# Sustainable Intelligent Public Facility Failure Management System Based on Large Language Models

Siguo Bi[a], Wei Ni[b], Xiangyang Long[a], Jilong Zhang[a,*]

[a]*Library, Fudan University, Shanghai, 200433, China*
[b]*Commonwealth Scientific and Industrial Research Organization, Sydney, 2122, Australia*

## Abstract

This paper presents the Large Language Model-based Smart Device Management framework, a pioneering approach designed to address the intricate challenges of managing intelligent devices within public facilities, with a particular emphasis on libraries. Our framework leverages state-of-the-art large language models to analyze and predict device failures, thereby enhancing operational efficiency and reliability. Through a prototype validation in real-world library settings, we have demonstrated the framework's practical applicability and its capacity to significantly reduce budgetary constraints on public facilities. The advanced and innovative nature of our model has been proven through its successful implementation in prototype testing. We plan to extend the framework's scope to include a wider array of public facilities and to integrate it with cutting-edge cybersecurity technologies, such as IoT security and machine learning algorithms for threat detection and response. This will result in a comprehensive and proactive maintenance system that not only bolsters the security of intelligent devices but also utilizes machine learning for automated analysis and real-time threat mitigation. By incorporating these advanced cybersecurity elements, our framework will be better positioned to tackle the dynamic challenges of modern public infrastructure, ensuring robust protection against potential threats and enabling facilities to anticipate and prevent failures, leading to substantial cost savings and enhanced service quality.

*Keywords:* Public Facility, Smart Devices, Large Language Models,

---

*Corresponding author
   Email address:* `jlzhfd@fudan.edu.cn` (Jilong Zhang)

## 1. Introduction

Large Language Models (LLMs) are gaining increasing prominence and importance in international applications. They have demonstrated the potential to enhance governance efficiency in government affairs and are showing strong application prospects in education, healthcare, finance, and industry, among other sectors[1, 2, 3, 4]. LLMs are pushing the boundaries of artificial intelligence by integrating multimodal data, exerting a profound impact on society[5]. With their robust capabilities in information integration, understanding, and production, these models are emerging as versatile personal information assistants, accelerating scientific discoveries, and fostering new forms of content creation in the creative industries[6]. Therefore, the application of LLMs across various fields is crucial for improving efficiency, fostering innovation, and strengthening services.

Amidst the ongoing trends of economic globalization and urbanization, urban development has shifted its focus towards sustainable growth, with public facilities such as libraries and museums playing a pivotal role[7, 8, 9]. In 2023, the Institute of Museum and Library Services (IMLS) allocated a substantial $266.4 million to projects aimed at enhancing the capabilities of museums, libraries, and associated institutions, underscoring the importance of research and optimization in the substantial investment in intelligent devices within these public facilities[10]. These investments not only elevate the operational efficiency of public facilities but are also crucial to the city's cultural capital and socio-economic development[11, 12, 13].

To maintain the high availability and efficiency of these public cultural facilities, substantial public expenditure is allocated to the procurement and deployment of smart devices to enhance management efficiency and user experience[14]. These advanced smart devices, such as smart self-service equipment, intelligent climate control devices, and smart security devices, have significantly improved the user experience[15]; see Figure 1. However, if not properly managed, the key risk performance indicators of these devices, such as reliability, could significantly threaten the sustainable development goals of urban cultural spaces[16]. Especially for devices at core central nodes and those frequently used, failure not only poses safety hazards but also weakens their public service functions and can severely impact user experience,
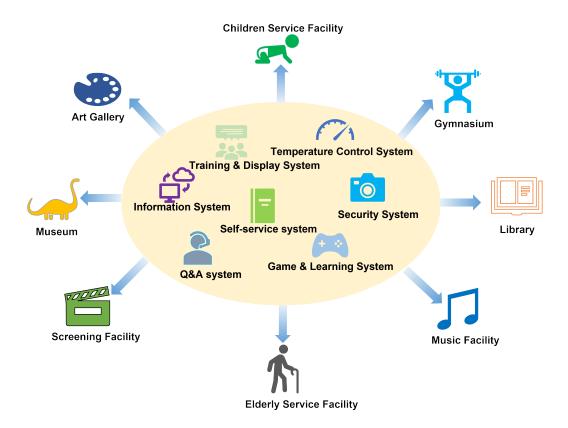
Figure 1: The typical public facilities where smart devices are widely used to provide various basic services.

increasing public fiscal budget expenditures[17]. Therefore, effectively identifying, analyzing, and predicting the failure risks of these devices is crucial for ensuring the sustainable development of cultural spaces[18].

Given the urgency of intelligent device management in cultural facilities, there is an immediate need for an efficient, intelligent, and convenient approach to integrated management. However, the data generated by various types of devices are heterogeneous and complex[19, 20], especially the large volumes of video or image data produced by security systems, along with a significant amount of audio data and textual information. Integrating these diverse and heterogeneous data sources for failure analysis and prevention poses a significant challenge[21]. The challenges lie in:

Firstly, the diversity and complexity of data make traditional data processing methods inadequate. Different types of data have varying formats,

structures, and semantics. How to effectively integrate video, audio, and textual data for subsequent analysis and decision-making is an issue that requires immediate resolution[20, 22]. Secondly, there is a high demand for real-time processing. The operation of cultural facilities requires real-time monitoring and analysis of device status to identify potential failures and take appropriate measures in a timely manner[21]. Additionally, data security and privacy protection are critical considerations. Especially when dealing with audio and video data that involve personal information, how to ensure effective analysis while maintaining data security to prevent data breaches and misuse is a challenge that managers must confront[20, 23]. Moreover, malfunctions in intelligent devices can cause disruptions to public services, severely degrading the user experience. This is especially critical in metro public facilities where operational efficiency and passenger satisfaction are paramount[23]. Failures in these systems not only impair service delivery but also undermine the trust and reliability of public service providers. Furthermore, the increasing diversification of specifications and parameters across multi-source devices has led to a complexity in identifying the causes of device failures and formulating effective countermeasures. This complexity poses a significant barrier to the integrated management of multi-source intelligent devices, as the intricate nature of these systems can lead to unforeseen interactions and challenges in maintaining seamless operation and service delivery[21].

