

AI-Powered Fault Diagnosis in Network Infrastructure: State-of-the-Art and Emerging Trends

Sridevi Allu¹, Bose babu Ravula²,Yudhveer Kandukuri³, Khaja Moiezuddin Mohammed⁴, Rashmika Jalagam⁵, Sivaraju Kuraku⁶

¹AT&T - Lead AI/ML Engineer

²John Wiley & Sons, Inc., Principal

³Afiniti Inc., (Senior DBA and DevOps Engineer)

⁴Iqvia - Sr Data Engineer

⁵Matilda Cloud - Cloud Engineer/Python Developer

⁶University of Cumberlands, Cybersecurity, KY, USA

ABSTRACT

The rapid expansion of IoT, cloud services, and next-generation communication networks has introduced unprecedented complexity and heterogeneity into modern infrastructures, making effective fault diagnosis increasingly critical. Conventional approaches such as centralized monitoring, threshold-based alerts, and periodic inspections are often insufficient for detecting subtle anomalies, intermittent failures, and large-scale disruptions. Artificial Intelligence (AI) offers advanced, data-driven methods that enable proactive, adaptive, and predictive fault diagnosis, ensuring greater resilience and efficiency. Machine learning techniques, including unsupervised, supervised, and semi-supervised approaches, have been successfully applied to anomaly detection, fault classification, and predictive maintenance, providing improved accuracy and scalability. Deep learning architectures, such as Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) models, further enhance the recognition of complex temporal and spatial patterns in high-dimensional data. Reinforcement learning contributes additional benefits by enabling adaptive resource allocation and optimized fault recovery strategies in dynamic environments. Emerging trends highlight hybrid AI models, federated learning, edge intelligence, explainable AI, and digital twin-based monitoring, all of which contribute to robust, transparent, and intelligent infrastructures.

Keywords: Fault diagnosis, Artificial Intelligence, Machine learning, IoT networks, Wireless Sensor Networks, Intelligent infrastructure

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2026); DOI: 10.18090/samriddhi.v18i03.08

INTRODUCTION

Modern communication infrastructures are experiencing rapid growth driven by the proliferation of IoT devices, cloud services, mobile applications, and the increasing demand for seamless connectivity [1]. These infrastructures are characterized as having larger and more heterogeneous topologies, high data transfer rates, and differing communication protocols, and therefore their administration and support become highly demanding. The conventional network management frameworks that are based on a static monitoring and centralized control model cannot usually address the needs of scalability, adaptability, and resilience. With the networks becoming smart and service-oriented ecosystems, fault diagnosis of services becomes significantly reliable, with an effective fault diagnosis mechanism that is able to detect, localize, and recover failures within the

Corresponding Author: Sridevi Allu, AT&T - Lead AI/ML Engineer, e-mail: srideviallu14@gmail.com

How to cite this article: Allu, S., Ravula, B.B., Kandukuri, Y., Mohammed, K.M., Jalagam, R., Kuraku, S. (2026). AI-Powered Fault Diagnosis in Network Infrastructure: State-of-the-Art and Emerging Trends. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology*, 18(3), 103-112.

Source of support: Nil

Conflict of interest: None

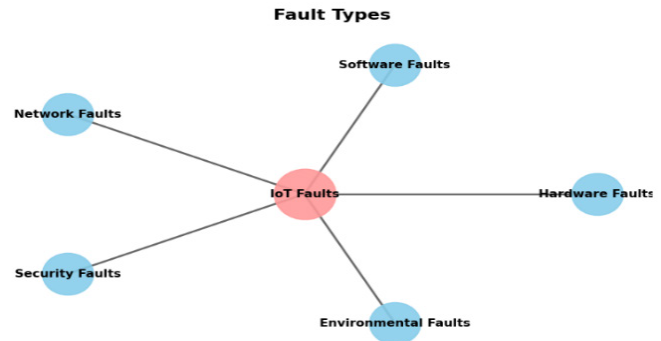
shortest time possible [2]. The distinction between faults (underlying causes) and failures (described as service disruptions) explains the significance of high level of precision in the diagnostic mechanisms of designing sound and reliable infrastructures [3].

The issue of fault diagnosis in network systems does not only relate to the detection of anomalies of the network system, but also the knowledge of their causes, elimination of their effects, and prevention of their recurrence [4]. The cause of faults may lie in the deterioration of hardware, software fluttering, misconfiguration, security attacks, external factors that may interfere with the operation and performance of services. Traditional methods are threshold, rule-based and periodic monitoring, which although easy to implement, can only work on large-scale, heterogeneous and dynamic networks [5]. They will overlook small deviations, failure incidents, and unscrupulous intrusions, leading to increased operation costs and loss of trust in online services. In this regard, therefore, more contemporary, automated and smarter solutions are required to provide efficiency, accuracy and durability of contemporary infrastructures.

Artificial Intelligence (AI) has been enabled as a paradigm enabler to such challenges by enabling the predictive, adaptive and scalable fault management. Machine learning, deep learning, and reinforcement learning are AI methods that are actively used in network fault diagnosis [6], which provide the possibility of real-time anomaly detection, pattern recognition, and proactive maintenance. Emerging approaches such as hybrid models, explainable AI, federated learning, and digital twin technologies further strengthen transparency, reliability, and resilience in fault management. By shifting from reactive troubleshooting to intelligent and proactive fault handling, AI-powered systems pave the way for robust, self-healing, and future-ready network infrastructures [7]. This positions AI-driven fault diagnosis as a cornerstone for sustaining intelligent digital ecosystems and next-generation communication networks.

Structure of the Paper

The paper is structured into six main sections. Section II examines fault types, causes, and limitations of conventional fault management approaches. Section III details AI-based approaches, covering ML, DL, and reinforcement learning techniques. The most recent approaches are covered in Section IV, along with current and future trends in the discipline. A thorough analysis of previous research is



presented in Section V. Finally, Section VI concludes the work and outlines directions for future research.

