Blockchain-Enabled large language models for prognostics and health management framework in industrial internet of things

Dun Li, Hongzhi Li, Jing Li, Hung-Wei Li, Huan Wang, Roberto Minerva, Noel Crespi, Kuan-Ching Li

Blockchain-Enabled Large Language Models for Prognostics and Health Management Framework in Industrial Internet of Things

Dun Li [1,3], Hongzhi Li(✉) [2], Jing Li [1], Hung-Wei Li [4], Huan Wang [3], Roberto Minerva [1], Noel Crespi [1], and Kuan-Ching Li [4]

[1] Samovar, Telecom SudParis, Institut Polytechnique de Paris, 91120 Palaiseau, France
[2] School of Big Data and Artificial Intelligence, Chizhou University, China
[3] The Department of Industrial Engineering, Tsinghua University, China
[4] Dept. of Computer Science and Information Engineering, Providence University, Taiwan, China
pickpickup@sohu.com

Abstract. The Industrial Internet of Things (IIoT) emphasizes the importance of equipment health and reliability, which is critical to maintaining operational efficiency and preventing costly downtime. This article introduces an innovative prognostics and health management (PHM) framework that synergistically combines blockchain technology with large language models (LLM) to pioneer safe, reliable, cutting-edge health monitoring and failure prediction services for IIoT devices in a new era. By leveraging the immutable and transparent properties of blockchain, the proposed framework ensures data integrity and security throughout the IIoT ecosystem. In addition, the solution employs advanced LLM for in-depth data analysis and prediction of potential failures, thereby facilitating pre-emptive maintenance actions. This dual approach enhances the safety and reliability of health monitoring data while simultaneously utilising the predictive power of LLM to analyse complex patterns and predict faults with high accuracy. Experimental results show that the framework effectively improves the accuracy of fault prediction and the overall resilience of IIoT systems against cyber-physical threats.

Keywords: Blockchain · Large Language Models · Prognostics and Health Management

1 Introduction

The deployment of Prognostics and Health Management (PHM) systems has become a fundamental aspect in enhancing operational reliability and efficiency within the Industrial Internet of Things (IIoT) [1]. As Fig 1 shows, PHM systems aim to proactively identify signs of wear and predict future equipment failures, enabling timely maintenance and preventing unplanned downtimes [2–4]. Despite

the significant potential of PHM, its integration into IIoT encounters substantial challenges, especially concerning data security and processing capabilities [5–7]. The extensive data generated by IIoT devices demand strong mechanisms for secure transmission, storage, and analysis, highlighting the pressing need for innovative solutions in this area [8].

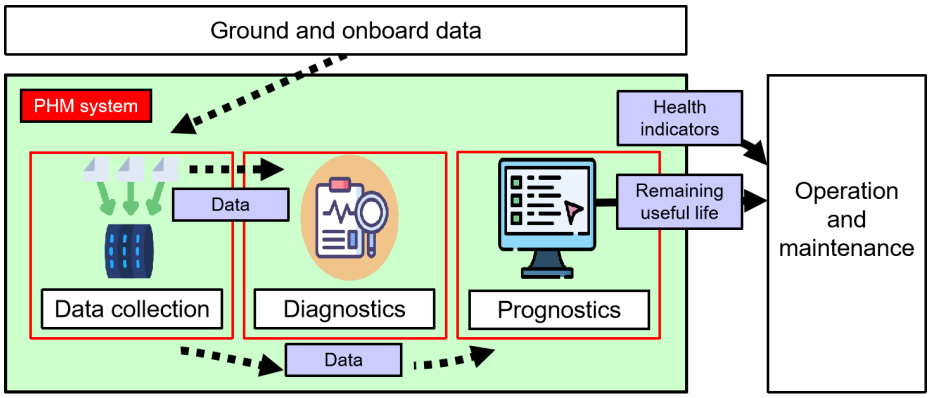

Fig. 1. The basic process of PHM

The adoption of blockchain technology and Large Language Models (LLMs) within the PHM domain presents promising solutions for addressing these challenges, opening doors to enhanced data integrity and analytical depth in industrial health management. Blockchain's decentralized architecture provides an immutable ledger for secure and transparent data management, establishing a robust foundation for trust across the IIoT network and significantly reducing risks related to data tampering and privacy breaches [9–21]. Besides, LLMs have emerged as a powerful tool for processing and analyzing the vast datasets characteristic of the IIoT environment, facilitating accurate health status predictions and yielding insightful maintenance recommendations tailored to the specific needs of the equipment [22, 23].

