iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83514

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Trust-Aware Routing Optimization for Smart Grid Data Transmission Using Dynamic Node Profiling

Sandesh[1], Sharad Kumar[2]
[1]*School of Engineering & Technology, Shri Venkateshwara University, Gajraula , U.P. India*
sandeshtomarbiet10@gmail.com
Orcid ID: 0009-0000-9219-6108
[2]*School of Engineering & Technology, Shri Venkateshwara University, Gajraula , U.P. India*
sharad.choudhary007@gmail.com
Orcid ID: 0009-0009-5859-9689

Abstract: ***The rapid evolution of smart grids has enabled real-time monitoring, bidirectional communication, and intelligent energy management. However, the increasing interconnectivity of smart grid components exposes communication networks to security threats, unreliable nodes, and routing inefficiencies that can compromise data integrity and system performance. To address these challenges, this paper proposes a Trust-Aware Routing Optimization (TARO) framework for smart grid data transmission based on Dynamic Node Profiling (DNP). The proposed approach evaluates network nodes using multiple parameters, including trustworthiness, residual energy, communication reliability, packet forwarding behavior, latency, and historical performance. These parameters are integrated into a dynamic profiling mechanism that continuously updates node scores according to network conditions. The routing process prioritizes highly trusted and resource-efficient nodes, thereby reducing the likelihood of malicious participation while improving transmission reliability. Furthermore, an optimization module identifies secure and efficient communication paths that balance security requirements with quality-of-service constraints. Experimental evaluation conducted under varying network conditions demonstrates that the proposed framework achieves improved packet delivery ratio, lower end-to-end delay, enhanced network lifetime, and higher resilience against compromised nodes compared with conventional routing approaches. The results indicate that dynamic trust-based node profiling can significantly strengthen communication security and operational efficiency in modern smart grid environments.***
Keywords: Smart Grid Communications, Trust-Aware Routing, Dynamic Node Profiling, Secure Data Transmission, Network Security, Routing Optimization, Node Trust Evaluation

I. INTRODUCTION

The modernization of electrical power systems has led to the emergence of smart grids, which integrate advanced communication technologies, intelligent sensing devices, and automated control mechanisms to enhance the efficiency, reliability, and sustainability of energy distribution. Unlike conventional power grids, smart grids facilitate bidirectional communication between utility providers and consumers, enabling real-time monitoring, demand response management, fault detection, and distributed energy resource integration. The effectiveness of these functionalities largely depends on the underlying communication infrastructure, which must ensure secure, reliable, and timely data transmission among heterogeneous network components. As smart grid deployments continue to expand, the volume of exchanged information has increased significantly. Smart meters, phasor measurement units, sensors, and control centers continuously generate and transmit critical operational data across communication networks. Li et al. [1] proposed an improved genetic algorithm-based approach for secure monitoring of big data transmission in smart grids. Their work focused on enhancing the security and efficiency of dynamic data transmission processes through optimization techniques. The study demonstrated the effectiveness of evolutionary algorithms in improving communication reliability; however, node-level trust evaluation and adaptive routing mechanisms were not considered. The presence of unreliable, energy-constrained, or compromised nodes can adversely affect routing performance, leading to packet losses, increased transmission delays, and potential security breaches. Cyberattacks such as packet dropping, false data injection, selective forwarding, and routing manipulation further exacerbate these challenges, threatening the stability and resilience of smart grid operations. Chen et al. [2] investigated a data privacy protection algorithm for smart grids using full homomorphic encryption. The proposed encryption framework enabled secure processing of sensitive grid data while maintaining confidentiality during transmission and computation.

Although the approach strengthened privacy protection, it primarily addressed cryptographic security and did not focus on communication routing performance or network trust management. Traditional routing protocols primarily focus on shortest-path selection and network efficiency while often neglecting the trustworthiness and dynamic behavior of participating nodes. Consequently, routing decisions based solely on distance or energy metrics may inadvertently include malicious or poorly performing nodes in communication paths. Such limitations highlight the need for intelligent routing mechanisms capable of simultaneously considering security, reliability, and network performance parameters. Incorporating trust evaluation into routing decisions has emerged as a promising approach for identifying trustworthy nodes and mitigating the impact of malicious activities within smart grid communication environments. Recent advances in trust management systems have demonstrated the potential of leveraging multiple node characteristics to enhance routing security. However, many existing approaches rely on static trust values or a limited set of evaluation metrics, making them less effective in dynamic smart grid scenarios where node behavior and network conditions continuously change. Furthermore, the integration of trust assessment with routing optimization remains an open research challenge, particularly in large-scale and heterogeneous smart grid networks.