Fault Diagnosis in Networks

Network infrastructure fault diagnosis Network infrastructure fault diagnosis is detecting, analyzing, and correcting faults in devices, software, and communication links to ensure dependable network operations. As the modern networks are becoming more complex and heterogeneous, it is crucial to detect network failures [8], disruption of services and security breaches in time to prevent system failures. The network infrastructure is shown in Figure 1:

Network Infrastructure[9]

The primary goal is to have a strong infrastructure with interoperating protocols, monitoring tools, and managerial mechanisms to guarantee the continuous running of servers, routers, switches, and applications. Effective fault diagnosis can provide one with resilience, reduction of maintenance costs and guaranteed service provision. More and more it was supported by further technological advances in automated monitoring, diagnostic algorithms and predictive analytics which helped in the proactive fault management of a network environment.

Types of Faults in Networks

These types of failures that fault tolerance methods deal with are shown in Figure 2 which is shown below:

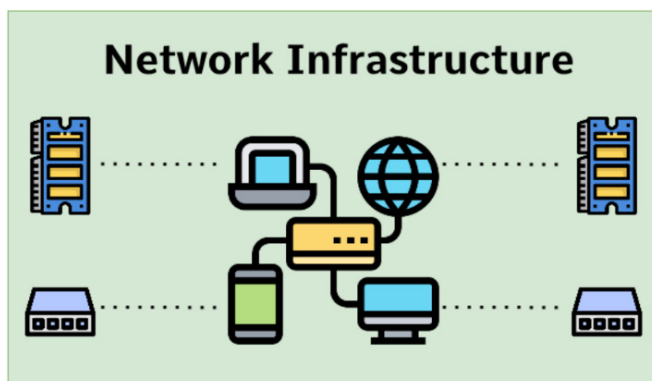
Types of the Fault

Hardware Faults

Such things as sensors, actuators, and network nodes can fail in this manner. Some of the usual mechanisms used to reduce their occurrence are redundancy and correcting errors.

Software Faults

The latter problems are associated with bugs or code errors in the software that governs Internet of Things (IoT) devices and applications. Software-based fault tolerance solutions are two, software rejuvenation, which is refreshing the software at periodic intervals to avoid malfunctions, and



rollback recovery, which is restoring the system to a previous state free of defects.

Network Faults

Some of these reasons include causes of lag, loss of packets and network connectivity interruptions. Nevertheless, FT solutions such as fault-tolerant network topologies and dynamic routing protocols provide a reliable network transfer of data [10].

Security Faults: The security faults are those faults when the IoT devices or networks are breached because of the weak security measures, unauthorized access, malware attacks, or denial-of-service. They may cause data breaches, sensor readings manipulation and general unavailability of the system.

Environmental Faults

These faults will be caused by the severe conditions of deployment (high or low temperatures, humidity, dust, vibrations, or radiation) that may cause damage to the IoT devices or decrease their accuracy. It is the case with such failures that lead to unreliable sensor data or full device malfunction.

Causes of Faults in IoT Infrastructure

Failure of IoT infrastructure comes about as a result of device complexities, communication connections, and system modules. The causes of these faults may be hardware degradation, unreliable sensors and actuators, software failures, network failures, human errors, and environmental factors. It is essential to identify the main sources of faults to create a strong IoT and introduce an efficient fault diagnosis system.

Hardware and Sensor Failures

IoT devices have a tendency to have failures due to processor, memory, or power supply problems [11]. Actuators and sensors are also more likely to fail because of wear or exposure to environmental factors or miscalibration and faults of nodes and sensors tend to coexist.

Communication and Network Faults

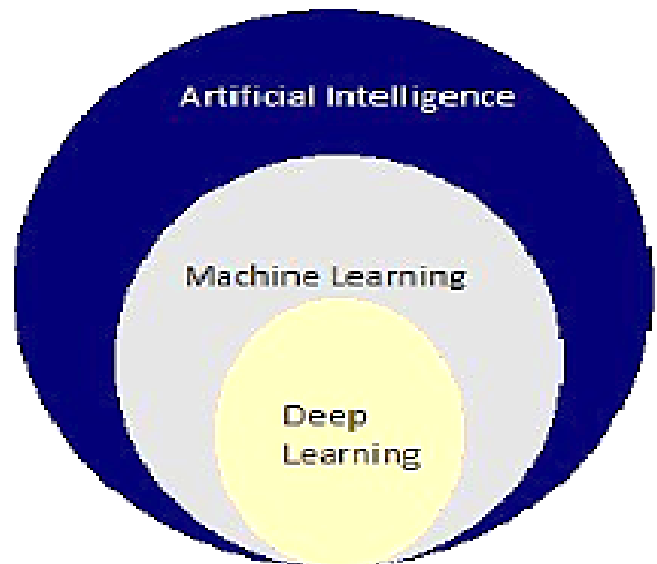
Signal loss, interference, protocol mismatch, or bandwidth constraints may cause failures during the transmission of data and network performance and may occur in gateways, base stations, sink nodes, or communication links.

Software and Human-Induced Faults

Software bugs, firmware incompatibility, misconfigurations, and insufficient maintenance are some of the factors that cause system faults and may increase hardware and network problems.

Limitations of Traditional Approaches

Some of the common traditional fault detection techniques in IoT such as centralized monitoring, threshold-based



alerts and periodic inspections have been extensively adopted because they are simple and easy to implement. Nonetheless, these solutions have difficulties in large-scale [12], heterogeneous networks and in the contemporary one. The key limitations are listed below:

The traditional centralized monitoring schemes are concentrated on fault detection at one node or server and thus prone to failure and unable to scale to large or distributed networks.

Threshold-based detection can usually fail to notice subtle variations or slow but steady performance deterioration, leading to the detection of faults later or later.

Periodic inspection of either manual or automation can fail to identify transient or intermittent faults, and it takes a lot of resources and time.

Traditional methods are not usually capable of supporting a network of heterogeneous sensors, actuators, and communication protocols and hence are restricted to use.

