in smart manufacturing, emphasizing its role in enhancing real-time equipment health monitoring. By integrating blockchain and IoT, the proposed framework offers a secure and efficient analysis of production trends, facilitating better anomaly detection and fault diagnostics. The use of a dual-directional convolutional neural network enhances real-time vulnerability detection and decision-making processes. Experimental results demonstrate the framework's effectiveness, showing improvements in delay efficiency, prediction accuracy, energy usage, model reliability, and stability. These advancements suggest promising applications across various industries, potentially leading to increased operational efficiency and reduced costs. Some of the important aspects are discussed ahead.

1. The model detects conditional vulnerabilities using digital twin technology for real-time monitoring, capturing continuous operational and environmental data. It employs blockchain for secure, immutable data handling and IoT devices for extensive data collection. A dual-directional convolutional neural network enhances pattern recognition, enabling rapid anomaly detection and real-time vulnerability assessment. This framework provides predictive insights and adaptive learning, ensuring precise and effective detection of vulnerabilities in manufacturing processes.
2. To adapt the anomaly detection framework using digital twin technology to different industries, major aspects need to be focused including:

   (a) **Industry-Specific Data Integration**

   - **Customization of Data Sources:** Integrate relevant industry-specific data, such as sensors and operational metrics, to ensure accurate monitoring and analysis.

   (b) **Tailored Algorithms and Models**

   - **Algorithm Adjustment:** Modify algorithms to address unique industry characteristics, ensuring effective anomaly detection and diagnostics.

   (c) **Regulatory and Compliance Considerations**

   - **Compliance with Regulations:** Adapt the framework to meet industry-specific regulations and compliance requirements, particularly regarding data security and privacy.

   (d) **Integration with Existing Systems**

   - **System Compatibility:** Ensure seamless integration with existing industry systems, such as ERP or MES, to enhance operational efficiency.

   By focusing on these aspects, the framework can be effectively customized to suit various industries, improving its applicability and performance.
3. The framework's sensitivity to hyperparameters, such as temporal window size, the number of BiGRU cells, and optimization parameters, is crucial for its generalization across industrial environments. Currently, these hyperparameters are empirically selected for specific datasets and environments.

(a) Future work can enhance robustness by employing automated hyperparameter optimization techniques like Bayesian optimization or grid search.
(b) Additionally, implementing adaptive mechanisms for temporal window size could allow dynamic adjustments based on input data characteristics.
(c) Cross-environment validation with diverse industrial datasets will further ensure the framework's generalization.

These strategies aim to reduce hyperparameter sensitivity and enhance scalability and reliability.

5. Conclusion

This research introduces a digital twin system designed to rapidly collect and analyze data using deep learning and Internet of Things (IoT) technologies, aimed at identifying conditional vulnerabilities in the industrial sector. The proposed solution addresses key challenges in smart manufacturing, including data security, sequential data processing, latency, and demand-driven immediacy. A comprehensive analysis of time and cost complexity demonstrates the method's effectiveness in detecting anomalies related to conditional vulnerability identification. The system achieves strong performance metrics in terms of Delay Efficiency (5.21 ms), Prediction Performance (Accuracy (92.25%), Sensitivity (93.25%), (Specificity (94.25%)), F-Measure (95.15%)), Energy Efficacy Analysis (1.18mJ), Model Reliability (95.24%), and Stability Analysis (79%). Additionally, the data processing cost is represented by $\theta((p-1)\log p)$, highlighting the method's efficiency. The study provides significant insights for academics by outlining a digital twin architecture optimized for smart manufacturing using advanced technologies. The proposed approach could also be applied to other fields, aiming to enhance detection efficiency and mitigate associated risks.

CRediT authorship contribution statement

Tariq Ahamed Ahanger: Writing – original draft. **Munish Bhatia:** Formal analysis, Conceptualization. **Abdulrahman Alabduljabbar:** Investigation. **Abdullah Albanyan:** Resources.

Ethical approval

Ethical approval was not required for the research.

