ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1824

A Smart Device Centric Local Network Architecture for Real-Time Control of IoT Physical Entities

Rajesh Kumar K.[1]; Mahimuda Sumaya Begam[2]; V. Nandini[3]; G. Sai Charan[4]; Mohammed Muaaz Basha[5]; Savasi Harini[6]; Yallamelli Sumalatha[7]; B. Divya[8]

[1]Assistant Professor, Department of CSE, MVSR Engineering College, Hyderabad, India
[2,3,4,5,6,7,8]BE Student, Department of CSE, MVSR Engineering College, Hyderabad, India

Publication Date: 2026/04/11

Abstract: The increasing adoption of Internet of Things (IoT) technologies has enabled intelligent interaction between digital systems and physical entities; however, most existing IoT solutions rely heavily on cloud-based infrastructures, which introduce challenges such as increased latency, continuous internet dependency, higher operational costs, and potential data privacy risks. The objective of this work is to design and implement a smart-device based local network architecture for controlling IoT physical entities efficiently without cloud dependency, thereby enhancing system responsiveness, reliability, and security. The novelty of the proposed approach lies in utilizing a commonly available smart device, such as a smartphone or tablet, as the central controller and user interface within a localized network, enabling direct communication with IoT nodes through lightweight local communication protocols. This architecture minimizes latency and ensures data privacy by confining all control and monitoring operations within the local network. The methodology involves establishing a local area network in which embedded IoT nodes comprising sensors and actuators are interconnected via a microcontroller platform, while the smart device communicates with these nodes to perform device discovery, command execution, and real-time monitoring. The system is implemented using standard networking protocols and tested under various operating conditions to evaluate parameters such as response time, reliability, scalability, and control accuracy. Experimental results demonstrate that the proposed local network–based IoT control system significantly outperforms conventional cloud-based solutions in terms of latency reduction and operational reliability. The findings also indicate improved system robustness during internet outages and enhanced security due to localized data handling. Furthermore, the system proves to be cost-effective, scalable, and easy to deploy, making it suitable for applications in smart homes, academic laboratories, healthcare environments, and small-scale industrial automation. Overall, this study confirms that controlling IoT physical entities using a smart device over a local network is a practical and efficient alternative to cloud-centric IoT architectures, offering improved performance, user autonomy, and data security while maintaining flexibility and ease of integration.

Keywords: *Internet of Things (IoT), Smart Device–Based Control, Local Area Network (LAN), Cloud-Independent Architecture, Real-Time Monitoring and Control.*

How to Cite: Rajesh Kumar K.; Mahimuda Sumaya Begam; V. Nandini; G. Sai Charan; Mohammed Muaaz Basha; Savasi Harini; Yallamelli Sumalatha; B. Divya (2026) A Smart Device Centric Local Network Architecture for Real-Time Control of IoT Physical Entities. *International Journal of Innovative Science and Research Technology*, 11(3), 3860-3867. https://doi.org/10.38124/ijisrt/26mar1824

I. INTRODUCTION

The evolution of industry has been marked by continuous technological advancements aimed at improving productivity, efficiency, and quality of human life. The First Industrial Revolution introduced mechanization through steam power, transforming manual labor into machine-assisted production. The Second Industrial Revolution further advanced industrial capabilities through electrification, mass production, and assembly-line manufacturing, significantly increasing output and reducing costs. The Third Industrial Revolution, often referred to as the digital revolution, introduced electronics, computers, and automation into industrial processes, enabling programmable control and improved precision. In recent decades, the Fourth Industrial Revolution, commonly known as Industry 4.0, has emerged, integrating cyber-physical systems, artificial intelligence, cloud computing, and the Internet of Things (IoT). This phase emphasizes intelligent decision-making, autonomous systems, and real-time data exchange between physical and digital entities. Industrial systems are no longer isolated; instead, they operate as interconnected networks capable of self-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1824

monitoring, self-optimization, and predictive maintenance. This transformation has reshaped manufacturing, healthcare, transportation, agriculture, and energy sectors. However, as industrial systems become more interconnected, challenges related to system complexity, security, latency, and dependency on centralized infrastructures have become increasingly significant. Addressing these challenges requires innovative architectures that balance connectivity, efficiency, and reliability while ensuring scalability and data privacy[1]-[2].