The unresponsive detection consumes both reliability of the system and increases the costs of maintenance and operational costs

Artificial Intelligence Approaches for Fault Diagnosis

AI plays a crucial role in fault diagnosis by enabling early detection, classification, and prediction of failures using historical and real-time data. Methods of ML, including unsupervised, supervised, and semi-supervised approaches, help identify anomalies and optimize predictive maintenance. Deep learning techniques enhance pattern recognition in complex data, while reinforcement learning supports adaptive fault management, ensuring reliability and resilience in dynamic network infrastructures. Figure 3 illustrates that DL is part of ML, which itself is a subset of the broader AI field.

Subsets of Artificial Intelligence[13]

Machine Learning Approaches

The AI technology in fault diagnosis in network infrastructure revolves around machine learning (ML) algorithms. Using historical and real-time network data in large amounts, these algorithms are capable of identifying anomalies, categorizing faults, and forecasting possible failures before they can disable operations. The most common ML algorithms applied in this field are:

Supervised Learning

Labelled datasets allow supervised learning algorithms to be trained with the outcome (such as success or failure) already known. In the presence of failure data from the past, these algorithms excel at predictive maintenance jobs because they learn to convert input data into the correct output. Common supervised learning techniques include:

Support Vector Machines (SVM)

Works well with binary classification issues, including determining whether a given equipment will break down in the course of a time period [14]. SVMs are also effective in high-dimensional spaces and they are resistant to overfitting (particularly where the training data is sparse).

Random Forests

An algorithm of ensemble learning that derives other decision trees and gives the average prediction of trees. Random Forests are specifically helpful dealing with nonlinear and complex relations in sensor or operational data and are less noise-sensitive.

Gradient Boosting Machines

The other ensemble technique constructs a sequence of weak learners (usually decision trees) one at a time. The new model aims at correcting mistakes of the old models and predicting equipment failures are highly predicted.

Unsupervised Learning

In the absence of labels, unsupervised learning algorithms scour unlabelled data for previously unseen structures, correlations, and patterns. This is why they are so valuable in predictive maintenance in situations when failure labels are hard to come by. Methods that are important for unsupervised learning include:

K-means Clustering

This is applied in order to cluster similar data points which can be used to determine the various operating conditions of an equipment and unusual behaviour that poses a precursor to a failure [15]. It is especially applicable in monitoring equipment that has several working modes where anomalies in regular clusters may indicate a malfunction.

Principal Component Analysis (PCA)

This is a dimensionality reduction method that converts sensor data with high dimensions into a smaller and uncorrelated feature set, to point out the most relevant patterns which might reveal possible faults. PCA is also useful in decreasing the computational complexity and noise in order to improve the efficiency of further analysis or modelling.

Autoencoders

This is a kind of neural network that is used in anomaly detection. Autoencoders are trained to recreate normal functioning behaviour, and variations between the reconstructions are identified as a possible anomaly. They are useful in detecting machinery faults early. They come in especially handy in events where data on faults labelled is scarce or not available.

Semi-Supervised Learning

Semi-supervised learning is a hybrid method involving the use of a limited number of labelled data and a larger data set which is unlabeled. This approach shines in industrial applications, where labeled data may prove expensive or time-consuming to obtain, or it may be labor-intensive. With its successful use of the large volume of unlabeled data, semi-supervised learning can enhance model accuracy, lessen labeling work, and further fault detection or predictive maintenance tasks and therefore is a viable solution to the real-world industrial setting.

Deep Learning Approaches

Predictive maintenance applications, especially those involving complicated data, have been greatly enhanced by DL, a kind of ML that relies on artificial neural networks [16], high-dimensional data from multiple sensors.

Convolutional Neural Networks (CNNs)

CNNs which were initially designed to process images have been used extensively in predictive maintenance to diagnose faults. They are able to process multi-sensor data as 2D or 3D input, analyze vibration or acoustic spectrograms, make automatic feature extraction of raw sensor data, allowing the accurate identification of equipment faults with little feature engineering by hand.

Recurrent Neural Networks (RNNs)

RNNs have found extensive application in network fault diagnosis due to their capability of modelling sequence data and the solution of temporal resolutions. RNNs have been useful in forecasting anomalies and tracking fault propagation because network traffic, network performance logs, and fault occurrences often exhibit time trends. Nevertheless, classic RNNs have problems such as vanishing gradient that inhibits their capacity to learn long-term correlations among complex network information.



Table 1: AI Methods for Fault Diagnosis in Network Infrastructure

<i>Method</i>	<i>Application</i>	<i>Key Features</i>	<i>Performance/ Findings</i>
SVM-BiLSTM (BiLSTM + SVM)	Gas Station IoT (GS-IoT) system	Analyzes operational process & human emotional reaction data; uses word segmentation mapping to low-dimensional space	Outperforms CNN, GRU, KBS, pure SVM, and BiLSTM in fault detection
BLSTM RNN	IoT network attack detection	Detects security faults; trained on UNSW-NB15 dataset	Achieves >95% accuracy in classifying normal and attack patterns
Random Forest	Wireless Sensor Networks (WSNs)	Evaluates classifiers using real-world datasets; metrics include True Positive Rate, MCC, F1-score	Random Forest showed highest fault detection rate among classifiers
SVM	Wireless Sensor Networks (WSNs)	Lightweight SVM at cluster heads for anomaly detection in resource-limited WSNs	Effective in detecting anomalous sensors in experimental study

Long Short-Term Memory (LSTM) Networks

LSTMs, which are a sophisticated form of RNN, solve the disadvantages of a traditional RNN by employing the memory cells and gating mechanisms to retain contextual information in the long term [17]. It has been shown that LSTMs are highly effective in discovering minute, but far-reaching relationships in fault diagnosis in both traffic and system behavior that enable faults to be discovered at an early stage and the prediction of potential faults. This is due to their high ability to process the noisy and dynamic network data, a feature that renders them very applicable in the area of real-time fault detection and proactive management.