Facing the serious challenges mentioned above, our contributions lie in:

- We leverage the efficient semantic recognition capabilities of large language models to meet the diverse intelligent device management needs of users effectively.

- Based on the multimodal data processing capabilities of large language models, we propose an integrated data fusion solution for heterogeneous data from multi-source devices, which efficiently complements each other to achieve fault identification.

- With the localized deployment of large language models, we have achieved data and model localization, fully ensuring the privacy and security of data.

- Faced with the increasing diversification of functions and parameters of multi-source intelligent devices, we have wisely proposed a local knowledge extraction based on intelligent device manuals, and provide users

4

with standardized and professional fault handling suggestions based on this localized expertise.

## 2. Literature Review

As Artificial Intelligence (AI) and machine learning technologies are becoming increasingly vital, an increasing number of IoT devices are being managed by various intelligent algorithms. In the domain of fault detection, several articles propose innovative solutions for identifying anomalies and potential failures within various systems. Ribeiro and Mack in [36] introduce a multi-vendor device management solution that automates event and fault file collection, which is pivotal for enhancing cybersecurity and NERC compliance among North American utilities, although it may struggle with the seamless integration of diverse vendor technologies. The private cloud-based platform discussed by West and Santitos García in [37] aims to bolster operational efficiency and grid reliability, potentially through advanced fault detection mechanisms, yet scalability with increasing data volumes remains a concern. Lee and Liu in [24] present a pluggable module for edge device management, which could encompass fault detection capabilities, although it may not be universally applicable to all edge devices. Liu et al. [38] predict power device fatigue failure with a novel approach, which can be seen as a form of fault detection, but it might not cover all failure modes. Enkhbaatar and Yamazaki [27] propose an automatic visual monitoring system for data centers, which is likely to include fault detection to reduce manual checks, but its effectiveness across all hardware anomalies is uncertain. Liu et al. [28] explore machine learning for substation equipment maintenance, which may involve fault detection to anticipate maintenance needs. Rasheed et al. [42] discuss IoT-enhanced solar device management, which could integrate fault detection for remote surveillance. Sharma et al. [41] utilize deep learning for fault detection and localization in power distribution systems, but the generalizability of their ANN models across different networks is questionable. Balestrieri et al. [35] present a big data platform for timeseries sensor data, which might serve fault detection purposes, though its scalability for increasing sensor data volumes is a concern.

Shifting focus to fault diagnosis, a number of articles delve into diagnosing and addressing the root causes of system malfunctions. Guo et al. [39] present DABAC, a smart contract-based access control system for IoT devices, which could assist in diagnosing security breaches within dynamic

environments, but its adaptability outside of smart contract platforms is doubtful. Liu et al. in [40] introduce Proteus, a home health monitoring infrastructure that may include diagnostic capabilities for health-related faults, though its suitability for large-scale commercial applications is uncertain. Mavromatis et al. [25] propose a software-defined IoT framework that could aid in diagnosing faults in distributed IoT settings, but it may not fully address security concerns. Loukil et al. [26] suggest a blockchain-based framework to maintain data privacy, which could involve diagnosing privacy violations. Zhang et al. [30] develop FusionTalk, an IoT-based system for object identification, which might be used for diagnosing identification and tracking issues. Guittoum et al. [31] propose a multi-agent system for managing IoT cascading failures, which could struggle with diagnosing failures in highly dynamic networks. Ribeiro and Mack [32] summarize a multi-vendor device management system, which might include diagnostic features for NERC compliance, but may not cover all compliance requirements. Ergun et al. [33] propose a dynamic reliability management technique for IoT edge computing, which could face challenges in managing reliability across heterogeneous IoT networks. Angappan et al. [34] develop a smart cold storage system with inventory monitoring, which might include diagnostic capabilities for storage conditions, but its optimization for energy consumption is uncertain.

The fault detection segment is frequently found wanting in its ability to address scalability and integration challenges, especially when dealing with a diverse array of technologies. Moreover, it often falls short in providing comprehensive coverage for all potential failure modes. The fault diagnosis segment, on the other hand, faces doubts regarding the efficiency and adaptability of fault diagnosis in dynamic environments. Its reliance on specific technology platforms, such as smart contracts, may also limit the broad applicability of the solutions. Both segments underscore an urgent need for solutions that are not only robust and adaptable but also comprehensive, capable of navigating the intricacies of fault detection and diagnosis across a spectrum of systems and scales.

Furthermore, a significant shortfall in these segments is the scarcity of work that provides strategies for failure prevention. This is particularly challenging when it comes to managing a multitude of heterogeneous IoT devices, which poses a considerable obstacle. The integration of large language models for IoT failure management offers distinct advantages. These are manifested in semantic interaction and proactive prevention strategies.

By semantically integrating diverse and heterogeneous data and combining it with localized knowledge bases specific to particular devices, these models not only efficiently accomplish failure identification and diagnosis but also enable the delivery of effective failure prevention strategies.

