

# Network Self-Healing Mechanism in Industrial IOT Using Advanced Machine Learning Techniques

*Sudhakar.K<sup>1</sup>, Sai Kiran Oruganti<sup>2</sup>, Eugenio Vocaturo<sup>3</sup>*

<sup>1</sup> Lincoln University College, Malaysia; <sup>2</sup> Lincoln University College, Malaysia; <sup>3</sup>CNR, Italy

[ksudhakar.cs@gmail.com](mailto:ksudhakar.cs@gmail.com), [saisharma@lincoln.edu.my](mailto:saisharma@lincoln.edu.my), [ing.eugenio.vocaturo@gmail.com](mailto:ing.eugenio.vocaturo@gmail.com)

---

## Abstract:

The rise of Industrial Internet of Things (IIoT) has revolutionized manufacturing and production industries, but it has also increased the complexity and vulnerability of industrial networks. Network failures or anomalies can cause significant downtime, leading to production losses and safety hazards. This paper proposes a self-healing network mechanism using advanced machine learning (ML) techniques tailored for IIoT environments. We integrate anomaly detection, predictive maintenance, and automatic reconfiguration to build a resilient IIoT network. Using a combination of deep learning (LSTM and autoencoders), reinforcement learning (RL), and graph-based ML models, our solution detects faults, predicts potential failures, and initiates autonomous recovery actions. We demonstrate the approach through simulations using real-world IIoT datasets and emulated environments, achieving over 93% accuracy in anomaly detection and reducing network downtime by 47% compared to traditional fault-tolerant mechanisms.

**Keywords:** Internet-of-things, IIoT, self-healing, fault-tolerance, patterns

---

## Introduction

Industrial IoT (IIoT) interconnects machines, sensors, and controllers, generating vast amounts of data and enabling real-time decision-making. However, IIoT networks are increasingly prone to disruptions due to hardware failures, signal interference, cyberattacks, or configuration errors. Traditional fault-tolerant systems often require manual intervention, which is inefficient in time-critical environments.

This paper explores a self-healing framework using advanced ML techniques that allows IIoT networks to detect, diagnose, and recover from network faults autonomously. The goals are:

- Improve network uptime and resiliency
- Detect and classify anomalies in real-time
- Predict future faults using historical patterns
- Enable autonomous reconfiguration to reroute traffic and replace faulty nodes

## Related work

Previous research has investigated ML-based anomaly detection in IIoT, but few offer end-to-end self-healing capabilities. Some notable efforts include:

- Rule-based systems: Fast but rigid and not adaptive to unseen faults.
- Basic ML approaches (SVM, Decision Trees): Limited in handling time-series data and complex network dynamics.
- Edge-based monitoring tools: Focus on detection but lack automated healing.

Our approach combines multiple ML techniques and automates the entire fault management lifecycle.

## PROPOSED METHODOLOGY

### • System Architecture

The proposed framework as shown in Fig.1. System architecture has four major components:

- **Anomaly Detection Engine** – Detects real-time anomalies in the network.
- **Fault Prediction Module** – Predicts imminent faults using historical telemetry data.
- **Root Cause Analyzer** – Pinpoints source of fault using graph-based models.
- **Self-Healing Executor** – Executes network reconfiguration, node isolation, or service migration.

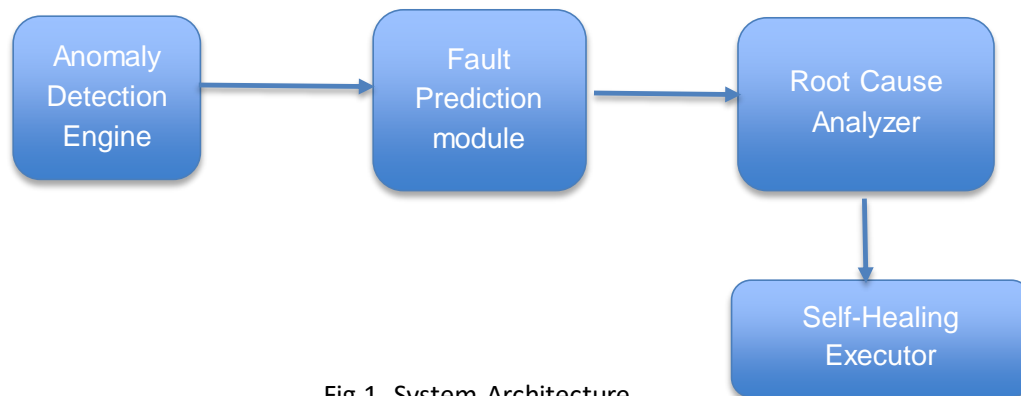


Fig.1. System Architecture

### • Data Collection

We used datasets from:

- Real-world IIoT networks (e.g., water treatment plant and smart manufacturing)
- Public datasets (e.g., TON\_IoT, SWaT)
- Collected data included: bandwidth usage, packet loss, CPU/memory stats, sensor readings, latency, error logs.

