AIHardMon: An AI-Driven Hardware Monitoring System for Anomaly Detection and Performance Analysis

K. Sri Harsha[1], K Vishweshwar Reddy[2], P. Sai Ranga[3] and N. Malarvizhi[4]
{vtu20355@veltech.edu.in[1], vtu19089@veltech.edu.in[2], vtu20408@veltech.edu.in[3], drnmalarvizhi@veltech.edu.in[4]}

UG Student, Department of CSE, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India[1,2,3]
Professor, Department of CSE, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India[4]

Abstract. Conventional hardware monitoring systems frequently suffer from false alarm rate (FAR) issues and lack prediction and contextual information. In this paper, we present AIHardMon, an AI-based hardware monitoring technique aiming to resolve these drawbacks. By utilizing machine learning methods such as Isolation Forest algorithms and considering context fan monitoring, AI-HardMon can provide proactive anomaly detection and advance the health control of such systems. Our experimental results demonstrate that AIHardMon effectively improves system reliability by reducing false positive alerts while accurately detecting genuine hardware anomalies. This is a smarter, more efficient and more predictable way of monitoring hardware health.

Keywords: artificial intelligence, computer hardware, anomaly detection, diagnostic systems, preventive maintenance, machine learning, temperature analysis.

1 Introduction

Modern computing infrastructure, such as cloud computing, industrial automation and Internet of Things (IoT), had evolved rapidly, presenting new performance, reliability and security requirements. For modern hardware systems that are becoming more and more complex with a high level of interconnectedness, traditional manual monitoring approach does not work in the era of big data. Therefore, there is a need for intelligent automatic processes to identify and react against the anomalies in real-time that are optimizing the network performance while improving robustness.

Anomaly detection is a crucial feature of hardware monitoring systems, since it is related essentially to the problem of detecting irregular pattern or behaviour in contrast with the expected one. By detecting anomalies promptly, systems can initiate preventive measures to avoid failures, minimize downtime, and maintain optimal operational performance. However, traditional methods of anomaly detection are based on rule and threshold which is not adaptive enough to dynamic system growth. This is also where technologies like AI have gone above and beyond simple hardware monitoring.

AI-based hardware monitoring systems use machine learning (ML) algorithms to automatically recognize patterns based on both historical and real-time data, which allows them to even detect new, complex anomalies. These systems provide significant advantages over traditional algorithms, namely that they are more accurate, robust to changes in the environment and can

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358082

enable high level management of large-scale systems with minimal human intervention. AI-powered anomaly detection also provides a deeper understanding of overarching system behaviour, enabling engineers and operators to diagnose the underlying causes of performance problems at their source and make better decisions.

As a matter of fact, adoption of AI-based anomaly detection in hardware systems have informed progress in several domains such as cloud infrastructures, IoT, industrial networks and 5G spaces. These have paved the way for more intelligent, self-healing systems to proactively prevent performance issues from escalating into large scale outages. With AI on tap for performance monitoring and anomaly detection, hardware can be more efficient, secure and reliable.

In this paper, we present AIHardMon, an AI-driven hardware monitoring system for anomaly detection and performance analysis. We examine the role of AI in addressing bottlenecks that current hardware systems face concerning to anomaly detection and performance improvement. Our only goal is to provide an in-depth study on these methods hoping that, by extracting knowledge from such state-of-the-art AI-centric hardware monitoring techniques and their potential effect at application level can be augmented.

2 Literature Review

Anomalies detection is the main task in hardware monitoring systems and occurs when certain actions are suspicious or performance of some devices and systems decreases. The application of AI in process and hardware monitoring as well as anomalies detection, has attracted great interests recently due to its enormous potential for improving system performances, security and reliability. We provide a literature review on the related studies that conduct AI (Artificial intelligence) to data-driven anomaly detection in hardware for performance analysis and monitoring.