Reinforcement Learning

Reinforcement learning (RL), a less popular method than supervised and unsupervised ones is gaining popularity as a method to diagnose and recover network faults. The RL can also optimize the fault recovery plans, resource allocation, and adaptive fault management using the trial-and-error interaction with the network environment. Its advantage is to enhance the resilience in the long term in complex, dynamic infrastructures. Nonetheless, practical deployment is constrained by issues like the need to have correct environment models, large-scale simulations and long training periods.

State-of-the-Art and Emerging Trends

Several current AI approaches for fault detection in network systems are summarized, leading methods, applications, and performance are illustrated, and how these techniques advance accuracy and reliability in IoT and WSNs.

For the purpose of fault detection in Gas Station Internet of Things (GS-IoT) system, Jiahao suggests a technique called SVM-BiLSTM, which combines a bidirectional BiLSTM network with a SVM. The technique uses a word segmentation method to convert data to a space with low dimensions, allowing it to analyse data pertaining to operational processes and human

emotional reaction behavioural mechanisms. The algorithm outperforms other methods like CNN, GRU, KBS, pure SVM, and BiLSTM in detecting faults [18].

Roy and Cheung, article introduces a new deep learning method for resolving security faults and detecting assaults in the IoT network. The method utilises a BLSTM RNN. Over 95% accuracy in attack detection is achieved by the model, which was trained using UNSWNB15 benchmark data. This demonstrates the model's efficacy in distinguishing attack and normal behaviours on the IoT network [19]. Noshad, study employs a variety of classifiers to identify problems in WSNs, which are susceptible to unpredictability in their settings. The researchers in this study evaluated their F1-score, True Positive Rate, Matthews Correlation Coefficients, and detection accuracy using datasets from the actual world. When compared to the other classifiers, the Random Forest (RF) algorithm identifies faults more frequently, according to the results [20]

Zidi, Moulahi and Alaya, discuss the challenges of fault detection in wireless sensor networks (WSNs) due to limited resources and diverse deployment fields. They propose the use of machine learning, specifically support vector machines (SVMs) classification method, which is lightweight and easy to execute at cluster heads to detect anomalous sensors. The effectiveness of SVM is demonstrated through an experimental study.[21]

Emerging Trends

Fault diagnosis based on AI is developing at a fast pace as network infrastructures grow more sophisticated. New trends are oriented on the accuracy, efficiency, and flexibility to fulfill the contemporary IoT and WSN demands.

Hybrid AI Models

The combination of techniques such as BiLSTM-SVM or CNN-LSTM is becoming more popular to both provide time and space characteristics of the network data and improve accuracy and strength of fault detection.

Table 2: Literature summary of AI-Powered Fault Diagnosis in Network Infrastructure

Reference	Study on	Key Findings	Challenges	Limitations	Future Work
Tertytchny & Michael (2020)	Instance-based dataset reduction for Intelligent Fault Detection (IFD) in IoT-based CPS	Dataset reduction up to 15.51% improves efficiency and average accuracy (17%) in classification models	Handling heterogeneous IoT data, scalability in real-world CPS	Evaluated only on two datasets; limited generalizability	Extend to real-time IoT fault detection; apply reduction techniques across diverse IoT domains
Gaddam et al. (2020)	Review of sensor fault, anomaly, and outlier detection in IoT	Highlighted sensor faults due to harsh environments, malicious attacks, and outliers; provided guidelines for selecting detection models	IoT differs from WSN frameworks; real-time adaptability	Mostly conceptual; lacks experimental validation in IoT settings	Develop robust outlier detection tailored for IoT; hybrid AI + edge processing solutions
Lo, Flaus & Adrot (2019)	AI approaches for fault diagnosis in complex systems (2002–2018)	AI enables automated diagnosis, supports self-maintenance in reconfigurable systems	Complexity of modern industrial systems; data availability	Focused on industrial systems, not network infrastructure	Apply AI-based diagnosis to emerging network systems (IoT, 5G, CPS)
Srinivasan et al. (2019)	ML-based link fault identification and localization (ML-LFIL) in IoT networks	ML models (SVM, MLP, RF) achieve high accuracy with reduced fault localization time	Differentiating link disconnections vs reconnections; passive monitoring challenges	Limited to Mininet experiments; may not scale to large dynamic IoT	Test on large-scale, real-world IoT/CPS; improve adaptability with deep learning
Casado-Vara et al. (2018)	Fault-tolerant IoT maintenance using predictive hybrid control	Proposed CTMC + cooperative control algorithm with virtual sensors for self-healing IoT	Real-time prediction and replacement of faulty nodes	Case study limited to smart supermarket; focus only on temperature monitoring	Extend to multi-parameter IoT monitoring; integrate AI-driven predictive fault diagnosis
Madapuzi et al., (2018)	ML-based traffic engineering (TE) approach for link failure detection in IoT and vehicular networks	Random Forest achieved $\geq 90\%$ accuracy in localizing link failures with lower delay	High overhead due to network complexity and dynamic topologies	Tested only in simulation (Mininet); limited node scaling	Explore deep learning for adaptive TE; apply to real vehicular/5G networks

Real-Time and Predictive Diagnosis

AI models are currently giving special attention to the proactive detection of faults that are going to happen. This minimizes the network downtimes, maintenance expenses and enhances reliability of critical systems.

Edge AI and Federated Learning

Decentralized AI models enable learning on the device and sharing knowledge on the networks. This minimizes the latency, maintains privacy and enables real-time detection in a distributed IoT environment.

Explainable AI (XAI)

Open AI models can also give information as to why faults are found, which enhances confidence, responsibility, and allows administrators to make effective choices in automated fault management environments.

LITERATURE REVIEW

The literature review addresses artificial intelligence-based fault diagnosis of IoT and network systems, the approaches

to sensor and link failure detection, limitations, challenges, and current trends, and refers to scalable, real-time, and intelligent solutions to the current network infrastructures.

Tertytchny and Michael (2020) introduce an AI system for reducing Intelligent Fault Detection (IFD) datasets in Cyber-Physical Systems (CPS) built on the IoT. While the framework will reduce the quantity of data required for training, it will also reduce the accuracy required for testing. Lightweight IFD approaches for embedded devices are made possible by this, which saves processing time and storage space for trained models. Experimental testing on two datasets revealed that the proposed framework outperformed the classification algorithms under consideration by an average of 17% and a margin of up to 15.51% [22]

Gaddam et al. (2020) research on IoTs emphasises the increasing significance of AI in identifying physical world sensor problems, anomalies, and outliers. The IoT is already fast becoming a digital nervous system of the world, with millions of individuals and businesses implementing smart sensors and advanced communication tools in the IoT. However, such sensors are often applied in difficult



conditions, which could lead to inaccurate measurements known as outliers. Poor research has been done within the setting of IoTs where the existing research is aimed at developing models of Wireless Sensor Networks (WSN) to identify anomalies and sensor faults. The use of AI and ML models in the IoT may lead to the diminution of the quality of data received, thereby leading to aberrant processes or outliers [23]

Lo, Flaus and Adrot (2019) highlight the fact that automated fault diagnosis in complex systems is on the rise and uses AI methods. This can be used in self-maintenance and reduce the cost of production, especially in reconfigurable systems, which AI can assist with. Based on the idea of using Machine Learning technologies as a center of interest, the study has systematized the studies on artificial intelligence approaches to problem diagnosis in industrial systems that took place between 2002 and 2018 [24]

Srinivasan et al. (2019) created a passive way of addressing the issue of locating and detecting link faults within networks like the Internet of Things. They developed a 3-step ML-LFIL framework that trains traffic behaviour during a normal working environment as well as the link failures under different environmental situations. To train the learning component of the model, random forests, multilayer perceptrons and support vector machines are applied. The results reveal that ML-LFIL is a viable tool in fault localisation of networks, as it has an excellent accuracy with significantly reduced time in fault localisation compared to other active probing tools [25]

Casado-Vara et al. (2018) proposed a new method of IoT network maintenance and reliability through cooperative control algorithm using the continuous-time Markov chains as a predictive hybrid control model. In order to ensure reliable monitoring and control, the algorithm regenerates broken nodes by replacing broken sensors with new ones. The model has been proven to be effective through a case study, and it is employed to ensure proper temperature monitoring of an intelligent supermarket [26]

Madapuzi et al. (2018) proposed a traffic engineering approach based on machine learning to detect and pinpoint link failures in complex communication networks. The model learns the behaviour of network traffic passively, taking into account factors such as average packet loss, number of flows, and propagation latency. The approach employs a variety of methods, including decision trees, logistic regression, support vector machines, naive Bayes, and random forests. At least 90% of link failures can be localised using this method, according to experiments conducted on the Mininet platform [27]

Table I shows the major focus on AI-based fault diagnosis in IoT and network infrastructure, the list of research works, key findings, challenges, limitations, and future directions, including the focus on scalability, real-time implementation, and data-driven and intelligent solutions.

CONCLUSION AND FUTURE WORK

Artificial Intelligence has rapidly transformed fault diagnosis in network infrastructures by providing intelligent, scalable, and proactive solutions. Traditional centralized and rule-based methods, although simple, struggle to address the demands of modern IoT-driven ecosystems that require real-time adaptability and resilience. AI-enabled models, unsupervised, spanning supervised, and semi-supervised learning, enhance anomaly detection, predictive maintenance, and fault classification with higher accuracy and efficiency. DL approaches like CNNs, RNNs, and LSTMs have demonstrated superior performance in recognizing complex temporal and spatial patterns within large-scale network data. Reinforcement learning further contributes by enabling adaptive recovery strategies and optimizing resource allocation in dynamic environments. The growing shift toward hybrid AI models, explainable AI, federated learning, and digital twins indicates a promising future where infrastructures can self-diagnose and self-heal while ensuring transparency and trust. Edge-based AI solutions also highlight the movement toward low-latency, privacy-preserving, and decentralized fault management. Future research should focus on large-scale deployment, integration with 5G/6G technologies, and the creation of lightweight yet robust AI models for resource-constrained IoT devices. Developing explainable, interoperable, and adaptive frameworks will be vital for ensuring resilient, intelligent, and secure network infrastructures capable of supporting increasingly complex digital ecosystems.

REFERENCES

- [1] G. Kakkavas, D. Gkatzoura, V. Karyotis, and S. Papavassiliou, "A Review of Advanced Algebraic Approaches Enabling Network Tomography for Future Network Infrastructures," *Futur. Internet*, vol. 12, no. 2, 2020, doi: 10.3390/fi12020020.
- [2] S. S. S. Neeli, "Optimizing Database Management with DevOps: Strategies and Real-World Examples," *J. Adv. Dev. Res.*, vol. 11, no. 1, 2020.
- [3] D. D. Rao, "Multimedia-Based Intelligent Content Networking for Future Internet," in *2009 Third UKSim European Symposium on Computer Modeling and Simulation*, 2009, pp. 55–59. doi: 10.1109/EMS.2009.108.
- [4] S. S. S. Neeli, "Real-Time Data Management with In-Memory Databases: A Performance-Centric Approach," *J. Adv. Dev. Res.*, vol. 11, no. 2, p. 8, 2020.
- [5] P. C. Fonseca and E. S. Mota, "A Survey on Fault Management in Software-Defined Networks," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2284–2321, 2017, doi: 10.1109/COMST.2017.2719862.
- [6] A. Balasubramanian, "Proactive Machine Learning Approach to Combat Money Laundering in Financial Sectors," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, pp. 1–15, 2019, doi: 10.5281/zenodo.14508474.
- [7] A. Balasubramanian and N. Gurushankar, "AI-Driven Supply Chain Risk Management : Integrating Hardware and Software for Real-Time Prediction in Critical Industries," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 8, no. 3, 2020, doi: 10.5281/zenodo.14565873.