Traditional industrial automation focused primarily on closed-loop control systems operating within confined environments using programmable logic controllers and supervisory control mechanisms. While these systems were effective for localized control, they lacked flexibility, remote accessibility, and adaptability to dynamic operational conditions. The growing demand for real-time monitoring, predictive analytics, and remote management necessitated the integration of communication technologies with automation system[3]s. This transition marked the shift from isolated automation toward connected systems capable of exchanging data across networks. Connectivity enabled industries to collect vast amounts of operational data, facilitating informed decision-making and process optimization. However, early connected systems were limited by proprietary protocols, high deployment costs, and restricted interoperability. The emergence of standardized communication technologies and low-cost embedded devices paved the way for more open and scalable solutions. Despite these advancements, many connected systems remain heavily reliant on centralized servers or cloud platforms, introducing latency, reliability concerns, and cybersecurity risks. These limitations highlight the need for decentralized and localized control architectures that can operate independently while maintaining intelligent functionality[4]-[3].

The concept of the Internet of Things has evolved from simple machine-to-machine communication to complex ecosystems involving billions of interconnected devices. Initially, IoT systems focused on basic sensing and data transmission, primarily for monitoring purposes. With advancements in wireless communication, embedded systems, and data analytics, IoT evolved into an intelligent framework capable of real-time control, automation, and decision-making[5]. Modern IoT systems integrate sensors, actuators, communication networks, and software platforms to enable seamless interaction between physical entities and digital environments. Applications of IoT now span smart homes, smart cities, healthcare monitoring, industrial automation, environmental sensing, and intelligent transportation systems[6]. Despite its widespread adoption, IoT architecture has largely cantered around cloud-based models, where data processing and control logic are executed remotely. While cloud integration offers scalability and computational power, it also introduces challenges such as latency, bandwidth consumption, dependency on internet connectivity, and concerns related to data ownership and privacy. These challenges become more critical in time-sensitive and safety-critical applications, emphasizing the importance of alternative IoT architectures[7]-[8].

IoT technologies offer numerous benefits, including enhanced operational efficiency, real-time monitoring, automation, and data-driven decision-making. By enabling continuous data collection from physical entities, IoT systems provide valuable insights into system performance, resource utilization, and environmental conditions. This capability supports predictive maintenance, reduces downtime, and improves asset management[9]. IoT also enhances user convenience by enabling remote control and monitoring of devices through smart interfaces. In industrial environments, IoT-driven automation improves productivity, quality control, and energy efficiency. In healthcare, IoT enables remote patient monitoring and timely medical intervention. Smart agriculture applications optimize water usage, crop monitoring, and yield prediction. These benefits demonstrate IoT's transformative potential across various domains. However, realizing these advantages requires reliable communication, low-latency control, and secure data handling, which are not always guaranteed in cloud-dependent architectures[10]-[11].

Despite their advantages, cloud-centric IoT systems face several inherent limitations. Dependence on continuous internet connectivity makes these systems vulnerable to network failures and service outages. Latency introduced by remote data processing can degrade system performance, particularly in real-time control applications. Additionally, transmitting large volumes of data to the cloud increases bandwidth requirements and operational costs. Security and privacy concerns also arise due to centralized data storage and potential exposure to cyberattacks. For applications operating in constrained or sensitive environments, these limitations can significantly impact system reliability and user trust. Consequently, there is growing interest in alternative IoT architectures that reduce reliance on cloud infrastructure while maintaining system intelligence and functionality[12]-[13].

