Journal of Trends in Computer Science and Smart Technology (ISSN: 2582-4104)
www.irojournals.com/tcsst/

The Role of Anomaly Detection in Industry 4.0: A Survey of Techniques and Applications

D Vishnu Prasad[1], S Saraswathi[2]

[1]Research Scholar, Department of Information Technology, Puducherry Technological University, Puducherry 605 014, India

[2]Professor, Department of Information Technology, Puducherry Technological University, Puducherry 605 014, India

Email: [1]vishnuprasad@pec.edu, [2]s.saraswathi@ptuniv.edu.in

Abstract

The integration of IIoT devices into Industry 4.0 marks a major shift towards smarter and more interconnected industrial processes. However, this progress also introduces intricate security vulnerabilities, specifically stemming from the emergence of anomalies that have the potential to undermine the dependability and efficiency of these advanced systems. Within the realm of Industry 4.0, this research undertakes a comprehensive examination of suitable anomaly detection techniques for IIoT devices. The study systematically analyzes the efficacy, scalability, and flexibility of various detection techniques, such as machine learning algorithms, hybrid approaches, and statistical models, in identifying and mitigating possible risks to IIoT environments. The investigation uncovers valuable insights into the performance of these techniques across various operational scenarios, shedding light on their advantages and constraints. This research examines the practical consequences of implementing these methods in real-life situations, emphasizing the crucial significance of anomaly detection in upholding the durability and dependability of Industry 4.0 systems. Through an extensive comparative examination, this research seeks to offer guidance to researchers, professionals,

DOI: https://doi.org/10.36548/jtcsst.2024.2.003
Received: 03.04.2024, received in revised form: 23.04.2024, accepted: 06.05.2024, published: 15.05.2024

and policymakers in choosing and executing efficient anomaly detection approaches, thus promoting the progress and safeguarding of IIoT ecosystems.

Keywords: Anomaly Detection, Industrial Internet of Things (IIoT), Cybersecurity, Statistical Techniques, Machine Learning, Industry 4.0, Hybrid Detection Systems, Scalability, Operational Dynamics, Application Scenarios

1. Introduction

Industry 4.0 represents a significant advancement in the digital transformation of industrial domains. This breakthrough combines cutting-edge technologies like artificial intelligence, machine learning, and the Industrial Internet of Things (IIoT) to produce incredibly efficient and automated systems. However, protecting IIoT device cybersecurity becomes crucial, particularly in light of any anomalies that can compromise operational integrity. As such, anomaly detection becomes an essential component of protecting these systems, necessitating a thorough comprehension of different methodologies and their applicability in the context of the IIoT. The Industrial Internet of Things (IIoT) is a core aspect of Industry 4.0, representing the integration of interconnected smart devices into industrial processes. IIoT connects various machines, sensors, and devices through a unified network that collects, analyzes, and responds to data in real-time. Industry 4.0 leverages the potential of IIoT by combining it with artificial intelligence, machine learning, and automation to create smarter and more efficient manufacturing environments.

1.1 Industry 4.0 and the Industrial Internet of Things (IIOT)

The Industrial Internet of Things (IIoT) transforms industries by connecting sensors, devices, and systems to improve efficiency, production, and safety via real-time data analysis, predictive maintenance, and automation, thereby reducing downtime and human error. System interoperability and strict cybersecurity are required. The IIoT is a fundamental element of Industry 4.0, often referred to as the Fourth Industrial Revolution. It merges digital technology with actual production, including artificial intelligence (AI), big data analytics, cloud computing, cybersecurity, and robotics. Industry 4.0 aims to digitize production by using digital innovations to increase industrial processes' productivity, efficiency, and flexibility.

1.2 Security Threats in Industry 4.0

The Industrial Internet of Things (IIoT) has revolutionized the way industries operate by bringing significant improvements in efficiency, productivity, and flexibility to key industrial operations. However, this interconnectedness also presents several security vulnerabilities that could jeopardize the reliability, security, and privacy of industrial systems. The main security risks associated with the IIoT are cyber-physical attacks, man-in-the-middle attacks, data breaches, malware and ransomware, denial of service (DoS), zero-day exploits, insider threats, supply chain vulnerabilities, insecure interfaces and APIs, insufficient encryption, and inadequate authentication.