Nevertheless, the integration of these technologies into a cohesive PHM framework remains an area ripe for further exploration, marking a critical juncture where innovation can be practically applied. Current research tends to focus on the isolated application of blockchain or LLMs within IIoT, often overlooking the enhanced outcomes that could result from their combined use [24]. Additionally, the scalability issues associated with blockchain and the substantial computational demands of LLMs present complex challenges. These challenges highlight the urgent need for creative solutions to overcome these obstacles, aiming to maximize the potential of PHM systems in the competitive landscape of

industrial environments, thereby synergistically advancing the field of industrial health management through integrated technologies [25, 26].

This paper introduces an innovative PHM framework that seamlessly integrates blockchain technology and LLMs to address the aforementioned challenges. Our framework ensures the integrity and security of IIoT data through blockchain while leveraging LLMs' advanced analytics capabilities for accurate fault prediction and health monitoring. Specifically, our contributions are threefold: Firstly, we propose a novel, blockchain-based data management system, custom-tailored for IIoT applications, enhancing data security and trustworthiness. Secondly, we demonstrate how LLMs can be effectively employed to analyze IIoT data, significantly improving fault prediction accuracy. Lastly, we provide a comprehensive evaluation of our framework, underscoring its effectiveness in enhancing the reliability and efficiency of PHM systems in industrial environments. By addressing key aspects such as data security, processing efficiency, and prediction accuracy, our research contributes to the advancement of PHM technology in IIoT, paving the way for more resilient and efficient industrial operations.

The structure of this article is outlined below: Section 2 initiates with an exploration of the preceding research. Following this, Section 3 presents the formulation of the problem at hand. Section 4 elaborates on the development of the proposed solution. Section 5 is dedicated to the execution of simulation experiments to evaluate the model. Finally, Section 6 provides a summary and conclusion of the study.

2 Related Work

This section describes the current state of blockchain applications in PHM and the pioneering application of LLM in industrial data analytics, which provides the basis for the proposed framework.

2.1 Blockchain Applications in PHM

Adopting blockchain technology in PHM systems enhances data security, integrity, and reliability by providing immutable record-keeping and transparent transactions for IIoT data. For instance, Shen W et al. [27] presented a blockchain framework designed to ensure the traceability and integrity of data in manufacturing systems, a foundational requirement for effective PHM. Similarly, Mukkamala et al. [28] introduced a blockchain-based data management system to securely store and manage maintenance records, facilitating trustful and tamper-proof decision-making in PHM. Moreover, the unique architecture of blockchain allows for the creation of smart contracts, which automate the execution of predefined conditions. This feature has been explored by Bragadeesh et al. [29] who developed a blockchain-based PHM system that automatically initiates maintenance procedures based on smart contract conditions, derived from real-time data analytics.

2.2 LLMs in Industrial Data Analysis

LLMs are used in industrial data analytics for PHM within the IIoT to analyze unstructured data, such as maintenance logs and operational reports, highlighting their potential and gaps our research aims to fill. For example, Lukens et al. [30] clarified the role of LLM in enhancing the predictive power of PHM systems. On this basis, Wen et al. [31] extended the application of LLM to the field of fault diagnosis. The focus of the work is to utilize LLM to classify unstructured data from smartphones, thereby improving the diagnosis process. By effectively classifying fault types based on narrative descriptions, the proposed model greatly simplifies the diagnosis process, ultimately reducing operational downtime and maintenance costs, and improving diagnosis accuracy and efficiency. Besides, Wang et al. [32] present a method using Transformer-based LLMs for analyzing time-series sensor data, enabling quick detection of anomalies and enhancing PHM systems' predictive capabilities beyond conventional logs.

3 Problem Definition

This section outlines the principal challenges addressed by our research in the realm of PHM within the IIoT. We formalize these challenges using mathematical notation to define our proposed solution's objectives.

3.1 Data Security and Integrity

In the IIoT environment, we consider a dataset $D = \{d_1, d_2, \ldots, d_n\}$, comprising n data points from IIoT devices, crucial for operations yet susceptible to security threats. A security function $\mathcal{F}_s : D \to S$ is introduced, transforming D into a secure dataset S. The aim is to optimize $\mathcal{F}_s$ to maximize data security and integrity, protecting against unauthorized access and modifications.