AI in Anomaly Detection

This work is surveyed in [1], where the authors Chandola, Banerjee, and Kumar (2009) survey a wider range of anomaly detection algorithms and application areas. Those techniques, as statistical ones, clustering and also classification-based methods are the foundations of AI approaches applied to anomaly detection in order to detect anomalous behaviour on hardware systems. The authors also highlight that AI is essential to automatically detect, in a scalable way (e.g., manual monitoring is not feasible for large-scale cloud/IoT systems), anomalies.

In recent research a lot of focus has been seen towards efficient real-time anomaly detection in hardware systems. For instance, Xu et al. ACGM (Xu, Xie and Chen (2015) [2] is a non-instrumented performance tracing and anomaly detection system for machine learning systems. This paper highlights the significance of AI in performance characterization, and presents a solution that avoids code instrumentation but can achieve low overhead and accurate performance behaviours. The eACGM technique is also compatible with hardware monitoring framework since it is a lightweight and scalable method, and providing real-time detecting capability of anomalous behaviour.

In cloud-based systems, Patel and Jain (2024) [3] study AI enabled anomaly detection algorithms for real-time performance monitoring. They discuss challenges associated with monitoring cloud and hardware infrastructure. They present a machine learning model for the

cloud that can detect anomalies in hardware performance in order to improve its functioning and prevent potential crashes.

AI for Hardware and IoT Monitoring

For industry as well, detecting anomalies is of crucial significance to ensure system reliability and avert costly systems' down-time. [4] is an extension work of utilizing AI-aided anomaly detection in securing IOT nodes in 5G empowered smart city scenario. Using machine learning, this approach can detect abnormal hardware behaviours and guarantee the security and normality of IoT devices applied in smart cities.

Kim (2022) [5] considers performance measures of the anomaly detection for time series data. These experimental findings are of critical importance for the future of AI-based hardware monitoring and indicates how it is fundamental over time to understand if these systems work on real-world hardware. The paper gives KPIs for early warning of degraded behaviour, which are utilized in AI-enabled solutions focusing on automatic execution of monitoring services over the hardware.

DeMedeiros et al. [6] survey AI-based anomaly detection methods for IoT and sensor networks, with applications to hardware monitoring. The article de-mystifies LS-SN, and proposes AI-based solutions for handling-and analyzing- sensor data, the pathology of which can signal a system fault. Such approaches become essential for hardware monitoring in a dynamic distributed environment that generates and scales data indefinitely.

Industrial and Network Systems

AI is also proving its value in anomaly detection of industrial control systems. Grunova et al. (2024) [7] give some insights about how machine learning is used for anomaly detection in industrial setups. Their work is positioned in the context of using AI to track hardware systems on a manufacturing floor where identifying abnormal system behaviour in real-time would mitigate against any operational downtime, as well as provide increased robustness of the system.

Stahmann et al. (2025) [8] explore real-time anomaly detection in industrial networks using AI. The authors describe a machine learning-supported system to monitor and detect anomalies in networked industrial automation plants. The work is especially relevant for hardware monitoring in the context of interconnected industrial networks and to achieve real-time detection of hardware related performance anomalies with a view to maximising productivity.

In IoT-powered factories, Aly et al. [9]) identify how machine learning can contribute to better anomaly detection and hence improve the performance of hardware systems. By using AI models, the authors present a technique to identify performance anomalies of devices and machines of manufacturing. Their method demonstrates that AI-powered anomaly detection can be scalable to monitor many IoT devices in a large factory.

Advanced Anomaly Detection Techniques

Birihanu et al. (2025) [10] investigate the application for explainable AI (XAI) on anomalous activity detection in industrial control systems. They propose a correlation-based method to achieve accurate anomaly detection and an interpretable model which can explain why certain anomalies are detected for users. Our approach can be useful in hardware monitoring systems

as well, where representing and explaining the sources of anomalies is essential for fault diagnosis and performance tuning.

Edozie et al. (2025) [11] describe the evolution of AI in anomaly detection for telecom networks. Although their work is focused on network systems, it has implication towards hardware monitoring in machines where the network performance significantly affects the functionality of the hardware. They emphasize that this method highlights the potential of AI-based models as enabling technology to enhance performance monitoring, and anomaly detection processes in interdependent systems such as telecom and hardware infrastructures.