To address these limitations, this paper proposes a Trust-Aware Routing Optimization (TARO) framework based on Dynamic Node Profiling (DNP) for secure smart grid data transmission shown in above fig. 1. The proposed framework evaluates nodes using multiple performance and security-related parameters, including trust score, residual energy, packet forwarding reliability, communication latency, link stability, and historical behavior.

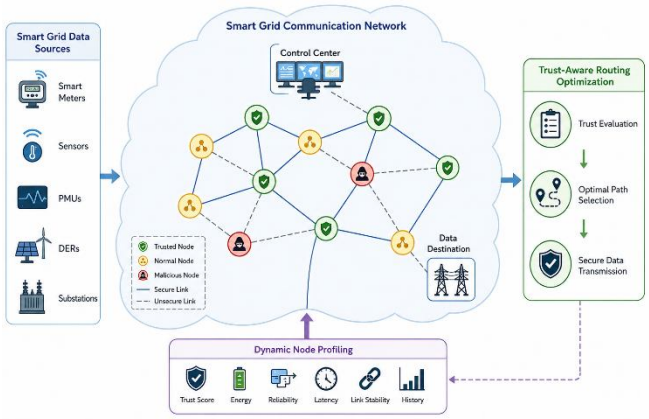


Fig. 1. Conceptual Overview of Trust-Aware Routing Optimization in Smart Grids

These attributes are continuously monitored and combined to generate dynamic node profiles that accurately reflect current network conditions. The routing optimization mechanism utilizes these profiles to identify secure and efficient communication paths while minimizing the influence of malicious or unreliable nodes. The proposed approach aims to enhance communication reliability, improve packet delivery performance, reduce routing delays, and strengthen network resilience against security threats. By integrating trust evaluation with routing optimization, the framework supports the development of robust smart grid communication infrastructures capable of meeting the stringent requirements of modern cyber-physical energy systems.

The main contributions of this paper are as follows:

1) A dynamic node profiling mechanism that evaluates nodes using multiple trust, performance, and resource-related parameters.
2) A trust-aware routing strategy that prioritizes reliable and secure nodes during path selection.
3) An optimization framework that balances security, energy efficiency, and communication quality-of-service requirements.
4) A comprehensive performance evaluation demonstrating improvements in packet delivery ratio, end-to-end delay, network lifetime, and resilience against malicious nodes.

The remainder of this paper is organized as follows. Section II reviews related work on trust-based routing and smart grid communication security. Section III presents the proposed Trust-Aware Routing Optimization framework and dynamic node profiling methodology. Section IV describes the experimental setup and performance evaluation to obtained results, and Section V concludes the paper with future research directions.