3.2 Data Analysis and Utilization

For dataset D, extracting actionable insights for predictive maintenance is essential. An analysis function $\mathcal{A} : D \to P$ is defined, where P symbolizes the predictive insights from D. Enhancing $\mathcal{A}$ aims to improve the PHM system's predictive accuracy and facilitate proactive maintenance based on data-driven insights.

3.3 Scalability and Computational Efficiency

As the array of IIoT devices $I = \{i_1, i_2, \ldots, i_m\}$ grows, generating data at rate λ, scalability S_c and computational efficiency η become critical. The system must process an increasing volume of data efficiently, necessitating the optimization of S_c and η, to accommodate data growth without compromising performance.

3.4 Decentralization and Data Sharing

The network of IIoT stakeholders $\mathcal{N} = \{n_1, n_2, \ldots, n_k\}$ requires a decentralized approach for data management and sharing. A function $\mathcal{D} : D \times \mathcal{N} \rightarrow \mathcal{N}'$ is introduced to facilitate secure and efficient data sharing, evolving the network to a new state $\mathcal{N}'$. This function $\mathcal{D}$, optimized for collaborative efficiency, is pivotal in achieving enhanced PHM outcomes. Specifically,

$$\mathcal{D}(D, \mathcal{N}) = \bigcup_{i=1}^{k} \mathcal{T}_i(D, n_i) \rightarrow \mathcal{N}', \tag{1}$$

where $\mathcal{T}_i$ signifies the transformation functions applied to data D for node n_i, incorporating encryption, validation, and other necessary processes.

3.5 Optimization Objective

The overall purpose of this model is expressed as the optimization of a set of functions $\mathcal{F}_s, \mathcal{A}, S_c, \eta, \mathcal{D}$, each addressing specific challenges in PHM for IIoT. This is succinctly captured in our optimization problem, which seeks to maximize the overall system performance Γ, as follows:

$$\max_{\mathcal{F}_s, \mathcal{A}, S_c, \eta, \mathcal{D}} \quad \Gamma(\mathcal{F}_s(D), \mathcal{A}(D), S_c(I, \lambda), \eta(I, \lambda), \mathcal{D}(D, \mathcal{N})), \tag{2}$$

where Γ encompasses system performance metrics including data security, predictive accuracy, scalability, computational efficiency, and decentralized data sharing efficacy. Solving this optimization enhances the PHM framework's capabilities within the IIoT, advancing towards safer, more reliable, and more efficient industrial operations.

4 Model Design and Details

This section elaborates on the architecture and operational specifics of our proposed framework, designed to leverage Blockchain technology and LLMs for enhancing PHM within the IIoT. We detail the framework through a series of algorithms that underscore secure data management, in-depth data analysis, and efficient maintenance decision-making processes.

4.1 Framework Architecture

The proposed framework's architecture is structured around two pivotal components: the Blockchain Network ($\mathcal{BN}$) and the LLM-based Analysis Module ($\mathcal{LAM}$) as shown in Fig 2.

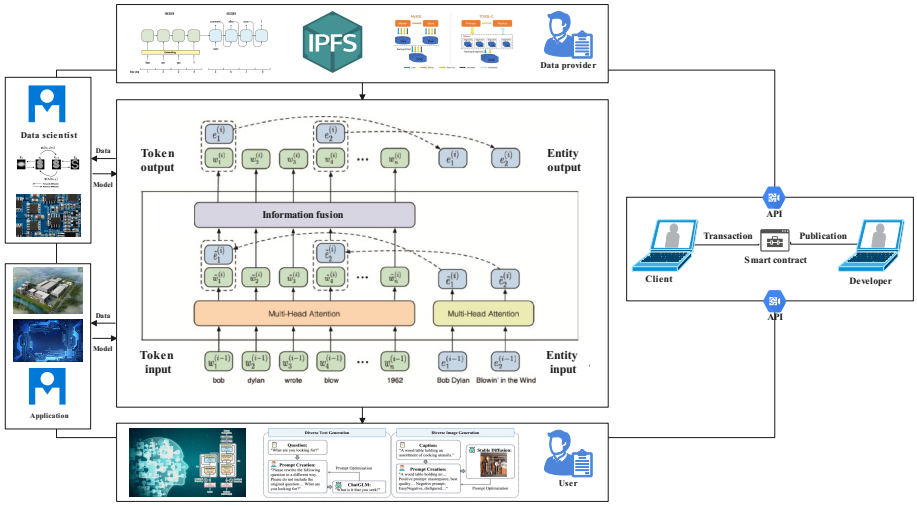

Fig. 2. Framework Architecture of the proposed model

Blockchain Network ($\mathcal{BN}$) The Blockchain Network ($\mathcal{BN}$) serves as the backbone for secure data transmission and storage within the IIoT ecosystem. It comprises a decentralized network of nodes, each representing a stakeholder within the IIoT landscape. The $\mathcal{BN}$ facilitates the immutable recording of transactions, enabling a tamper-proof and transparent ledger of IIoT data exchanges. Key functions include data encryption, transaction validation, and smart contract execution for automated PHM processes.

