International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

AI and Machine Learning for Predictive Monitoring in IT Operations

Yash Jani

Sr. Software Engineer at Docusign, Fremont, California, USA
Email: *yjani204[at]gmail.com*

Abstract: ***In modern IT operations, anticipating and preventing system failures is critical to maintaining operational continuity and minimizing downtime. Traditional reactive monitoring approaches are needed in complex and dynamic IT environments. This paper explores the application of AI and machine learning (ML) in predictive monitoring for IT operations. We delve into advanced algorithms, data processing techniques, model deployment strategies, and the integration of predictive monitoring within IT infrastructure. Furthermore, we address the challenges of scalability, data quality, and model interpretability and discuss future trends that shape the landscape of predictive monitoring.***

Keywords: AI, Machine Learning, Predictive Monitoring, IT Operations, Predictive Analytics, Anomaly Detection, Data Science, IT Infrastructure.

1. Introduction

The complexity of IT infrastructures has grown exponentially, driven by the increasing demand for digital services, cloud computing, and large-scale data processing. Traditional monitoring systems, which primarily rely on static thresholds and reactive responses, often need to be revised to address modern IT environments' dynamic and multifaceted nature. This limitation has led to the rise of predictive monitoring, a sophisticated approach that leverages AI and ML to anticipate and mitigate issues before they impact operations.[1][2]

Predictive monitoring represents a paradigm shift in IT operations. AI models can identify subtle patterns and trends that may indicate future problems by analyzing vast amounts of historical and real-time data. This proactive approach minimizes downtime and enhances IT systems' overall performance and reliability. As organizations embrace digital transformation, adopting AI-driven predictive monitoring is increasingly essential for maintaining competitive advantage and operational efficiency.[3]

This paper aims to comprehensively analyze AI and ML's role in predictive monitoring for IT operations. We will explore the underlying technologies, discuss their applications, and examine organizations' challenges in implementing these advanced systems. Additionally, we will look into future trends and innovations that will further enhance predictive monitoring capabilities in IT. [4]

2. Overview of Predictive Monitoring in IT Operations

a) Definition and Scope

Predictive monitoring in IT operations refers to using AI and ML techniques to analyze and interpret large datasets to predict potential system failures or performance degradation. The scope of predictive monitoring extends across various aspects of IT infrastructure, including servers, networks, applications, and databases. Unlike traditional monitoring, which triggers alerts only when predefined conditions are met, predictive monitoring aims to foresee issues before they arise, allowing IT teams to address them proactively.[1][2]

Predictive monitoring systems collect and analyze data from multiple sources, such as log files, performance metrics, and user interactions. By applying machine learning algorithms to this data, these systems can identify patterns and correlations that are not immediately apparent through traditional analysis methods. This enables IT teams to take preemptive actions, such as adjusting resource allocation, updating software, or replacing hardware components before any significant impact on operations occurs.[6]

b) Evolution of Monitoring Techniques

The evolution of monitoring techniques in IT operations can be traced back to the early days of computing when system administrators manually monitored system performance and responded to issues as they occurred. As IT infrastructures became more complex, automated monitoring tools were developed, allowing for real-time system health tracking through thresholds and alerts.

Despite these advancements, traditional monitoring techniques have inherent limitations. Threshold-based alerts can generate numerous false positives, overwhelming IT teams with unnecessary notifications. Moreover, these systems often fail to detect issues that do not conform to predefined patterns, leading to missed critical events.[7]
Introducing AI and ML into IT operations has transformed monitoring from a reactive process into a predictive one. By analyzing historical data and learning from past incidents, AI-driven systems can anticipate potential problems with greater accuracy and reduce the burden on IT teams by filtering out noise and focusing on actionable insights.[8]

c) Importance of Predictive Monitoring

In today’s highly interconnected and data-driven world, the reliability and performance of IT systems are critical to business success. Downtime, system failures, and

performance bottlenecks can lead to significant financial losses, damage to reputation, and customer dissatisfaction. Predictive monitoring addresses these challenges by enabling IT teams to maintain high system availability and performance levels.[9][10]

Predictive monitoring is critical in environments where continuous uptime is essential, such as financial services, healthcare, and e-commerce. Organizations can avoid costly outages by identifying and addressing potential issues before they escalate and ensuring their IT systems operate smoothly. Furthermore, predictive monitoring can help optimize resource utilization by identifying inefficiencies and recommending adjustments, leading to cost savings and improved performance.[11]

