International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 10, Issue 02, ISSN No. 2455-2143, Pages 82-85
Published Online June 2025 in IJEAST (http://www.ijeast.com)

AN IOT BASED SMART GRID SYSTEM FOR ADVANCED COMMUNICATION

Abhijeet Rajendra Bedarkar, Prof. R. N. Patil
Department of Electrical
MIT, Chh. Sambhajinagar, Maharashtra, India.

Abstract— **The Internet of Things (IoT) is transforming traditional systems by enabling autonomous device communication, data sharing, and real-time monitoring without centralized control. In the context of electric power systems, IoT enables the development of intelligent environments that optimize energy usage and reliability. Traditional electric grids, composed of aging infrastructure and diverse power generation units (coal, gas, hydro, etc.), face challenges in maintenance, scalability, and efficiency. Upgrading these systems requires significant investments and time. Smart Grid (SG) technology, enhanced by IoT integration, introduces a cyber–physical system that supports two-way communication between devices. This advancement allows the grid to recognize and respond to dynamic energy demands while facilitating the incorporation of renewable energy sources. IoT Infrastructure (IoTI) offers a flexible, secure platform for monitoring and managing operations under diverse conditions. This paper presents a comprehensive study of IoT applications in smart grids, with a focus on cybersecurity, system architecture, and device classification. It highlights the benefits of IoT-enabled smart grids in improving power quality, operational efficiency, and data-driven decision-making, while addressing future challenges related to scalability, security, and interoperability.**

Keywords— **Cyber security, IOT Infrastructure (IOTI), Smart grid, Strategic management, Network monitoring**

I. INTRODUCTION

Modern electric grids consist of numerous nodes and power plants utilizing diverse power generation units such as coal, gas, and hydro sources [1]. Most traditional grid infrastructure, including equipment and transmission lines, has been operational for decades. Due to high replacement costs and extended deployment times, much of this infrastructure is outdated, requiring continuous maintenance to ensure reliable power delivery [2,3]. The evolution of the grid from small, localized systems to vast interconnected networks spanning countries and continents presents increasing complexity in monitoring, stability, and resilience.

To meet growing energy demands and environmental goals, the energy sector is gradually embracing digitalization through advanced communication and monitoring technologies. This digital transformation is embodied in the concept of the Smart Grid (SG), which integrates cyber-physical systems and leverages the Internet of Things (IoT) to enable two-way communication, real-time data acquisition, and adaptive control of energy flows [4,5]. Smart grids support a bidirectional flow of information and energy, allowing devices and systems to autonomously interact, monitor, and respond to environmental and load conditions [6,7].

The IoT-based smart grid enhances operational efficiency, supports renewable energy integration, and improves grid reliability by using intelligent sensors, edge computing, and cloud-based analytics. The system supports distributed generation, self-healing, adaptive protection, and real-time monitoring, transforming passive consumers into active participants in energy management [8,9]. This shift is crucial for managing energy consumption, reducing peak loads, and achieving sustainability targets.

Despite its benefits, the increasing reliance on interconnected digital devices raises significant cybersecurity challenges. The review also focuses on the importance of secure communication protocols, resilience against cyber threats, and the need for robust architectures that ensure data integrity and grid stability [10,11].

Traditional power grids are increasingly inadequate in meeting modern demands for efficiency, reliability, and sustainability. With growing reliance on renewable energy and the need for dynamic load management, legacy systems lack the flexibility and intelligence required for real-time control and optimization. The integration of IoT technologies introduces both opportunities and vulnerabilities, necessitating a critical review of their implementation, performance, and security in the context of smart electric grids.

Objectives of the Review

- To explore the current state and potential of IoT integration in smart grids.
- To examine the architecture and communication technologies used in IoT-based power systems.
- To identify the challenges and solutions for cybersecurity in IoT-enabled smart grids.
- To analyze the comparative advantages of IoT-based smart grids over traditional systems.

International Journal of Engineering Applied Sciences and Technology, 2025
Vol. 10, Issue 02, ISSN No. 2455-2143, Pages 82-85
Published Online June 2025 in IJEAST (http://www.ijeast.com)

- To highlight future directions and research opportunities in smart grid communication and control.

II. IOT-BASED SMART GRID ARCHITECTURE

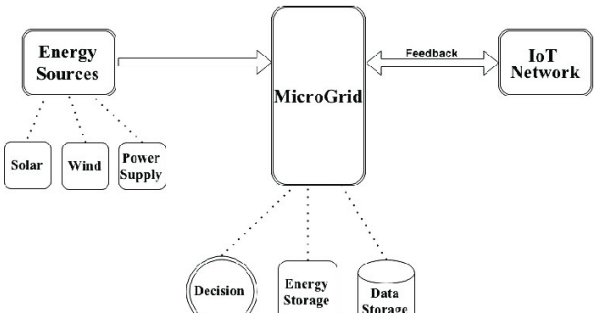

Fig.1: IOT based smart grid architecture

The architecture of an IoT-based smart grid integrates various layers and components to enable efficient, real-time monitoring, control, and management of electrical power systems. Typically, it consists of the following layers:

1. **Perception Layer:** This layer includes physical devices such as sensors, smart meters, actuators, and IoT-enabled devices. These devices collect real-time data on electricity generation, consumption, voltage levels, and environmental conditions.
2. **Network Layer:** It facilitates secure and reliable communication between devices and the central control units. This layer employs various communication technologies like Wi-Fi, ZigBee, 5G, LoRaWAN, and cellular networks to transmit data across the grid.
3. **Data Processing Layer:** This layer processes the large volume of data gathered by IoT devices. It often utilizes cloud computing and edge/fog computing to analyze data, enabling timely decision-making and system optimization.
4. **Application Layer:** The application layer supports smart grid functionalities such as demand response, fault detection, energy management, and integration of renewable energy sources. It provides interfaces for users, utility operators, and automated control systems.

III. LITERATURE SURVEY

The transition from traditional power systems to IoT-based smart grids is driven by the need for more efficient, secure, and sustainable energy infrastructures. Multiple studies have explored different dimensions of this transformation.

Sonawane and Naik [1] developed an IoT-based smart grid system integrated with cloud computing to enable remote monitoring and control of renewable energy sources. Their model allows for improved fault detection, system efficiency, and user accessibility in managing distributed energy resources.

Goudos et al. [2] provided a comprehensive review of communication protocols tailored for smart grid applications. They emphasized the role of MQTT, CoAP, 6LoWPAN, and Zigbee in establishing secure, low-latency communication across heterogeneous IoT devices, forming the backbone of smart grid connectivity.

Yadav et al. [3] explored the synergy between AI and IoT technologies in smart grid environments. They highlighted applications such as load forecasting, demand response, and real-time anomaly detection, paving the way for predictive intelligence in grid operations.

Gawande and Sheikh [4] implemented a prototype that demonstrates practical deployment of IoT-based monitoring and control, focusing on low-cost, scalable infrastructure suitable for localized energy networks and microgrid environments.

Alomar [5] proposed a novel IoT-based smart grid system featuring cooperative transmission and communication, which significantly enhances real-time data accuracy, power flow optimization, and system robustness under dynamic conditions.

Yang et al. [6] addressed security issues in smart grids through a trust evaluation model for secure routing in wireless sensor networks. This is essential for preserving data integrity and ensuring trustworthy operation in IoT-integrated grids.

Jiang et al. [7] introduced an AI-based model for automatic control in smart grids. Their solution leverages machine learning for system access control, fault prediction, and operational automation, improving grid autonomy and resilience.

Rathor and Saxena [8] outlined key challenges in energy management systems for smart grids. They identified the need for decentralized control, energy forecasting, and integration of intermittent renewable sources, where IoT platforms can offer real-time visibility and adaptive control.

Nair et al. [9] presented a novel framework for minimizing energy consumption in blockchain operations, which is crucial for incorporating secure, tamper-proof transactions in smart grid data logging and billing systems.

Pabbuleti and Somlal [10] proposed a bidirectional multi-level converter system for power balancing in hybrid AC/DC microgrids, with an emphasis on IoT-enabled control strategies to facilitate optimal energy distribution.
Fang et al. [11] provided a foundational survey of smart grid technologies and identified the core features of modern grids such as self-healing, real-time monitoring, and automated metering infrastructure (AMI), all of which rely on IoT integration.
Li et al. [12] highlighted the advantages of Narrowband IoT (NB-IoT) for smart grid communication, including low power consumption, long-range connectivity, and support for massive device deployment, making it suitable for rural and urban applications.

IV. COMMUNICATION TECHNOLOGIES AND PROTOCOLS: CHALLENGES AND LIMITATIONS

Reliable and secure communication is the backbone of IoT-enabled smart grid systems. It enables seamless data exchange among sensors, controllers, actuators, and management systems across the entire grid infrastructure. However, the integration of varied communication technologies and protocols introduces a range of challenges and limitations that must be addressed to ensure robust and scalable grid operations.

1. **Common Communication Technologies in Smart Grids**

Smart grids employ a mix of wired and wireless communication technologies tailored to specific use cases:

- **Wired**: Power Line Communication (PLC), Optical Fiber, Ethernet.
- **Wireless**: Zigbee, Wi-Fi, Bluetooth, LoRaWAN, NB-IoT, LTE, 5G.
- **Hybrid models** are often used to meet the coverage, speed, and reliability requirements of different smart grid segments.

Each technology has trade-offs in latency, range, bandwidth, cost, and power consumption, which must be considered during system design.

2. **Widely Used IoT Protocols**

Common IoT protocols in smart grid communication include:

- **MQTT (Message Queuing Telemetry Transport)**: Lightweight protocol suitable for constrained devices; however, it lacks built-in security and may require additional encryption layers.
- **CoAP (Constrained Application Protocol)**: Designed for RESTful interactions in constrained environments, but limited in robustness over lossy networks.
- **6LoWPAN (IPv6 over Low power Wireless Personal Area Networks)**: Enables IP-based addressing for low-power devices, but is challenged by limited payload and susceptibility to interference.
- **Zigbee**: Offers low power and short-range communication, ideal for home area networks but suffers from limited interoperability with internet-based services.
- **Modbus & DNP3**: Used in substation automation, but legacy versions lack cyber security protections.

Table 1: Challenges and Limitations

Challenge	Description
Scalability	Managing large volumes of IoT devices increases network complexity and congestion.
Latency Sensitivity	Delay in data transmission can lead to delayed control actions and system instability.
Bandwidth Limitations	Many wireless technologies provide limited bandwidth, impacting data-rich applications.
Interference and Signal Loss	Wireless communication is vulnerable to environmental noise and physical obstructions.
Security Vulnerabilities	Protocols like MQTT, Zigbee, and DNP3 may lack encryption and authentication mechanisms.
Interoperability	Integrating devices from different vendors using different standards and protocols is difficult.
Energy Constraints	IoT nodes are often battery-operated and must balance data transmission frequency with energy use.
Reliability	Communication disruptions can lead to monitoring gaps and operational failures.

V.CONCLUSION

The integration of Internet of Things (IoT) technologies into smart grid systems marks a significant advancement in the modernization of traditional power infrastructures. IoT enhances real-time monitoring, automation, efficient energy management, and dynamic control of grid components. This review has highlighted various architectural models, communication technologies, protocols, and applications of IoT in the smart grid domain.

Despite its immense potential, the deployment of IoT-based smart grids faces critical challenges, including communication security, device interoperability, energy constraints, and protocol limitations. Addressing these issues requires the development of robust communication standards, scalable architectures, and intelligent algorithms supported by edge computing and AI-based decision-making.

Continued research and innovation are essential to overcome existing limitations, ensure reliable integration of renewable energy sources, and meet future energy demands. A secure, efficient, and intelligent IoT-enabled smart grid promises to be a cornerstone of sustainable and resilient energy ecosystems.

VI. REFERENCE

[1] Aishwarya Sanjay Sonawane, A.V.Naik, “IOT Based Smart Grid to Remotely Monitor and Control Renewable Energy Sources using Cloud Computing”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 12 Issue VI June 2024.

[2] Goudos, S.K., Sarigiannidis, P., Dallas, P.I., Kyriazakos, S. (2019). Communication Protocols for the IoT-Based Smart Grid. In: Siozios, K., Anagnostos, D., Soudris, D., Kosmatopoulos, E. (eds) IoT for Smart Grids. Power Systems. Springer, Cham. https://doi.org/10.1007/978-3-030-03640-94.

[3] Monika Yadav; Amritansh Mehrotra; Devender Kumar Saini,"5 Internet of things (IoT)-based smart grids," in Artificial Intelligence and Internet of Things for Renewable Energy Systems, De Gruyter, 2022, pp.165-184.

[4] Akshata A. Gawande, Heena Sheikh, “IOT Based Smart Grid System”, 2021 JETIR January 2021, Volume 8, Issue 1. Journal of Emerging Technologies and Innovative Research (JETIR).

[5] Madani Abdu Alomar, An IOT based smart grid system for advanced cooperative transmission and communication, Physical Communication, Volume 58, 2023, 102069, ISSN 1874-4907, https://doi.org/10.1016/j.phycom.2023.102069.

[6] T. Yang, et al., A secure routing of wireless sensor networks based on trust evaluation model, Procedia Comput. Sci. 131 (2018) 1156–1163.

[7] D.Y. Jiang, H. Zhang, H. Kumar, Q.N. Naveed, C. Takhi, V. Jagota, R. Jain, Automatic control model of power information system access based on artificial intelligence technology, Math. Probl. Eng. (2022) 2022.

[8] S.K. Rathor, D. Saxena, Energy management system for smart grid: An overview and key issues, Int. J. Energy Res. 44 (6) (2020) 4067–4109.

[9] R. Nair, S. Gupta, M. Soni, P.K. Shukla, G. Dhiman, An approach to minimize the energy consumption during blockchain transaction, Mater. Today: Proc. (2020).

[10] B. Pabbuleti, J. Somlal, Implementation of multi-level bidirectional inter allied converter community for global power sharing in hybrid AC/DC microgrids, Int. J. Recent Innov. Trends Comput. Commun. 10 (6) (2022) 52–62.

[11] X. Fang, et al., Smart grid—The new and improved power grid: A survey, IEEE Commun. Surv. Tutor. 14 (4) (2011) 944–980.

[12] Y. Li, et al., Smart choice for the smart grid: Narrowband internet of things (NB-IoT), IEEE Internet Things J. 5 (3) (2017) 1505–1515.