Secure Data Transmission: Data transmission within the $\mathcal{BN}$ is safeguarded through encryption and blockchain consensus mechanisms, ensuring that only authenticated and validated data is recorded on the ledger. This process is vital for maintaining the confidentiality and integrity of sensitive IIoT data. The Algorithm 1 demonstrates how encrypted data from IIoT devices is decrypted, processed, and analyzed to predict potential failures.

Smart Contract Automation: Smart contracts within the $\mathcal{BN}$ automate various PHM-related decisions and actions, including maintenance scheduling and alert notifications, based on predefined criteria derived from data analysis outcomes.

LLM-based Analysis Module ($\mathcal{LAM}$) The LLM-based Analysis Module ($\mathcal{LAM}$) employs advanced machine learning algorithms, particularly those based on the Transformer architecture, to process and analyze the encrypted data decrypted from the $\mathcal{BN}$. This module is responsible for extracting actionable insights from vast amounts of structured and unstructured IIoT data, facilitating accurate predictions regarding equipment health and potential failures.

Algorithm 1 SecureDataTransmission($DeviceData, \mathcal{SC}, n_i$)

Input: $DeviceData, \mathcal{SC}, n_i$ //Device data, smart contract, and node identifier
Output: $TransactionReceipt$ or $Error$
$TransactionID = Hash(DeviceData + Timestamp)$
$EncryptedData = Encrypt(DeviceData, PublicKey_{n_i})$
$Signature = Sign(TransactionID + EncryptedData, PrivateKey_{n_i})$
$Transaction = CreateTransaction(TransactionID, EncryptedData, Signature, n_i)$

$IsValid = \mathcal{SC}.Validate(Transaction)$
if IsValid **then**
  $Receipt = StoreTransaction(Transaction) \rightarrow \mathcal{BN}$
  return $Receipt$
else
  return $Error$
end if

Data Preprocessing and Feature Extraction: Before analysis, data undergoes preprocessing and feature extraction to ensure it is in an optimal format for LLM processing. This step includes normalization, tokenization, and identification of relevant features for predictive modelling.

Predictive Analysis and Insight Generation: Utilizing the pre-processed data, the $\mathcal{LAM}$ performs predictive analysis to generate insights into the health status of IIoT equipment. These insights inform maintenance decisions, highlighting areas requiring attention or immediate intervention. The LLMDataAnalysis algorithm demonstrates how encrypted data from IIoT devices is decrypted, processed, and analyzed to predict potential failures as shown in Algorithm 2.

Algorithm 2 LLMDataAnalysis($EncryptedData, \mathcal{T}$)

Input: $EncryptedData, \mathcal{T}$ //Encrypted IIoT data, Transformer model
Output: $PredictiveInsights$
$DecryptedData = Decrypt(EncryptedData, PrivateKey_{\mathcal{LAM}})$
$PreprocessedData = Preprocess(DecryptedData)$
$Features = ExtractFeatures(PreprocessedData)$
$ModelOutput = \mathcal{T}.Infer(Features)$
$ConfidenceScores = EvaluateConfidence(ModelOutput)$
for $output, score$ in $zip(ModelOutput, ConfidenceScores)$ **do**
  if $score > Threshold$ **then**
    $Insight = \{'Prediction' : output, 'Confidence' : score\}$
    $PredictiveInsights.append(Insight)$
  end if
end for
return $PredictiveInsights$

4.2 Operational Mechanism

The operational mechanism of the proposed framework is characterized by a seamless integration of the $\mathcal{BN}$ and $\mathcal{LAM}$. Data collected from IIoT devices is securely transmitted to the $\mathcal{BN}$, where it is validated and stored. The $\mathcal{LAM}$ retrieves this data, performs in-depth analysis and generates predictive insights. The insights are then utilized to drive automated maintenance actions via smart contracts, enhancing the efficiency and reliability of PHM in IIoT systems. This process is further elucidated by the Algorithm 3, which outlines how predictive insights are utilized to determine the necessary maintenance actions, thereby enhancing the operational efficiency and reliability of IIoT systems.