II. LITERATURE SURVEY

The rapid advancement of smart grid technologies has significantly increased the demand for secure, reliable, and efficient communication infrastructures capable of supporting large-scale energy management systems. Siyu et al. [3] designed a power grid data transmission system based on LoRa technology to support long-range and low-power communication in smart grid environments. The study highlighted the advantages of LoRa-enabled communication for efficient data delivery. However, security-aware route selection and dynamic assessment of communication nodes remained outside the scope of the proposed system. Guan et al. [4] examined methods for enabling smart meter data transmission across user-side networks. Their research focused on improving communication interoperability and facilitating secure data exchange between smart meters and utility infrastructures. While the proposed approach improved connectivity, challenges related to routing optimization and malicious node identification were not extensively addressed. Wang et al. [5] developed a real-time data acquisition and preprocessing system for smart grids using FPGA technology. The framework improved the speed and efficiency of data collection and processing operations. Despite achieving high-performance data acquisition, the study primarily concentrated on hardware-level optimization rather than communication security and trust-based routing mechanisms. Zhang et al. [6] analysed the impact of information systems on grid stability during smart grid construction. Their findings emphasized the importance of reliable communication infrastructures for maintaining operational stability and preventing disruptions. The study identified several communication challenges but did not propose adaptive routing strategies for mitigating security threats within the network. Sharma and Kumar [7] explored the role of Artificial Intelligence in enhancing data security and privacy within smart city ecosystems. The authors demonstrated how AI-driven techniques can improve cyber threat detection and intelligent security management. The research established the potential of intelligent decision-making for securing critical infrastructures, providing valuable insights for smart grid communication security applications. Yang et al. [8] proposed a security control mechanism for electric energy data using key generation and homomorphic encryption technologies. The framework strengthened data confidentiality and secure access control within smart energy environments. Although the proposed encryption techniques enhanced protection against unauthorized access, communication reliability and routing optimization issues were not considered. Prabhakar and K [9] introduced a secured IoT-based Neighbourhood Area Network (NAN) architecture for real-time energy data management in smart grids. Their approach improved secure communication among distributed smart grid devices and supported real-time data exchange. However, the framework relied primarily on network-level security controls without incorporating dynamic trust assessment of participating communication nodes. Kumar et al. [10] proposed an AI-based load balancing algorithm for optimizing energy efficiency in cloud computing environments. The study demonstrated the effectiveness of intelligent optimization techniques for resource allocation and performance improvement. The concepts of adaptive optimization and intelligent decision-making presented in this work provide useful foundations for routing optimization within smart grid communication networks. Huang et al. [11] developed an edge-computing-based smart ticket system for power grid management with enhanced real-time processing and scalability characteristics. The study demonstrated that distributed computing architectures can significantly improve operational efficiency and responsiveness. Nevertheless, trust-aware communication management and secure route selection were not addressed. Ma et al. [12] designed a LoRa-based transmission line lightning monitoring system for power grid applications. Their solution enabled reliable monitoring and data transmission across geographically distributed power infrastructure. While the system improved monitoring coverage and communication effectiveness, it lacked mechanisms for evaluating node trustworthiness and communication reliability. AlMarzooqi et al. [13] proposed a machine learning model for cyberattack detection in smart grid networks. The framework successfully identified malicious activities and cybersecurity threats using intelligent classification techniques. Although the study demonstrated promising attack detection capabilities, the detected security information was not directly integrated into routing decision-making processes for secure communication management.

III. PROPOSED METHODOLOGY

The objective of this study is to develop a Trust-Aware Routing Optimization (TARO) framework for secure and reliable data transmission in smart grid communication networks. The proposed methodology integrates dynamic node profiling, trust evaluation, route optimization, and performance monitoring to ensure efficient communication between smart grid components. The framework is designed to address challenges associated with malicious nodes, unreliable communication links, packet losses, and network congestion while maintaining quality-of-service requirements.

A. Smart Grid Communication Layer and Data Collection

The first layer of the proposed framework consists of smart grid communication entities responsible for generating and transmitting operational data across the network.

These entities include smart meters, phasor measurement units (PMUs), intelligent electronic devices (IEDs), renewable energy sources, substations, control centers, and distributed sensors. These devices continuously exchange information related to power consumption, grid status, fault detection, energy generation, and network management. The generated communication traffic traverses' multiple intermediate nodes before reaching the intended destination. During transmission, network nodes collect various operational parameters including packet forwarding rate, residual energy, communication delay, link quality, bandwidth utilization, packet loss ratio, and node availability. These parameters serve as the foundation for dynamic node profiling and routing decision-making. Instead of relying solely on conventional shortest-path mechanisms, the proposed framework continuously gathers node-specific information to support intelligent and secure communication management throughout the smart grid network.