- [8] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, no. March, pp. 10–28, 2017, doi: 10.1016/j.jnca.2017.04.002.
- [9] S. K. Yellanki, "Smart Services and Network Infrastructure: Building Seamless Digital Ecosystems," *Glob. Res. Dev. ISSN 2455-5703*, vol. 1, no. 12, pp. 1–23, 2016.
- [10] A. Adya, P. Bahl, R. Chandra, and L. Qiu, "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks," in *Proceedings of the 10th annual international conference on Mobile computing and networking*, 2004, pp. 30–44.
- [11] J. Hare, X. Shi, S. Gupta, and A. Bazzi, "A review of faults and fault diagnosis in micro-grids electrical energy infrastructure," in *2014 IEEE Energy Conversion Congress and Exposition (ECCE)*, IEEE, Sep. 2014, pp. 3325–3332. doi: 10.1109/ECCE.2014.6953852.
- [12] F. Benayas, A. Carrera, and C. A. Iglesias, "Towards an autonomic Bayesian fault diagnosis service for SDN environments based on a big data infrastructure," in *2018 Fifth International Conference on Software Defined Systems (SDS)*, IEEE, Apr. 2018, pp. 7–13. doi: 10.1109/SDS.2018.8370415.
- [13] S. V. N. S. and P. M., "An Empirical Science Research On Bioinformatics In Machine Learning," *J. Mech. Contin. Math. Sci.*, vol. spl7, no. 1, Feb. 2020, doi: 10.26782/jmcms.spl.7/2020.02.00006.
- [14] A. Mahapatro and P. M. Khilar, "Fault Diagnosis in Wireless Sensor Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2000–2026, 2013, doi: 10.1109/SURV.2013.030713.00062.
- [15] B. Dong, Z. O'Neill, and Z. Li, "A BIM-enabled information infrastructure for building energy Fault Detection and Diagnostics," *Autom. Constr.*, vol. 44, pp. 197–211, 2014.
- [16] D. Minovski, E. Rondeau, and J.-P. Georges, "Monitoring the energy consumed by a network infrastructure to detect and isolate faults in communication architecture," in *Technology for Smart Futures*, Springer, 2017, pp. 219–234.
- [17] T. Adimulam, M. Bhojar, and P. Reddy, "AI-Driven Predictive Maintenance in IoT-Enabled Industrial Systems," *Iconic Res. Eng. ...*, vol. 2, no. 11, pp. 398–410, 2019.
- [18] Y. Jiahao, X. Jiang, S. Wang, K. Jiang, and X. Yu, "SVM-BiLSTM: A Fault Detection Method for the Gas Station IoT System Based on Deep Learning," *IEEE Access*, vol. 8, pp. 203712–203723, 2020, doi: 10.1109/ACCESS.2020.3034939.
- [19] B. Roy and H. Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," in *2018 28th International Telecommunication Networks and Applications Conference, ITNAC 2018*, 2018. doi: 10.1109/ATNAC.2018.8615294.
- [20] Syed, M. H., Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., Shyam, D., & Manoharan, P. (2025). Enhancing Retail Sector Customer Engagement Through the Application of Modern and Intelligent AI-Driven Analytical Techniques. *International Journal of Humanities and Information Technology*, 7(01), 19–26.
- [21] Shyam, D., Manoharan, P., Syed, M. H., Ragireddy, U. K., Addepalli, P. V., & Bandaru, S. R. (2025). An AI-Driven Classification System for Early Detection of Customer Churn in E-Commerce Platforms. *Journal of Computer Science and Technology Studies*, 7(11), 452–462.
- [22] Bandaru, S. R., Shyam, D., Manoharan, P., Syed, M. H., Ragireddy, U. K., & Addepalli, P. V. (2025). Customer Sentiment Analysis for Online Shopping Platforms Using NLP and Deep Learning Methods. *Journal of Cyber-Physical Security and Robotics*, 1(02), 1–11.
- [23] Mylavarapu, K. B., Pilli, J., Jannu, P. K., Mohammad, J. A., Panchali, S. H., & Kavirayani, U. M. (2025). An Enhanced Intrusion Detection Architecture Using ML-Based Anomaly Detection on Large-Scale Data. *International Journal of Humanities and Information Technology*, 7(01), 20–26.
- [24] Panchali, S. H., Mylavarapu, K. B., Pilli, J., Jannu, P. K., & Mohammad, J. A. (2025). Review of Secure Communication Systems for Cyber-Physical Systems and Industrial IoT. *Journal Of Engineering And Computer Sciences*, 4(6), 349–362.
- [25] Pilli, J., Jannu, P. K., Mohammad, J. A., Panchali, S. H., Kavirayani, U. M., & Mylavarapu, K. B. (2025). Data-Driven Artificial intelligence (AI)-based System for Identifying Fraudulent Telephony Activities. *Journal of Cyber-Physical Security and Robotics*, 1(02), 23–31.
- [26] Jannu, P. K., Mohammad, J. A., Panchali, S. H., Kavirayani, U. M., Mylavarapu, K. B., & Pilli, J. (2025). A Review of Sensor Data Acquisition Methods for Accurate and Timely Detection of Faults in Mechanical Systems. *Journal of Computer Science and Technology Studies*, 7(9), 796–803.
- [27] Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., Dasari, A., & Chilakapati, V. K. (2025). Emerging Communication Technologies for IoT: 5G and Edge Networking Perspectives. *International Journal of Humanities and Information Technology*, 7(01), 19–28.
- [28] Dasari, A., Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., & Pathani, A. K. (2025). Transforming Undergraduate Education Through Modern Pedagogical Innovations. *Journal of Computer Science and Technology Studies*, 7(12), 547–556.
- [29] Pathani, A. K., Dasari, A., Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., & Kavuluri, H. V. R. (2025). Big Data and Cloud Computing Integration: A Review of Scalable Information Retrieval Techniques. *Journal of Cyber-Physical Security and Robotics*, 1(02), 12–22.
- [30] Suresh, A. (2025). AI-Driven Business Intelligence Automation: Integrating Data Engineering, Auto-BI, and Large Language Models. *International Journal of AI, BigData, Computational and Management Studies*, 6(3), 97–108. <https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I3P112>
- [31] Suresh, A. (2025). Conversational Analytics Using LLMs: Transforming Enterprise Data Consumption through Natural Language Interfaces. *American International Journal of Computer Science and Technology*, 7(5), 92–102. <https://doi.org/10.63282/3117-5481/AIJCST-V7I5P108>
- [32] Syed, M. H., Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., Shyam, D., & Manoharan, P. (2026). AI-Powered Data Analytics for Strengthening Customer Loyalty and Personalization in Retail. *Journal of Data Analysis and Critical Management*, 2(01), 28–36.
- [33] Manoharan, P., Syed, M. H., Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., & Shyam, D. (2026). A Review of Digital Tools and Technologies for Enhancing Customer Engagement in Financial Services. *Journal of Contemporary Science and Technology Management*, 2(01), 13–25.
- [34] Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., Shyam, D., Manoharan, P., & Syed, M. H. (2026). Predictive Customer Segmentation in Retail Using Machine Learning and Behavioral Analytics. *European Journal of Applied Science, Engineering and Technology*, 4(2), 268–278.
- [35] Suresh, "Architectural Design of LLM- Powered Conversational BI Systems for High-Volume Enterprise Data Warehouses,"



- 2026 International Conference on Machine Learning and Autonomous Systems (ICMLAS), Bangkok, Thailand, 2026, pp. 1333-1341, doi: 10.1109/ICMLAS67792.2026.11483861.
- [36] Taluri, R. (2024). A Hybrid Data Engineering and Generative AI Architecture for Intelligent Data Governance, Metadata Management, and Automated Data Quality Assessment on AWS. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, 5(2), 230-240. <https://doi.org/10.63282/3050-9262.IJAIDSML-V5I2P126>
- [37] Suresh, A. (2024). Auto-BI Frameworks Powered by Generative Artificial Intelligence for Scalable Self-Service Data Analytics in Large Organizations. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, 5(3), 191-201. <https://doi.org/10.63282/3050-9262.IJAIDSML-V5I3P119>
- [38] Taluri, R. (2024). A Cloud-Native Reference Architecture for Data Engineering, Generative AI, and Decision Intelligence Using AWS and Amazon Bedrock. *International Journal of AI, BigData, Computational and Management Studies*, 5(1), 218-227. <https://doi.org/10.63282/3050-9416.IJAIDCMS-V5I1P122>
- [39] Suresh, A. (2025). AI-Driven Business Intelligence Automation: Integrating Data Engineering, Auto-BI, and Large Language Models. *International Journal of AI, BigData, Computational and Management Studies*, 6(3), 97-108. <https://doi.org/10.63282/3050-9416.IJAIDCMS-V6I3P112>
- [40] Taluri, R. (2021). Cloud-Native Architectures for Enterprise Financial Data Management, Analytics, and Regulatory Reporting Compliance. *International Journal of Emerging Trends in Computer Science and Information Technology*, 2(2), 101-111. <https://doi.org/10.63282/3050-9246.IJETSIT-V2I2P112>
- [41] Suresh, A. (2025). Conversational Analytics Using LLMs: Transforming Enterprise Data Consumption through Natural Language Interfaces. *American International Journal of Computer Science and Technology*, 7(5), 92-102. <https://doi.org/10.63282/3117-5481/AIJCSIT-V7I5P108>
- [42] Taluri, R. (2022). Cloud Data Engineering Strategies for Large-Scale Financial Data Integration and Intelligent Corporate Performance Reporting. *International Journal of Emerging Research in Engineering and Technology*, 3(4), 176-188. <https://doi.org/10.63282/3050-922X.IJERET-V3I4P119>
- [43] Jannu, P. K., Mohammad, J. A., Panchali, S. H., Kavirayani, U. M., Mylavarapu, K. B., & Pilli, J. (2026). Recent Advances in Anomaly Identification for IoT Devices Using Machine and Deep Learning Models. *Journal of Data Analysis and Critical Management*, 2(01), 37-47.
- [44] Mylavarapu, K. B., Pilli, J., Jannu, P. K., Mohammad, J. A., Panchali, S. H., & Kavirayani, U. M. (2026). Early Diagnosis of Heart Conditions Using AI-Driven on Electronic Health Data. *Journal of Contemporary Science and Technology Management*, 2(01), 26-37.
- [45] Pilli, J., Jannu, P. K., Mohammad, J. A., Panchali, S. H., Kavirayani, U. M., & Mylavarapu, K. B. (2026). A Survey on Power Optimization Techniques in Contemporary Mobile SoC Architectures. *European Journal of Applied Science, Engineering and Technology*, 4(2), 321-333.
- [46] Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., & Dasari, A. (2026). A Survey on Generative AI Chatbots in Customer Service: Challenges, Benefits, and Use Cases. *Journal of Data Analysis and Critical Management*, 2(01), 17-27.
- [47] Pathani, A. K., Dasari, A., Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., & Kavuluri, H. V. R. (2026). Transforming Customer Support with AI: Emerging Tools, Trends and Their Service Effectiveness. *Journal of Contemporary Science and Technology Management*, 2(01), 1-12.
- [48] Dasari, A., Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., & Pathani, A. K. (2026). Applications of Machine Learning in Predicting Customer Churn in Telecommunications: A Review Analysis. *European Journal of Applied Science, Engineering and Technology*, 4(2), 257-267.
- [49] Kumar, A., Wadhwa, M., Kalla, D., Konduru, S. C., Nandawat, C., & Sharma, M. (2025, October). Benchmarking the Trade-Offs in Object Detection: Accuracy, Speed, and Energy Efficiency. In *International Conference on Artificial Intelligence and Networking* (pp. 410-422). Cham: Springer Nature Switzerland.
- [50] NR, A. R., Rajasri, T., Praveen, R., Kalla, D., Bendale, S. P., & Venu, N. (2025, April). CAC Training-A Unified Cybersecurity Training Program for Military Staff. In *2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI)* (Vol. 3, pp. 569-573). IEEE.
- [51] Kalla, D., Kuraku, D. S., & Samaah, F. (2021). Enhancing cyber security by predicting malwares using supervised machine learning models. *International Journal of Computing and Artificial Intelligence*, 2(2), 55-62.
- [52] Zeeshan, M., Bhadauria, K., Pahal, L., Nagrath, P., & Kalla, D. (2025, June). Ensemble-Based Deep Learning for Automated Diabetic-Retinopathy Detection Using CNNs and Transfer Learning. In *International Conference on Data Analytics & Management* (pp. 216-228). Cham: Springer Nature Switzerland.
- [53] Aggarwal, A., Agarwal, L., Rella, B. P. R., Nagpal, N., Kalla, D., & Sharma, M. (2025, June). A Performance Comparison of Machine Learning Models for Rain Prediction. In *International Conference on Data Analytics & Management* (pp. 319-328). Cham: Springer Nature Switzerland.
- [54] Nagrath, P., Saini, I., Zeeshan, M., Komal, Komal, & Kalla, D. (2025, June). Predicting Mental Health Disorders with Variational Autoencoders. In *International Conference on Data Analytics & Management* (pp. 38-51). Cham: Springer Nature Switzerland.
- [55] NR, A. R., Rajasri, T., Praveen, R., Kalla, D., Bendale, S. P., & Venu, N. (2025, April). CAC Training-A Unified Cybersecurity Training Program for Military Staff. In *2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI)* (Vol. 3, pp. 569-573). IEEE.
- [56] Kalla, D., Smith, N., Samaah, F., & Polimetla, K. (2024). Hybrid scalable researcher recommendation system using azure data lake analytics. *Journal of Data Analysis and Information Processing*, 12, 76-88.
- [57] Kumar¹, A., Wadhwa¹, M., Kalla, D., Konduru, S. C., Nandawat, C., & Sharma, M. (2026, May). Benchmarking the Trade-Offs in Object Detection: Accuracy, Speed, and Energy. In *Proceedings of International Conference on Artificial Intelligence and Networks: ICAIN 2025, Volume 4* (Vol. 4, p. 410). Springer Nature.
- [58] A. Suresh, "Large Language Models for Explainable and Self-Service Business Intelligence in Large Enterprises," 2026 6th International Conference on Expert Clouds and Applications (ICOECA), Bengaluru, India, 2026, pp. 1571-1578, doi: 10.1109/ICOECA68095.2026.11485058.
- [59] A.Suresh, "A Comprehensive Study on Auto - BI Systems using Generative AI for Scalable and Explainable Enterprise Analytics," 2026 6th International Conference on Expert Clouds and Applications (ICOECA), Bengaluru, India, 2026, pp. 1579-1585, doi: 10.1109/ICOECA68095.2026.11485569.
- [60] Krishnappa, K. H., R, M., & Chavan, L. (2026). ML-Driven Automated Functional Verification Framework for Digital

