Strategic Predictive Maintenance for Internet System Security and Risk Management: A Roadmap

Meriem Hafsi, Juba Agoun

Strategic Predictive Maintenance for Internet System Security and Risk Management: A Roadmap

Meriem Hafsi*
mhafsi@cesi.fr
CESI LINEACT, 15C Av. Albert Einstein
Villeurbanne 69100, France

Juba Agoun
juba.agoun@univ-lyon2.fr
Université Lumière Lyon 2, ERIC UR3083
Bron 69500, France

Abstract

Recent technological advancements have profoundly transformed companies and businesses, enabling them to achieve high levels of performance. Today, system and network infrastructures are crucial and indispensable, requiring continuous corrections and maintenance to ensure superior security, reliability, and availability. However, various risks related to software, hardware, and malicious threats can cause failures, attacks, data loss, service interruptions, and breaches of rights or confidentiality. Ensuring the robustness, reliability, and security of infrastructures or data centers is essential. While detection techniques are used, they often fail to provide alerts before a failure or attack occurs and rely on risk assessments without concrete data from the infrastructure. In this article, we explore the paradigm of predictive maintenance and prognostics applied to IT and network infrastructures and data center equipment. The aim is to establish a literature review of solutions that predict attacks or failures by detecting early warning signals and to propose a roadmap for enhancing security and reliability by predicting the remaining useful life of the components.

Keywords

Fault Prognostic, Predictive Maintenance, Cybersecurity, Condition-Based Monitoring, Risk Management.

ACM Reference Format:
Meriem Hafsi and Juba Agoun. 2024. Strategic Predictive Maintenance for Internet System Security and Risk Management: A Roadmap. In *Proceedings of The 8th International Conference on Future Networks & Distributed Systems (ICFNDS).* ACM, New York, NY, USA, 9 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

Technological advancements have revolutionized enterprise infrastructures, leading to unprecedented levels of performance and capacity. The rise of hyperconnectivity through the Internet, coupled with the advent of the Internet of Things (IoT) and the Industrial IoT, has fundamentally transformed business operations. Furthermore, new paradigms of remote storage, such as cloud computing and edge computing, have introduced greater flexibility and efficiency. These innovations have not only enhanced operational capabilities but also provided numerous advantages, enabling companies to achieve superior performance, optimize resources, and deliver enhanced services. However, with these advancements come increased demands for security, reliability, availability, and confidentiality [40]. As businesses become more dependent on these advanced systems, ensuring their robustness becomes paramount. Malicious attacks, data breaches, and operational failures can have devastating impacts, leading to data loss, service interruptions, and breaches of confidentiality [6, 18]. Therefore, it is essential to guarantee and maintain these systems to safeguard against potential threats and failures [23]. These systems must meet stringent security standards to protect sensitive information, maintain high reliability to ensure continuous operation, and uphold availability to prevent downtime. Ensuring confidentiality is also critical to protect proprietary and customer data from unauthorized access [1]. These requirements are fundamental to maintaining customer trust and the overall integrity of business operations. To achieve this, infrastructure components must be meticulously maintained and regularly updated to prevent exposure to malicious attacks and breaches of confidentiality [45]. Despite these efforts, failures can still occur, impacting network functionality or infrastructure and potentially leading to operational shutdowns or data loss. Given the high reliability these systems demand, it is crucial to implement monitoring dashboards to track activities and conduct regular maintenance to ensure optimal performance. However, current methods often fall short in preemptively addressing all potential risks. Traditional approaches may not provide timely alerts or predictive insights, leaving systems vulnerable to unexpected failures and attacks. This underscores the urgent need for more robust and proactive solutions to enhance the security, reliability, and overall resilience of enterprise infrastructures [33, 40]. Inspired by Prognostic and Health Management (PHM) works [46] and gaining prominence with the rise of Industry 4.0 [3], predictive maintenance (PdM) [30] is a proactive approach to industrial maintenance which involves the use of advanced analytics, Machine Learning (ML), and real-time data to anticipate equipment failures before they occur [27]. By analyzing data from various sensors and historical performance metrics, PdM aims to estimate the remaining useful life (RUL) of equipments or components. This approach not only enhances the reliability and efficiency of industrial operations but also reduces downtime and maintenance costs. As Industry 4.0 continues to integrate smart technologies and interconnected systems, PdM has become a crucial element in optimizing asset management, improving operational performance, and fostering innovation across various sectors. Notable applications include manufacturing, batteries, wind turbines, and railways, where PdM helps to maintain system integrity and

ICFNDS, December 11–12, 2024, Marrakech, Maroc

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/XXXXXXX.XXXXXXX

performance. PdM for network infrastructure involves prediction and prevention of potential failures or performance issues in network components. By monitoring network performance metrics, such as bandwidth utilization, latency, and packet loss, businesses can identify anomalies or patterns that indicate potential problems. This enables proactive maintenance and repair actions, minimizing downtime and ensuring optimal network performance.

In this paper, we review existing PdM approaches within network infrastructure and cybersecurity. Our main contributions include a detailed assessment of PdM's potential in these fields and a systematic literature review. We also provide a roadmap for integrating PdM to enhance the reliability, availability, and security of services.

2 Background

PdM applications in Industry 4.0 and their extension to network maintenance and infrastructure management have shown promising resultsenhancing reliability, robustness, and availability while reducing downtime, repair and maintenance costs. By proactively addressing potential issues, businesses can minimize service interruptions, optimize network performance, and improve security. Additionally, PdM offers valuable insights for better planning and budgeting, enabling compagnies to efficiently manage their network operations and prepare for future demands as illustrated in Figure 1[1]. Overall, PdM is a crucial tool for driving business efficiency and success in modern industries.