To address the limitations of cloud-centric models, local and edge-based IoT architectures have gained attention. These approaches involve processing data closer to the source, reducing latency and network dependency[14]. Local networks enable direct communication between IoT devices and control interfaces, improving responsiveness and reliability. Edge computing allows preliminary data processing and decision-making to occur at the device or gateway level. While these architectures improve performance, their implementation often requires specialized hardware or complex system integration. Simplifying local IoT architectures using commonly available smart devices presents an opportunity to enhance accessibility and adoption[15].

Smart devices such as smartphones and tablets are equipped with powerful processors, intuitive user interfaces, and multiple communication capabilities. Their widespread availability makes them ideal candidates for acting as central controllers in local IoT networks. Using smart devices for IoT control reduces system complexity and eliminates the need for dedicated servers. Smart-device–based control enables real-time interaction with physical entities, offering flexibility and user-friendly operation. This approach aligns with the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1824

growing trend toward decentralized and user-centric system design[16]-[17].

Although significant research has been conducted on IoT architectures, gaps remain in developing efficient, low-cost, and fully localized control systems. Many existing solutions still rely partially on cloud services or complex edge infrastructure[18]. There is limited focus on leveraging smart devices as standalone controllers within local networks. Additionally, performance evaluation under network constraints and offline conditions is often insufficiently addressed. These gaps motivate the exploration of smart-device–centric local IoT architectures[19].

The motivation for this research stems from the need for reliable, secure, and low-latency IoT control systems that can operate independently of cloud infrastructure. By establishing a local network controlled by a smart device, the proposed approach aims to overcome existing limitations while preserving the benefits of IoT technologies. This approach supports real-time control, enhances data privacy, and improves system robustness, particularly in environments with limited internet connectivity[20].

This study focuses on designing and evaluating a smart-device–based local IoT control framework for managing physical entities. The contribution lies in demonstrating a practical, scalable, and cost-effective architecture that bridges the gap between traditional automation and modern IoT systems. The proposed approach offers a balanced solution that combines connectivity, control efficiency, and security, paving the way for future research and real-world deployment in diverse application domains.

II. PROPOSED METHODOLOGY

The proposed methodology focuses on designing and implementing a smart-device–centric local IoT network architecture for controlling and monitoring physical entities without dependency on cloud infrastructure. The methodology emphasizes low latency, enhanced security, cost effectiveness, and operational reliability. The overall system architecture consists of IoT physical entities, an embedded processing unit, a local communication network, and a smart device acting as the central controller and user interface. The methodological framework is divided into system architecture design, communication strategy, control logic implementation, data handling, and performance evaluation.

- *System Architecture*

The proposed system is designed around a local area network (LAN) where all IoT devices and the smart device are connected within the same network. Physical entities such as sensors and actuators are interfaced with a microcontroller or embedded processing unit. The smart device communicates directly with the embedded unit through local communication protocols, enabling real-time control and monitoring.

Unlike conventional cloud-based IoT systems, the proposed architecture eliminates remote servers and external internet dependency. This localized structure ensures that data remains within the system boundary, significantly reducing latency and enhancing data privacy. The smart device acts as the central decision-making and visualization unit, while the embedded controller manages real-time hardware interactions.