3. Role of AI and ML in Predictive Monitoring

1) AI and ML Algorithms for Predictive Monitoring

The success of predictive monitoring largely depends on the AI and ML algorithms used to analyze data and generate predictions. Various algorithms are employed based on the data's nature and the monitoring system's specific goals.

a) **Supervised Learning:** In predictive monitoring, supervised learning algorithms such as regression models, decision trees, and support vector machines (SVM) are commonly used. These algorithms learn from labeled datasets where the outcome of interest (e.g., system failure) is known. The algorithms can predict future outcomes based on new data inputs by analyzing this historical data. For example, a regression model might predict the likelihood of a server failure based on its temperature and workload.[12]

b) **Unsupervised Learning:** Unsupervised learning techniques, such as clustering and anomaly detection, are valuable for identifying patterns in data that do not have predefined labels. In IT operations, these algorithms can detect unusual behavior that may indicate an impending issue. For instance, clustering algorithms can group similar performance metrics together, making identifying outliers that deviate from the norm easier.[13][14]

c) **Reinforcement Learning:** Reinforcement learning is used in scenarios where the system learns to make decisions based on the outcomes of previous actions. In predictive monitoring, reinforcement learning can optimize IT operations by continuously improving the decision-making process based on feedback from the environment. For example, a reinforcement learning model might adjust server configurations to maximize performance while minimizing energy consumption.[15]

2) Data Sources and Preprocessing

Data is the backbone of predictive monitoring. Collecting data from various sources within the IT infrastructure is crucial to building effective AI and ML models. Common data sources include:

a) **Log Files**: System logs provide information about system activities, errors, and performance metrics. They are a primary source of data for predictive monitoring.

b) **Performance Metrics:** Metrics such as CPU usage, memory consumption, network throughput, and disk I/O are essential for understanding the health and performance of IT systems.

c) **User Interactions:** Monitoring user interactions with applications can provide insights into potential usability issues or performance bottlenecks.

d) **External Data Sources:** In some cases, external data such as weather conditions, market trends, or social media activity may be relevant to predictive monitoring, especially in industries like finance or logistics.[11][16][17][18]

Before this data can be used to train AI and ML models, it must undergo preprocessing. This involves cleaning the data to remove noise and inconsistencies, normalizing it to ensure consistency across different sources, and transforming it into a format suitable for analysis. Feature engineering, which involves selecting and creating relevant features from the raw data, is a critical step in this process. Well-engineered features can significantly improve the accuracy of predictive models.[19][20]

3) Model Training and Deployment

Once the data is preprocessed, it is used to train AI and ML models. The training process involves feeding the data into the chosen algorithms and adjusting the model parameters to minimize prediction errors. Depending on the complexity of the system and the data, training can be computationally intensive and may require specialized hardware, such as GPUs or TPUs.

After training, the models are deployed in a real-time monitoring environment. In production, these models continuously receive new data, make predictions, and trigger alerts or automated actions as needed. The deployment phase also involves integrating the models with existing IT infrastructure and monitoring tools, ensuring that predictions are seamlessly incorporated into the operational workflow.[21][22]

4) Continuous Learning and Model Updating

IT environments are dynamic, with constant changes in workloads, configurations, and usage patterns. Predictive monitoring models must be continuously updated with new data to remain effective. This process, known as continuous learning, allows the models to adapt to changes and maintain their accuracy over time.

In practice, continuous learning can be implemented through online learning, where the model is updated incrementally as new data becomes available. Alternatively, models can be retrained periodically using a batch of recent data. In both cases, the goal is to ensure the predictive monitoring system remains relevant and effective in a changing environment.[23]

5) Architecture for AI-Driven Predictive Monitoring

a) Data Collection Layer

The first layer of the predictive monitoring architecture is the data collection layer. This layer is responsible for gathering data from various sources within the IT infrastructure. Effective data collection is crucial for building accurate predictive models, as the quality and quantity of data directly impact the performance of AI and ML algorithms. Data collection tools such as Prometheus, Nagios, and Splunk are commonly used in this layer. These tools collect data from

servers, applications, network devices, and other components of the IT environment. They provide real-time monitoring capabilities, enabling the continuous data flow into the predictive monitoring system.[24][25][26]

b) Data Processing and Feature Engineering Layer

Once the data is collected, it moves to the data processing and feature engineering layer. This layer is responsible for cleaning, normalizing, and transforming the raw data into a format suitable for AI and ML analysis. The data processing involves removing inconsistencies, filling in missing values, and filtering out irrelevant information.

Feature engineering is a critical aspect of this layer. It involves selecting the most relevant features from the raw data and creating new features that can enhance the predictive power of the models. For example, a feature could be the average CPU usage over the past hour, or the rate of change in disk I/O over time. Well-designed features can significantly improve the accuracy and reliability of predictive models.[12][27][28]

c) AI/ML Model Layer

The AI/ML model layer is the core of the predictive monitoring architecture. This layer involves developing, training, and deploying AI and ML models that analyze the processed data and generate predictions. The choice of algorithms and model architectures depends on the monitoring system's specific requirements and the data's nature.

In this layer, models are trained using historical data to learn patterns and correlations that indicate potential system failures or performance issues. Once trained, these models are deployed in the monitoring environment, continuously analyzing real-time data and providing predictions. The AI/ML model layer is designed to be flexible and scalable, allowing for the integration of new models and the adaptation to changing IT environments.[29][30]

d) Prediction and Alerting Layer

The prediction and alerting layer is where the AI/ML models' outputs are translated into actionable insights. In this layer, predictions are evaluated, and if certain thresholds are met, alerts are generated for the IT team. Alerts can be delivered through various channels like email, SMS, or integrated IT service management (ITSM) platforms like ServiceNow.

In addition to generating alerts, this layer can trigger automated actions based on the predictions. For example, suppose a model predicts that a server will likely fail within the next hour. In that case, the system can automatically initiate a failover to a backup server or scale up resources to prevent service disruption. This layer aims to ensure that potential issues are addressed before they impact operations, reducing downtime and improving system reliability.[31]

e) Feedback and Improvement Layer

The feedback and improvement layer is essential for maintaining the predictive monitoring system's effectiveness over time. This layer collects feedback from the predictions and actions taken, which is then used to refine and improve the AI and ML models.

Continuous feedback allows the models to learn from their predictions and adjust their behavior accordingly. For example, if a model consistently generates false positives, the feedback loop can help identify the root cause and adapt the model to reduce such occurrences. Similarly, if a model fails to predict a significant issue, the feedback loop can help identify gaps in the data or model that must be addressed.

This layer also involves retraining models with new data, ensuring that they remain accurate and relevant in a changing IT environment. By incorporating continuous feedback and improvement, the predictive monitoring system can evolve and adapt to new challenges, maintaining its effectiveness over the long term.[32][33][34]

4. Case Studies and Applications

a) Predictive Monitoring in Cloud Infrastructure

Cloud computing environments are highly dynamic, with resources allocated and deallocated based on demand. Predictive monitoring in cloud infrastructure helps manage resources efficiently, prevent outages, and ensure high availability.

For example, Amazon Web Services (AWS) uses predictive monitoring to anticipate hardware failures and automatically migrate workloads to healthy instances before disruption occurs. AI models analyze metrics such as CPU utilization, disk I/O, and network latency to predict potential issues. This proactive approach reduces downtime and improves the overall user experience by ensuring cloud services remain available and responsive.

Another application of predictive monitoring in cloud environments is autoscaling. AI models predict future demand based on historical data and current trends, allowing the system to automatically scale resources up or down as needed. This ensures that resources are used efficiently, reducing costs while maintaining performance.[35][36][37]

b) Predictive Maintenance in Data Centers

Data centers are the backbone of modern IT infrastructure, housing the servers and storage systems that power digital services. Predictive maintenance in data centers is critical for preventing hardware failures and minimizing downtime.

AI-driven predictive monitoring systems in data centers analyze data from sensors and logs to predict when components such as hard drives, power supplies, or cooling systems are likely to fail. For example, an AI model might analyze a hard drive's temperature, vibration, and error rates to predict when it is likely to fail. IT teams can replace the component before it fails, preventing data loss and service interruptions.

Predictive maintenance also helps optimize the lifecycle of data center equipment. By accurately predicting when components will fail, organizations can plan maintenance activities more effectively, reducing the need for costly emergency repairs and extending the lifespan of their equipment.[38][39]

c) AI-Powered Network Monitoring

Networks are the lifeblood of IT operations, connecting servers, applications, and users. Ensuring networks' reliability and performance is critical to any IT operation's success. AI-powered network monitoring uses predictive algorithms to detect and address potential issues before they impact users.

For instance, AI models can analyze network traffic patterns to identify anomalies indicating a security breach or a potential bottleneck. By predicting these issues in advance, the system can take proactive measures, such as rerouting traffic, adjusting bandwidth allocations, or applying security patches to prevent disruptions.

In addition to security and performance monitoring, AI-powered network monitoring can optimize network configurations. For example, AI models can predict the optimal routing paths for data packets, reducing latency and improving the network's overall performance.[40][41]

5. Challenges and Limitations

Future Directions

a) Integration with Edge Computing

Integrating AI-driven predictive monitoring with edge computing is a promising area for future research and development. Edge computing involves processing data closer to the source, such as on IoT devices or local servers, rather than in a centralized cloud environment.

By combining predictive monitoring with edge computing, organizations can reduce latency and improve the efficiency of their IT operations. For example, predictive models running on edge devices can analyze data in real-time, detecting and addressing potential issues immediately without relying on centralized systems. This approach is particularly valuable in industries such as manufacturing, healthcare, and autonomous vehicles, where real-time decision-making is critical.[42][43]

b) Advances in Explainable AI (XAI)

As the need for transparency in AI models grows, research in explainable AI is gaining momentum. Future predictive monitoring systems may incorporate XAI techniques to provide more interpretable and trustworthy predictions.

Explainable AI aims to make AI models more transparent by providing insights into how decisions are made. This can involve techniques such as feature importance analysis, model visualization, or generating human-readable explanations of model outputs. By incorporating XAI into predictive monitoring, organizations can increase user trust and improve the adoption of AI-driven systems.[44]

c) AI-Driven Automation

The future of predictive monitoring lies in AI-driven automation, where predictions trigger alerts and initiate automated responses. For example, AI models could automatically scale resources, restart services, or apply security patches based on predictions, reducing the need for manual intervention.

AI-driven automation can significantly enhance the efficiency and responsiveness of IT operations, allowing organizations to manage increasingly complex environments with fewer resources. As AI and ML technologies continue to advance, the scope and capabilities of automated predictive monitoring will expand, enabling more sophisticated and effective IT management.

d) Enhanced Cybersecurity Monitoring

With the increasing threat of cyberattacks, AI and ML will play a crucial role in predictive cybersecurity monitoring. Predictive models can analyze network traffic, user behavior, and system logs to identify potential vulnerabilities and predict the likelihood of a security breach.

Future predictive monitoring systems will incorporate advanced AI techniques to detect and mitigate cyber threats in real-time. For example, AI models could predict the likelihood of a phishing attack based on email patterns or identify potential insider threats by analyzing user behavior. By proactively addressing security risks, organizations can protect their IT systems and data from malicious actors.[45]

6. Conclusion

AI and Machine Learning have revolutionized predictive monitoring in IT operations, offering a proactive approach to managing complex infrastructures. Organizations can anticipate and mitigate potential issues by leveraging data-driven models, ensuring higher system reliability, optimized resource utilization, and reduced operational costs. However, challenges such as data quality, model interpretability, and integration with legacy systems must be addressed to realize the potential of AI-driven predictive monitoring fully. As the field continues to evolve, future advancements in edge computing, explainable AI, and automation will further enhance the capabilities and adoption of predictive monitoring in IT operations [66].

This detailed exploration highlights the transformative potential of AI and ML in predictive monitoring, offering a roadmap for organizations seeking to enhance their IT operations through advanced technologies. By embracing these innovations, businesses can achieve greater efficiency, reliability, and resilience in an increasingly complex digital landscape [67].

References

[1] P. Kubiak and S. Rab, "An Overview of Data-Driven Techniques for IT-Service-Management," *Institute of Electrical and Electronics Engineers*, vol. 6, pp. 63664-63688, 2018.

[2] J. Bogatinovski, S. Nedelkoski, A. Acker, F. Schmidt, T. Wittkopp, S. Becker, J. Cardoso, and O. Kao, "Artificial Intelligence for IT Operations (AIOPS) Workshop White Paper," *Cornell University*, 2021.

[3] J. Chen, C. P. Lim, K. H. Tan, K. Govindan, and A. Kumar, "Artificial intelligence-based human-centric decision support framework: an application to predictive maintenance in asset management under pandemic environments," *Springer Science+Business Media*, 2021.

[4] W. Pourmajidi, J. Steinbacher, T. Erwin, and A. Miranskyy, "On Challenges of Cloud Monitoring," *Cornell University*, 2018.
[5] I. Teinemaa, N. Tax, M. de Leoni, M. Dumas, and F. M. Maggi, "Alarm-Based Prescriptive Process Monitoring," *Cornell University*, 2018.
[6] C. Connelly, B. Cox, T. Forell, R. Liu, D. Milojičić, A. Nemeth, P. Piet, S. Shivanna, and W. Wang, "Reiki: Serviceability Architecture and Approach for Reduction and Management of Product Service Incidents," 2009.
[7] P. Venkateswaran, A. Malapati, M. Natu, and V. Sadaphal, "Towards next-generation alert management of data centers," 2016.
[8] H. Mao, T. Zhang, and Q. Tang, "Research Framework for Determining How Artificial Intelligence Enables Information Technology Service Management for Business Model Resilience," *Multidisciplinary Digital Publishing Institute*, vol. 13, no. 20, pp. 11496-11496, 2021.
[9] Y. Ran, X. Zhou, P. Lin, Y. Wen, and R. Deng, "A Survey of Predictive Maintenance: Systems, Purposes and Approaches," *Cornell University*, 2019.
[10] F. Salfner, M. Lenk, and M. Malek, "A survey of online failure prediction methods," *Association for Computing Machinery*, vol. 42, no. 3, pp. 1-42, 2010.
[11] A. Metzger, P. Leitner, D. Ivanović, E. Schmieders, R. Franklin, M. Carro, S. Dustdar, and K. Pohl, "Comparing and Combining Predictive Business Process Monitoring Techniques," *Institute of Electrical and Electronics Engineers*, vol. 45, no. 2, pp. 276-290, 2015.
[12] S. Basak, S. Sengupta, and A. Dubey, "Mechanisms for Integrated Feature Normalization and Remaining Useful Life Estimation Using LSTMs Applied to Hard-Disks," *Cornell University*, 2018.
[13] A. Pathak, "Study of Machine learning Algorithms for Stock Market Prediction," *International Research Publication House*, vol. V9, no. 06, 2020.
[14] S. Cateni, V. Colla, and M. Vannucci, "Outlier Detection Methods for Industrial Applications," 2008.
[15] M. Donoval, F. Kieran, J. Duggan, E. Howley, and E. Barrett, "A reinforcement learning approach for dynamic selection of virtual machines in cloud data centres," 2016.
[16] N. Tax, I. Verenich, M. La Rosa, and M. Dumas, "Predictive Business Process Monitoring with LSTM Neural Networks," *Springer Science+Business Media*, pp. 477-492, 2017.
[17] Y. Ran, X. Zhou, P. Lin, Y. Wen, and R. Deng, "A Survey of Predictive Maintenance: Systems, Purposes and Approaches," *Cornell University*, 2019.
[18] N. Davari, B. Veloso, G. de Assis Costa, P. Pereira, R. P. Ribeiro, and J. Gama, "A Survey on Data-Driven Predictive Maintenance for the Railway Industry," *Multidisciplinary Digital Publishing Institute*, vol. 21, no. 17.
[19] K. Feldman, L. Faust, X. Wu, C. Huang, and N. V. Chawla, "Beyond Volume: The Impact of Complex Healthcare Data on the Machine Learning Pipeline," *Springer Science+Business Media*, pp. 150-169, 2017.
[20] J. A. M. Sidey-Gibbons and C. Sidey-Gibbons, "Machine learning in medicine: a practical introduction," *BioMed Central*, vol. 19, no. 1, 2019.
[21] T. Diethe, T. Borchert, E. Thereska, B. Balle, and N. D. Lawrence, "Continual Learning in Practice," *Cornell University*, 2019.
[22] M. Bohlke-Schneider, S. Kapoor, and T. Januschowski, "Resilient Neural Forecasting Systems," *Cornell University*, 2022.
[23] C. Alippi, G. Boracchi, M. Roveri, G. Ditzler, and R. Polikar, "Adaptive Classifiers for Nonstationary Environments," pp. 265-288, 2015.
[24] R. Khan and S. U. Khan, "Design and implementation of an automated network monitoring and reporting back system," *Elsevier BV*, vol. 9, pp. 24-34, 2018.
[25] S. R. Sreeja and S. Chaudhari, "Study on Grid Resource Monitoring and Prediction," *Elsevier BV*, vol. 45, pp. 815-822, 2015.
[26] M. Sahasrabudhe, M. Panwar, and S. Chaudhari, "Application performance monitoring and prediction," 2013.
[27] S. Izrailev and J. M. Stanley, "Machine Learning at Scale," *Cornell University*, 2014.
[28] E. W. Fulp, G. Fink, and J. Haack, "Predicting computer system failures using support vector machines," pp. 5-5, 2008.
[29] W. S. Dong, "AIOps Architecture in Data Center Site Infrastructure Monitoring," *Hindawi Publishing Corporation*, vol. 2022, pp. 1-12, 2022.
[30] S. Parsaeefard, I. Tabrizian, and A. Leon-Garcia, "Artificial Intelligence as a Service (AI-aaS) on Software-Defined Infrastructure," 2019.
[31] M. Toy, "High Availability Layers and Failure Recovery Timers for Virtualized Systems and Services," *Elsevier BV*, vol. 114, pp. 126-131, 2017.
[32] A. Ajayi, O. Akinyemi, and M. S. Kurdi, "Using Predictive Analytics for Asset Management: A Case Study of Early Warning Prediction Application," 2013.
[33] B. Lü, D. B. Durocher, and P. Stemper, "Online and nonintrusive continuous motor energy and condition monitoring in process industries," 2008.
[34] C. Ponsard, A. Majchrowski, and M. Goeminne, "Predicting Alarms through Big Data Analytics: Feedback from Industry Pilots," *Elsevier BV*, pp. 1-31, 2018.
[35] Y. Hu, B. Deng, and F. Peng, "Autoscaling prediction models for cloud resource provisioning," 2016.
[36] B. B. J.V. and D. Dharma, "HAS: Hybrid auto-scaler for resource scaling in cloud environment," *Elsevier BV*, vol. 120, pp. 1-15, 2018.
[37] E. G. Radhika, G. S. Sadasivam, and J. F. Naomi, "An Efficient Predictive technique to Autoscale the Resources for Web applications in Private cloud," 2018.
[38] Z. A. Bukhsh and I. Stipanović, "Predictive Maintenance for Infrastructure Asset Management," *IEEE Computer Society*, vol. 22, no. 5, pp. 40-45, 2020.
[39] J. J. Montero-Jiménez, S. Schwartz, R. Vingerhoeds, B. Grabot, and M. Salaün, "Towards multi-model approaches to predictive maintenance: A systematic literature survey on diagnostics and prognostics," *Elsevier BV*, vol. 56, pp. 539-557, 2020.

[40] M. A. Ridwan, N. A. Mohamed Radzi, F. Abdullah, and Y. E. Jalil, "Applications of Machine Learning in Networking: A Survey of Current Issues and Future Challenges," *Institute of Electrical and Electronics Engineers*, vol. 9, pp. 52523-52556, 2021.

[41] S. Chen, X. Chen, Z. Yao, J. Yang, Y. Li, and F. Wu, "Evolving Switch Architecture toward Accommodating In-Network Intelligence," *Institute of Electrical and Electronics Engineers*, vol. 58, no. 1, pp. 33-39, 2020.

[42] S. Becker, F. Schmidt, A. Gulenko, A. Acker, and O. Kao, "Towards AIOps in Edge Computing Environments," 2020.

[43] B. Soret, L. D. Nguyen, J. Seeger, A. Bröring, C. Ben Issaid, S. Samarakoon, A. Elgabli, V. Kulkarni, M. Bennis, and P. Popovski, "Learning, Computing, and Trustworthiness in Intelligent IoT Environments: Performance-Energy Tradeoffs," *Institute of Electrical and Electronics Engineers*, vol. 6, no. 1, pp. 629-644, 2022.

[44] L. H. Gilpin, D. Bau, B. Z. Yuan, A. Bajwa, M. Specter, and L. Kagal, "Explaining Explanations: An Overview of Interpretability of Machine Learning," *Cornell University*, 2018.

[45] S. K. Jagatheesaperumal, Q. Pham, R. Ruby, Z. Yang, C. Xu, and Z. Zhang, "Explainable AI Over the Internet of Things (IoT): Overview, State-of-the-Art and Future Directions," *IEEE Communications Society*, vol. 3, pp. 2106-2136, 2022.