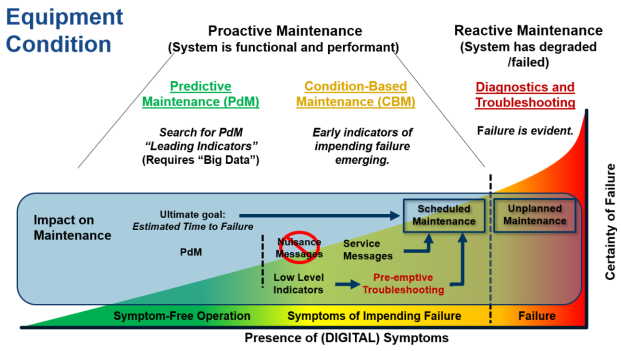

Figure 1: Comparison of proactive and reactive maintenance strategies.

Enhanced Security: PdM is vital for enhancing network security by proactively detecting and addressing vulnerabilities and threats before they are exploited. By monitoring network traffic and analyzing patterns, PdM systems identify anomalies indicative of malicious activities, enabling early intervention such as patching vulnerabilities and blocking suspicious actions [18]. This proactive approach helps protect sensitive data, ensure regulatory compliance, and maintain the integrity of network infrastructure against evolving cyber threats.

Service Availability and Reduced Downtime: PdM ensures high service availability and minimizes downtime by using advanced analytics and real-time monitoring to detect early signs of network failures or performance issues. This proactive approach allows businesses to address potential problems before they cause major disruptions, reducing unplanned outages and maintaining mission-critical services. Consequently, PdM enhances network stability and reliability, supporting business continuity and operational efficiency.

Cost Reduction: With early detection of failures and potential issues, PdM presents significant cost-saving opportunities by preventing costly repairs or replacements of network components. By identifying and addressing problems at an early stage, businesses can avoid the high expenses associated with emergency repairs or unplanned downtime, while also extending the lifespan of critical assets, leading to a more efficient use of resources and enhances overall operational efficiency.

Optimization and Planning: PdM offers invaluable insights into the health and performance of network infrastructure and services. Armed with this detailed information, companies can optimize their planning for network upgrades, maintenance schedules, and capacity expansion. This proactive approach allows businesses to anticipate future network demands and align their resources accordingly, ensuring that their infrastructure remains robust and capable of supporting evolving business needs. By strategically planning for maintenance and upgrades, companies can avoid reactive, last-minute decisions, thereby reducing costs and minimizing disruptions. Ultimately, PdM enables more efficient allocation of resources and better preparedness for future growth, driving long-term operational success.

3 Context

In the realm of Internet System Security and Risk Management, a data center stands as the technological backbone of modern enterprise operations. It serves as the critical IT infrastructure that powers the delivery of resources and services to users. As the central hub for data processing, storage, and communication, the security and reliability of a data center are paramount. Any disruption or breach can have far-reaching consequences, making it essential to implement robust and evolutive security measures and effective risk management strategies to ensure uninterrupted business continuity.

Datacenters provide substantial and specialized spaces meticulously engineered to meet the demands of space, power, cooling, management, reliability, and security for IT infrastructure, ensuring they can address the computing needs of enterprises for consolidation, business continuity, and security, while enabling emerging service-oriented architectures, infrastructure virtualization, and on-demand computing. Indeed, a data center represents one of the largest and most costly assets a company owns. Therefore, companies must pay close attention to the complexities involved in data center design and construction. It is crucial to ensure that the facility not only meets current business needs but also adapts to future changes and challenges throughout its operational lifecycle.

Two fundamental parts compose a data center as illustrated in Figure 2 [20]: the physical facility and the IT (Information Technology) infrastructure it contains. These elements, while interdependent, represent distinct aspects of the data center's overall operation. The physical facility includes the structural, environmental, and

[1]https://veryon.com/blog/defining-prognosis-and-diagnosis-within-the-digital-data-world

operational elements necessary for housing and supporting technology. This encompasses the building's architecture, power supply systems, cooling mechanisms, security measures, and other critical infrastructure designed to maintain optimal conditions for IT equipment. On the other hand, the IT infrastructure consists of the hardware, software, and network components that carry out the essential computing tasks. These components include servers, storage systems, networking equipment, and the software that drives data processing and communication. While these two aspects must function in unison to deliver reliable and efficient data services, each plays a unique role in ensuring the data center's operational success.

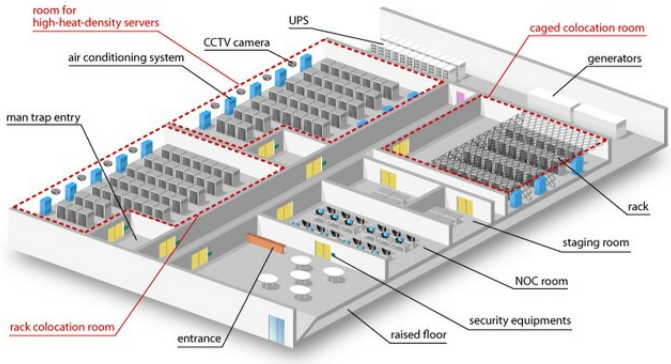

Figure 2: Schematic Representation of a Data Center and Its Key Components.

3.1 Physical facilities

The physical facilities architecture is designed to provide the highest levels of security, efficiency, and reliability. The infrastructure includes several key features that are crucial for the optimal functioning of Information Technology systems. These features include:

- **Cooling Systems:** manage the heat generated by data center equipment using Heating, Ventilation, and Air Conditioning (HVAC systems), Computer Room Air Conditioners (CRAC) units, and advanced cooling solutions to maintain optimal operating conditions.
- **Power:** infrastructure ensures stable and reliable electricity through redundant systems, including UPS, generators, and surge protection, supporting continuous IT operations.
- **Security:** includes physical access controls, surveillance, and network protection through firewall and intrusion detection systems to safeguard infrastructure and data.
- **Management:** uses monitoring tools like Data Center Infrastructure Management (DCIM) for optimizing performance, resource allocation, and PdM to ensure efficient operation.
- **Fire protection systems:** include smoke detectors and gas-based suppression systems, designed to quickly detect and suppress fires without damaging sensitive equipment.