The utilization of large language models in IoT device management represents a paradigm shift. These models excel in their ability to understand and process complex data through advanced natural language processing capabilities. This enables a more nuanced and context-aware approach to failure management, which is crucial in the landscape of IoT where devices operate in varied and often unpredictable conditions. The semantic fusion of multi-source data, augmented by device-specific knowledge, allows for a more precise and swift response to potential failures, thereby enhancing the overall resilience and reliability of IoT ecosystems.
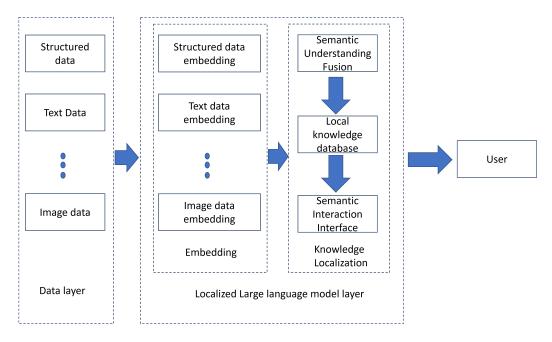


Figure 2: The structure of Large Language Model-based Smart Device Failure Management, where the semantic integration of multi-source heterogeneous data is achieved, and it is combined with the efficient understanding and processing capabilities of large language models.

## 3. Proposed Solution

Given the challenges previously discussed, we propose an intelligent device management framework based on large language models that is sustainable and effective. As depicted in Figure 2, heterogeneous data from multi-source intelligent devices is centrally uploaded and undergoes integration and fusion through a unified semantic approach, serving as an efficient and specialized local knowledge base for large language models to handle faults and failures.

The framework operates by integrating diverse data sources, such as table, textual data, image data, and even video data, into a unified semantic representation. This semantic fusion allows for a more comprehensive understanding of the device's operational context, which is crucial for identifying potential failure points. By harnessing the power of large language models, the framework can interpret and process this semantic information with high efficiency, leading to more accurate and timely detection of device malfunctions. This proactive approach to failure identification and prevention allows for early intervention, reducing the likelihood of device failure and the associated costs and downtime. Moreover, the framework is tailored to meet the specific needs of users, providing them with customized insights and recommendations that enhance their experience with smart devices. This personalization is achieved by analyzing user behavior and preferences, as well as the performance metrics of the devices, to offer targeted suggestions for maintenance and optimization. The end result is an improved user experience, as the devices are more reliable and responsive to user needs.

This framework leverages the semantic integration of multi-source heterogeneous data and combines it with the efficient understanding and processing capabilities of large language models. It is designed to address the issues of faults and failures in smart devices through customized and efficient failure identification and prevention. By intervening proactively at various stages where devices are at risk of failure, the framework provides constructive suggestions for preemptive maintenance and failure prevention of smart devices. Not only does this framework enable efficient semantic management of smart devices, but it also significantly enhances the quality of service for users' intelligent device usage. Furthermore, it offers constructive recommendations for budgetary decisions in the procurement of equipment for public cultural facilities.

In addition to enhancing user satisfaction, the framework also plays a critical role in supporting decision-making for the procurement of equipment

in public cultural facilities. By providing data-driven insights into the performance and maintenance needs of various devices, the framework assists in making informed budgetary decisions. This helps in allocating resources more effectively, ensuring that the equipment is not only cost-efficient but also aligned with the long-term strategic goals of the facility. Overall, the proposed framework is a significant step towards the sustainable and intelligent management of devices, contributing to the operational efficiency and user satisfaction in a variety of settings.
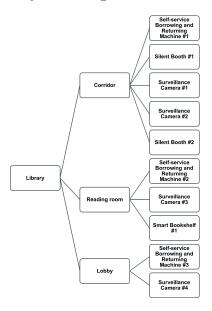


Figure 3: The schema of the considered smart devices deployed in the library for simulation.

## 4. Scene Simulation

Building upon the concept of scenario simulation, we have chosen the quintessential public cultural facility, the library, as our experimental testbed. Our large language model foundation is based on XXX. Our experiment is predicated on three distinct positions within the library: the Corridor, the Reading Room, and the Lobby. Library administrators are keen to implement intelligent semantic management for fault and failure identification and prevention of smart devices in these locations. The smart devices under consideration include the Self-service Borrowing and Returning Machine, Silent Booth, Smart Bookshelf, and Surveillance Camera.

The Self-service Borrowing and Returning Machine, Silent Booth, and Smart Bookshelf primarily generate operational log text data or structured tabular data, which are crucial for monitoring their performance and identifying potential malfunctions. These devices are pivotal to the library's operations, enhancing user experience through seamless services and efficient resource management. On the other hand, the Surveillance Camera, while not directly considered for fault and failure status, plays a significant role in this experiment. It is utilized to test the large language model's ability to process multimodal data. By analyzing images or video footage, the model can monitor the operational status of the other three devices, providing a visual layer of observation that complements the textual and structured data.

This integrated approach allows for a comprehensive understanding of the devices' health and performance. The Self-service Borrowing and Returning Machine, for instance, can be monitored for mechanical failures or software glitches through its log data, while the Silent Booth and Smart Bookshelf can be assessed for user interaction issues or technical malfunctions. The Surveillance Camera's footage can then be analyzed to correlate visual evidence with the data from these devices, offering a holistic view of their operational status. Specifically, traditional front-facing cameras can be replaced with desktop screenshot methods to capture faults. In fact, both approaches have been proven to validate the effectiveness of the solution.

By leveraging the capabilities of large language models to interpret multimodal data, we can enhance the proactive management of these smart devices. This not only improves the reliability and efficiency of library services but also contributes to a safer and more user-friendly environment. The experiment aims to demonstrate the potential of advanced data analytics in maintaining the optimal functioning of smart devices within public facilities, setting a precedent for the broader application of such technologies in the management of public infrastructure.