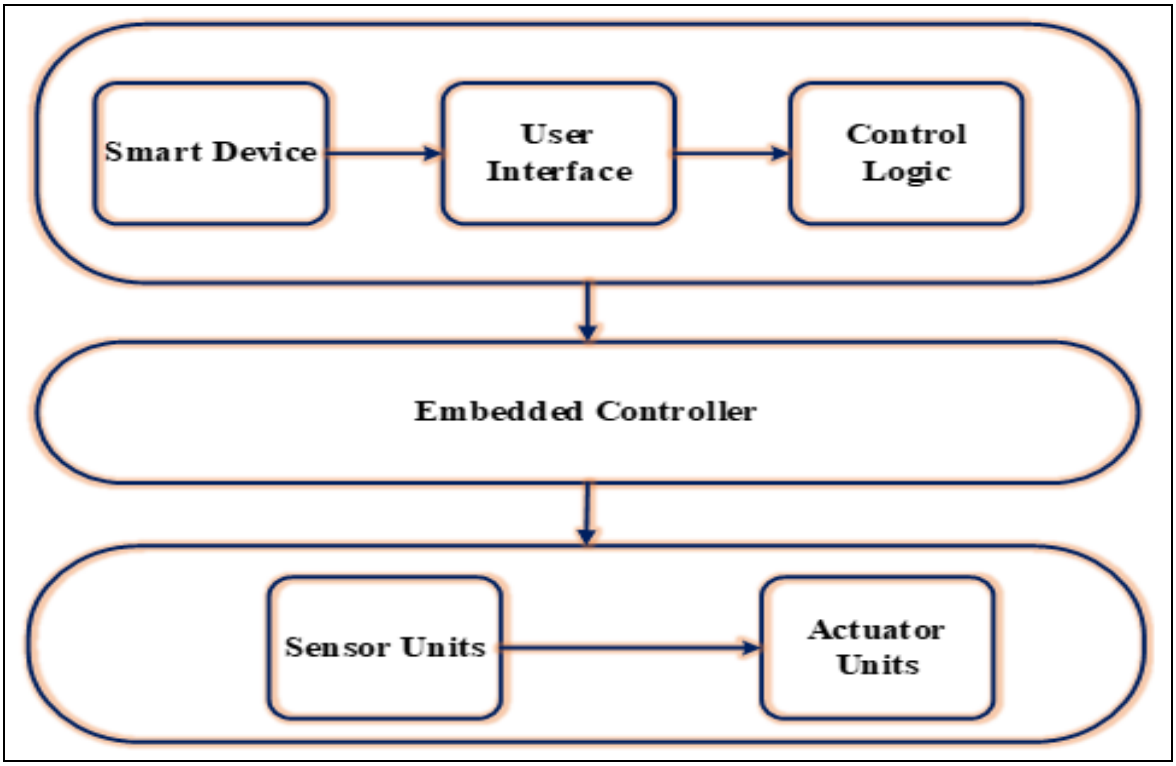

Fig 1 Illustrates the Smart-Device–Based Local IoT Control Architecture.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1824

➢ *Hardware Layer Design*

The hardware layer consists of physical entities, including sensors and actuators, connected to an embedded controller. Sensors may include temperature, humidity, light, motion, or voltage and current sensors depending on the application. Actuators may include relays, motors, solenoid valves, or lighting units. The embedded controller acts as the interface between the physical layer and the communication network.

Fig 2 Hardware Architecture

The embedded controller is responsible for acquiring sensor data, executing actuator commands, and maintaining communication with the smart device. It is configured to operate within the local network and handle multiple device connections. Power management, signal conditioning, and electrical isolation are incorporated to ensure reliable and safe operation.

➢ *Smart Device as Central Controller*

In the proposed methodology, the smart device plays a crucial role as the central control and monitoring unit. It provides a graphical user interface (GUI) that allows users to interact with IoT physical entities intuitively. The GUI includes options for device selection, status visualization, parameter configuration, and manual or automated control.

The smart device runs an application that contains the control logic and communication modules. By executing control algorithms locally on the smart device, the system avoids delays associated with cloud processing. This approach enables immediate response to user commands and real-time feedback from physical entities.

➢ *Communication Strategy*

Communication between the smart device and the embedded controller is established through a local network using standard networking protocols. The embedded controller is assigned a local IP address, allowing the smart device to send control commands and receive sensor data directly.

- *The Communication Workflow Includes:*

✓ Device discovery within the local network
✓ Establishment of a secure communication channel
✓ Transmission of control commands
✓ Reception of sensor data and system status

Data packets are designed to be lightweight to minimize network overhead and ensure fast transmission. Periodic status updates are transmitted to the smart device to enable continuous monitoring.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1824

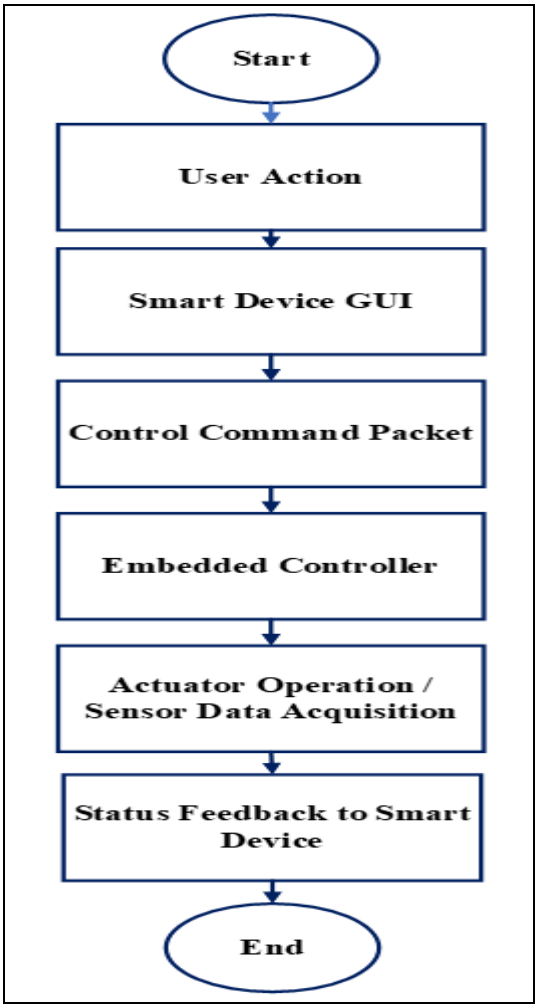

Fig 3 Shows the Bidirectional Communication Flow Between the Smart Device and IoT Nodes.

➢ *Control Logic Implementation*

Control logic is implemented at two levels: the smart device level and the embedded controller level. The smart device executes high-level decision-making algorithms, including user-defined rules, scheduling, and automation logic. The embedded controller executes low-level control tasks, such as actuator switching and sensor data acquisition.

This layered control approach improves system reliability and ensures that critical operations can continue even if the smart device temporarily disconnects. Safety constraints and threshold conditions are implemented to prevent system malfunction.

➢ *Data Handling and Processing*

Sensor data acquired by the embedded controller is transmitted to the smart device for visualization and analysis. Data processing is performed locally on the smart device, eliminating the need for cloud storage. Historical data can be stored locally for trend analysis and system diagnostics.

Local data handling enhances data privacy and reduces vulnerability to cyber threats. Additionally, it minimizes bandwidth usage and operational costs associated with cloud services.

➢ *Security Considerations*

Security is a key component of the proposed methodology. Since the system operates within a local network, exposure to external threats is significantly reduced. Authentication mechanisms are implemented to restrict access to authorized smart devices. Data encryption techniques are employed to protect communication between devices.

The absence of cloud connectivity further reduces the attack surface, making the system suitable for security-sensitive environments such as laboratories and industrial facilities.

➢ *Scalable Local IoT Network Architecture*

The proposed architecture supports scalability by allowing additional IoT nodes to be integrated into the local network. The smart device application is designed to dynamically detect and manage new devices. Modular hardware and software design enable easy expansion and customization based on application requirements.

This flexibility makes the system adaptable to various domains, including smart homes, academic laboratories, healthcare monitoring, and small-scale industrial automation.