Funding

The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through project number PSAU/2025/01/1446.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the author(s) used Monica.AI in order to improve English Quality and Grammarly to correct grammatical mistakes. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

References

Akash, Sadman Sakib, Ferdous, Md Sadek, 2022. A blockchain based system for healthcare digital twin. IEEE Access 10, 50523–50547.
Amofa, Sandro, Xia, Qi, Xia, Hu, Obiri, Isaac Amankona, Adjei-Arthur, Bonsu, Yang, Jingcong, Gao, Jianbin, 2024. Blockchain-secure patient digital twin in healthcare using smart contracts. PLoS One 19 (2), e0286120.
Ayvaz, Serkan, Alpay, Koray, 2021. Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time. Expert Syst. Appl. 173, 114598.
Bariah, Lina, Debbah, Merouane, 2024. The interplay of ai and digital twin: Bridging the gap between data-driven and model-driven approaches. IEEE Wirel. Commun. 31 (3), 219–225.
Borowski, Piotr F., 2021. Digitization, digital twins, blockchain, and industry 4.0 as elements of management process in enterprises in the energy sector. Energies 14 (7), 1885.
Chen, Wei, 2020. Intelligent manufacturing production line data monitoring system for industrial internet of things. Comput. Commun. 151, 31–41.
Guo, Shuxiang, Cao, Sheng, Guo, Jian, 2021. Study on decentralization of spherical amphibious multi-robot control system based on smart contract and blockchain. J. Bionic Eng. 18 (6), 1317–1330.
Haghshenas, Amirashkan, Hasan, Agus, Osen, Ottar, Mikalsen, Egil Tennfjord, 2023. Predictive digital twin for offshore wind farms. Energy Inform. 6 (1), 1.
Huang, Jintang, Huang, Sihan, Moghaddam, Shokraneh K, Lu, Yuqian, Wang, Guoxin, Yan, Yan, Shi, Xuejiang, 2024. Deep reinforcement learning-based dynamic reconfiguration planning for digital twin-driven smart manufacturing systems with reconfigurable machine tools. IEEE Trans. Ind. Inform..
Ihekoronye, Vivian Ukamaka, Nwakanma, Cosmas Ifeanyi, Anyanwu, Goodness Oluchi, Kim, Dong-Seong, Lee, Jae-Min, 2021. Benefits, challenges and practical concerns of iot for smart manufacturing. In: 2021 International Conference on Information and Communication Technology Convergence. ICTC, IEEE, pp. 827–830.
Jagtap, Sandeep, Garcia-Garcia, Guillermo, Rahimifard, Shahin, 2021. Optimisation of the resource efficiency of food manufacturing via the internet of things. Comput. Ind. 127, 103397.
Jwo, Jung-Sing, Hsieh, Han-Yi, Lee, Cheng-Hsiung, Lin, Ching-Sheng, Wang, Po-Wen, Hong, Chen-Yu, King, Jen-Kai, Hsu, Hao-Chien, 2022. Simulation and modeling of a data twin service for the autoclave curing process. IEEE Access 10, 111879–111887.
Khan, Abdullah Ayub, Laghari, Asif Ali, Rashid, Mamoon, Li, Hang, Javed, Abdul Rehman, Gadekallu, Thippa Reddy, 2023. Artificial intelligence and blockchain technology for secure smart grid and power distribution automation: A state-of-the-art review. Sustain. Energy Technol. Assess. 57, 103282.
Khang, Alex, Rath, Kali Charan, Satapathy, Suresh Kumar, Kumar, Amaresh, Das, Sudhansu Ranjan, Panda, Manas Ranjan, 2023. Enabling the future of manufacturing: integration of robotics and IoT to smart factory infrastructure in industry 4.0. In: Handbook of Research on AI-Based Technologies and Applications in the Era of the Metaverse. IGI Global, pp. 25–50.
Leng, Jiewu, Zhou, Man, Xiao, Yuxuan, Zhang, Hu, Liu, Qiang, Shen, Weiming, Su, Qianyi, Li, Longzhang, 2021. Digital twins-based remote semi-physical commissioning of flow-type smart manufacturing systems. J. Clean. Prod. 306, 127278.
Li, Xiang, Yu, Shupeng, Lei, Yaguo, Li, Naipeng, Yang, Bin, 2024. Dynamic vision-based machinery fault diagnosis with cross-modality feature alignment. IEEE/CAA J. Autom. Sin. 11 (10), 2068–2081.
Liu, Yuehua, Yu, Wenjin, Rahayu, Wenny, Dillon, Tharam, 2023. An evaluative study on IoT ecosystem for smart predictive maintenance (IoT-SPM) in manufacturing: Multiview requirements and data quality. IEEE Internet Things J. 10 (13), 11160–11184.
Pallisco, Aldo Anthony, 2023. Additive Manufacturing in the Automotive Industry: Framework for Product & Service Life-Cycle Management (Ph.D. thesis). Wayne State University.
Peng, Zhenlong, Han, Aowei, Wang, Chenlin, Jin, Hongru, Zhang, Xiangyu, 2024. Ultrasonic vibration cutting of advanced aerospace materials: a critical review of in-service functional performance. J. Intell. Manuf. Spec. Equip. 5 (1), 137–169.
Rahim, Messaoud, Lalouani, Wassila, Toubal, Elbahi, Emokpae, Lloyd, 2024. A digital twin-based platform for medical cyber-physical systems. IEEE Access.
Rath, Kali Charan, Khang, Alex, Roy, Debanik, 2024. The role of internet of things (IoT) technology in industry 4.0 economy. In: Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy. CRC Press, pp. 1–28.
Ren, Zijie, Wan, Jiafu, Deng, Pan, 2022. Machine-learning-driven digital twin for lifecycle management of complex equipment. IEEE Trans. Emerg. Top. Comput. 10 (1), 9–22.
Roumeliotis, Christos, Dasygenis, Minas, Lazaridis, Vasilis, Dossis, Michael, 2024. Blockchain and digital twins in smart industry 4.0: The use case of supply chain-a review of integration techniques and applications. Designs 8 (6), 105.