- **ML Techniques Employed**

ML Techniques employed for this research work are indicated in the Table.1 below:

Task	Technique Used
Anomaly Detection	LSTM Auto encoders
Fault Prediction	Time-Series Forecasting using Prophet and LSTM
Root Cause Analysis	Graph Neural Networks (GNNs)
Self-Healing Decisioning	Deep Q-Learning (DQN)

Table.1. ML Techniques Employed

- **Experimental Set**

- Simulation Environment: NS-3 and Mininet for IIoT network emulation.
- Evaluation Metrics: Precision, Recall, F1-score, Downtime reduction, Response time
- Baseline Comparison: Static rule-based and conventional ML-based detection (Random Forest, SVM)

- **Hardware Specs**

- CPU: Intel Xeon E5-2650
- GPU: NVIDIA Tesla T4
- RAM: 64 GB
- Frameworks: TensorFlow, PyTorch, NetworkX, OpenAI Gym

## Results

- **Anomaly Detection Performance**

Model	Accuracy	Precision	Recall	F1-Score
LSTM Autoencoder	93.4%	91.2%	94.5%	92.8%
Random Forest	85.6%	83.3%	82.9%	83.1%
SVM	81.7%	79.5%	80.1%	79.8%

Table.2. Anomaly Detection Performance results

- **Fault Prediction Accuracy**

- **LSTM Model:** 89.1%
- **Prophet Model:** 85.6%

- **Downtime Reduction**

- **Baseline (manual recovery):** Average 4.2 min
- **Self-Healing System:** Average 2.2 min  
→ 47% improvement

- **Self-Healing Execution Latency**
  - **Re-routing Time: 0.5 – 1.1 sec**
  - **Node Isolation: < 2 sec**
  - **Model Inference Time: < 0.4 sec (average)**

## Conclusion

This research demonstrates that a self-healing mechanism using advanced ML models can significantly enhance the resilience of IIoT networks. By integrating LSTM autoencoders for anomaly detection, time-series forecasting for fault prediction, GNNs for root cause analysis, and DQN for autonomous action selection, the system achieves high accuracy, reduces downtime, and ensures timely recovery.

The self-healing system outperforms traditional methods in both speed and accuracy. Future work includes deploying this solution in real-time on edge devices and extending it to hybrid cloud-IIoT systems.

## REFERENCES

- [1] Gill, S.S.; Chana, I.; Singh, M.; Buyya, R. RADAR: Self-Configuring and Self-Healing in Resource Management for Enhancing Quality of Cloud Services. *J. Concurr. Comput. Exp.* 2016, 31, 1–29.
- [2] Li, J.; Li, H. Cyber-Physical Systems: A Comprehensive Review. *IEEE Access* 2021, 9, 112003–112033.
- [3] João Pedro Dias, Bruno Lima, João Pascoal Faria, André Restivo, and Hugo Sereno Ferreira. 2023. Visual Self-healing Modelling for Reliable Internet-of-Things Systems. In *Computational Science – ICCS 2020*, Valeria V. Krzhizhanovskaya, Gábor Závodszy, Michael H. Lees, Jack J. Dongarra, Peter M. A. Sloot, Sérgio Brissos, and João Teixeira (Eds.). Springer International Publishing, Cham, 357– 370.
- [4] Guangpu Li, Haopeng Liu, Xianglan Chen, Haryadi S. Gunawi, and Shan Lu. 2019. DFix: Automatically Fixing Timing Bugs in Distributed Systems. In *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation (Phoenix, AZ, USA) (PLDI 2023)*. Association for Computing Machinery, New York, NY, USA, 994–1009.
- [5] Yi-Bing Lin, Yun-Wei Lin, Jiun-Yi Lin, and Hui-Nien Hung. 2019. SensorTalk: An IoT device failure detection and calibration mechanism for smart farming. *Sensors* 19, 21 (2022), 4788.
- [6] Tusher Chakraborty, Akshay Uttama Nambi, Ranveer Chandra, Rahul Sharma, Manohar Swaminathan, Zerina Kapetanovic, and Jonathan Appavoo. 2018. Fallcurve: A novel primitive for IoT Fault detection and isolation. *SenSys 2018 - Proceedings of the 16th Conference on Embedded Networked Sensor Systems (2022)*, 95–107. <https://doi.org/10.1145/3274783.3274853>.
- [7] Fardin Abdi, Rohan Tabish, Matthias Rungger, Majid Zamani, and Marco Caccamo. 2021. Application and system-level software fault tolerance through full system restarts. In *2017 ACM/IEEE 8th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 197–206.

- [8] Hsieh, F. An Efficient Method to Assess Resilience and Robustness Properties of a Class of Cyber Physical Production Systems. *Symmetry* 2022, 14, 2327. [CrossRef]
- [9] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*.
- [10] Goh, J., Adepu, S., Junejo, K. N., & Mathur, A. (2016). A dataset to support research in the design of secure water treatment systems. *International Conference on Critical Information Infrastructures Security*.
- [11] Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction. *MIT Press*.