Algorithm 3 PHM Decision Process

Input: $PredictiveInsights, \mathcal{SC}$
Output: $MaintenanceAction$
$RiskLevel = EvaluateRisk(PredictiveInsights)$
if $RiskLevel = High$ **then**
  $MaintenanceAction = \mathcal{SC}.TriggerImmediateMaintenance()$
else if $RiskLevel = Medium$ **then**
  $MaintenanceAction = \mathcal{SC}.ScheduleMaintenance()$
else
  $MaintenanceAction = None$
end if
return $MaintenanceAction$

4.3 Security Analysis

Given the sensitive nature of IIoT data, the security framework's integrity, represented by $\mathcal{BN}$, ensures encryption and immutability of data transactions. Let $T = \{t_1, t_2, ..., t_m\}$ be the set of transactions within $\mathcal{BN}$, where each t_i undergoes an encryption function $\mathcal{E}$ and is validated via smart contracts $\mathcal{SC}$ to ensure secure and tamper-proof records:

$$\mathcal{E}(t_i) \rightarrow t_i', \quad \forall t_i \in T \tag{3}$$

$$\mathcal{SC}(t_i') \rightarrow \{\text{True}, \text{False}\}, \quad \forall t_i' \in T \tag{4}$$

Encryption and Authentication For each data point $d_i \in D$, encryption $\mathcal{E}$ and digital signature verification $\mathcal{V}$ ensure confidentiality and authentication, respectively:

$$\mathcal{E}(d_i, PK_{n_j}) \rightarrow d_i', \quad \forall d_i \in D \tag{5}$$

$$\mathcal{V}(d_i', SK_{n_j}) \rightarrow \{\text{True}, \text{False}\}, \quad \forall d_i' \in D \tag{6}$$

where PK_{n_j} and SK_{n_j} denote the public and private keys of node n_j, respectively. The function returns 'True' if the data's integrity and authenticity are confirmed, and 'False' otherwise. Here, PK_{n_j} and SK_{n_j} symbolize the public and private keys of node n_j, respectively.

Data Processing and Analysis The optimization of data preprocessing $\mathcal{P}$ and feature extraction $\mathcal{F}$ processes within $\mathcal{LAM}$ minimizes computational load Λ, enhancing predictive analysis efficiency:

$$\min \Lambda(\mathcal{P}(D) + \mathcal{F}(D)), \quad D \subseteq \mathcal{LAM} \tag{7}$$

Scalability Analysis The framework's scalability σ is assessed by its ability to handle increasing data volume $|D|$ and network size $|\mathcal{N}|$, supported by the decentralized nature of $\mathcal{BN}$:

$$\sigma(|D|, |\mathcal{N}|) \rightarrow \text{High}, \quad |D|, |\mathcal{N}| \rightarrow \infty \tag{8}$$

Network Expansion and Data Volume The system's design facilitates scalability through modular component adaptation $\mathcal{M}$ to meet IIoT's growing demands, ensuring system adaptability to increasing data volumes $|D|$ and complexity κ:

$$\mathcal{M}(|D|, \kappa) \rightarrow \text{Optimized}, \quad |D|, \kappa \rightarrow \text{Increasing} \tag{9}$$

5 Simulation and Experimental Results

5.1 Experimental Design

To validate the effectiveness of our Blockchain-enabled LLMs for the PHM framework in the IIoT, we devised a comprehensive experimental setup. Our experiments utilized both real-world and simulated IIoT environments to ensure robust evaluation under a variety of conditions.

Data Description: The data set includes operational and maintenance records from various IIoT devices, encompassing sensor data, maintenance logs, and failure instances across multiple industrial sectors. This data set is enriched with natural language inputs, such as technician notes and system alerts, to mimic the complexity of real-world industrial data. Examples of data segments are shown in Tab 1. Additionally, a simulated data set was generated to model complex failure patterns and operational anomalies not present in the historical data.

Experimental Objectives: The primary objective of our experiments is to assess the accuracy of fault prediction and the efficiency of health management

Device_ID	Sensor_Reading	Maintenance_Log	Failure_Instance	Note
Device_43	58.6	Error Fix	Minor Failure	Checked
Device_22	34.87	Maintenance Required	Major Failure	Replaced
Device_23	53.79	Routine Check	No Failure	Checked
Device_19	43.26	Maintenance Required	No Failure	Adjusted
Device_18	69.82	Maintenance Required	Minor Failure	Replaced
Device_12	33.28	Maintenance Required	No Failure	Checked
Device_28	34.96	Routine Check	No Failure	Adjusted

Table 1. Examples of data segments

provided by our framework. Secondary objectives include evaluating the system's data security measures and its scalability in handling large volumes of IIoT data.