3.2 Infrastructure

A data center infrastructure encompasses the comprehensive collection of IT equipment deployed within the facility. This equipment supports the execution of applications and the delivery of services to the business and its users. A typical data center infrastructure includes the following components[2]:

- **Servers:** Physical or virtual machines that host applications and store data.
- **Storage:** Devices and technologies for storing large volumes of data, such as SAN, NAS, and SSD arrays.
- **Networking utilities:** Network equipments such as routers, switches, firewalls, and load balancers that manage data traffic and connectivity.
- **Racks and cables**: Miles of wires interconnect IT gear, and physical server racks are used to organize servers and other gear within the facility space. Structured cabling systems for network, power, and data connections.
- **Backup Power:** Uninterruptible power supply (UPS), flywheel and other emergency power systems are critical to ensure orderly infrastructure behavior in the event of a main power disruption.
- **Management platforms:** Software and hardware solutions for monitoring, managing, and automating data center operations (DCIM).

3.3 Architecture

The distributed and dynamic nature of cloud, edge, and fog computing can lead to various challenges in failure prediction. These complexities often result in difficulties in monitoring and forecasting potential failures across diverse environments.

4 Research Methodology

This comprehensive systematic literature review aims to provide an in-depth analysis of current trends and recent advancements in PdM within data centers and network infrastructures, highlighting innovative techniques and methodologies. The research questions defined below will guide our review and form the basis for the answers we seek to provide.

4.1 Research Questions

This paper aims to provide a comprehensive overview of recent works in PdM and address the following research questions, which serve as a framework to conduct research and analyze data effectively:

RQ1: What are the current trends and recent advancements in PdM for Network infrastructures and datacenters?

RQ2: What are the major challenges and limitations with PdM implementaiton in datacenters?

RQ3: How can the benefits of PdM be maximized, particularly in terms of reliability, safety, and cost reduction?

RQ4: How can PdM help detect cyber-attacks and strengthen cybersecurity?

[2]https://www.techtarget.com/searchdatacenter/How-to-design-and-build-a-data-center

4.2 Search Strategy

An advanced search strategy was employed to gather relevant publications from various data sources, as shown in Figure 3, involving identification of key research libraries such as Google Scholar [3], ResearchGate [4], Springer, DBLP Computer Science Bibliography, MDPI Open Access Journals [5], and finally, Arxiv. Articles were selected through targeted keyword searches along with application keywords including Datacenters, Infrastructures network, cybersecurity. Priority was given to articles published between 2015 and 2024. Evaluation criteria for selected works included relevance, novelty, and originality, with consideration given to application fields, data types, and types of approaches utilized, such as single, hybrid, or model fusion methodologies.

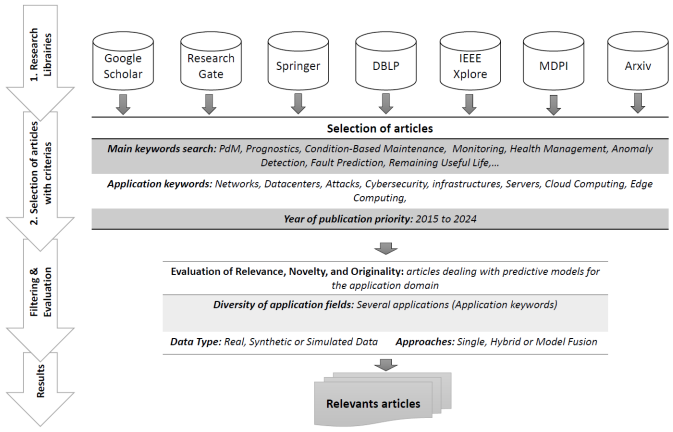

Figure 3: Research methodology

Our goal is to provide answers to the research questions outlined earlier. To achieve this, we must first conduct a comprehensive review of existing and emerging solutions. Before proceeding, it is essential to consolidate knowledge in our research domain by thoroughly analyzing the literature selected through our methodology.

5 Literature Background

Although data center engineers have long managed power-related failures and developed strategies to mitigate or adapt to them, there remains a significant need for companies to focus more on the overall resilience of their data center infrastructures. Many organizations lack a deep understanding of their system architectures, interdependencies, and failure patterns, often neglecting to plan for failure contingencies. Despite improvements in equipment, management, and industry maturity, failures continue to pose a major and costly challenge. PdM in this context offers a promising solution. It involves using predictive engines to collect data from devices, apply analytics to identify potential issues early, and generate alerts for proactive maintenance. By setting thresholds and analyzing signal data, trends can be predicted to anticipate service disruptions in communication networks. Automating the scheduling of maintenance jobs within data centers is essential, with the main challenge being the accurate prediction of job durations to minimize server downtime and operational costs. Several works have been explored in the literature and are presented below.

5.1 Failure Prediction in Physical Infrastructure

Several studies have been conducted on failure prediction in data center facilities, with a focus on critical components such as cooling systems, power supply units, and other essential equipment (Table 1). In [10], an optimal approach to data center cooling is proposed through the development of predictive models combining sensor data and ML algorithms to identify potential failure points before they occur. In [25], PdM is applied to supercomputing environment by estimating the hydraulic cooling system RUL using a deep learning (DL) hybrid approach, combining a Fully Convolutional Neural Network, Long Short-Term Memory, and a Multilayer Perceptron.

Elsewhere, predictive models have been applied to cooling systems to anticipate issues related to temperature regulation and airflow, while power systems are monitored for anomalies in voltage, current, and battery health. In [40], a Condition-Based Maintenance for Data Center Operations Management. In [22] network security risk prediction algorithm for power control systems is introduced, combining a classification-constrained Boltzmann machine and a Markov time-varying model. The algorithm effectively classifies network security risks and predicts future risks with high accuracy, outperforming other methods such as Hidden Markov Models and Bayesian Networks. Experimental results show high precision and adaptability, making the method well-suited for complex power system environments. These predictive approaches not only improve system reliability but also reduce downtime and operational costs, making them a vital area of research in ensuring the resilience of data center operations.

5.2 PdM for Network Infrastructure

PdM has been increasingly applied to network equipments to enhance operational reliability and prevent unexpected failures. Summarized in Table 2, recent research focuses on utilizing advanced analytics and ML algorithms to monitor the condition and performance of network devices, such as routers, switches [36, 44], and servers [14] [41].