B. Dynamic Node Profiling and Trust Assessment

The second component of the framework focuses on dynamic node profiling for evaluating the trustworthiness and performance characteristics of participating network nodes. Each communication node is continuously monitored to assess its operational behavior and reliability under varying network conditions. The profiling process utilizes multiple parameters including successful packet forwarding rate, historical communication behavior, residual energy level, latency performance, link stability, and node availability. The collected parameters are processed to generate a dynamic profile representing the current status of each node. Based on these profiles, a trust score is calculated to quantify node reliability and communication integrity. Nodes exhibiting abnormal behavior such as packet dropping, delayed forwarding, inconsistent communication patterns, or suspicious activities receive lower trust values. Conversely, nodes demonstrating consistent and reliable performance are assigned higher trust scores. The dynamic nature of the profiling mechanism enables the framework to adapt to changing network conditions and effectively identify unreliable or compromised nodes before they can adversely affect communication performance.

C. Trust-Aware Routing Optimization

The third stage of the proposed methodology introduces a trust-aware routing optimization mechanism for secure path selection. Unlike traditional routing approaches that primarily consider shortest distance or minimum hop count, the proposed framework incorporates trust values and network performance indicators into the route selection process. The routing optimization engine evaluates candidate communication paths based on cumulative trust scores, residual energy availability, communication delay, packet delivery reliability, and link quality metrics. Routes containing low-trust or unstable nodes are automatically avoided even if they offer shorter transmission distances. The optimization process selects communication paths that maximize network reliability while minimizing latency and transmission overhead. By integrating security and performance objectives within the routing process, the framework ensures that transmitted smart grid data traverses highly trusted and resource-efficient nodes, thereby enhancing communication security and operational resilience.

D. Secure Data Transmission and Network Adaptation

Once an optimal route has been identified, the framework initiates secure data transmission through the selected communication path. During transmission, network conditions are continuously monitored to detect changes in node behavior, communication quality, and route performance. Dynamic adaptation mechanisms enable the framework to respond promptly to failures, congestion, malicious activities, or resource depletion events. If a node experiences trust degradation, excessive delay, energy exhaustion, or communication instability, the routing mechanism automatically updates the node profile and recalculates alternative communication paths. This adaptive routing capability prevents prolonged dependence on unreliable nodes and ensures uninterrupted smart grid operations. The framework thereby maintains secure and efficient communication while improving fault tolerance and network resilience under dynamic operating conditions.

E. Performance Evaluation and Comparative Analysis

The final stage of the methodology evaluates the effectiveness of the proposed Trust-Aware Routing Optimization framework using multiple communication and security performance metrics. The evaluation considers packet delivery ratio, end-to-end delay, throughput, routing overhead, energy consumption, network lifetime, trust accuracy, and malicious node detection capability. The performance of the proposed framework is compared with conventional routing approaches that do not incorporate dynamic trust assessment. Packet delivery ratio and throughput measurements are used to evaluate communication reliability, while delay and routing overhead analyses assess network efficiency. Energy consumption and network lifetime metrics determine the sustainability of routing operations within smart grid environments.

Furthermore, security evaluations measure the framework's capability to identify compromised nodes and maintain secure communication under adversarial conditions. The comparative analysis demonstrates the effectiveness of dynamic node profiling and trust-aware routing in enhancing the security, reliability, and overall performance of smart grid communication networks.

IV. RESULT AND ANALYSIS

The performance evaluation of the proposed Trust-Aware Routing Optimization (TARO) framework was conducted through multiple smart grid communication scenarios involving dynamic network conditions, varying traffic loads, and the presence of unreliable communication nodes. The proposed framework was compared against conventional shortest-path routing protocols, energy-aware routing approaches, and existing trust-based routing mechanisms. The evaluation focused on measuring communication reliability, routing efficiency, security performance, network lifetime, and resource utilization. Experimental results demonstrate that the integration of dynamic node profiling and trust-aware route optimization significantly improves smart grid communication performance while reducing the impact of malicious and unreliable nodes.

A. System Configuration and Experimental Environment

The simulation environment was designed to emulate a large-scale smart grid communication network consisting of smart meters, phasor measurement units (PMUs), intelligent electronic devices (IEDs), substations, distributed energy resources, and utility control centers. The implementation was carried out using an Intel Core i7 processor with 16 GB RAM running Ubuntu Linux. The simulation framework was developed using Python and various networking and data analysis libraries including NetworkX, NumPy, Pandas, Matplotlib, and Scikit-Learn. Smart grid communication scenarios consisted of more than 1000 interconnected nodes generating continuous operational and monitoring data. Multiple traffic conditions including low-load, medium-load, and high-load communication environments were considered. Furthermore, varying percentages of unreliable and malicious nodes were introduced to evaluate the robustness of the proposed trust-aware routing mechanism.