3 Existing System

The increasing complexity of industry standard hardware has created the need to develop a multitude of monitoring approaches in order to ensure an acceptable level of performance and reliability. Existing systems for hardware monitoring utilize various methodologies to keep track of performance and detect abnormal patterns. However, with the development of hardware many such classical systems were not able to be scaled easily on Big Data which possess very complex and correlated data. In this section, we consider previous systems and methods for hardware monitoring and anomaly detection, including legacy techniques as well as modern AI-based mechanisms.

3.1. Traditional Hardware Monitoring Systems

There are rule-based approaches based traditional hardware monitoring systems for performance anomaly detection. These systems work based on threshold models of performance indicators (CPU utilization, memory usage, disk access rate and network bandwidth). These measurements are reported and system can alert system administrator when they go above or under certain thresholds. Simple and Intuitive, however, rule-based monitors have several cons:

- **Fixed Thresholds:** The use of fixed thresholds can result in either false positives (when an anomaly is flagged unnecessarily) or false negatives (when a real anomaly is missed). These thresholds often fail to adapt to changing system conditions or workloads.
- **Limited Scalability:** As the number of monitored devices and sensors increases, traditional systems can struggle with scalability, particularly when monitoring distributed systems such as large data centres or IoT networks.
- **Lack of Contextual Awareness:** Rule-based systems typically cannot account for the contextual relationships between different system components, making it difficult to identify complex, multi-dimensional anomalies that may involve interactions between multiple hardware components.

3.2. Anomaly Detection in Cloud Infrastructure

The widespread adoption of cloud technologies has driven organizations to migrate on-premises applications to cloud-based alternatives. Cloud systems are typically distributed, and monitoring in real time is needed to guarantee the availability and performance of services. Detection of anomalies on cloud systems generally depends on machine learning algorithms, which are able to process a large monitoring data set from several cloud services and hardware devices.

For example, time-series analysis or clustering based methods to detect patterns in virtual machine performance data, storage systems, and network devices' performance information are deployed by cloud monitoring solutions. Such systems can detect anomalies that can be indicative of hardware failure – e.g. resource usage growing inexplicably or networks traffic activity deviating from typical patters. However, despite the promise of such machine-learning-based methods, these solutions are prone to high requirements of data labelling and processing in real-time and of ability to react promptly to changes in the workload status due to the shifting and fast requirements.

3.3. IoT-Based Hardware Monitoring

In the IoT, hardware monitoring & surveillance solutions are implemented to observe and monitor the functioning as well as the health of thousands of interconnected devices, sensors and actuators. The massive IoT networks and diversified devices introduce unique obstacles in the anomaly detection. Machine learning-based algorithms that can infer semantic from sensor data at runtime are employed in many IoT monitoring systems.

Anomaly detection in IoT hardware systems using AI can be used to spot abnormal sensor readings, device breakdowns, or network failures. However, IoT systems are generally resource-poor devices in terms of computation power and memory. As a consequence, several IoT-based monitoring solutions use edge computing approaches in which data is already processed on the device or near the network edge to be analyzed centrally at another server afterwards. Although this mitigates the issue of latency and bandwidth, challenges remain to build anomaly detection models that are accurate and scalable across a large number of devices.

3.4. Industrial Control Systems (ICS) and SCADA

Industrial Control Systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) systems are utilized for monitoring and controlling critical infrastructure, e.g. power plants, manufacturing plants or water purification cleansing stations. Due to the critical role of such systems, anomaly detection in ICS has become an open issue for maintaining stability and safety in industry.

Statistical techniques are commonly used in conventional ICS MAs for monitoring of device operation and early failure detection. These systems, however, are now more and more combined with AI / machine learning approaches to enhance the precision of detections and minimize false alarms. AI (artificial intelligence) approaches -such as neural network and clustering for anomaly detection- are investigated to improve the management of high dimensional data, and to identify potential performance problem that are difficult to be detected by conventional techniques.