By analyzing real-time data from these devices, predictive models can identify patterns and anomalies that signal potential issues before they cause significant disruptions. For instance, techniques such as time-series analysis and anomaly detection are employed to forecast hardware failures or performance degradation. These approaches not only help in scheduling timely maintenance but also in optimizing resource utilization and reducing overall downtime. As network infrastructure becomes more complex, the implementation of PdM strategies proves crucial in maintaining system stability and efficiency.

5.3 PdM for Storage Systems

In modern datacenters, hard disks are the primary storage devices due to their stability and cost-effectiveness [5]. However, the growth of Internet technology and cloud computing has led to massive data storage demands, creating challenges for storage systems, especially as hard disk failures have become more frequent due to their

[3]Google Scholar: https://scholar.google.com/
[4]ResearchGate: https://www.researchgate.net/
[5]MDPI Open Access Journals: https://www.mdpi.com/

Table 1: Summary of Research Studies on Data Center Physical Infrastructure Failure Prediction.

Ref	Actif	Goal	Proposition
[10]	Cooling System	Efficient datacenter cooling	Optimal approach to datacenter cooling through the development of predictive models for the analysis of component silicon reliability and sensitivity
[25]	Hydraulic Cooling System	Predict the RUL of an equipment before the occurrence of failures	Hybrid approach based on a combination of Fully Convolutional Neural Network, Long Short-Term Memory and Multilayer Perceptron
[22]	Power Control System Network Security	Prevention of malicious network attacks and ensure power control system security	Network security risk prediction algorithm for power control systems, based on categorization-constrained Boltzmann machine and Markov time-varying model
[40]	Power Distribution System	How to identify potential problems in early state before component and system failures are the key to prevent planed and unplanned downtime	Model of preventive and PdM (PPM) for PDS (Power distribution system) of data center

Table 2: A comparative study of common PdM Applications.

Ref	Actif/Category	Goal	Proposition
[14]	Server	Prediction of upcoming errors, increase the average productivity	Failure prediction solution
[41]	Server	Prediction server failure and boosting server reliability and driving industry transformation	PdM of Server using ML and DL
[44]	Switch	Failure prediction	PreFix Framework: Switch Failure Prediction in Datacenter Networks
[36]	Switch	Failure prediction and Data analysis	Estimate the expected time-to-failure, or survival time, of datacenter switches and quantify the factors that affect it
[23]	Component networks	Failure prediction	Predictive group maintenance for multi-system multi-component networks

vulnerability [16]. Ensuring storage system reliability is critical, as failures can result in data corruption or permanent data loss [29]. Hard disk drive (HDD) failures can be costly and disruptive to data center performance and availability. To mitigate this, vendors have introduced measures to reduce failure rates, leveraging Self-Monitoring, Analysis, and Reporting Technology (SMART) data collected during HDD operations [15].

Disk failure prediction is essential for ensuring data security in modern storage systems. Traditional reactive fault tolerance responds to failures after they occur, while proactive fault tolerance aims to predict and prevent failures, enhancing system reliability without compromising performance [5, 29]. Various ML algorithms have been proposed for disk failure prediction based on SMART data. In [16] LSTM networks are used for disk failure prediction with an application to the public dataset provided by Backblaze. In [43], authors proposed a failure prediction method based on Transfer Learning of heterogeneous disk systems.

5.4 PdM for Cloud Infrastructure

PdM in cloud computing, particularly in edge cloud environments, is crucial for ensuring system reliability and performance [35]. As highlighted by [13], anomaly detection plays a vital role in maintaining cloud infrastructure, where resource constraints and the scarcity of labeled data make accurate detection challenging. By leveraging advanced ML techniques such as transfer learning, knowledge distillation, and deep sequential models, PdM can overcome these limitations and enhance anomaly detection accuracy. These methods are essential for identifying and addressing potential failures before they impact the system, thereby ensuring seamless operation and reducing downtime in cloud environments. In [4], authors investigate the effectiveness of AI/ML-driven optimization techniques in improving the performance and security of edge infrastructure within edge computing environments. The study focuses on dynamic resource allocation, detecting and mitigating security threats, optimizing workload distribution, and assessing the impact of AI/ML optimizations on reducing latency, improving bandwidth efficiency, and enhancing system reliability. In [37], authors present a new failure prediction method that automatically identifies message patterns as failure indicators by grouping similar messages, independent of format, and adapts to changing configurations by re-learning patterns. In [8], the challenge of anomaly detection in supercomputers is highlighted, and a solution based on autoencoders within the context of High-Performance Computing Systems is proposed [24].

Table 3: Key Works on PdM for Storage Systems.

Ref	Actif	Goal	Method
[42]	Disk System	Failure prediction	A minority disk failure prediction model named TLDFP based on a Transfer learning approach
[16]	Storage systems	Disk failure prediction	Disk failure prediction system based on LSTM networks
[29]	SSD	SSD Failures in Datacenters	Presentation of an extensive characterization of SSD failures using field data
[5]	Disk system	Disk failure prediction	Presentation of a systematic study of data loss in large datacenters when the disk failure prediction is not accurate
[43]	Heterogeneous Disk Systems	Disk Failure prediction	Minority Disk Failure Prediction Based on Transfer Learning in Large Data Centers of Heterogeneous Disk Systems

Table 4: Summary of Studies on PdM for Cloud Infrastructure.