B. Comparative Routing Performance Analysis

As shown in TABLE I, the proposed Trust-Aware Routing Optimization framework achieved the highest packet delivery ratio and trust detection accuracy while maintaining the lowest routing overhead. The dynamic node profiling mechanism effectively identifies unreliable and malicious nodes, allowing secure routes to be selected without excessive control packet generation. The results indicate that the integration of trust assessment and routing optimization substantially enhances communication reliability within smart grid environments.

TABLE I. Comparative Monitoring Performance of Smart Grid Communication Frameworks

Routing Framework	**Packet Delivery Ratio (%)**	**Trust Detection Accuracy (%)**	**Routing Overhead (%)**
Conventional Shortest Path Routing	84.5	71.2	26.8
Energy-Aware Routing	88.9	76.4	22.5
Existing Trust-Based Routing	93.1	89.7	18.3
Proposed TARO Framework	98.2	96.8	10.9

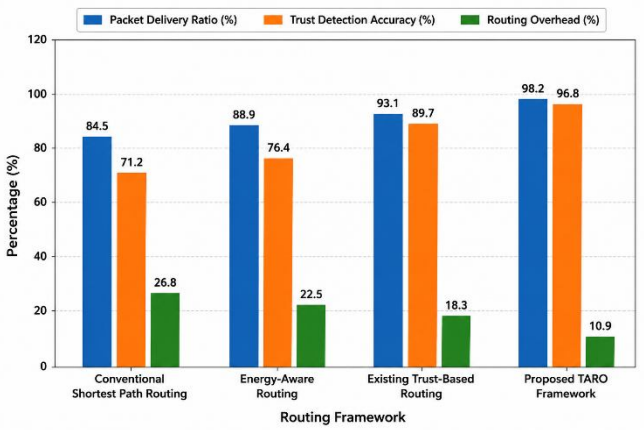


Fig. 2. Comparative Packet Delivery Ratio and Routing Overhead Analysis of Smart Grid Routing Frameworks

Fig. 2 demonstrates that the proposed TARO framework outperforms existing routing approaches by achieving superior communication reliability while simultaneously reducing unnecessary routing operations.

C. Latency and Throughput Performance Analysis

The latency and throughput evaluation examines the capability of the proposed framework to support real-time smart grid communication applications under varying traffic conditions shown in TABLE II.

TABLE II. Comparative Latency, Throughput, and Network Lifetime Analysis

Framework	Average Delay (ms)	Throughput (Mbps)	Network Lifetime (Hours)
Conventional Shortest Path Routing	118	46.2	720
Energy-Aware Routing	96	58.5	894
Existing Trust-Based Routing	81	67.8	1012
Proposed TARO Framework	52	82.6	1187

The proposed TARO framework achieved the lowest communication delay and highest throughput among all evaluated routing mechanisms. The trust-aware optimization engine selects stable communication paths with reliable forwarding behavior, thereby minimizing retransmissions and communication interruptions. Furthermore, the inclusion of residual energy metrics during route selection contributes to prolonged network lifetime by preventing excessive utilization of individual nodes.

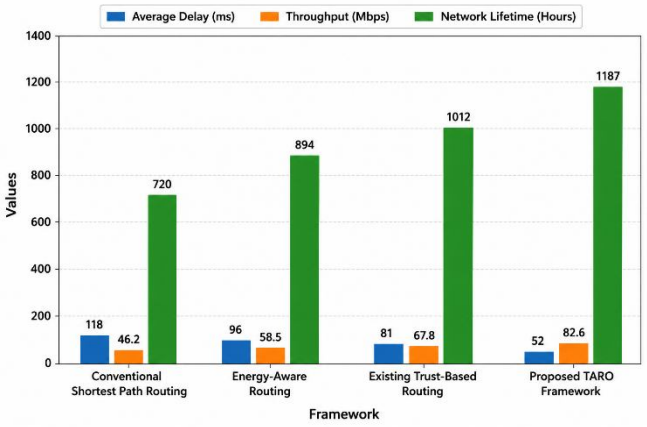


Fig. 3. Comparative Latency and Throughput Analysis of Smart Grid Routing Frameworks

Fig. 3 illustrates that the proposed framework consistently delivers superior communication performance under both normal and high-traffic smart grid operating conditions.