3.5. AI-Based Anomaly Detection Systems

AI driven anomaly detection is becoming a big part of the solution to classic monitoring infrastructure in an increasingly complex hardware. AI methods, such as supervised learning, unsupervised learning and deep-learning can analyse live data on a large scale to find patterns a deviation from normal behaviour. These methods are flexible and scalable, automatically adjusting to system behaviour through continuous learning from new training data—something not possible with traditional approaches.

AI driven anomaly detection is extremely valuable in situations where real time monitoring and fast response is essential. E.g., machine learning models can analyze raw hardware performance counters to proactively predict imminent failures or hot spots before they impact system operations. Moreover, AI models can offer additional insight into the root causes behind anomalies, aiding engineers in not only identifying something is awry, but why.

3.6. Challenges with Existing Systems

Despite the advantages of AI-based approaches, there are several challenges that need to be addressed for effective hardware monitoring and anomaly detection:

- **Data Quality and Availability:** AI-based systems require high-quality data for training and prediction. Incomplete, noisy, or biased data can degrade the accuracy of anomaly detection models.
- **Real-Time Processing:** While AI models offer powerful detection capabilities, ensuring that these models can process data in real-time is a significant challenge, especially for systems with high data throughput.
- **Interpretability:** Many AI-based anomaly detection models, particularly deep learning models, are often viewed as "black boxes." This lack of interpretability can hinder the identification of the underlying causes of anomalies, making it difficult for operators to take corrective actions.
- **Scalability:** As the number of monitored devices and the volume of generated data continue to grow, ensuring that AI-based anomaly detection systems can scale effectively becomes increasingly important.

3.7. Emerging Trends

Several emerging trends are shaping the future of hardware monitoring and anomaly detection:

- **Explainable AI (XAI):** There is growing emphasis on developing AI models that both detect anomalies and provide explanations for their detection decisions in automated monitoring systems by allowing engineers to understand the rationale behind anomaly detections.
- **Edge Computing:** As hardware systems become more distributed, edge computing is gaining traction as a way to process data locally, reducing latency and bandwidth consumption while enabling real-time anomaly detection.
- **Federated Learning:** Federated learning allows AI models to be trained across decentralized devices without sharing sensitive data. This approach is particularly useful in scenarios where privacy and security are concerns, such as in IoT or healthcare systems.

4 Proposed System

The proposed AIHardMon system overcomes traditional hardware monitoring limitations by integrating machine learning with comprehensive system analytics. It comprises five core components and a Data Collection Module to collect metrics from CPU, memory, storage,

network, thermal, and fan subsystems; an Anomaly Detection Engine that uses Isolation Forests and expert models to detect anomalous behaviour with contextual fan analysis; and a Hardware Compatibility Analyzer to analyse system appropriateness for gaming, development, content creation, and productivity. The system features configurable monitoring intervals and intelligent fallback mechanisms for limited-sensor environments, ensuring broad hardware compatibility. Figure 1 illustrates the architecture of the proposed system.

AIHardMon's Recommendation Engine provides actionable advice by integrating rule-based knowledge with history, providing step-by-step fixes, alternate fixes, and proactive maintenance suggestions. The Visualization Interface provides information through an easy-to-use dashboard, e.g., status snapshots, history trend plots with highlighted exceptions, and interactive compatibility measures. Even to a non-technical audience, it achieves a compromise between high-level overview and granular diagnostics. AIHardMon fills the gap between detection and fix, unlike the usual tools.

It uses learning-based methods for anomaly detection to replace the static thresholds with learned typical behaviours of different hardware setups. The context sensitive fan monitoring makes the use of the best compromise between fan speed and cooling performance possible and thanks to compatibility analyser, covering the entire system even for support from components beyond systems requirements. AIHardMon is less than 2% CPU usage and 100MB memory AI based intelligent monitoring. These improvements address major short-comings of the prior art with a full proactive user entered hardware health and optimization solution.