Sayed, Amged, Alshathri, Samah, Hemdan, Ezz El-Din, 2024. Conditional generative adversarial networks with optimized machine learning for fault detection of triplex pump in industrial digital twin. Processes 12 (11), 2357.

Shekari, Saeed, Ray, Sourav, 2024. Monitoring technologies in industrial systems. J. Mark. Res. 00222437241282308.

Singh, R Raja, Bhatti, Ghanishtha, Kalel, Dattatraya, Vairavasundaram, Indragandhi, Alsaif, Faisal, 2023. Building a digital twin powered intelligent predictive maintenance system for industrial AC machines. Machines 11 (8), 796.

Son, Seunghwan, Kwon, Deokkyu, Lee, Joonyoung, Yu, Sungjin, Jho, Nam-Su, Park, Youngho, 2022. On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain. IEEE Access 10, 75365–75375.

Soori, Mohsen, Arezoo, Behrooz, Dastres, Roza, 2023. Internet of things for smart factories in industry 4.0, a review. Internet Things Cyber-Physical Syst. 3, 192–204.

Suhail, Sabah, Hussain, Rasheed, Jurdak, Raja, Hong, Choong Seon, 2021. Trustworthy digital twins in the industrial internet of things with blockchain. IEEE Internet Comput. 26 (3), 58–67.

Thakur, Garima, Kumar, Pankaj, Jangirala, Srinivas, Das, Ashok Kumar, Park, Youngho, et al., 2023. An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment. IEEE Access 11, 26877–26892.

Thamotharan, Padmapritha, Srinivasan, Seshadhri, Kesavadev, Jothydev, Krishnan, Gopika, Mohan, Viswanathan, Seshadhri, Subathra, Bekiroglu, Korkut, Toffanin, Chiara, 2023. Human digital twin for personalized elderly type 2 diabetes management. J. Clin. Med. 12 (6), 2094.

Wu, Chunlong, Zhou, Youcheng, Pessôa, Marcus Vinicius Pereia, Peng, Qingjin, Tan, Runhua, 2021. Conceptual digital twin modeling based on an integrated five-dimensional framework and TRIZ function model. J. Manuf. Syst. 58, 79–93.

Xu, Wenjun, Cui, Jia, Li, Lan, Yao, Bitao, Tian, Sisi, Zhou, Zude, 2021. Digital twin-based industrial cloud robotics: Framework, control approach and implementation. J. Manuf. Syst. 58, 196–209.

Yang, Hanbo, Sun, Zheng, Jiang, Gedong, Zhao, Fei, Lu, Xufeng, Mei, Xuesong, 2020. Cloud-manufacturing-based condition monitoring platform with 5G and standard information model. IEEE Internet Things J. 8 (8), 6940–6948.

Yu, Wenjin, Liu, Yuehua, Dillon, Tharam, Rahayu, Wenny, Mostafa, Fahed, 2021. An integrated framework for health state monitoring in a smart factory employing IoT and big data techniques. IEEE Internet Things J. 9 (3), 2443–2454.