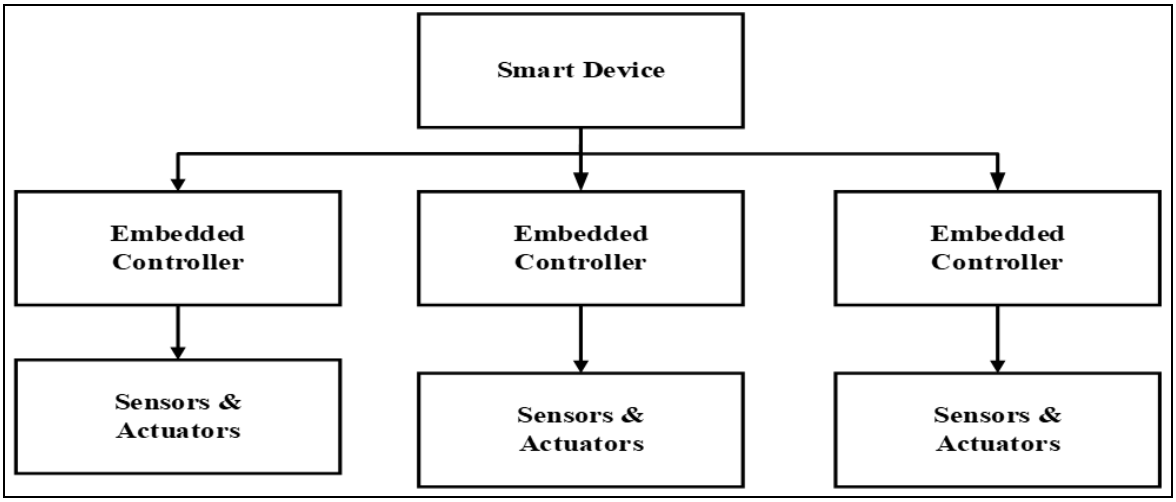

Fig 4 Demonstrates Scalability Through Multiple Embedded Controllers.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1824

➢ *Performance Evaluation*

The system is evaluated under different operating conditions to assess performance metrics such as response time, communication reliability, and control accuracy. Tests are conducted with varying numbers of connected devices and different network loads. Performance during internet outages is also evaluated to demonstrate system robustness.

III. CONCLUSION

This work demonstrated that controlling IoT physical entities using a smart device over a locally established network is an effective and practical alternative to conventional cloud-centric IoT architectures. By eliminating continuous dependence on external cloud services, the proposed approach significantly reduces communication latency, improves real-time responsiveness, and enhances overall system reliability, particularly in environments with limited or unstable internet connectivity. The smart device, functioning as the central control and monitoring unit, provides an intuitive interface and executes high-level control logic, while the embedded controller ensures precise interaction with sensors and actuators, resulting in efficient and reliable system operation. Localized data processing and storage improve data privacy and minimize exposure to cybersecurity threats, addressing one of the major concerns in large-scale IoT deployments. The experimental observations confirm that the proposed system achieves faster response times and stable control performance compared to cloud-based solutions, while also reducing bandwidth usage and operational costs. Additionally, the modular and scalable nature of the architecture allows seamless integration of additional IoT nodes, making it suitable for diverse applications such as smart homes, academic laboratories, healthcare monitoring, and small-scale industrial automation. Overall, the proposed smart-device centric local IoT framework offers a secure, cost-effective, and flexible solution that bridges the gap between traditional automation systems and modern IoT technologies, and it provides a strong foundation for future research focused on edge intelligence, autonomous decision-making, and hybrid IoT architectures.

REFERENCES

[1]. N. Nireekshana, “A POD Modulation Technique Based Transformer less HERIC Topology for PV Grid Tied-Inverter,” in E3S Web of Conferences, EDP Sciences, 2025, p. 01001. Accessed: Apr. 11, 2025. [Online]. Available: https://www.e3s-conferences.org/articles/e3sconf/abs/2025/16/e3sconf_icregcsd2025_01001/e3sconf_icregcsd2025_01001.html

[2]. N. Nireekshana, A. Archana, and K. Pullareddy, “A Classical H6 Topology for Modern PV Inverter Design,” in Power Energy and Secure Smart Technologies, CRC Press, 2025, pp. 1–7. Accessed: Dec. 02, 2025. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003661917-1/classical-h6-topology-modern-pv-inverter-design-namburi-nireekshana-archana-pullareddy-kanth-rajini

[3]. N. Namburi Nireekshana and K. R. Kumar, “A Modern Distribution Power Flow Controller With A PID-Fuzzy Approach: Improves The Power Quality”, Accessed: Dec. 02, 2025. [Online]. Available: https://www.academia.edu/download/112956747/ijeer_120124.pdf

[4]. C. P. Prasad and N. Nireekshan, “A Higher Voltage Multilevel Inverter with Reduced Switches for Industrial Drive,” Int. J. Sci. Eng. Technol. Res. IJSETR, vol. 5, no. 1, 2016, Accessed: Dec. 02, 2025. [Online]. Available: https://methodist.edu.in/web/uploads/naac/2019-11-19%2012_24_22pm%2092.pdf

[5]. N. Nireekshana, K. P. Reddy, A. Archana, and P. R. Kanth, “Solar-Assisted Smart Driving System for Sustainable Transportation,” Int. J. Innov. Sci. Res. Technol., vol. 10, no. 8, pp. 168–173, 2025.

[6]. Namburi Nireekshana, A. Archana, Setla Manvitha, Mohammed Saad Ahmed, Nisar Ahmed Khan, and Akellu George Muller, “Unique Facts Device for Power Quality Mitigation,” Feb. 2024, doi: 10.5281/ZENODO.10652911.

[7]. N. Nireekshana, R. Ramachandran, and G. V. Narayana, “A New Soft Computing Fuzzy Logic Frequency Regulation Scheme for Two Area Hybrid Power Systems,” Int. J. Electr. Electron. Res., vol. 11, no. 3, pp. 705–710, 2023.

[8]. N. Nireekshana, R. Ramachandran, and G. Narayana, “A Novel Swarm Approach for Regulating Load Frequency in Two-Area Energy Systems,” Int J Electr Electron Res, vol. 11, pp. 371–377, 2023.

[9]. N. Nireekshana, M. A. Goud, R. B. Shankar, and G. N. S. Chandra, “Solar Powered Multipurpose Agriculture Robot,” Int. J. Innov. Sci. Res. Technol., vol. 8, no. 5, p. 299, 2023.

[10]. N. Nireekshana, R. Ramachandran, and G. V. Narayana, “A Peer Survey on Load Frequency Contol in Isolated Power System with Novel Topologies,” Int J Eng Adv Technol IJEAT, vol. 11, no. 1, pp. 82–88, 2021.

[11]. N. Nireekshana, R. Ramachandran, and G. V. Narayana, “An innovative fuzzy logic frequency regulation strategy for two-area power systems,” Int. J. Power Electron. Drive Syst. IJPEDS, vol. 15, no. 1, pp. 603–610, 2024.

[12]. N. Nireekshana, T. H. Nerlekar, P. N. Kumar, and M. M. Bajaber, “An Innovative Solar Based Robotic Floor Cleaner,” Int. J. Innov. Sci. Res. Technol. IJISRT, vol. 8, no. 4, pp. 1880–1885, 2023.

[13]. N. Nireekshana, R. R. Chandran, and G. V. Narayana, “Frequency Regulation in Two Area System with PSO Driven PID Technique,” J Power Electron Power Syst, vol. 12, no. 2, pp. 8–20, 2022.

[14]. N. NIREEKSHANA, A. SHIVA, A. FURKHAN, M. SRIDHAR, A. OMPRAKASH, and K. K. SHIVA, “SIX PULSE TYPE SEGMENTED THYRISTOR CONTROLLED REACTOR WITH FIXED CAPACITOR FOR REACTIVE POWER COMPENSATION,” Int. J., pp. 3153–3159, 2024.

[15]. N. Nireekshana, R. Ramachandran, and G. V. Narayana, “Novel Intelligence ANFIS Technique for

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1824

Two-Area Hybrid Power System's Load Frequency Regulation," in E3S Web of Conferences, EDP Sciences, 2024, p. 02005. Accessed: Dec. 02, 2025. [Online]. Available: https://www.e3s-conferences.org/articles/e3sconf/abs/2024/02/e3sconf_icregcsd2023_02005/e3sconf_icregcsd2023_02005.html

[16]. N. Nireekshana, S. Unissa, B. R. Jaleja, C. Mukta Tejaswi, P. Mangathayaru Mahitha, and P. Vaishnavi, "FACTS: Present and Future," Int. J. Innov. Sci. Res. Technol. IJISRT, pp. 2350–2358, Oct. 2024, doi: 10.38124/ijisrt/IJISRT24SEP1424.

[17]. Namburi Nireekshana, Tanvi H Nerlekar, P. N. Kumar, and M. M. Bajaber, "An Innovative Solar Based Robotic Floor Cleaner," May 2023, doi: 10.5281/ZENODO.7918621.

[18]. Namburi Nireekshana, Onteru Divya, Mohammed Abdul Saquib Adil, Rathod Rahul, and Mohammed Shoaib Mohiuddin, "An Innovative SSSC Device for Power Quality Enhancement," Feb. 2024, doi: 10.5281/ZENODO.10670526.

[19]. C. P. Prasad and N. Nireekshan, "A Higher Voltage Multilevel Inverter with Reduced Switches for Industrial Drive," Int. J. Sci. Eng. Technol. Res. IJSETR, vol. 5, no. 1, 2016, Accessed: Feb. 18, 2025. [Online]. Available: https://methodist.edu.in/web/uploads/naac/2019-11-19%2012_24_22pm%2092.pdf

[20]. N. Nireekshana, T. H. Nerlekar, N. Kumar, and M. Mohsin, "An Innovative Solar Based Robotic Floor Cleaner," Int. J. Innov. Sci. Res. Technol. IJISRT, vol. 8, no. 4, pp. 1880–1885, 2023.

AUTHOR'S PROFILE

Mr K Rajesh Kumar is working as an Assistant Professor at MVSR Engineering College. He published 5 Scopus-indexed journals, 2 international conferences. His research focusses on MPPT extraction topologies

Mahimuda Sumaya Begam is pursuing BE Third year CSE at MVSR Engineering College. She completed Intermediate at SRI CHAITANYA JUNIOR KALASA and she completed schooling at CHANAKYA HIGH SCHOOL

V Nandini is pursuing BE Third year CSE at MVSR Engineering College.She completed Intermediate at VISHRA JUNIOR KALASALA and she completed schooling at RBVR REDDY M H S

G Sai Charan is pursuing BE Third year CSE at MVSR Engineering College.He completed diploma at Sree dattha Institute of engineering and science and he completed shooling at Brilliant High School

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1824

Mohammed Muaaz Basha is pursuing BE Third year CSE at MVSR Engineering College. He completed diploma at Govt polytechnic for minorities, Kurnool, AP and he completed schooling at Sri Lakshmi High School.

Savasi Harini is pursuing BE Third year CSE at MVSR Engineering College. She completed a diploma at TRR COLLEGE OF TECHNOLOGY and she completed schooling at BUDS AND FLOWERS HIGH SCHOOL

Yallamelli Sumalatha is pursuing BE Third year CSE at MVSR Engineering College. She completed a diploma at QQ GOVT POLYTECHNIC and she completed schooling at Govt High School chandrayanagutta Hyd

B. Divya is pursuing BE Third year CSE at MVSR Engineering College. She completed diploma at GPW Suryapet and she completed schooling at KGBV chinnagudur