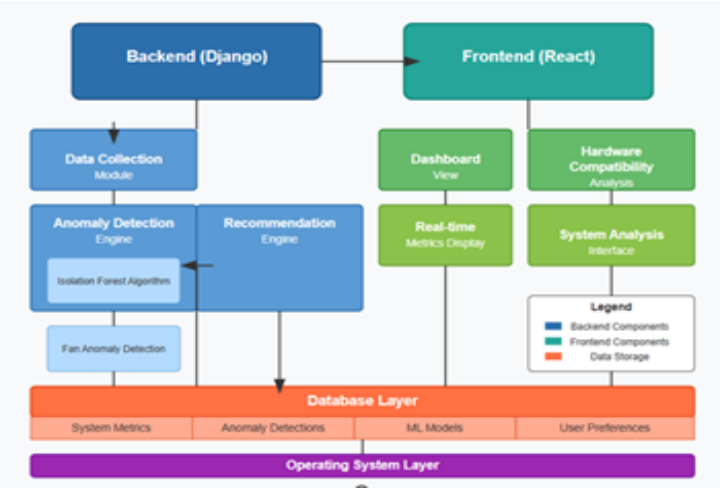

Fig. 1. Illustrates the architecture of the proposed system.

5 Methodology

AIHardMon is developed using hierarchical model and measurements aggregations design, we have 3 level of metrics to monitor, basic (CPU, memory, disk), extended (temperatures, fan speed) 1 and specific one such as GPU readings measurements. AIHardMon implements robust failover mechanisms to ensure continuous monitoring across diverse hardware configurations. When certain sensors are unavailable or malfunctioning, the system employs sensible fallback strategies with reasonable default configurations to maintain monitoring validity.

The system applies dynamic normalization, outlier removal, and feature extraction to transform collected metrics into meaningful analytical inputs. The anomaly detection mechanism extends beyond basic Isolation Forest algorithms by incorporating feature weighting and ensemble modelling to reduce false positive rates while maintaining detection accuracy The Contextual Fan Analysis algorithm evaluates cooling efficiency by analyzing thermal states and workload conditions dynamically, rather than relying solely on fixed threshold limits.

The Hardware Compatibility Analyzer evaluates system suitability for various use cases including gaming, application development, and content creation by examining both static hardware parameters and dynamic performance characteristics under different workload conditions. The Recommendation Engine, for identified issues; suggests precise recommendations based on Rule Based expertise as well as statistical performance scoring over 200+ solution patterns. The proposals are ranked based on knowledge base and filtered at the fly by system level setting, the user's taste. The visualization interface provides an intuitive dashboard that enables users to quickly assess system health through comprehensive status displays and intelligent diagnostic information.

6 Results and Discussion

The primary dashboard shows essential system resources using three circular progress bars. CPU usage (28%) is indicated in green, whereas Memory and Disk Storage (about 70% each) are indicated in red, pointing out possible resource shortages as in Fig 2. This clean design allows for instant evaluation of system health upon scanning.

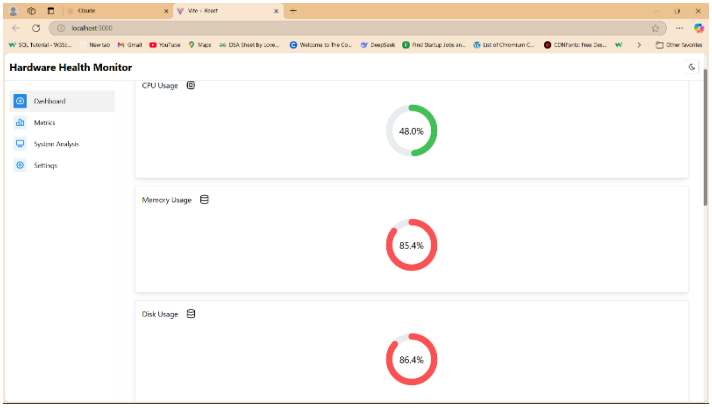

Fig. 2. Hardware Components Monitor.