Ref	Problem	Proposition
[13]	Anomaly Detection in Edge Clouds	Improving the efficiency and accuracy of anomaly detection in edge cloud environments through ML techniques, including transfer learning, knowledge distillation, reinforcement learning, deep sequential models, and deep ensemble learning
[35]	Cloud-enhanced PdM	Enhancing predictive condition-based maintenance decision-making through a cloud-based approach leveraging comprehensive information
[9]	Failure Prediction of Jobs in Compute Clouds	A Google Cluster case study
[37]	Failure prediction in cloud datacenters	Online failure prediction in cloud datacenters by real-time message pattern learning
[8]	Anomaly detection in High Performance Computing systems	Anomaly detection method using autoencoders
[4]	Enhancing the performance and security of edge infrastructure	Exploration of the efficacy of AI/ML-enabled optimization techniques in enhancing the performance and security within the context of edge computing environments

5.5 Real-Time Prediction of Cyber-Attacks

Cybersecurity is considered one of the serious challenges for researchers [7]. In this context, prediction models have become vital for anticipating cyber-attacks. These models analyze patterns in network activity, detect vulnerabilities, and predict potential threats before they materialize. Leveraging advanced techniques like ML and DL, they enable more accurate and proactive security measures. In [19], an Artificial Neural Network (ANN) technique is proposed for prediction of cyber-Attack using Intrusion Detection System. In [7], authors proposed a more reliable and accurate ensemble-based approach to classify benign and malicious activities to identify and prevent possible cyber threats. In [28], authors propose using a Hidden Markov Model (HMM) to predict an attacker's next action in real-time, also forecasting the potential impact. In [18] a security breach prediction using ANN is proposed. In [2], authors propose an AI model-based DL and different machine and ensemble learning classifiers to detect cyber-attacks on the IoT with SMOTE (Synthetic Minority Over-sampling Technique) implementation for Predicting Cybersecurity Attacks on the Internet of Things. In [1], a combined prediction model of network security situation based on the EMD-ELPSO-BiGRU model is established for network security situation data series.

5.6 Supervision, Monitoring and Risks Management

PdM is increasingly being integrated into risk management, network and component maintenance, and to enhance cybersecurity. Several methods are employed to detect and anticipate security risks, primarily based on ML or DL techniques [38]. These approaches allow for more accurate forecasting of potential threats, enabling proactive measures to prevent failures or attacks before they occur. A summary of promising work is presented in Table 6.

To address the complex and time-consuming management of network security and monitoring, exacerbated by the rise in cyberattacks due to remote work during the COVID-19 pandemic, the authors propose in [31] automating security configurations and monitoring. They implement infrastructure as code (IaC) for automating the security and monitoring of network infrastructure, including IDS, honeypot, and SIEM, using Ansible tools to improve efficiency and security. In [32] propose a solution called "BlockSD-5GNet" to enhance security of 5G network through Blockchain-SDN mith ML-based bandwidth prediction. To optimize maintenance scheduling, a ML system called "Acela" (Predictable Datacenter-level Maintenance Job Scheduling) is proposed [12]. It uses quantile regression to bias predictions toward overestimation, reducing the number of servers taken offline and significantly decreasing server

Table 5: A Summary of Works on the Application of Predictive Models in Cyber-Attack Analysis.

Ref	Problem	Proposition
[19]	Prediction of cyber-Attacks	Neural network approach to intrusion detection system threat prediction
[7]	classification of benign and malicious activities to identify and prevent possible cyber threats	Reliable and accurate ensemble-based approach to classify benign and malicious activities to identify and prevent possible cyber threats
[28]	Prediction of the next action of the attacker in real time	Cyber attacker's next action prediction on dynamic real-time behavior model based on a Hidden Markov Model (HMM) to facilitate robust security decisions
[2]	Prediction of cyber-Attack in IoT networks	ML models for detecting malware including two single classifiers (KNN and SVM), eight ensemble classifiers (Random Forest, Extra Trees, AdaBoost, LGBM), and four DL architectures (LSTM, GRU, RNN)

Table 6: Summary of works on predictive models in supervision, monitoring and risks Management.

Ref	Problem	Proposition
[32]	Enhancing 5G network security	BlockSD-5GNet using Blockchain-SDN and ML-based bandwidth prediction
[31]	Network infrastructure monitoring and failure prediction	Infrastructure as Code for automating the security and monitoring of network infrastructure
[11]	Self-optimization in telecom	Application of ML-PdM to improve network and telecommunication services quality and ensure service availability
[26]	Computer network security technology	Application analysis based on network security maintenance
[34]	IoT security intrusion decisions	Integrated multilayered framework
[38]	Detection and anticipation of security risks in software testing	Literature analysis of DL models, including datasets and performance indicators
[1]	Network security situation prediction	EMD-ELPSO-BiGRU, BP, LSTM, BiGRU, and ELPSO-BiGRU models are used to predict the network security
[21]	Predicting Catastrophic Machine Failures in DataCenters	DC-Prophet: a two-stage framework for forecasting machine failures using One-Class SVM and Random Forest
[12]	Maintenance job scheduling in datacenters	Acela system using quantile regression to optimize maintenance scheduling
[39]	Online Failure Prediction	Failure prediction method based on learning and classification of message patterns as signs of failure

downtime, ensuring fair and regular server maintenance in large-scale datacenters. This approach optimizes maintenance scheduling, enhances network efficiency, and helps prevent potential security breaches and system failures [18]. In [11], improvements in network and telecommunication service quality and the assurance of service availability through PdM of telecom networks and autonomous self-adaptive networks are proposed.

6 Discussion

The Industry 4.0 sector is continuously evolving and adapting to new challenges, particularly with the advancements in computational power. Electronic components and computers are providing increasing computational capabilities. However, if such power falls into the hands of malicious users, physical systems could be compromised, potentially jeopardizing the security of entire industries.

In the previous sections, we have listed and compared various solutions proposed by the PdM (Predictive Maintenance) community. First, it is important to note that a series of studies aim to detect faults or attacks on physical infrastructure, utilizing both classical methods and more sophisticated approaches that dynamically adapt. Whether the threat is directed at the network or the cooling system, the latest PdM approaches integrate machine learning models and convolutional networks.

One of the most significant challenges remains cyber-attacks. Most research focuses on optimizing system performance through PdM, rather than emphasizing security. Indeed, in an era where speed is the key to a system's success, latency in an Industry 4.0 setting could lead to large-scale failures. In the following, we will present our vision to address the new challenges facing PdM in an Industry 4.0 environment. It is widely recognized that cyber resources and services can be penetrated and maliciously exploited, and that attacks are becoming more potent and persistent. The main goal of our idea is to develop an innovative Resilient PdM.