- Designs. *Electronics*, 15(12), 2687.
- [61] Kalla, D., & Samaah, F. (2023). Exploring Artificial Intelligence And Data-Driven Techniques For Anomaly Detection In Cloud Security. Available at SSRN 5045491.
- [62] Suresh, "Architectural Design of LLM- Powered Conversational BI Systems for High-Volume Enterprise Data Warehouses," 2026 International Conference on Machine Learning and Autonomous Systems (ICMLAS), Bangkok, Thailand, 2026, pp. 1333-1341, doi: 10.1109/ICMLAS67792.2026.11483861.
- [63] Vadisetty, R., Polamarasetti, A., Varadarajan, V., Kalla, D., & Ramanathan, G. K. (2025, May). Cyber Warfare and AI Agents: Strengthening National Security Against Advanced Persistent Threats (APTs). In International Conference on Intelligence-Based Transformations of Technology and Business Trends (pp. 578-587). Cham: Springer Nature Switzerland.
- [64] Z. Noshad *et al.*, "Fault Detection in Wireless Sensor Networks through the Random Forest Classifier," *Sensors*, vol. 19, no. 7, 2019, doi: 10.3390/s19071568.
- [65] S. Zidi, T. Moulahi, and B. Alaya, "Fault Detection in Wireless Sensor Networks Through SVM Classifier," *IEEE Sens. J.*, vol. 18, no. 1, pp. 340–347, 2018, doi: 10.1109/JSEN.2017.2771226.
- [66] G. Tertytchny and M. K. Michael, "Dataset Reduction Framework For Intelligent Fault Detection In IoT-based Cyber-Physical Systems Using Machine Learning Techniques," in 2020 International Conference on Omni-layer Intelligent Systems (COINS), 2020, pp. 1–6. doi: 10.1109/COINS49042.2020.9191393.
- [67] A. Gaddam, T. Wilkin, M. Angelova, and J. Gaddam, "Detecting Sensor Faults, Anomalies and Outliers in the Internet of Things: A Survey on the Challenges and Solutions," *Electronics*, vol. 9, no. 3, 2020, doi: 10.3390/electronics9030511.
- [68] N. G. Lo, J.-M. Flaus, and O. Adrot, "Review of Machine Learning Approaches in Fault Diagnosis applied to IoT Systems," in 2019 International Conference on Control, Automation and Diagnosis (ICCAD), 2019, pp. 1–6. doi: 10.1109/ICCAD46983.2019.9037949.
- [69] S. M. Srinivasan, T. Truong-Huu, and M. Gurusamy, "Machine Learning-Based Link Fault Identification and Localization in Complex Networks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6556–6566, 2019, doi: 10.1109/JIOT.2019.2908019.
- [70] R. Casado-Vara, Z. Vale, J. Prieto, and J. M. Corchado, "Fault-Tolerant Temperature Control Algorithm for IoT Networks in Smart Buildings," *Energies*, vol. 11, no. 12, 2018, doi: 10.3390/en1123430.
- [71] S. Madapuzi Srinivasan, T. Truong-Huu, and M. Gurusamy, "TE-Based Machine Learning Techniques for Link Fault Localization in Complex Networks," in 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), 2018, pp. 25–32. doi: 10.1109/FiCloud.2018.00012.