The Cooling System monitor page as in Fig 3 includes a Hardware Issues indicator displaying normal operation and circular gauges for CPU and Chassis Fan status. Visual indicators indicate healthy cooling system function with a recommendation section verifying all fans are normal. This screen demonstrates AIHardMon's unique thermal analysis capabilities.

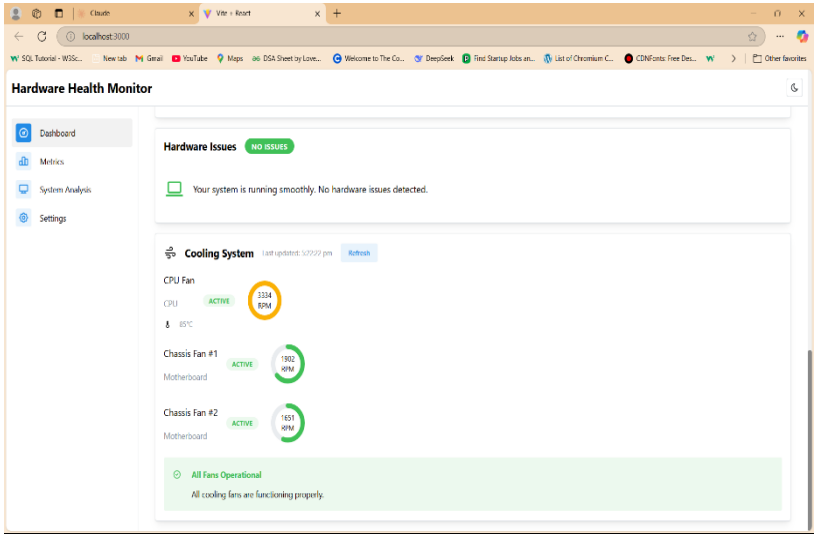

Fig. 3. Fan Component Monitor.

The Metrics History UI shows system performance metrics in the form of a timeline table showing CPU, memory, and disk percentages with status markers as Fig 4 shows. Green status markers in the far-right column show normal running across all logged intervals, and users can thus detect patterns and correlations in the behavior of a system over time.

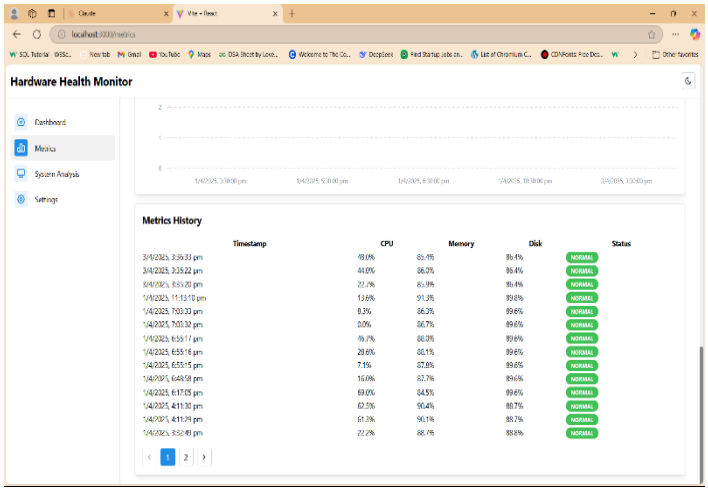

Fig. 4. Metrics Monitor.

The Hardware Health Monitor's Gaming Compatibility dashboard in Fig 5 included gaming performance analysis with color-coded compatibility ratings for Basic, Mid-Range, and High-End gaming types. It also included Development Tasks Compatibility with clear indicators for Web and Mobile Development appropriateness. This interface successfully converts elaborate hardware capabilities into understandable visual indicators.