D. Scalability and Dynamic Node Profiling Analysis

The scalability analysis evaluates the effectiveness of the proposed framework as the number of participating smart grid communication nodes increases listed in TABLE III.

TABLE III. COMPARATIVE LATENCY, THROUGHPUT, AND NETWORK LIFETIME ANALYSIS

Number of Nodes	Conventional Routing PDR (%)	Existing Trust Routing PDR (%)	Proposed TARO PDR (%)
500 Nodes	89.3	94.2	98.5
1000 Nodes	87.1	93.4	98.2
2000 Nodes	84.7	92.1	97.8
4000 Nodes	81.9	90.8	97.1
6000 Nodes	79.5	89.3	96.5

The proposed TARO framework maintains consistently high packet delivery performance even as network size increases significantly. The dynamic node profiling mechanism continuously updates trust assessments and network conditions, enabling adaptive routing decisions under large-scale deployments.

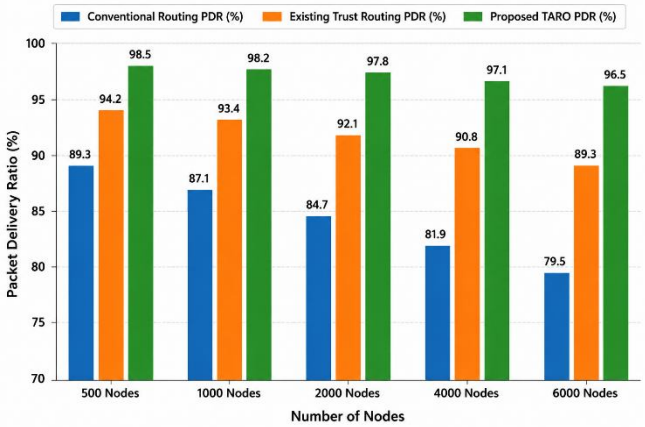


Fig. 4. Scalability Analysis of Trust-Aware Routing Optimization Framework Under Increasing Smart Grid Node Density

The results presented in Fig. 4 confirm that the proposed framework provides superior scalability, routing reliability, communication efficiency, and security performance for next-generation smart grid communication infrastructures. The combination of dynamic node profiling and trust-aware route optimization enables resilient and adaptive data transmission capable of supporting large-scale smart grid deployments.

V. CONCLUSION AND FUTURE SCOPE

This paper presented a Trust-Aware Routing Optimization (TARO) framework for secure and efficient data transmission in smart grid communication networks using Dynamic Node Profiling. The proposed framework integrates trust evaluation, node behavior assessment, residual energy monitoring, communication reliability analysis, and adaptive route optimization to identify secure and efficient communication paths. Experimental results demonstrated that the TARO framework significantly improves packet delivery ratio, throughput, network lifetime, and trust detection accuracy while reducing communication delay and routing overhead compared with conventional routing approaches. The dynamic profiling mechanism effectively identifies unreliable and malicious nodes, thereby enhancing network security, communication resilience, and operational reliability in smart grid environments.

Future research can focus on integrating machine learning and deep learning techniques for predictive trust assessment and autonomous routing decisions in highly dynamic smart grid networks. Furthermore, the incorporation of blockchain-based trust management, federated learning for distributed intelligence, and quantum-resistant security mechanisms can further strengthen communication security and scalability. The proposed framework can also be extended to support next-generation smart energy infrastructures, including renewable energy integration, vehicle-to-grid communications, and large-scale Internet of Energy ecosystems.

REFERENCES

[1] R. Li, J. Feng, X. Liu, F. Du and C. Xing, "An Improved Genetic Algorithm-Based Approach to Secure Monitoring of Big Data for Dynamic Transmission in Smart Grids," 2024 6th International Conference on Frontier Technologies of Information and Computer (ICFTIC), Qingdao, China, 2024, pp. 15-18, doi: 10.1109/ICFTIC64248.2024.10913078.