1.3 Components of IIOT In Industry 4.0

IIoT systems in Industry 4.0 comprise several critical components:

- **Sensors and Devices:** Devices like temperature, humidity, and vibration sensors collect real-time data on operational conditions.
- **Communication Networks:** Wired (Ethernet) and wireless (5G, Zigbee) networks connect sensors and devices to a central processing system using protocols like MQTT (Message Queuing Telemetry Transport) and OPC UA (Open Platform Communications Unified Architecture).
- **Edge and Cloud Computing:** Edge devices provide real-time data processing, while cloud platforms store and analyze data.
- **Cybersecurity Infrastructure:** Firewalls, intrusion detection systems, and encryption protect data integrity.
- **Analytics Platforms:** Big data frameworks like Hadoop and Spark, along with machine learning and deep learning frameworks such as TensorFlow and PyTorch, enable advanced data analysis.

1.4 Role of Anomaly Detection in Industry 4.0

Anomaly detection plays a crucial role in maintaining the security and reliability of Industry 4.0 systems. It involves identifying patterns or behaviors that deviate from the norm, indicating potential threats like cyber-attacks or equipment malfunctions. Techniques range

from simple statistical models to advanced machine learning algorithms. Accurate anomaly detection ensures minimal downtime, enhanced cybersecurity, and optimal performance in smart manufacturing systems.

1.5 Anomaly Detection Techniques in IIOT

- **Statistical Models:** Methods like Z-score and moving averages identify data points that deviate significantly from historical trends.
- **Machine Learning Approaches:** Supervised learning models (e.g., SVM, Random Forest) classify known anomalies, while unsupervised models (e.g., k-means clustering) detect unknown anomalies.
- **Deep Learning Models:** Autoencoders, Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks handle complex and high-dimensional data effectively.
- **Hybrid Methods:** Combining statistical models with machine learning or deep learning improves detection accuracy.

2. Related Works

Recent advancements in deep learning methods have significantly enhanced anomaly detection in Industry 4.0. The following research in Table 1 and 2 highlights various techniques used in anomaly detection:

Table 1. Analysis of Existing Techniques to Detect Anomalies

Sl.No	Reference	Techniques	Threat type	Merits	Demerits
1	(Benaddi et al. 2022)	Distributional RL and GAN	Cyber attacks	Balances data, improves minority attack detection	GAN training complexity

2	(Cai et al. 2022)	Content-Agnostic Payload-Based Model	Application-layer attacks	Efficient in application layer detection	Limited to specific protocol anomalies
3	(DeMedeiros, Hendawi, and Alvarez 2023)	AI-based Techniques Survey	General	Comprehensive overview, identifies gaps	No new model proposed
4	(Feng et al. 2022)	Full Graph Autoencoder	Group anomalies	Handles irregular structures, robust	May not generalize to all IIoT environments
5	(Gyamfi and Jurcut 2023)	OI-SVDD, AS-ELM	Network intrusions	Lightweight, real-time detection	May require frequent updates
6	(Khan et al. 2022)	Deep Learning (Autoencoder, CNN)	Cyber threats	Explainability, effective feature extraction	Requires large datasets
7	(Kong et al. 2023)	Generative Adversarial Networks, LSTM	Time-series anomalies	High detection accuracy, handles unlabeled data	Computationally intensive
8	(Bin Mofidul et al. 2022)	AI-Integrated Secured IIoT	Energy data anomalies	Secured infrastructure, real-time monitoring	Specific to energy data
9	(Nizam et al. 2022)	CNN-LSTM Autoencoder	Time-series data anomalies	Real-time processing, edge computing integration	High resource requirement on edge devices
10	(Wang et al. 2022)	Hierarchical Federated Learning	Cybersecurity threats	Privacy-preserving, high accuracy	Complexity in implementation
	(Yang et al.	Stacked	Intrusion	Efficient	Limited to one-

11	2023)	OCBLS	detection	training, captures high-level features	class scenarios
12	(Yazdinejad et al. 2022)	Federated Learning	Blockchain-based network attacks	Privacy preservation, decentralized	Blockchain complexity
13	(Wu et al. 2023)	In-Network Computing	Acoustic data interference	Accelerates data separation, reduces latency	Implementation complexity
14	(Qi et al. 2022)	Isolation Forest, LSH, PCA	Multiaspect data anomalies	Effective in dynamic data, fast	May miss complex anomalies
15	(Velasquez et al. 2022)	Hybrid ML Ensemble	Real-time systems	Improved accuracy, real-time detection	Complexity in tuning ensemble weights
16	(Karadayi, Aydin, and Öğ˘renci 2020)	CNN-LSTM Autoencoder	Multivariate data anomalies	Extracts features from multivariate spatio-temporal datasets	Requires high computational resources
17	(Maggipinto, Beghi, and Susto 2022)	Deep Convolutional Autoencoder	Industrial manufacturing faults	Robust anomaly detection in semiconductor manufacturing	Limited to specific manufacturing processes
18	(Salam et al. 2023)	Transformer-based Model	Web-based cyber-attacks	High accuracy, precision, and recall	High computational resources required

Table 2. Best Techniques to Detect Anomalies

Techniques	Description	Key Features	Application Area
Deep Learning Frameworks (XAI)	Utilize complex data processing	Interpret model decisions, Attention Mechanism	Broad applicability in IoT and sensor networks
Hierarchical Federated Learning	Distributed learning strategy	Scalability, privacy preservation	Suitable for decentralized IoT environments
Bidirectional LSTM and Attention	Enhances sequence data processing	Superior handling of time-series data	Effective in IoT anomaly detection
Distributional RL & GANs	RL approach with GANs	Innovative detection, synthetic data	Robust detection against sophisticated anomalies

3. Case Studies / Real-World Applications

3.1 Anomaly Detection in Manufacturing Plant Using Edge Computing

A large manufacturing plant struggled with unplanned downtime due to sudden equipment failures. They implemented an anomaly detection system based on edge computing to monitor critical machinery in real-time. Sensors collected data on vibration, temperature, and operational conditions, which edge devices processed using isolation forest and autoencoder models. The models identified unusual patterns and alerted the maintenance team before critical failures occurred. This solution reduced unplanned downtime by 30%, improved maintenance scheduling, and optimized resource allocation, demonstrating the value of anomaly detection in predictive maintenance. The Figure 1. depicts the architecture of anomaly detection in a manufacturing plant.

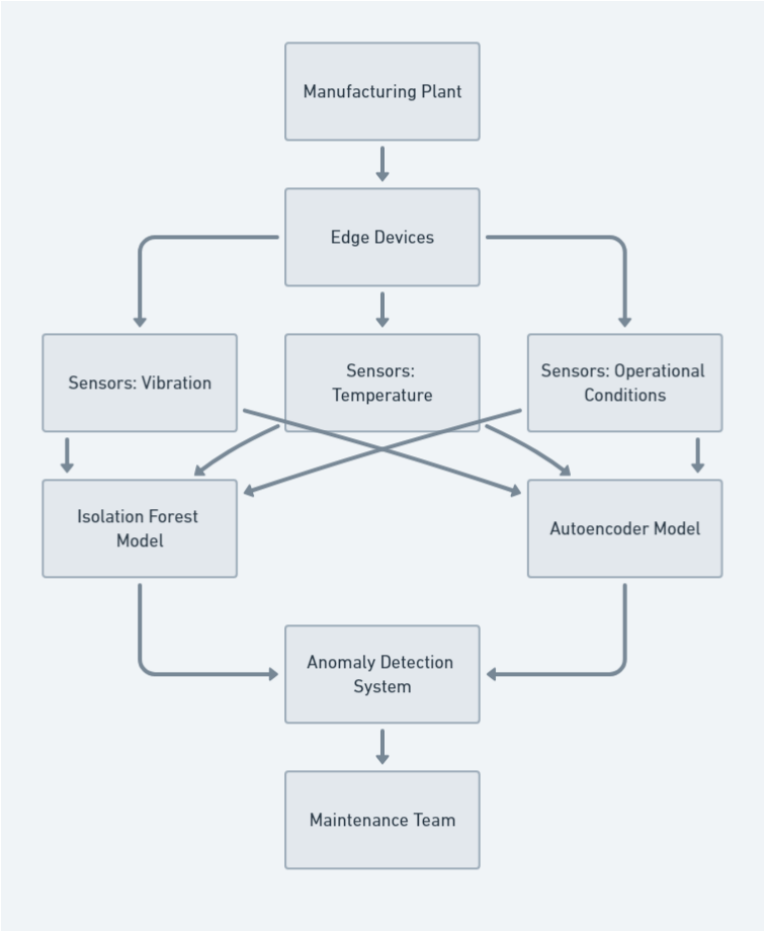

Figure 1. Architecture of Anomaly Detection in a Manufacturing Plant

3.2 Network Intrusion Detection in Smart Grid Infrastructure

A smart grid infrastructure faced frequent Distributed Denial of Service (DDoS) attacks that threatened to disrupt power distribution. The organization deployed a hybrid anomaly detection framework combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to detect unusual traffic patterns. The framework integrated with existing firewalls and intrusion detection systems to provide a comprehensive security solution. By leveraging both statistical and deep learning models, the system improved detection accuracy by 40% and reduced false positives to just 3%. This case study highlights the importance of anomaly detection in safeguarding critical infrastructure. The Figure 2. Illustrates the architecture of smart grid infrastructure anomaly detection.

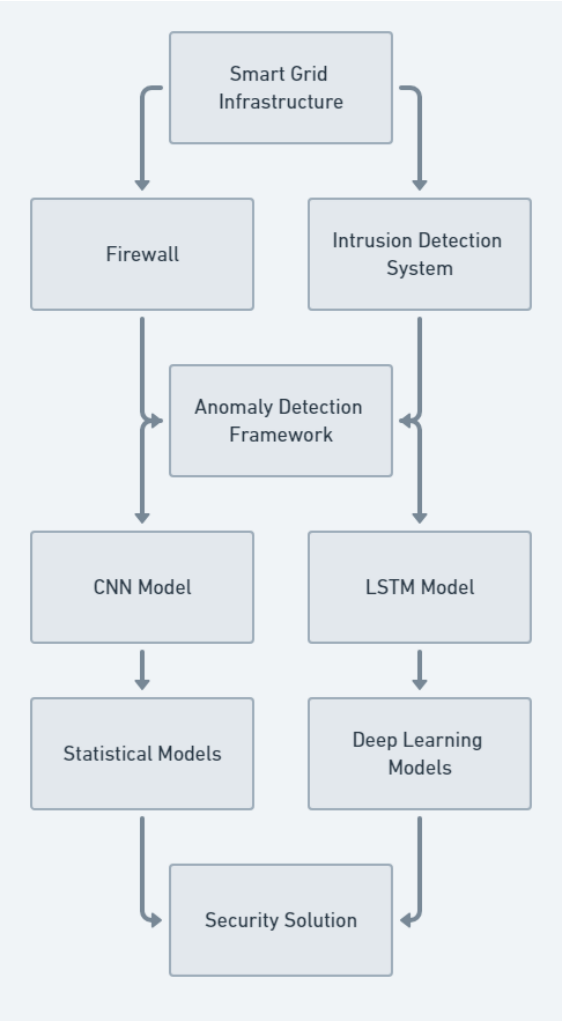

Figure 2. Architecture of Smart Grid Infrastructure Anomaly Detection

4. Contributions

This paper provides a comprehensive survey of anomaly detection techniques in Industry 4.0, analyzing their strengths and weaknesses across various operational scenarios. By identifying gaps in scalability, explainability, and accuracy, this research offers practical recommendations for deploying anomaly detection frameworks in real-world IIoT environments. The comparative analysis of statistical, machine learning, and hybrid models serves as a valuable guide for researchers, practitioners, and policymakers in enhancing IIoT security.

5. Challenges in Existing Anomaly Detection Techniques

5.1 Scalability and Real-Time Processing

Challenge: High data volume and velocity require real-time analysis.

Solution: Edge computing and distributed learning models can reduce latency and process data efficiently.

5.2 Complexity of IIoT Environments

Challenge: Diverse devices, heterogeneous data sources, and dynamic network topologies complicate anomaly detection.

Solution: Hybrid models combining statistical and machine learning approaches, along with transfer learning techniques, can improve detection accuracy.

5.3 Lack of Labeled Data

Challenge: Limited labeled data hinders the training of supervised models.

Solution: Semi-supervised learning and synthetic data generation with Generative Adversarial Networks (GANs) can augment labeled datasets.

6. Solutions to Address the Challenges

6.1 Federated Learning and Distributed Anomaly Detection: Decentralized training across multiple edge devices preserves data privacy and reduces computational costs.

6.2 Explainable AI Frameworks: Attention mechanisms and explainable AI models improve interpretability, making anomaly detection decisions more transparent.

6.3 Synthetic Data Generation with GANs: GANs generate synthetic anomaly data to augment training datasets, improving model robustness and accuracy.