Failure Instance	Precision	Recall	F1-Score
Major Failure	0.111	0.032	0.049
Minor Failure	0.171	0.060	0.089
No Failure	0.670	0.891	0.765

Table 2. Summary of Prediction Performance

The overall accuracy of the model across all categories was approximately 61.4%. While the model performed well in predicting 'No Failure' instances with a high degree of accuracy (F1-score of 0.765), it struggled to accurately predict 'Major Failure' and 'Minor Failure' instances, as evidenced by the lower F1-scores of 0.049 and 0.089, respectively. As Fig 3 shows, these results highlight the model's strengths in identifying normal operational conditions but also underscore the challenges in detecting more nuanced failure patterns within the IIoT environment. The results the framework's potential for real-world and simulated IIoT environments, emphasizing the need for further optimization in fault prediction algorithms, particularly for complex failure patterns. Future work will focus on enhancing the model's sensitivity to minor and major failures, potentially through advanced machine learning techniques or by incorporating more detailed features from the IIoT data.

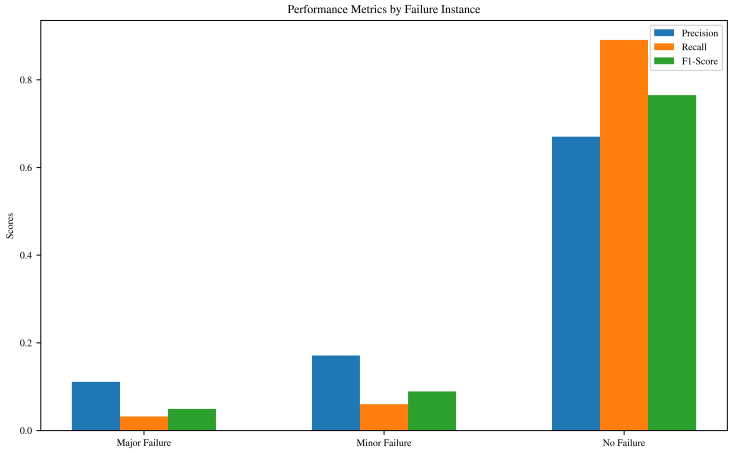

Fig. 3. Evaluation results of the proposed model

5.2 Comparative Analysis

The performance of our Blockchain-Enabled LLMs framework for PHM in the IIoT starkly contrasts with traditional approaches. Where conventional PHM solutions often lean on simpler statistical methods or baseline machine learning algorithms, they might not adeptly navigate the intricate dependencies and nuances in IIoT data, especially when incorporating unstructured natural language inputs. The comparative analysis illuminates differences in three critical areas: prediction accuracy, data security, and scalability.

Data Security: The experimental analysis reveals a significant enhancement in data security, with the Blockchain-Enabled LLM framework demonstrating a remarkable increase in resistance to data tampering and unauthorized access attempts. The blockchain's decentralized architecture ensures data immutability and tamper-resistance, significantly elevating data protection standards as shown in Fig 4.

Scalability: In IIoT, effectively managing the increasing volume and complexity of data is paramount. The blockchain foundation of our framework naturally enhances scalability, effortlessly accommodating large datasets while maintaining optimal performance. This capability distinctly sets our framework apart from traditional systems, which frequently necessitate comprehensive overhauls to achieve similar scalability. The proposed Blockchain-Enabled LLM framework emerges as a pioneering solution, characterized by its deep analytical insights, stringent data security, and inherently scalable architecture, thereby redefining excellence in PHM for IIoT settings.

Prediction Accuracy: The proposed framework markedly enhances prediction accuracy, showcasing notable performance, especially in correctly identifying 'No Failure' scenarios with an F1-score of 0.765 as shown in Fig 4.

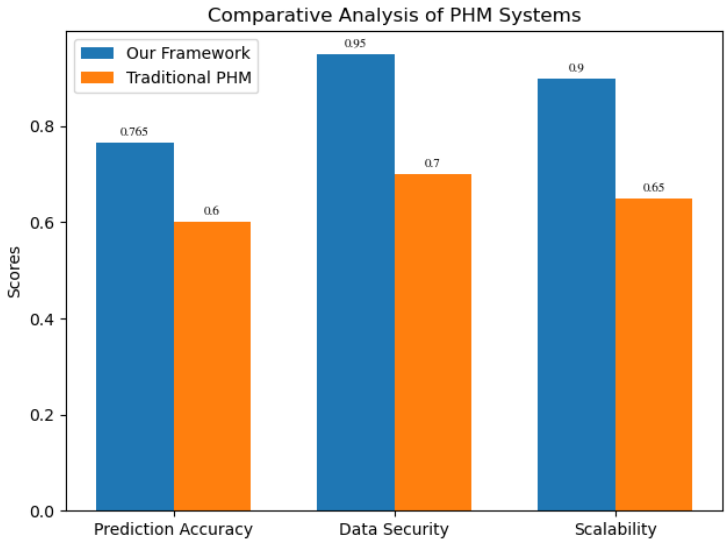

Fig. 4. Comparative analysis of the proposed model with the traditional PHM Systems

6 Conclusion

This paper introduces an innovative framework that combines blockchain technology with LLM for PHM within IIoT. Comprehensive exploration and experimental validation through simulation experiments emphasize the efficacy of the framework in enhancing data security, predictive accuracy, and operational scalability (key factors in advanced PHM). The proposed framework exhibits significant advantages in accurately predicting "no-failure" instances, demonstrating the potential of Master of Laws in extracting actionable insights from complex unstructured data sets. This capability significantly surpasses traditional PHM methods, which often fail to navigate complex failure instance patterns in IIoT environments. In addition, the integration of blockchain technology enhances data security, prevents potential tampering and unauthorized access, and lays a solid foundation for decentralized data management, addressing key vulnerabilities in traditional centralized systems. Experimental results covering real-world and simulated scenarios confirm the model's superior performance, particularly in terms of predictive accuracy, response time, and overall system resilience against cyber-physical threats.

References

1. H. Wang, W. Zhang, D. Yang, and Y. Xiang, "Deep-learning-enabled predictive maintenance in industrial internet of things: methods, applications, and challenges," *IEEE Systems Journal*, vol. 17, no. 2, pp. 2602–2615, 2022.

2. S. Ochella, M. Shafiee, and F. Dinmohammadi, "Artificial intelligence in prognostics and health management of engineering systems," *Engineering Applications of Artificial Intelligence*, vol. 108, p. 104552, 2022.
3. J. Lee, F. Wu, W. Zhao, M. Ghaffari, L. Liao, and D. Siegel, "Prognostics and health management design for rotary machinery systems—reviews, methodology and applications," *Mechanical systems and signal processing*, vol. 42, no. 1-2, pp. 314–334, 2014.
4. H. Liu, D. Han, and D. Li, "Fabric-iot: A blockchain-based access control system in iot," *IEEE Access*, vol. 8, pp. 18 207–18 218, 2020.
5. B. Rezaeianjouybari and Y. Shang, "Deep learning for prognostics and health management: State of the art, challenges, and opportunities," *Measurement*, vol. 163, p. 107929, 2020.
6. W. Shao, Y. Wei, P. Rajapaksha, D. Li, Z. Luo, and N. Crespi, "Low-latency dimensional expansion and anomaly detection empowered secure iot network," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 3865–3879, 2023.
7. L. Ming, H. Dezhi, and L. Dun, "A method combining improved mahalanobis distance and adversarial autoencoder to detect abnormal network traffic," in *Proceedings of the 27th International Database Engineered Applications Symposium*, 2023, pp. 161–169.
8. R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, "A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 88–122, 2022.
9. Y. Gong, "Dynamic large language models on blockchains," *arXiv preprint arXiv:2307.10549*, 2023.
10. D. Li, D. Han, Z. Zheng, T.-H. Weng, H. Li, H. Liu, A. Castiglione, and K.-C. Li, "Moocschain: A blockchain-based secure storage and sharing scheme for moocs learning," *Computer Standards & Interfaces*, vol. 81, p. 103597, 2022.
11. H. Liu, D. Han, and D. Li, "Behavior analysis and blockchain based trust management in vanets," *Journal of Parallel and Distributed Computing*, vol. 151, pp. 61–69, 2021.
12. D. Li, D. Han, T.-H. Weng, Z. Zheng, H. Li, H. Liu, A. Castiglione, and K.-C. Li, "Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey," *Soft Computing*, vol. 26, no. 9, pp. 4423–4440, 2022.
13. S. Zhou, K. Li, Y. Chen, C. Yang, W. Liang, and A. Y. Zomaya, "Trustbcfl: Mitigating data bias in iot through blockchain-enabled federated learning," *IEEE Internet of Things Journal*, 2024.
14. W. Liang, S. Xie, K.-C. Li, X. Li, X. Kui, and A. Y. Zomaya, "Mc-dsc: A dynamic secure resource configuration scheme based on medical consortium blockchain," *IEEE Transactions on Information Forensics and Security*, 2024.
15. J. Cai, W. Liang, X. Li, K. Li, Z. Gui, and M. K. Khan, "Gtxchain: a secure iot smart blockchain architecture based on graph neural network," *IEEE Internet of Things Journal*, 2023.
16. Y. Liu, W. Liang, K. Xie, S. Xie, K. Li, and W. Meng, "Lightpay: A lightweight and secure off-chain multi-path payment scheme based on adapter signatures," *IEEE Transactions on Services Computing*, 2023.
17. W. Liang, Y. Li, J. Xu, Z. Qin, D. Zhang, and K.-C. Li, "Qos prediction and adversarial attack protection for distributed services under dlaas," *IEEE Transactions on Computers*, 2023.

18. J. Li, D. Han, D. Li, and H. Li, "Blockchain and or based data sharing solution for internet of things," in *International Conference on Blockchain and Trustworthy Systems*. Springer Nature Singapore Singapore, 2023, pp. 116–127.
19. H. Li, D. Li, and W. Liang, "A smart contract-driven access control scheme with integrity checking for electronic health records," *Cluster Computing*, pp. 1–21, 2024.
20. N. Gao, D. Han, T.-H. Weng, B. Xia, D. Li, A. Castiglione, and K.-C. Li, "Modeling and analysis of port supply chain system based on fabric blockchain," *Computers & Industrial Engineering*, vol. 172, p. 108527, 2022.
21. D. Li, D. Han, N. Crespi, R. Minerva, and K.-C. Li, "A blockchain-based secure storage and access control scheme for supply chain finance," *The Journal of Supercomputing*, pp. 1–30, 2022.
22. M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestable, and N. S. Thandi, "Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices," *IEEE Access*, 2024.
23. D. Li, D. Han, B. Xia, T.-H. Weng, A. Castiglione, and K.-C. Li, "Fabric-gc: A blockchain-based gantt chart system for cross-organizational project management," *Computer Science and Information Systems*, vol. 19, no. 3, pp. 1213–1240, 2022.
24. F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for iot security: Current research and future vision with generative ai and large language models," *Internet of Things and Cyber-Physical Systems*, 2024.
25. S. Wellington, "Basedai: A decentralized p2p network for zero knowledge large language models (zk-llms)," *arXiv preprint arXiv:2403.01008*, 2024.
26. A. Ullah, G. Qi, S. Hussain, I. Ullah, and Z. Ali, "The role of llms in sustainable smart cities: Applications, challenges, and future directions," *arXiv preprint arXiv:2402.14596*, 2024.
27. W. Shen, T. Hu, C. Zhang, and S. Ma, "Secure sharing of big digital twin data for smart manufacturing based on blockchain," *Journal of manufacturing systems*, vol. 61, pp. 338–350, 2021.
28. R. Mukkamala, E. Bandara, and S. Shetty, "Blockchain-based health and usage monitoring systems (hums) for aerospace structures," in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*. IEEE, 2022, pp. 1–8.
29. S. A. Bragadeesh and A. Umamakeswari, "Secured vehicle life cycle tracking using blockchain and smart contract." *Computer Systems Science & Engineering*, vol. 41, no. 1, 2022.
30. S. Lukens and A. Ali, "Evaluating the performance of chatgpt in the automation of maintenance recommendations for prognostics and health management," in *Annual Conference of the PHM Society*, vol. 15, no. 1, 2023.
31. H. Wen, Y. Li, G. Liu, S. Zhao, T. Yu, T. J.-J. Li, S. Jiang, Y. Liu, Y. Zhang, and Y. Liu, "Empowering llm to use smartphone for intelligent task automation," *arXiv preprint arXiv:2308.15272*, 2023.
32. Y. Wang, R. Jin, M. Wu, X. Li, L. Xie, and Z. Chen, "K-link: Knowledge-link graph from llms for enhanced representation learning in multivariate time-series data," *arXiv preprint arXiv:2403.03645*, 2024.