[2] C. Chen, S. Shen, Y. Yan, D. Yan and S. Zheng, "Research on Data Privacy Protection Algorithm of Smart Grid Based on Full Homomorphic Encryption," 2025 International Conference on Electrical Drives, Power Electronics & Engineering (EDPEE), Athens, Greece, 2025, pp. 1148-1154, doi: 10.1109/EDPEE65754.2025.00207.

[3] C. Siyu, S. Hang, W. Yiqun, T. Lingyi, S. Xiaojing and H. Fengzhu, "Design and Research of Power Grid Data Transmission System Based on LoRa Technology," 2024 IEEE 3rd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), Changchun, China, 2024, pp. 1524-1528, doi: 10.1109/EEBDA60612.2024.10485668.

[4] T. Guan, Q. Zhang, X. Zhao, H. Chen and T. Zhang, "Research on the Method of Smart Meter Data Crossing the User-Side Network," 2025 7th International Conference on Electronics and Communication, Network and Computer Technology (ECNCT), Guangzhou, China, 2025, pp. 654-659, doi: 10.1109/ECNCT66493.2025.11172440.

[5] L. Wang, Z. Zhang, X. Kong, L. Guo, X. Li and W. Xue, "Design of Real-Time Data Acquisition and Preprocessing System for Smart Grid Based on FPGA," 2025 IEEE 26th China Conference on System Simulation Technology and its Applications (CCSSTA), Shenzhen, China, 2025, pp. 337-341, doi: 10.1109/IEEECONF65522.2025.11137156.

[6] J. Zhang, Z. Li, R. Dong, J. Wang and X. Qiao, "Analysis of the Impact of Information Systems on Grid Stability in Smart Grid Construction," 2025 2nd International Conference on Computer Communication, Networks and Information Science (CCNIS), Newcastle, United Kingdom, 2025, pp. 366-369, doi: 10.1109/CCNIS69465.2025.00070.

[7] V. Sharma and S. Kumar, "Role of Artificial Intelligence (AI) to Enhance the Security and Privacy of Data in Smart Cities," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 596-599, doi: 10.1109/ICACITE57410.2023.10182455.

[8] L. Yang, B. Lv, J. Yu, G. Wang and X. Lai, "Research on the Security Control of Electric Energy Data Based on Key Generation and Homomorphic Encryption Technology," 2025 International Conference on Digital Analysis and Processing, Intelligent Computation (DAPIC), Incheon, Korea, Republic of, 2025, pp. 665-669, doi: 10.1109/DAPIC66097.2025.00128.