Figure 4 illustrates the three layers essential for a production process framework. The layer representing the physical space continuously generates data on the production status of devices and machines. Both machines and sensors can pose potential threats or failures. We propose an AI-based architecture that, instead of relying on a single predictive model, employs a set of models coupled

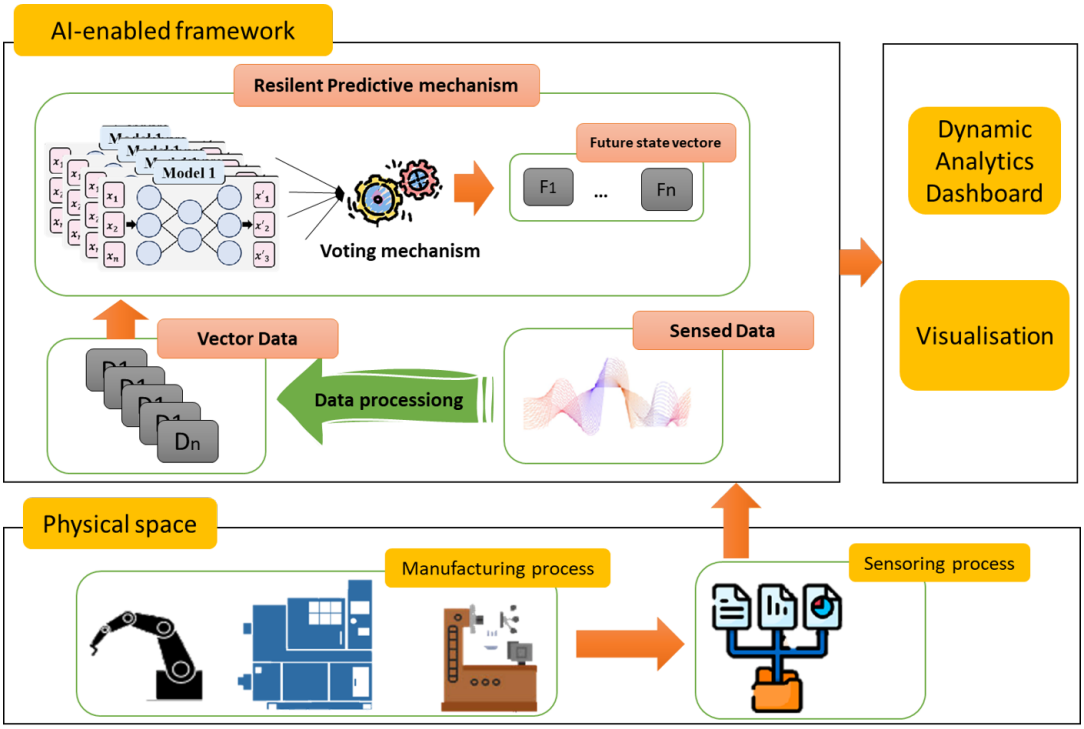

Figure 4: Resilient Framework for datacenter Security

with a voting mechanism. The Resilient AI-enabled mechanism component generates Future State Vectors based on a consensus between multiple models. This approach mitigates the risk of relying on a single compromised or faulty model. Additionally, this method avoids the limitations of traditional systems that focus on static thresholds for attack detection. For instance, we could adopt an Exponentially Weighted Moving Average (EWMA) approach [17].

Finally, we propose implementing a dynamic dashboard that visualizes various metrics through adaptive graphs based on crisis scenarios. The metrics should be prioritized and displayed according to the severity and type of disaster scenario at hand. A Future of Network Reliability: PdM is no longer a luxury but a necessity in the hyper-connected world. By proactively anticipating and addressing potential issues, telecom companies can ensure network resilience, optimize costs, and maintain a competitive edge. As new technologies like 5G and IoT drive network complexity, PdM will become even more critical in safeguarding the seamless flow of information that powers our lives.

7 Conclusion

Recent technological advancements have significantly enhanced company performance, making system and network infrastructures critical to business operations. These infrastructures demand ongoing maintenance to ensure high levels of security, reliability, and availability. Despite the use of various detection techniques, many still fall short in providing timely alerts before failures or attacks occur. This article has explored the potential of PdM and prognostics in IT and network infrastructures, emphasizing the importance of early warning signals to predict attacks and failures. Our review highlights the benefits of PdM in enhancing the reliability, availability, and security of data center components, network elements, and cloud architectures. The promising results of current studies underline the need for further research, addressing challenges such as massive data processing, overfitting, lack of labeled data, and model adaptability. Leveraging techniques such as transfer learning, continual learning, and federated learning could help overcome these limitations and ensure data confidentiality, paving the way for more robust and adaptive PdM solutions.

References

[1] Saif Aamer and Lubna Kadhim. 2023. Prediction system for network security state. *AIP Conference Proceedings* 2591, 030033. https://doi.org/10.1063/5.0119532

[2] Omar Azib Alkhudaydi, Moez Krichen, and Ans D. Alghamdi. 2023. A Deep Learning Methodology for Predicting Cybersecurity Attacks on the Internet of Things. *Information* 14, 10 (2023). https://doi.org/10.3390/info14100550

[3] I. S. Amangeldy and A. S. Bissembayev. 2024. ENHANCING OPERATIONAL EFFICIENCY IN INDUSTRY 4.0: A PREDICTIVE MAINTENANCE APPROACH. *Herald of the Kazakh-British technical university* (2024). https://api.semanticscholar.org/CorpusID:270993635

[4] Sahil Arora and Pranav Khare. 2024. AI/ML-Enabled Optimization of Edge Infrastructure: Enhancing Performance and Security. *International Journal of Advanced Research in Science Communication and Technology* 4 (06 2024), 230–242.

[5] Jayanta Basak and Randy Katz. 2017. Significance of Disk Failure Prediction in Datacenters. (07 2017).

[6] Fatmir Basholli. 2024. SECURITY IN TELECOMMUNICATION NETWORKS AND SYSTEMS. (02 2024). https://doi.org/10.13140/RG.2.2.21224.65284

[7] Bohdan Bebeshko, Karyna Khorolska, Nataliia Kotenko, Oleksander Kharchenko, and Tetyana Zhyrova. 2021. Use of Neural Networks for Predicting Cyber-attacks. In *Paper Proceedings of the Selected Papers on Publishing Papers with*

CEUR-WS co-located with Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Kyiv, Ukraine, January 28, 2021 (online) (CEUR Workshop Proceedings, Vol. 2923), Volodymyr Buriachok, Dmytro Ageyev, Valeriy Lahno, and Volodymyr Sokolov (Eds.). CEUR-WS.org, 213–223. https://ceur-ws.org/Vol-2923/paper23.pdf

[8] Andrea Borghesi, Andrea Bartolini, Michele Lombardi, Michela Milano, and Luca Benini. 2019. Anomaly Detection Using Autoencoders in High Performance Computing Systems. *Proceedings of the AAAI Conference on Artificial Intelligence* 33 (07 2019), 9428–9433. https://doi.org/10.1609/aaai.v33i01.33019428

[9] Xin Chen, Charng-Da Lu, and Karthik Pattabiraman. 2014. Failure Prediction of Jobs in Compute Clouds: A Google Cluster Case Study. *Proceedings - IEEE 25th International Symposium on Software Reliability Engineering Workshops, ISSREW 2014* (12 2014), 341–346. https://doi.org/10.1109/ISSREW.2014.105

[10] Abishai Daniel and Nishi Ahuja. 2015. Optimizing component reliability in datacenters using predictive models. In *2015 31st Thermal Measurement, Modeling & Management Symposium (SEMI-THERM)*. 324–326. https://doi.org/10.1109/SEMI-THERM.2015.7100181

[11] Mahmoud Fouad Darwish. 2021. A Survey of Predictive Maintenance and Self-optimization in Telecom Field Based on Machine Learning. In *2021 8th International Conference on Soft Computing & Machine Intelligence (ISCMI)*. 9–14.

[12] Yi Ding, Aijia Gao, Thibaud Ryden, Kaushik Mitra, Sukumar Kalmanje, Yanai Golany, Michael Carbin, and Henry Hoffmann. 2022. Acela: Predictable Datacenter-level Maintenance Job Scheduling. arXiv:2212.05155 [cs.DC] https://arxiv.org/abs/2212.05155

[13] Javad Forough. 2024. *Machine learning for anomaly detection in edge clouds*. Ph. D. Dissertation. Umeå University. https://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-220246

[14] David García-Retuerta. 2021. *Predictive Maintenance Proposal for Server Infrastructures*. 256–259. https://doi.org/10.1007/978-3-030-53829-3_30

[15] Wenwen Hao, Ben Niu, Yin Luo, Kangkang Liu, and Na Liu. 2022. Improving accuracy and adaptability of SSD failure prediction in hyper-scale data centers. *SIGMETRICS Perform. Eval. Rev.* 49, 4 (jun 2022), 99–104. https://doi.org/10.1145/3543146.3543169

[16] Lihan Hu, Lixin Han, Zhenyuan Xu, Tianming Jiang, and Huijun Qi. 2020. A disk failure prediction method based on LSTM network due to its individual specificity. *Procedia Computer Science* 176 (2020), 791–799. https://doi.org/10.1016/j.procs.2020.09.074 Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 24th International Conference KES2020.

[17] J Stuart Hunter. 1986. The exponentially weighted moving average. *Journal of quality technology* 18, 4 (1986), 203–210.

[18] Jayaganesh Jagannathan and M.Y. Mohamed Parvees. 2022. Security breach prediction using Artificial Neural Networks. *Measurement: Sensors* 24 (2022), 100448. https://doi.org/10.1016/j.measen.2022.100448

[19] Jay Kumar Jain and Akhilesh Waoo. 2023. An Artificial Neural Network Technique for Prediction of Cyber-Attack using Intrusion Detection System. *Journal of Artificial Intelligence, Machine Learning and Neural Network* (02 2023), 33–42. https://doi.org/10.55529/jaimlnn.32.33.42

[20] Yazid Kaced. 2018. *Études du refroidissement par free cooling indirect d'un bâtiment exothermique : application au centre de données*. Ph. D. Dissertation.

[21] You-Luen Lee, Da-Cheng Juan, Xuan-An Tseng, Yu-Ting Chen, and Shih-Chieh Chang. 2017. DC-Prophet: Predicting Catastrophic Machine Failures in DataCenters. (2017), 64–76.

[22] Siwei Li and Wenyu Zhang. 2024. Risk Prediction Techniques for Power Control System Network Security. *Journal of Control, Automation and Electrical Systems* 35 (04 2024). https://doi.org/10.1007/s40313-024-01087-9

[23] Zhenglin Liang and Ajith Kumar Parlikad. 2020. Predictive group maintenance for multi-system multi-component networks. *Reliability Engineering & System Safety* 195 (2020), 106704. https://doi.org/10.1016/j.ress.2019.106704

[24] André Lima, Vítor Aranha, Caio Jordão de Lima Carvalho, and Erick Giovani Sperandio Nascimento. 2021. Smart predictive maintenance for high-performance computing systems: a literature review. *The Journal of Supercomputing* 77 (11 2021), 1–20. https://doi.org/10.1007/s11227-021-03811-7

[25] André Lima, Vítor Aranha, and Erick Giovani Sperandio Nascimento. 2022. Predictive maintenance applied to mission critical supercomputing environments: remaining useful life estimation of a hydraulic cooling system using deep learning. *The Journal of Supercomputing* 79 (09 2022), 1–25. https://doi.org/10.1007/s11227-022-04833-5

[26] Xiang Ma. 2022. Application Analysis of Computer Network Security Technology Based on Network Security Maintenance. In *Frontier Computing*, Jason C. Hung, Neil Y. Yen, and Jia-Wei Chang (Eds.). Springer Nature Singapore, Singapore, 1253–1258.

[27] Hafsi Meriem, Hamour Nora, and Ouchani Samir. 2023. Predictive Maintenance for Smart Industrial Systems: A Roadmap. *Procedia Computer Science* 220 (2023), 645–650. https://doi.org/10.1016/j.procs.2023.03.082 The 6th International Conference on Emerging Data and Industry 4.0 (EDI40).

[28] Maryam Mohammadzad, Jaber Karimpour, and Farnaz Mahan. 2024. Cyber attacker's next action prediction on dynamic real-time behavior model. *Computers and Electrical Engineering* 113 (2024), 109031. https://doi.org/10.1016/j.compeleceng.2023.109031

[29] Iyswarya Narayanan, Kushagra Vaid, Di Wang, Myeongjae Jeon, Bikash Sharma, Laura Caulfield, Anand Sivasubramaniam, Ben Cutler, Jie Liu, and Badriddine Khessib. 2016. SSD Failures in Datacenters: What? When? and Why? 1–11. https://doi.org/10.1145/2928275.2928278

[30] P. Nunes, J. Santos, and E. Rocha. 2023. Challenges in predictive maintenance – A review. *CIRP Journal of Manufacturing Science and Technology* 40 (2023), 53–67.

[31] Wahyu Putra, Agus Nurwa, Dimas Priambodo, and Muhammad Hasbi. 2022. Infrastructure as Code for Security Automation and Network Infrastructure Monitoring. *Matrik Jurnal Manajemen Teknik Informatika dan Rekayasa Komputer* 22 (11 2022), 201–214. https://doi.org/10.30812/matrik.v22i1.2471

[32] Anichur Rahman, Md Khan, Antonio Montieri, Md Islam, Md Razaul, Mahedi Hasan, Dipanjali Kundu, Mostofa Nasir, and Antonio Pescapè. 2024. BlockSD-5GNet: Enhancing Security of 5G Network through Blockchain-SDN with ML-based Bandwidth Prediction. *Transactions on Emerging Telecommunications Technologies* 35 (04 2024).

[33] Elisabetta Ronchieri, Luca Giommi, Luigi Scarponi, Luca Torzi, Alessandro Costantini, Doina Duma, and Davide Salomoni. 2024. Anomaly Detection in Data Center IT & Physical Infrastructure. *EPJ Web of Conferences* 295 (05 2024). https://doi.org/10.1051/epjconf/202429507004

[34] Hassen Sallay. 2023. An Integrated Multilayered Framework for IoT Security Intrusion Decisions. 36 (01 2023), 429–444. https://doi.org/10.32604/iasc.2023.030791

[35] Bernard Schmidt and Lihui Wang. 2018. Cloud-enhanced predictive maintenance. *International Journal of Advanced Manufacturing Technology* 99 (10 2018), 5–13. https://doi.org/10.1007/s00170-016-8983-8

[36] Rachee Singh, Muqeet Mukhtar, Ashay Krishna, Aniruddha Parkhi, Jitendra Padhye, and David Maltz. 2021. Surviving switch failures in cloud datacenters. *SIGCOMM Comput. Commun. Rev.* 51, 2 (may 2021), 2–9.

[37] Masataka Sonoda, Shinji Kikuchi, Yukihiro Watanabe, Hiroshi Otsuka, and Yasuhide Matsumoto. 2012. Online failure prediction in cloud datacenters by real-time message pattern learning. *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*, 504–511. https://doi.org/10.1109/CloudCom.2012.6427566

[38] Raees Suman, Khan. 2024. Survey on identification and prediction of security threats using various deep learning models on software testing. *Multimedia Tools and Applications* (02 2024), 1–12. https://doi.org/10.1007/s11042-024-18323-8

[39] Yukihiro Watanabe and Yasuhide Matsumoto. 2014. Online Failure Prediction in Cloud Datacenters. *Fujitsu Scientific and Technical Journal* 50 (01 2014), 66–71.

[40] Montri Wiboonrat. 2019. Condition Based Maintenance for Data Center Operations Management. In *2019 16th International Joint Conference on Computer Science and Software Engineering (JCSSE)*. 73–78. https://doi.org/10.1109/JCSSE.2019.8864169

[41] Anjali Yeole. 2024. Predictive Maintenance of Server using Machine Learning and Deep Learning. *Journal of Electrical Systems* 20 (05 2024), 2828–2833. https://doi.org/10.52783/jes.3188

[42] Ji Zhang, Ke Zhou, Ping Huang, Xubin He, Zhili Xiao, Bin Cheng, Yongguang Ji, and Yinhu Wang. 2019. Transfer Learning based Failure Prediction for Minority Disks in Large Data Centers of Heterogeneous Disk Systems. In *Proceedings of the 48th International Conference on Parallel Processing* (Kyoto, Japan) *(ICPP '19)*. Association for Computing Machinery, New York, NY, USA, Article 66, 10 pages. https://doi.org/10.1145/3337821.3337881

[43] Ji Zhang, Ke Zhou, Ping Huang, Xubin He, Ming Xie, Bin Cheng, Yongguang Ji, and Yin Wang. 2020. Minority Disk Failure Prediction Based on Transfer Learning in Large Data Centers of Heterogeneous Disk Systems. *IEEE Transactions on Parallel and Distributed Systems* PP (04 2020), 1–1. https://doi.org/10.1109/TPDS.2020.2985346

[44] Shenglin Zhang, Yuzhi Zhang, Yu Chen, Hui Dong, Xianping Qu, Lei Song, Ying Liu, Weibin Meng, Zhiling Luo, Jiahao Bu, Sen Yang, Peixian Liang, Dan Pei, and Jun Xu. 2018. PreFix: Switch Failure Prediction in Datacenter Networks. 64–66. https://doi.org/10.1145/3219617.3219643

[45] Langrui Zhou, Yufen Qin, Pamela Thompson, Z. Hou, Krzysztof Marasek, Chéng Li, Nick Wu, Cui Li, Torben Ferber, Denise Toth, M. Akemoto, Jinlin Nie, M. Bertani, Yudong Shao, Nobu Katayama, Kerry Whisnant, Junji Haba, Masafumi Tawada, and Takayuki Sumiyoshi. 2024. Security management in IT service operation and maintenance. (03 2024).

[46] Enrico Zio. 2022. Prognostics and Health Management (PHM): Where are we and where do we (need to) go in theory and practice. *Reliability Engineering & System Safety* 218 (2022), 108119.