*4.1. Test Data*

The main experimental test scenario is set in a corridor, with the positions of the devices deployed along the corridor as shown in Figure 4. It is worth noting that the aforementioned experimental scenario is merely a simplified demonstration to test the effectiveness of the proposed solution. In actual scenarios, the locations of the various devices can be more flexibly configured according to practical needs. We have manually generated log data, based on real scenarios, for the Self-service Borrowing and Returning Machine, as
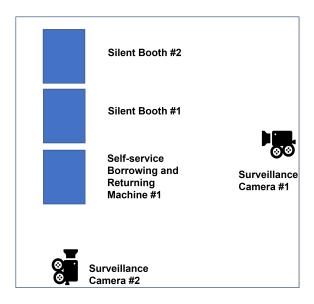
Figure 4: The schematic layout of smart devices in the corridor.

shown in Figure 7, as well as the synthetic image data from the Surveillance Camera, as shown in Figure 5 and 6, in order to evaluate the supportiveness and efficiency of the proposed solution for handling multi-source heterogeneous data. It is noteworthy that images captured by surveillance cameras often include timestamps. These timestamps, once effectively recognized and semantically organized by large language models, can be further correlated and integrated with the timestamps from logs. This process allows for the verification of the effectiveness of heterogeneous data fusion from multiple intelligent devices.

*4.2. Failure Identification and Provenance*

We have contemplated several typical user scenarios to enhance the intelligence of semantic management within the library. The typical work scenarios for failure management include: Inquiry about Device Availability, Fault and Anomaly Queries, Cause of Device Malfunctions, and Comprehensive Risk Assessment and Cause Analysis. We have integrated the workflows of these four scenarios in Figure 8, where the key paths corresponding to each work scenario are already identified. It is worth noting that in the Path 4 of Figure 8, we have constructed the capability of the large language model to recognize semantic text from video images into a RESTful local web API service. Similarly, audio files can also leverage web API services (In the experiment, we
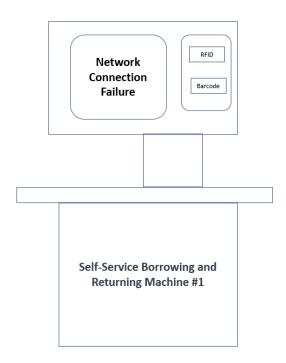
2024-12-05 08:30:45

Network Connection Failure

RFID

Barcode

Self-Service Borrowing and Returning Machine #1

Figure 5: The image of Self-service Borrowing and Returning Machine #1 taken from the front by Surveillance Camera #1 .

only considered the semantic transformation of image data, as we are meant to conduct a prototype verification of multi-source heterogeneous data fusion using large language model technology). This could be further imported into the local knowledge base or local database for online querying. Through a semantic approach, we efficiently integrate heterogeneous data generated by multiple smart devices. These scenarios include:

**Inquiry about Device Availability:** Users may want to know which devices are available in a specific area, corresponding to the Path 1, as labeled in Figure 8. For instance, a user could ask about the presence of certain smart devices in the Reading Room or the Lobby, seeking to locate them for use. For more detailed information, please refer to 9,10,11.

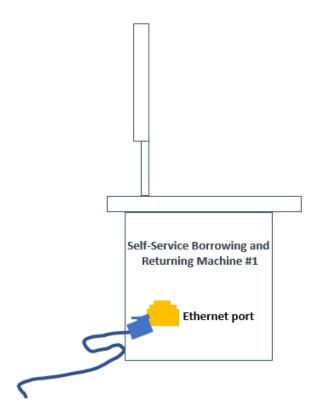**Fault and Anomaly Queries:** Users might inquire about the status of

2024-12-05 08:30:45



Figure 6: The image of Self-service Borrowing and Returning Machine #1 taken from the side by Surveillance Camera #2.



Figure 7: The sample of log information for the Self-service Borrowing and Returning Machine.

devices within a particular area, specifically whether there are any malfunctions or anomalies, corresponding to the Path 2, as labeled in Figure 8. A common question could be whether the Self-service Borrowing and Returning Machine in the Corridor is experiencing any issues that would prevent
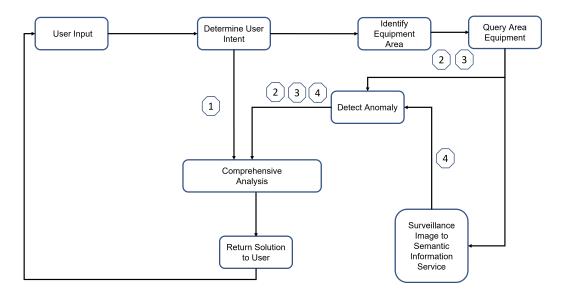
Figure 8: The integrated workflows of four scenarios for failure management, where the key paths corresponding to each scenario are identified with numbers.
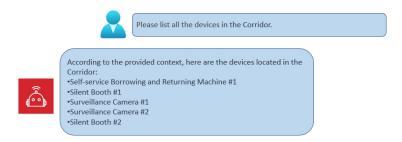


Figure 9: The interactive dialogue for querying the simple statistics of devices deployed in the corridor between the user and the Large Language Model.

its use; see Figure 12.

**Cause of Device Malfunctions:** Users may also seek to understand the reasons behind the malfunctions of specific devices, corresponding to the Path 3, as labeled in Figure 8. For example, a user might ask why a Silent Booth is not functioning properly, looking for insights into the cause of the problem; see Figure 13.

**Comprehensive Risk Assessment and Cause Analysis:** Generally, users are interested in understanding the broader risks of failure across the library's devices and the causes behind them, corresponding to the Path 4, as labeled in Figure 8. In such complex scenarios, the ability to conduct a
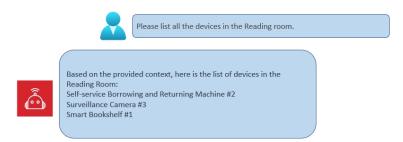
14

Figure 10: The interactive dialogue for querying the simple statistics of devices deployed in the reading room between the user and the Large Language Model.
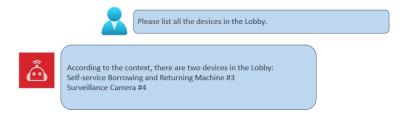


Figure 11: The interactive dialogue for querying the simple statistics of devices deployed in the lobby between the user and the Large Language Model.
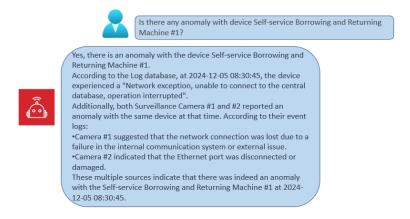


Figure 12: The interactive dialogue for querying the fault and anomaly of devices deployed in the designated area between the user and the Large Language Model.

comprehensive analysis is built upon the integration of the three aforementioned scenarios, leveraging the sophisticated reasoning capabilities of the large language model and its precision in identifying key processes within intricate workflows. The model must thoroughly understand the true inten-

What caused the anomaly in device Self-service Borrowing and Returning Machine #1 at 2024-12-05 at 08:30:45?

I have extracted the time of the anomaly from the Log database, which occurred on 2024-12-05 at 08:30:45. I then queried the Device_Position database and found that the surveillance cameras in the area, used for anomaly detection, are Surveillance Camera #1 and #2.
Next, I retrieved the surveillance event information from the Monitoring database for that time and combined it with the device's log records. After a comprehensive analysis, the cause of the anomaly in device Self-service Borrowing and Returning Machine #1 was determined to be a combination of factors:
• The internal communication system failed, likely due to a software issue or hardware malfunction.
• The Ethernet port was disconnected or damaged, possibly caused by accidental disconnection by a user or potential damage during transportation.
The surveillance cameras' event logs provided additional insight into the situation, suggesting that the device's network connection was lost due to one of these issues.

Figure 13: The interactive dialogue for querying the causes resulting in the fault and anomaly of devices deployed in the designated area between the user and the Large Language Model.

I need a report on all devices with anomalies in corridor.

After conducting a comprehensive analysis for the Corridor area, I have compiled a report on devices with anomalies:
Device Anomaly Report - Corridor Area
1.Self-service Borrowing and Returning Machine #1
    1. Anomaly: Network exception, unable to connect to the central database, operation interrupted
    2. Time of Anomaly: 2024-12-05 at 08:30:45
    3. Surveillance Cameras: Camera #1 and #2
    4. Cause of Anomaly: Combination of internal communication system failure and Ethernet port disconnection/damage
I have cross-referenced the Device_Position database with the Log database to identify devices in the Corridor area, and then analyzed their log records for anomalies. The report above includes detailed information on each device with an anomaly, including the type of anomaly, time of occurrence, surveillance cameras involved, and potential cause.
Please note that this report is based on the most recent data available in our local knowledge base. If you need further details or assistance, feel free to ask.

Figure 14: The interactive dialogue for requiring a comprehensive report for the fault and anomaly cases of devices deployed in the designated area between the user and the Large Language Model.

**Self-Service Borrowing and Returning Machine**

**User Manual**

---

Safety Precautions

Important: Before using the Self-Service Borrowing and Returning Machine, please read the following safety precautions carefully. Adhering to these guidelines will ensure your safety and the normal operation of the equipment.

**Electrical Safety**

- Ensure that the Self-Service Borrowing and Returning Machine is properly grounded to prevent electrical failures.
- Do not use damaged power cords or adapters.
- Disconnect the power supply before cleaning or maintaining the equipment.

**Operational Safety**

- Only authorized personnel are allowed to operate the Self-Service Borrowing and Returning Machine.
- Do not open the machine cabinet or attempt to repair the equipment while it is operating.
- Do not use flammable liquids, gases, or dust near the equipment.

**Environmental Safety**

- Ensure that the Self-Service Borrowing and Returning Machine is placed in a dry and well-ventilated environment.
- Avoid exposing the equipment to extreme temperatures, humidity, or direct sunlight.

**Physical Safety**

- Do not place heavy objects on the Self-Service Borrowing and Returning Machine.
- Do not play or run around the equipment to prevent accidental injuries.

**Emergency Handling**

- If you notice smoke, flames, or unusual noises, immediately turn off the power and evacuate the area.
- In case of an emergency, contact a professional for assistance.

Figure 15: The sample for the general safety precautions part in the product manual.

tions of the users, traverse and search through various paths, and determine the optimal query trajectory to swiftly return accurate information on smart device failures. To achieve this, we have meticulously fine-tuned the large lan-

**Self-Service Borrowing and Returning Machine**

**User Manual**

Troubleshooting

This section provides solutions for common issues you may encounter with the Self-Service Borrowing and Returning Machine. If you experience any problems, please follow the steps below. If the issue persists, please contact our technical support team.

1. **No Display or Display Malfunction**
   - o Check if the power connection is secure.
   - o Ensure the power switch is turned on.
   - o Restart the device.

2. **Barcode Scanner Not Reading**
   - o Clean the window of the barcode scanner.
   - o Ensure the barcode is clear and legible.
   - o Make sure the barcode is at an appropriate distance from the scanner.

3. **Unable to Recognize Borrower or Return Cards**
   - o Ensure the borrower or return card is not expired and is not damaged.
   - o Check if the card is correctly placed in the sensing area.
   - o Reinsert the card and try again.

4. **Books Cannot Be Borrowed or Returned**
   - o Ensure the book's barcode is not damaged or obscured.
   - o Check if the book is registered in the system.
   - o Reposition the book and try again.

5. **Touch Screen Unresponsive or Slow**
   - o Clean the surface of the touch screen.
   - o Restart the device.
   - o Check for software updates.

6. **Network Connection Issues**
   - o Check if the network cable connections are secure.
   - o Restart the router and the device.
   - o Contact your network service provider.

Figure 16: The sample for the general troubleshooting part in the product manual.

guage model with prompt words, enabling it to possess the aforementioned capabilities. This could involve a request for a comprehensive analysis of the potential failure risks for all smart devices in the library, along with the factors that might be contributing to these issues; see Figure 14.

By addressing these user scenarios, we aim to provide a more responsive and informed management system that not only meets the immediate needs of library users but also proactively maintains the efficiency and reliability of the library's smart devices. This approach will lead to a more integrated and user-centric library experience, where the causes of device malfunctions are quickly identified and resolved, minimizing disruption to the library's services.

## 4.3. Failure Mitigation and Prevention

Previously, we primarily discussed the identification and tracing of faults or failures in smart devices. However, to achieve proactive failure prevention and intervention, a set of strategies for the prevention of faults or failures in smart devices is essential. General large models often possess extensive global knowledge, and to some extent, they can provide users with failure or failure prevention strategies through appropriate prompts in the Prompt. To further supplement the general knowledge of large language models, extracting failure or failure prevention schemes from the product manuals of smart devices has become a very promising approach for the following reasons:

1. Product manuals typically contain product parameters, safety instructions, troubleshooting, and other content, which often implicitly includes specific failure or failure prevention strategies for the product.
2. Smart device manuals often have copyright protection, but as purchasers of the products, public service institutions might stipulate the usage rights of these documents during the procurement process or contract establishment. Moreover, since the model is deployed locally, the security of the data can be ensured to a certain extent.

Here, we consider two typical parts of general product manual, i.e., safety instructions and troubleshooting, for experiment, as shown in Figure 15 and 16, respectively. The sample of extracted information from product manuals is shown in Figure 17. By leveraging the information contained within product manuals, we can enhance the capabilities of large language models to offer targeted and effective failure prevention strategies. This approach not

only leverages the detailed knowledge specific to each device but also ensures compliance with copyright laws while maintaining the privacy and security of the data.

| Failure or Malfunction Name | Description of Failure or Malfunction | Failure or Malfunction Prevention Strategy |
|---|---|---|
| Network Connection Issues | Unable to connect to the network. | Regularly update the machine's software and firmware to ensure it has the latest security patches and features. Ensure that the machine is properly connected to the network and that the network connection is stable. |
| Touch Screen Unresponsive or Slow | The touch screen becomes unresponsive or slow. | Clean the touch screen regularly to remove dirt and dust that may affect its responsiveness. Use high-quality touch screens that are designed for heavy use. |
| Books Cannot Be Borrowed or Returned | Unable to borrow or return books. | Ensure that the machine is properly configured and that all necessary settings are correct. Regularly update the machine's software and firmware to ensure it has the latest features and security patches. |
| Barcode Scanner Not Reading | The barcode scanner fails to read barcodes. | Use high-quality barcode scanners and ensure they are properly installed and calibrated. Regularly clean the barcode scanner to remove dirt and dust that may affect its performance. |
| Disconnect from power supply | Disconnecting from power supply | Regularly inspect and maintain power cords and adapters to ensure they are in good condition. Use surge protectors to prevent damage from electrical surges. Avoid overloading outlets or using damaged extension cords. |

Figure 17: The semantic sample returned by the Large Language Model based on both safety precautions and troubleshooting part in the product manual.

## 5. Discussion

In the rapidly evolving landscape of smart public infrastructure, the integration of advanced technologies plays a pivotal role in enhancing operational efficiency and reliability. Our research has been at the forefront of this technological revolution, focusing on leveraging the power of artificial intelligence, particularly large language models, to transform the way we manage and maintain intelligent devices in public facilities. Below, we outline our key contributions that not only push the boundaries of current capabilities but also hold the potential to redefine the future of sustainable public infrastructure management.

20

Our pioneering contribution lies in the innovative application of cutting-edge large language model technology to the realm of public infrastructure. Specifically, we have harnessed this technology for the intelligent analysis and prevention of malfunctions and failures in public facility devices. This innovative approach not only enhances the sustainability of device maintenance and usage but also significantly reduces the budgetary strain on public facilities by optimizing resource allocation and operational efficiency.

We have introduced a novel method of semantically integrating heterogeneous data generated by various intelligent devices through the power of large language models. This integration is not just a technical feat but a strategic advancement that bolsters the intelligent monitoring of devices, ensuring their longevity and performance. By streamlining data from diverse sources into a cohesive and meaningful format, we support the continuous improvement and sustainability of intelligent device operations.

We have developed and proposed astute strategies for failure prevention and data acquisition that are grounded in practical intelligence. By leveraging localized knowledge bases derived from product manuals, we offer tailored and precise services for the prevention of device malfunctions and failures. This approach is not only proactive but also dynamic, adapting to the unique needs of a wide array of intelligent devices and providing them with the most effective preventive measures.

These contributions represent a significant leap forward in the field of public infrastructure management, where the intelligent use of data and advanced language models can lead to more sustainable, efficient, cost-effective, and resilient systems.

## 6. Conclusion and Future Work

We initially proposed the Large Language Model-based Smart Device Management framework, designed to address the complex challenges of intelligent device management in public facilities. Building upon this foundation, we focused on the smart device failure management within a typical representative of public infrastructure—the library. We conducted a prototype validation of our proposed framework model in real-world scenarios specific to libraries, demonstrating the effectiveness and feasibility of our approach.

Our work has not only highlighted the versatility and robustness of the proposed Large Language Model-based Smart Device Management framework but also its practical applicability in enhancing the operational effi-

ciency and reliability of intelligent devices in libraries. The prototype validation has fully showcased the advanced and innovative nature of our proposed model, proving its merit in practical settings.

Looking forward, we aim to expand the scope of our framework to encompass a broader range of public facilities beyond libraries. We are committed to further refining our model to handle an even more diverse set of scenarios and to improve its predictive capabilities for device failures. Additionally, we plan to explore the integration of our framework with advanced cybersecurity technologies, such as the Internet of Things (IoT) security and machine learning algorithms designed for threat detection and response . This integration aims to create a more comprehensive and proactive maintenance system that not only enhances the security posture of intelligent devices but also leverages machine learning's capabilities for automated analysis, real-time threat detection, and adaptive security measures . By incorporating these cutting-edge cyber security elements, our framework will be better equipped to address the dynamic and complex challenges of modern public infrastructure, ensuring robust protection against a wide range of potential threats. This will enable public facilities to not only respond to failures but also to anticipate and prevent them, leading to significant cost savings and improved service quality.

# References

[1] C.-D. Truong, B. T. Doan, Optimizing the accuracy of chatbot applications based on the gpt-3.5 turbo platform of openai to provide service prices to customers, Lecture Notes in Networks and Systems 1077 LNNS (2024) 658 – 667.

[2] A. Mekrache, A. Ksentini, C. Verikoukis, Intent-based management of next-generation networks: an llm-centric approach, IEEE Network 38 (5) (2024) 29 – 36.

[3] Y. Jin, J. Ma, Large language model as parking planning agent in the context of mixed period of autonomous vehicles and human-driven vehicles, Sustainable Cities and Society 117 (2024).

[4] A. Arora, A. Arora, The promise of large language models in health care, The Lancet 401 (10377) (2023) 641.

[5] S. Sandmann, S. Riepenhausen, L. Plagwitz, J. Varghese, Systematic analysis of chatgpt, google search and llama 2 for clinical decision support tasks, Nature Communications 15 (1) (2024).

[6] C. Patsakis, N. Lykousas, Man vs the machine in the struggle for effective text anonymisation in the age of large language models, Scientific Reports 13 (1) (2023).

[7] S.-K. Tan, H.-H. Lim, S.-H. Tan, Y.-S. Kok, A cultural creativity framework for the sustainability of intangible cultural heritage, Journal of Hospitality and Tourism Research 44 (3) (2020) 439–471.

[8] S. Bi, C. Wang, B. Wu, Y. Gong, W. Ni, An accurate book-localization approach based on passive ultra-high-frequency rfid, Lecture Notes in Electrical Engineering 920 LNEE (2022) 584 – 591.

[9] S. Bi, W. Ni, Y. Jiang, X. Wang, Novel recommendation-based approach for multidisciplinary development of future universities, Sustainability (Switzerland) 14 (10) (2022).

[10] Institute of Museum and Library Services, Accessed: [2024-11] (2024).
URL https://www.imls.gov/

[11] E. Oteros-Rozas, B. Mártin-López, N. Fagerholm, C. Bieling, T. Plieninger, Using social media photos to explore the relation between cultural ecosystem services and landscape features across five european sites, Ecological Indicators 94 (2018) 74–86.

[12] L. D. Rivero Moreno, Sustainable city storytelling: Cultural heritage as a resource for a greener and fairer urban development, Journal of Cultural Heritage Management and Sustainable Development 10 (4) (2020) 399–412.

[13] Institute of Museum and Library Services, 2021 Annual Financial Report, Tech. Rep. IMLS/2021-11, Institute of Museum and Library Services, Washington, D.C. (2021).
URL https://www.imls.gov/sites/default/files/2021-11/2021afr.pdf

[14] R. Florida, The Rise of the Creative Class, Basic, 2002.

[15] A. Chianese, F. Marulli, V. Moscato, F. Piccialli, Smartweet: a location-based smart application for exhibits and museums, in: International Conference on Signal Image Technology and Internet Based Systems, 2013, pp. 408–415.

[16] F. Amato, A. Chianese, A. Mazzeo, V. Moscato, A. Picariello, F. Piccialli, The talking museum project, Procedia Computer Science 21 (2013) 114–121.

[17] A. Chianese, F. Piccialli, G. Riccio, Designing a smart multisensor framework based on beaglebone black board, computer science and its applications, Computer Science and Its Applications (2015) 391–397.

[18] T. Ruotsalo, K. Haav, A. Stoyanov, S. Roche, E. Fani, R. Deliai, E. Makela, Smartmuseum: A mobile recommender system for the web of data, Journal of Web Semantics 20 (2013) 50–76.

[19] Y. Shi, P. Fan, Z. Zhu, C. Peng, F. Wang, K. B. Letaief, Sam: An efficient approach with selective aggregation of models in federated learning, IEEE Internet of Things Journal 11 (11) (2024) 20769 – 20783.

[20] C. Xu, Z. Li, G. Q. Huai, J. Zhao, Y. Zhu, X. Ma, H. Wang, Enabling lightweight immersive user interaction in smart buildings through learning-based mobile panorama streaming, Computer Communications 222 (2024) 68 – 76.

[21] S. Bi, C. Wang, B. Wu, S. Hu, W. Huang, W. Ni, Y. Gong, X. Wang, A comprehensive survey on applications of ai technologies to failure analysis of industrial systems, Engineering Failure Analysis 148 (2023).

[22] G. Wu, F. Liu, S. Li, Q. Song, Z. Tang, Ac-dnn: An adaptive compact dnns architecture for collaborative learning among heterogeneous smart devices, IEEE Internet of Things Journal 11 (12) (2024) 21072 – 21082.

[23] D. Thakur, A. Guzzo, G. Fortino, Intelligent adaptive real-time monitoring and recognition system for human activities, IEEE Transactions on Industrial Informatics 20 (11) (2024) 13212 – 13222.

[24] S.-H. Lee, J.-Z. Liu, A pluggable module for enabling a trusted edge device management system based on microservice, Journal of Communications and Networks 25 (3) (2023) 381 – 391.

[25] A. Mavromatis, C. Colman-Meixner, A. P. Silva, X. Vasilakos, R. Nejabati, D. Simeonidou, A software-defined iot device management framework for edge and cloud computing, IEEE Internet of Things Journal 7 (3) (2020) 1718 – 1735.

[26] F. Loukil, C. Ghedira-Guegan, K. Boukadi, A.-N. Benharkat, E. Benkhelifa, Data privacy based on iot device behavior control using blockchain, ACM Transactions on Internet Technology 21 (1) (2021).

[27] M. Enkhbaatar, T. Yamazaki, Automatic visual monitoring system for data center device management, 2022, p. 22 – 25.

[28] Z. Liu, X. Zhu, J. Ma, C. Hu, H. Fu, K. Zhao, Application of optimization technology for overhaul decision of substation equipment based on machine learning, Vol. 2066, 2021.

[29] F. Osimani, B. Stecanella, G. Capdehourat, L. Etcheverry, E. Grampín, Managing devices of a one-to-one computing educational program using an iot infrastructure, Sensors (Switzerland) 19 (1) (2019).

[30] L.-Y. Zhang, H.-C. Lin, K.-R. Wu, Y.-B. Lin, Y.-C. Tseng, Fusiontalk: An iot-based reconfigurable object identification system, IEEE Internet of Things Journal 8 (9) (2021) 7333 – 7345.

[31] A. Guittoum, F. Aïssaoui, S. Bolle, F. Boyer, N. De Palma, Solving the iot cascading failure dilemma using a semantic multi-agent system, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 14266 LNCS (2023) 325 – 344.

[32] B. Ribiero, D. Mack, Leveraging technology for automation and nerc compliance, Vol. 2022-April, 2022, p. 65 – 67.

[33] K. Ergun, R. Ayoub, P. Mercati, T. S. Rosing, Dynamic reliability management of multigateway iot edge computing systems, IEEE Internet of Things Journal 10 (5) (2023) 3864 – 3889.

[34] S. Angappan, A. Nataraj, L. N. Krishnan, A. Palanisamy, Development of an internet of things based smart cold storage with inventory monitoring system, International Journal of Electrical and Computer Engineering 15 (1) (2025) 89 – 98.

[35] M. Balestrieri, J. Capuzzi, K. Chang, H. Valizadehhaghi, An open-framework big data analytic platform applied to timeseries sensor data, 2024.

[36] B. Ribiero, D. Mack, Enhancing cybersecurity and nerc compliance through multi-vendor device management, 2024.

[37] A. West, Z. Santitos García, Grid automation device management in the cloud, 2021.

[38] Y. Liu, L. Jia, L. Wang, J. Wang, J. Zhang, Z. Zhang, An accurate and intelligent approach to predicting the power device fatigue failure process, IEEE Transactions on Power Electronics 39 (3) (2024) 3568 – 3579.

[39] F. Guo, G. Shen, Z. Huang, Y. Yang, M. Cai, L. Wei, Dabac: Smart contract-based spatio-temporal domain access control for the internet of things, IEEE Access 11 (2023) 36452 – 36463.

[40] M. Liu, M. Elbadry, Y. Hua, Z. Xie, S. Baral, I. Park, F. Ye, Proteus: An easily managed home-based health monitoring infrastructure, IEEE Internet of Things Journal (2024).

[41] N. Sharma, Pankaj, J. Rai, S. Nagarajan, Advanced deep learning approaches for fault detection and localization in power distribution systems, 2024, p. 447 – 452.

[42] K. Rasheed, S. Saad, S. Ammad, I. Badshah, Iot enhanced solar device management: Integrating remote surveillance and energy efficiency for sustainable operation, 2023.

[43] M. Casillo, C. Guida, M. Lombardi, A. Lorusso, F. Marongiu, D. Santaniello, Predictive preservation of historic buildings through iot-based system (2022) 1194–1198.

[44] M. Rossi, D. Bournas, Structural health monitoring and management of cultural heritage structures: a state-of-the-art review, Applied Sciences 13 (11) (2023) 6450.

[45] X. Liang, F. Liu, L. Wang, B. Zheng, Y. Sun, Internet of cultural things: current research, challenges and opportunities, Computers Mater Continua 74 (1) (2023) 469–488.

[46] O. Menaguale, Digital twin and cultural heritage – the future of society built on history and art, in: The Digital Twin, Springer International Publishing, 2023, pp. 1081–1111.

[47] J. Garcia-Valldecabres, A. Galiano-Garrigós, L. Meseguer, M. López González, Hbim work methodology applied to preventive maintenance: A state of the art review, Automation in Construction 121 (2021) 157–169.

[48] C. Trigona, E. Costa, G. Politi, A. Gueli, Iot-based microclimate and vibration monitoring of a painted canvas on a wooden support in the monastero of santa caterina (palermo, italy), Sensors 22 (14) (2022).

[49] N. Mitro, M. Krommyda, A. Amditis, Smart tags: Iot sensors for monitoring the micro-climate of cultural heritage monuments, Applied Sciences 12 (5) (2022).

[50] Y. Huang, S. Yu, J. Chu, et al., Using knowledge graphs and deep learning algorithms to enhance digital cultural heritage management, Heritage Science 11 (204) (2023).

[51] A. Attanasio, M. Maravalle, H. Muccini, F. Rossi, G. Scatena, F. Tarquini, Visitors flow management at uffizi gallery in florence, italy, Information Technology & Tourism 24 (3) (2022) 409–434.