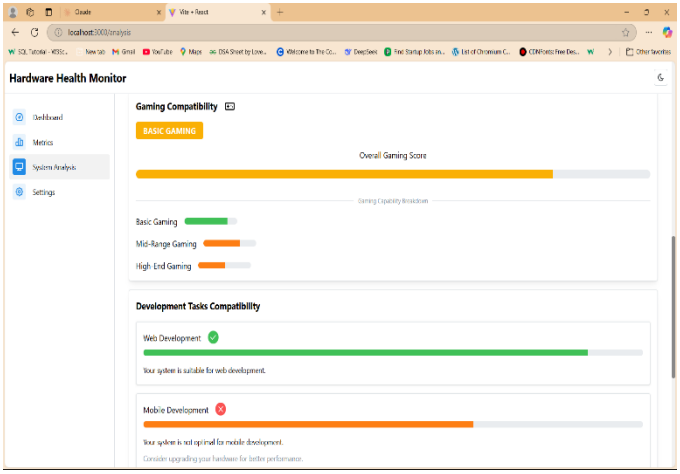

Fig. 5. Comparison of features for Compatibility Future Work.

7 Conclusion and Future Work

Conclusion In this paper, we present the concept of AIHardMon as a significant advancement in hardware monitoring by going beyond simple threshold-based checking (and addressing the need for greater accuracy over higher dimensions) and instead employing well-tuned ML-based anomaly detection. Its combined model methodology of analysing mutually dependent hardware metrics and system-specific tuning ensures accurate diagnostics. Of note is its context-sensitive fan monitoring algorithm which monitors cooling capacity as well as temperature (not just fixed thresholds). Smart compatibility analysis is an approach that can be used in a flexible way to generate dedicated hardware compatibility analysis tailored for gaming, content creation and other uses in the sense that AIHardMon could achieve even better accuracy than traditional solutions but with less system overhead. Additionally, the automated recommendation system makes hardware diagnostics accessible to non-technical users, enabling them to address common issues independently. AIHardMon can be further enhanced by integrating prognosis failure analysis from life-span modelling and anticipatory warnings for proactive maintenance. Future enhancements should include predictive failure analysis with lifespan modelling for proactive maintenance warnings. Integration of GPU-specific monitoring, memory diagnostics for interference source tracking, and enhanced automated correction with secure step-by-step debugging guidance would transform AIHardMon into a comprehensive hardware management solution.

References

[1] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882

[2] Xu, R., Xie, Z., & Chen, P. (2025). eACGM: Non-instrumented performance tracing and anomaly detection towards machine learning systems. arXiv. https://arxiv.org/abs/2506.02007

[3] Patel, M., & Jain, R. (2024). AI-powered anomaly detection for real-time performance monitoring in cloud systems. International Journal of Scientific Research in Science and Technology, 11(6), 592–601. https://www.researchgate.net/publication/387222329_AI-Powered_Anomaly_Detection_for_Real-Time_Performance_Monitoring_in_Cloud_Systems

[4] Reis, M. J. C. S. (2025). AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities. MDPI Sensors, 14(12), 2492. https://www.mdpi.com/2079-9292/14/12/2492
[5] Kim, G. Y. (2022). A study on performance metrics for anomaly detection in time-series data. MDPI Electronics, 11(8), 1213. https://www.mdpi.com/2079-9292/11/8/1213
[6] DeMedeiros, K., et al. (2023). A survey of AI-based anomaly detection in IoT and sensor networks. PMC. https://pmc.ncbi.nlm.nih.gov/articles/PMC9920825/
[7] Grunova, D., et al. (2024). Machine learning for anomaly detection in industrial environments. MDPI. https://www.mdpi.com/2673-4591/70/1/25
[8] Stahmann, P., et al. (2025). AI-based real-time anomaly detection in industrial networks. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S0360835225003821
[9] Aly, M., et al. (2025). Enhancing anomaly detection in IoT-driven factories using machine learning. Nature Scientific Reports. https://www.nature.com/articles/s41598-025-08436-x
[10] Birihanu, E., et al. (2025). Explainable correlation-based anomaly detection for industrial control systems. Frontiers in Artificial Intelligence. https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1508821/full
[11] Edozie, E., et al. (2025). Artificial intelligence advances in anomaly detection for telecom networks. Springer. https://link.springer.com/article/10.1007/s10462-025-11108-x