7. Future Directions and Recommendations

7.1 Privacy-Preserving Frameworks: Blockchain and federated learning can ensure data security and privacy.

7.2 Collaborative Anomaly Detection: Shared intelligence across organizations enhances detection capabilities.

7.3 Hybrid and Multi-Stage Models: Combining multiple techniques can improve detection rates and reduce false positives.

8. Conclusion

This survey has investigated a range of sophisticated deep learning frameworks and methodologies for anomaly detection in Industrial IIOT devices, demonstrating the significant potential for these methods to enhance the accuracy, dependable nature, and efficiency of anomaly identification in complex, high-dimensional data settings. Specifically, the incorporation of explainable AI (XAI) and attention methods into deep learning frameworks is a noteworthy development that provides enhanced anomaly detection processes with more transparency and interpretability in addition to better performance. The need for effective, precise, and comprehensible anomaly detection systems will only increase with the proliferation of IoT devices and their massive data generation. The importance of deep learning approaches in addressing these problems is emphasized in this overview study, which also lays the groundwork for upcoming developments that will raise the bar for anomaly detection for IoT and sensor networks.

References

[1] Benaddi, H ;, M ; Jouhari, K ; Ibrahimi, Othman Ben, Hafsa Benaddi, Mohammed Jouhari, Khalil Ibrahimi, Jalel Ben Othman, and El Mehdi Amhoud. 2022. “Anomaly Detection in Industrial IoT Using Distributional Reinforcement Learning and Generative Adversarial Networks.” Sensors 2022, Vol. 22, Page 8085 22 (21): 8085. https://doi.org/10.3390/S22218085.

[2] Cai, Jun, Qi Wang, Jianzhen Luo, Yan Liu, and Liping Liao. 2022. “CapBad: Content-Agnostic, Payload-Based Anomaly Detector for Industrial Control Protocols.” IEEE Internet of Things Journal 9 (14): 12542–54. https://doi.org/10.1109/JIOT.2021.3138534.

[3] DeMedeiros, Kyle, Abdeltawab Hendawi, and Marco Alvarez. 2023. “A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks.” Sensors 2023, Vol. 23, Page 1352 23 (3): 1352. https://doi.org/10.3390/S23031352.

[4] Feng, Yong, Jinglong Chen, Zijun Liu, Haixin Lv, and Jun Wang. 2022. “Full Graph Autoencoder for One-Class Group Anomaly Detection of IIoT System.” IEEE Internet of Things Journal 9 (21): 21886–98. https://doi.org/10.1109/JIOT.2022.3181737.

[5] Gyamfi, Eric, and Anca Delia Jurcut. 2023. “Novel Online Network Intrusion Detection System for Industrial IoT Based on OI-SVDD and AS-ELM.” IEEE Internet of Things Journal 10 (5): 3827–39. https://doi.org/10.1109/JIOT.2022.3172393.

[6] Karadayi, Yildiz, Mehmet N. Aydin, and A. Selçuk Öğ˘renci. 2020. “A Hybrid Deep Learning Framework for Unsupervised Anomaly Detection in Multivariate Spatio-Temporal Data.” Applied Sciences 2020, Vol. 10, Page 5191 10 (15): 5191. https://doi.org/10.3390/APP10155191.

[7] Khan, Izhar Ahmed, Nour Moustafa, Dechang Pi, Karam M. Sallam, Albert Y. Zomaya, and Bentian Li. 2022. “A New Explainable Deep Learning Framework for Cyber Threat Discovery in Industrial IoT Networks.” IEEE Internet of Things Journal 9 (13): 11604–13. https://doi.org/10.1109/JIOT.2021.3130156.

[8] Kong, Fanhui, Jianqiang Li, Bin Jiang, Huihui Wang, and Houbing Song. 2023. “Integrated Generative Model for Industrial Anomaly Detection via Bidirectional LSTM and Attention Mechanism.” IEEE Transactions on Industrial Informatics 19 (1): 541–50. https://doi.org/10.1109/TII.2021.3078192.

[9] Maggipinto, Marco, Alessandro Beghi, and Gian Antonio Susto. 2022. “A Deep Convolutional Autoencoder-Based Approach for Anomaly Detection with Industrial, Non-Images, 2-Dimensional Data: A Semiconductor Manufacturing Case Study.” IEEE Transactions on Automation Science and Engineering 19 (3): 1477–90. https://doi.org/10.1109/TASE.2022.3141186.

[10] Mofidul, Raihan Bin, Md Morshed Alam, Md Habibur Rahman, and Yeong Min Jang. 2022. “Real-Time Energy Data Acquisition, Anomaly Detection, and Monitoring System: Implementation of a Secured, Robust, and Integrated Global IIoT Infrastructure with Edge and Cloud AI.” Sensors 2022, Vol. 22, Page 8980 22 (22): 8980. https://doi.org/10.3390/S22228980.

[11] Nizam, Hussain, Samra Zafar, Zefeng Lv, Fan Wang, and Xiaopeng Hu. 2022. “Real-Time Deep Anomaly Detection Framework for Multivariate Time-Series Data in Industrial IoT.” IEEE Sensors Journal 22 (23): 22836–49. https://doi.org/10.1109/JSEN.2022.3211874.

[12] Qi, Lianyong, Yihong Yang, Xiaokang Zhou, Wajid Rafique, and Jianhua Ma. 2022. “Fast Anomaly Identification Based on Multiaspect Data Streams for Intelligent Intrusion Detection Toward Secure Industry 4.0.” IEEE Transactions on Industrial Informatics 18 (9): 6503–11. https://doi.org/10.1109/TII.2021.3139363.

[13] Salam, Abdu, Faizan Ullah, Farhan Amin, and Mohammad Abrar. 2023. “Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach.” Technologies 2023, Vol. 11, Page 107 11 (4): 107. https://doi.org/10.3390/TECHNOLOGIES11040107.

[14] Velasquez, David, Enrique Perez, Xabier Oregui, Arkaitz Artetxe, Jorge Manteca, Jordi Escayola Mansilla, Mauricio Toro, Mikel Maiza, and Basilio Sierra. 2022. “A Hybrid Machine-Learning Ensemble for Anomaly Detection in Real-Time Industry 4.0 Systems.” IEEE Access 10: 72024–36. https://doi.org/10.1109/ACCESS.2022.3188102.

[15] Wang, Xiaoding, Sahil Garg, Hui Lin, Jia Hu, Georges Kaddoum, Md Jalil Piran, and M. Shamim Hossain. 2022. “Toward Accurate Anomaly Detection in Industrial Internet of Things Using Hierarchical Federated Learning.” IEEE Internet of Things Journal 9 (10): 7110–19. https://doi.org/10.1109/JIOT.2021.3074382.

[16] Wu, Huanzhuo, Yunbin Shen, Xun Xiao, Giang T. Nguyen, Artur Hecker, and Frank H.P. Fitzek. 2023. “Accelerating Industrial IoT Acoustic Data Separation With In-Network Computing.” IEEE Internet of Things Journal 10 (5): 3901–16. https://doi.org/10.1109/JIOT.2022.3176974.

[17] Yang, Kaixiang, Yifan Shi, Zhiwen Yu, Qinmin Yang, Arun Kumar Sangaiah, and Huanqiang Zeng. 2023. "Stacked One-Class Broad Learning System for Intrusion Detection in Industry 4.0." IEEE Transactions on Industrial Informatics 19 (1): 251–60. https://doi.org/10.1109/TII.2022.3157727.

[18] Yazdinejad, Abbas, Ali Dehghantanha, Reza M. Parizi, Mohammad Hammoudeh, Hadis Karimipour, and Gautam Srivastava. 2022. "Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks." IEEE Transactions on Industrial Informatics 18 (11): 8356–66. https://doi.org/10.1109/TII.2022.3168011.

Author's Biography

Mr. D. Vishnu Prasad is a diligent researcher currently pursuing his Ph.D. at Puducherry Technological University, focusing on the Internet of Things (IoT), Artificial Intelligence (AI), and Machine Learning (ML). He holds a Master of Technology degree in IoT and completed his Bachelor's degree at Christ College of Engineering and Technology, Pondicherry University. With a passion for technology-driven innovation, Vishnu has contributed to the scholarly community by presenting his research at an IEEE international conference. His interests lie in the intersection of IoT, AI, and ML, where he seeks to pioneer transformative solutions. Email ID: vishnuprasad@pec.edu

Dr. S. Saraswathi is Professor in the Department of Information Technology, Puducherry Technological University. She completed her PhD, in the area of speech recognition for Tamil language. Her areas of interest are Natural Language Processing, Design of Intelligent Systems and Speech Processing. Email ID: s.saraswathi@ptuniv.edu.in