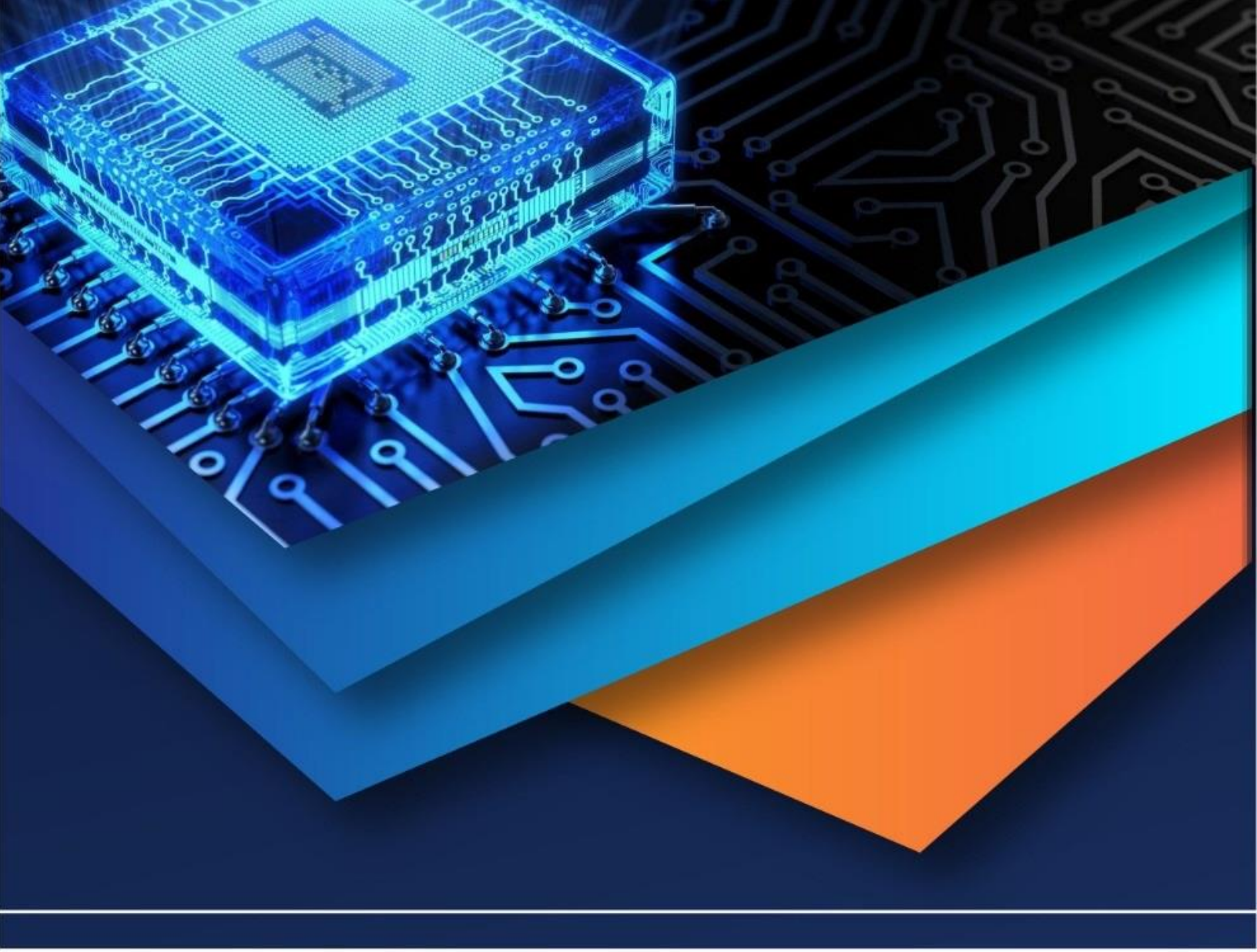
[9] G. Prabhakar and K. S, "Secured IoT-Based Neighborhood Area Network for Real-Time Energy Data Management in Smart Grids," 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), Vellore, India, 2024, pp. 1-5, doi: 10.1109/ic-ETITE58242.2024.10493344.

[10] M. Kumar, K. K. Gautam, V. Sharma, B. Samania, T. K. Vashishth and S. Chaudhary, "Enhancing Cloud Computing Performance: A Novel Approach for Optimizing Energy Efficiency through AI- Based Load Balancing Algorithm," 2025 International Conference on Intelligent Computing and Knowledge Extraction (ICICKE), Bengaluru, India, 2025, pp. 1-6, doi: 10.1109/ICICKE65317.2025.11136754.

[11] C. Huang, J. Zeng, F. Zhang, Y. Zhang and W. Zhang, "Real-time and Scalability of Smart Two Ticket System Based on Edge Computing in Power Grid Management," 2024 Second International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2024, pp. 1-5, doi: 10.1109/ICDSIS61070.2024.10594464.

[12] X. Ma, X. Liu, S. Fan, L. Cheng and Z. Chen, "Design of Transmission Line Lightning Monitoring System Based on LoRa Technology," 2025 IEEE International Conference on Power Systems and Smart Grid Technologies (PSSGT), Chongqing, China, 2025, pp. 151-155, doi: 10.1109/PSSGT64932.2025.11034201.

[13] H. AlMarzooqi, Y. Walweel, M. Saeed, H. A. Hamadi, G. A. Hussain and M. Hasan, "Machine Learning Model for Cyber Security Attack Detection in Smart Grid Network," 2025 IEEE PES Conference on Innovative Smart Grid Technologies - Middle East (ISGT Middle East), Dubai, United Arab Emirates, 2025, pp. 1-5, doi: 10.1109/ISGTMiddleEast65737.2025.11314444.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY