I.J. Information Technology and Computer Science, **2026, 1, 1-13**
Published Online on February 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2026.01.01

IoT Driven HRES Smart Grid with Advanced Routing and IQKM Security Mechanism

J. B. Shriram*
Department of Information Technology, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, Tamil Nadu, India
E-mail: shriramjbs@gmail.com
ORCID iD: https://orcid.org/0009-0001-9073-9444
*Corresponding author

P. Anbalagan
Department of Electrical and Electronics, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, Tamil Nadu, India
E-mail: anbu@aubit.edu.in
ORCID iD: https://orcid.org/0000-0003-1514-1298

A. Vegi Fernando
Department of Computer Science and Engineering (AIML), Dayananda Sagar University, Bengaluru, Karnataka-562112, India
E-mail: a.vegifernando@gmail.com
ORCID iD: https://orcid.org/0009-0000-3272-7448

Srikanth Mylapalli
Faculty of Computer Science and Engineering, Tirumala Engineering College, Jonnalagadda, Narasaraopet, Guntur, A.P, India
E-mail: kanth582@gmail.com
ORCID iD: https://orcid.org/0009-0002-3487-7903

Received: 07 July 2025; Revised: 19 August 2025; Accepted: 11 October 2025; Published: 08 February 2026

Abstract: Expansion of Internet of Things (IoT) technologies has greatly enhanced monitoring and management of energy systems, especially in Hybrid Renewable Energy Systems (HRES). This paper presents an IoT-based HRES smart grid framework with a modified Brain Storm Optimization (BSO) algorithm for routing optimization and an Improved Quantum Key Management (IQKM) is a quantum inspired protocol for better data security. The enhanced BSO algorithm, hosted in the cloud infrastructure, optimizes IoT sensor data routing paths, thus diminishing packet transmission latency and improving the network throughput. In contrast to conventional BSO techniques, the enhancement is through dynamic cluster refinement and adaptive node prioritization, designed specifically for real-time cloud-integrated energy systems. In order to protect sensitive energy transmission information, the IQKM protocol includes strong quantum-aided encryption processes and dynamic key creation. These enhancements directly counter the dangers of man-in-the-middle and replay attacks, which exceed capabilities of standard encryption approaches by facilitating low-latency, quantum-resistant communication between HRES nodes. Both Photovoltaic (PV) and wind-based energy sources are utilized by the system to provide power consistently, with cloud-based analytics and IoT sensors ensuring real-time monitoring. Experimental testing via the Adafruit platform reports a 23% Packet Delivery Ratio (PDR) enhancement and 17% encryption/decryption delay reduction compared to baseline and traditional routing algorithms. Such findings ensure the potential for stable, secure, and scalable grid performance by the proposed system.

Index Terms: IoT, HRES, Shortest Routing Path, BSO, Advanced Encryption and Improved Quantum Key Management (IQKM).

1. Introduction

Smart grid system is designed for monitoring the flow of electricity and operational information over a robust and reliable communication network [1]. Smart grids incorporate information and digital communication approaches into power grid systems [2]. At present, smart grid has drastically developed and created an uprising revolution in electric grid system [3, 4]. IoT integrated smart grid systems enable improved capability for providing enhanced generation, transmission and distribution of electricity [5]. Significantly, smart grid provides various benefits including real-time monitoring of data for achieving optimized energy flow, process management, and production management in HRES [6,7]. Hence, communication topologies play an essential role in smart grid advancement as they allow the transmission of data and information among various components of system [8]. Thus, several topologies and techniques are innovated for obtaining enhanced transmission of data with distributed energy monitoring [9].

These topologies are developed to attain energy-efficient and reliable smart grid operation, despite this, selecting shortest or optimum routing path for data or information transmission in smart grid includes evaluating several attributes such as reliability, scalability, bandwidth for data transmission and grid requirements [10]. Various approaches are considered for achieving shortest routing path in smart grid systems such as, SMAx algorithm-based routing for smart grid is introduced in [11] for attaining energy efficient routing. The utilization of SMAx enables to minimize the network collisions by adjusting the routing paths on the basis of real time grid monitoring conditions. Nevertheless, SMAx algorithm is prone to transmission overhead issues, thereby reducing the reliability of the model. Significantly, [12-15] introduces a fault-tolerant routing algorithm for attaining efficient routing towards smart grid. The deployment of fault fault-tolerant routing algorithms enables to eliminate crowding transmissions of information within the network, thus reducing network latency with assured distribution balancing while choosing optimum routing path. Despite these benefits, their implementation is quite expensive with higher complexity and scalability issues. The authors in [16] utilized Reposition Particle Swarm Optimization (RA-RPSO) based algorithm to acquire an enhanced routing algorithm. Integrating RA-RPSO for high-dimensional routing in large-scale networks provides effective path optimization with energy-efficient routing, However, RA-RPSO is sensitive to network parameters and requires further parameter tuning.

Similarly, the authors in [17] innovated PSO with Grey Wolf Optimization (PSO-GWO) based energy efficient optimal routing algorithm for selecting the optimum route which attains enhanced global search ability, thereby, achieving real-time routing in dynamic networks. Nevertheless, they struggle with transmission overhead and overfitting issues. Hence, achieving efficient path routing is considered as an essential part, in addition to selecting an optimum routing path, it is equally crucial to achieve enhanced security and protected information transmission against cyber threats. Henceforth, various conventional key management for improved data security while transmitting is listed below in Table 1 along with its benefits and shortcomings.

Table 1. Conventional key management techniques

Key management Technique	Benefits	Shortcomings
Symmetric Key management [18]	Fast and Efficient	Complex key management
Asymmetric Key management [19]	Easy to accomplish secure transmission of data	Slow processing time
Identity-based key management [20]	Enhanced encryption with secure key transmission	Sensitive to quantum attack
Kerberos Key Management [21]	Applicable for larger networks	Still not completely reliable as they require secure channel-based transmission

1.1. Research Problem

The existing smart grid routing protocols such as SMAx, fault-tolerant and hybrid-metaheuristic approaches struggle from transmission overhead incur transmission overhead, network parameter sensitivity, and scalability issues. The smart grid needs an adaptive, low-complexity routing mechanism that adjusts dynamically to real-time grid parameters while reducing latency and guaranteeing smooth data propagation in HRES-based smart grids.

Henceforth, to overcome the above-discussed limitations associated with optimum shortest path routing and key management, this paper proposes an IoT-driven HRES smart grid with an advanced routing IQKM security mechanism. The integration of BSO algorithm for routing with IQKM security approach provides improved transmission and monitoring of HRES based smart grid system with highly secured and protected information transmission.

1.2. Contribution

- IoT Sensors constitute the data acquisition layer, allowing the real-time monitoring of PV, wind turbine, battery, and grid conditions.
- The sensory inputs are computed through a cloud-based infrastructure, which implements both the Modified BSO algorithm for adaptive routing and implements the IQKM protocol for secure communication.
- The HRES is the physical energy foundation, dynamically providing power, and the IoT–cloud integration provides transparency of data, adaptive control, and low-latency encrypted transfer.

The tri-layer integration increases overall system robustness by dynamically adapting transmission routes according to real-time grid metrics through cloud-hosted BSO, and facilitating smooth data exchange with end-to-end visibility for predictive fault identification and energy efficiency.

The major outline and objectives of the proposed work is listed below,

- To provide a stable and efficient power supply while allowing secure, intelligent data communication, a hybrid renewable energy system-based smart grid structure is used.
- For guaranteeing strong, delay-sensitive routing in dynamic energy networks, a modified BSA algorithm is used. It chooses best paths with both transmission efficiency and cryptographic constraints in mind to provide secure and reliable data flow.
- To provide security and integrity of data, an improved quantum key management protocol is incorporated. It co-evolves with the routing policy by dynamically adjusting key refresh rates and encryption strength according to route stability, exposure risk, and network conditions

2. Proposed Modelling

The developed work represented in Fig.1, is innovated by combining IoT with HRES-based smart grid for optimized energy distribution and secured information transmission. The process begins with HRES where, IoT based sensors are utilized for real-time monitoring of PV, wind, Battery and grid outputs. This real-time HRES monitoring enables end user to receive rapid information regarding grid fault or any other interferences, hence, to transmit these data to the end user without delay, BSO based shortest routing path algorithm is utilized. After, selecting the optimum routing path for data transmission, to ensure secure and protected information transmission IQKM security mechanism is deployed.

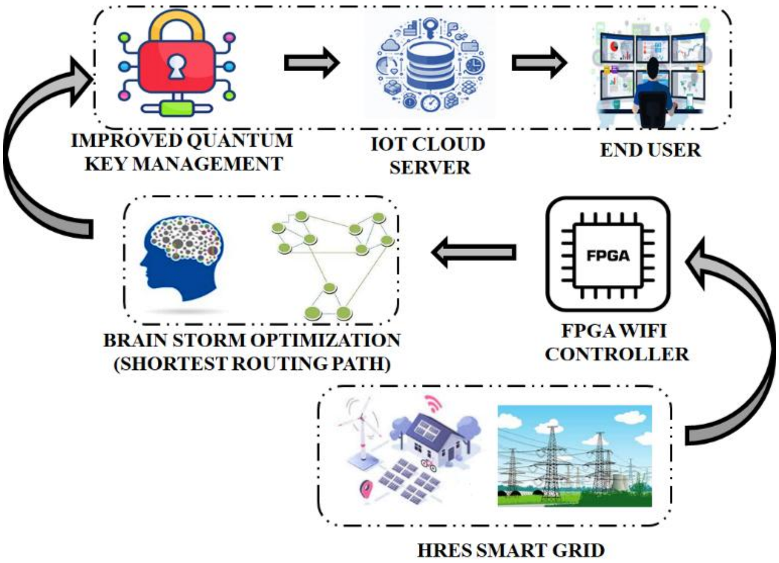


Fig.1. Proposed system block diagram

IQKM enables secure data transmission by protecting it against cyber threats and attacks. Later, these data is fed to IoT cloud server which processes and stores the data for easy management and accessibility. From the cloud server, the data then given to end user, enabling real-time monitoring and management of HRES based smart grid. Therefore, the system as a whole assures advanced routing utilizing BSO algorithm with highly secure transmission using IQKM security mechanism.

2.1. Modelling of HRES Smart Grid

HRES comprises of PV array, Wind turbines and one battery as illustrated in Fig.2, for providing enhanced power supply for the smart grid system. The modelling of each component of the HRES is discussed in detail below,

A. Modelling of Photovoltaic (PV) System

The PV system consists of PV cells, which is commonly known as solar cells, is utilized for converting sunlight directly to electricity. The PV system is attached to the HRES DC-bus using the DC–DC converters. The deployment of DC-DC converters enables, PV array to extract maximum power by controlling the PV terminal voltage. The nonlinear relationship existing between power and voltage of the PV panels is called as P-V characteristics.

The PV system performance efficiency depends on the PV module parameters such as solar irradiation and ambient temperature. The PV power generated is determined using,

$$P_{\mathrm{PV}}(t) = \mathrm{H}_t(t).\,\mathrm{PVA}.\,\eta_c\,(t).\,\eta_{\mathrm{DC}} \tag{1}$$

Where, $H_t\ (t)$ represents the solar irradiation on PV array (PVA), $\eta_c\ (t)$ denotes the convergence efficiency, η_{DC} implies the converter efficiency respectively.

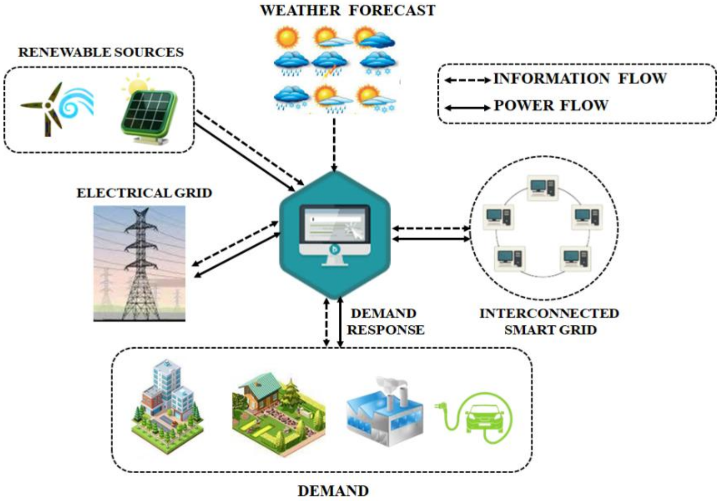


Fig.2. Architecture of HRES based Smart grid system

$$\eta_c\ (t) = \eta_{cr}[1 - \beta_t.(T_c\ (t) - T_{cr}\ )] \tag{2}$$

$$T_c\ (t) = T_a\ (t) + 3H_t\ (t) \tag{3}$$

Where, T_{cr} represents rated temperature, $T_c\ (t)$ implies current temperature of PV cells and β_t denotes temperature coefficient.

B. Modelling of Wind Energy System

The wind turbine is utilized for generating electricity form wind speed. For attaining increased electricity production, wind turbines are installed on higher altitudes where the wind speed is altered to elevation of wind turbine at the height of wind turbine which is mathematically expressed as,

$$u(h) = u(h_g)\left(\frac{h}{h_g}\right)^{\propto} \tag{4}$$

Where, $u(h)$ and $u(h_g)$ indicates wind speed at hub height (h) and anemometer height (h_g). The output obtained from wind turbine is termed as,

$$P_w(u) = \begin{cases} 0, \quad u\langle u_c\ or\ u\rangle u_f \\ p_r \dfrac{u_2 - u_c^2}{u_r^2 - u_c^2}, u_c \le u \le u_r \\ p_r, u_r \le u \le u_f \end{cases} \tag{5}$$

Where, P_w is the wind turbine output power, p_r represent the rated output power, u_c indicate the cut-in wind speed and u_f represent the cut-off wind speed respectively. Additionally, IoT sensors are utilized for monitoring the smart grid performance and for sending these gathered data inside the HRES framework, routing algorithm plays an essential role, thus BSO based routing algorithm is utilized for attaining optimum routing path.

2.2. Modelling of Modified BSO based Routing Algorithm

The brainstorming process, which is a swarm intelligent algorithm based on the human idea creation process, provides the foundation for the development of modified BSO. Modified BSO is widely utilized in energy optimization process of smart grid and further simplified to attain local and global search. Modified BSO is typically a search space reduction-based algorithm in which solutions are divided into various clusters which are denoted as problem's local optima. Initially, Modified BSO, information area comprises of solutions with finest values which are procreated from one cluster to another. Modified BSO at first, analyze the decision space and later examine and exploit state of equilibrium after iterations and Fig. 3 represents the Modified BSO algorithm flowchart.

Algorithm 1: Modified BSO operation procedure

1 Generate n candidate solutions randomly and assess their fitness based on predefined metrics.
2 Continue the optimization process up to a specified maximum number of iterations or until the optimal solution is found.
3 Partition n solutions into m distinct clusters using a clustering algorithm (e.g., K-means) to facilitate localized search.
4 Randomly select one or two clusters to synthesize new individuals based on intra- and inter-cluster attributes.
5 Evaluate the newly generated candidate against its index-matched counterpart in the population; retain the superior individual for the next generation.
6 Reassess all n solutions in the updated population to prepare for the next iteration cycle.

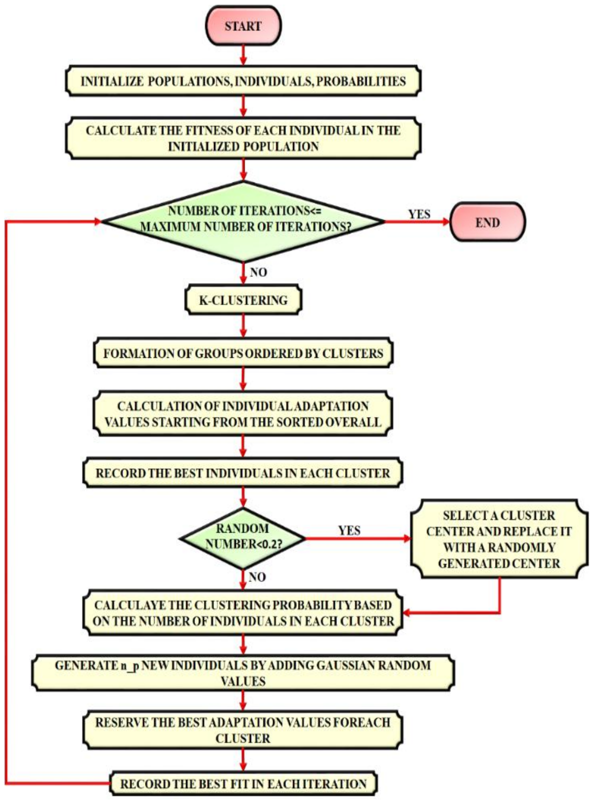


Fig.3. Modified BSO algorithm flow chart

Modified BSO comprises of clustering, generation, and selection which further discussed.

A. Clustering

Individuals for each objective are clustered in each iteration, and clusters are formed in objective space. Person who does better in the majority of the goals is chosen for the following iterations.

Algorithm 2: Solution clustering Approach

1 Partition the n candidate solutions into m clusters using the K-means clustering algorithm.
2 Within each cluster, rank the individuals based on fitness and designate top-ranked individual as the cluster center.
3 Generate a random scalar $r_{clustering} \in [0, 1)$;
4 If $r_{clustering} < P_{clustering}$ (a pre-determined probability) then.
5 Randomly select a cluster center.
6 Stochastically generate a new candidate solution to replace chosen cluster center.

B. New Individual Generation

Newly synthesized solution originate from a single entity, multiple candidate individuals, or representative clusters depending on the generation logic and optimization strategy. A probability value of $p_{generation}$ is used for evaluating the new individual. Generating clusters from one cluster eventually improves the search space and enhances the exploitation capability. The new cluster is generated using,

$$x^i_{new} = x^i_{old} + \xi(t) \times rand() \tag{6}$$

$$\xi(t) = logsig\left(\frac{0.5 \times T - t}{k}\right) \times rand() \tag{7}$$

Where t is the maximum number of iterations, k is the coefficient to change the slope of the $logsig$ () function of the step size function $\xi\ (t)$, which is used to adjust the algorithm's convergence speed, and x^i_{new} and x^i_{old} are the ith dimensions of x_{new} and x_{old} .

C. Selection

This stage is used for attaining finest solution for all individuals and better solutions is kept by chosen stage after each cluster production. The clustering and individual approach introduces new solutions to the swarm intelligence algorithm, thus enhancing the overall diversity of the algorithm. However, it is crucially important to transmit these data safely by protecting it against cyber threats, due to this reason IQKM based security mechanism is implemented which is discussed in the later section.

D. Modified BSO Adaptation for Smart Grid Routing

The modified BSO technique is improved specially for energy-focused smart grid settings through the addition of dynamic cluster refinement and node priority adaptation mechanisms. These adaptations enable the routing framework to effectively cope with real-time fluctuations in grid parameters like load demand, latency sensitivity, and transmission reliability. Within the clustering stage, K-means is supplemented with grid-state-weighted rankings that rank nodes according to their energy contribution and fault exposure levels. When generating individuals, the algorithm incorporates time-sensitive convergence control by employing a logarithmic sigmoid function to trade off exploration and exploitation so that routing paths that are energy efficient as well as topologically resilient are formed. These intelligent grid-related enhancements make BSO a responsive and scalable routing solution for dynamic HRES-based IoT environments.

2.3. Modelling of IQKM Security Mechanism

Improved Quantum Key Distribution (IQKD) is a growing approach for attaining enhanced security, it extends the working principles of Quantum Key Distribution (QKD) with two key enhancements specially designed for use in smart grid environments: dynamic key refresh logic and routing-integrated encryption strength modulation. In contrast to standard QKD systems, where fixed intervals of key generation and static cryptographic strength are supported, IQKM co-evolves with the routing dynamics and fault exposure levels of the system. IQKD functions by generating and distributing shared key among the sender and the receiver. The security key of IQKD is generally based on the fundamental principles of quantum mechanism and the structure of basic IQKD is represented in Fig. 4.

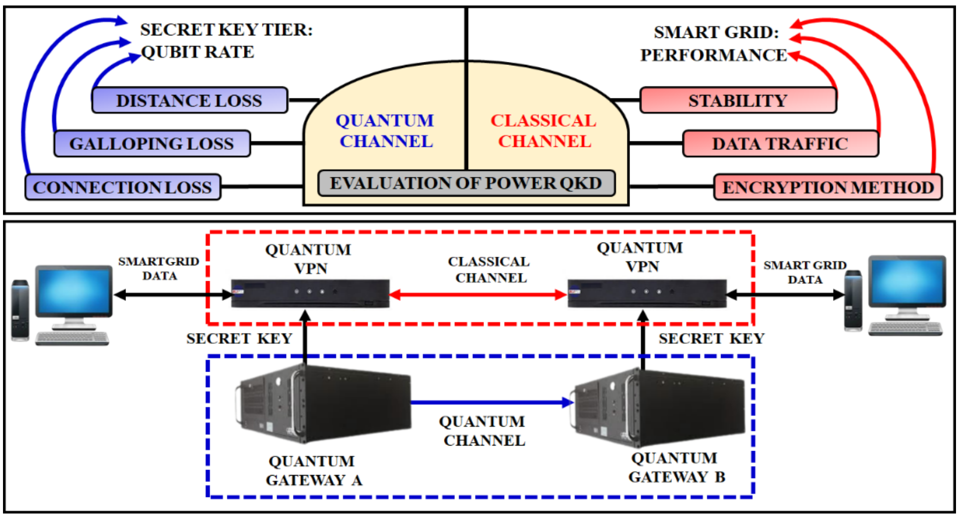


Fig.4. IQKD structure

Key distribution between two parties is accomplished using both quantum and classical channels and is expressed as,

$$Q = 2\times\left[A + \frac{\log\frac{\frac{Q}{2}}{\log 2}}{\log 2} + S\frac{Q}{2} + L\right] \tag{8}$$

Where, Q refers to the original key, A represents the length of the final key, S refers to the percentage of the original key and L denotes the number of bits leaked through the key reconciliation process.

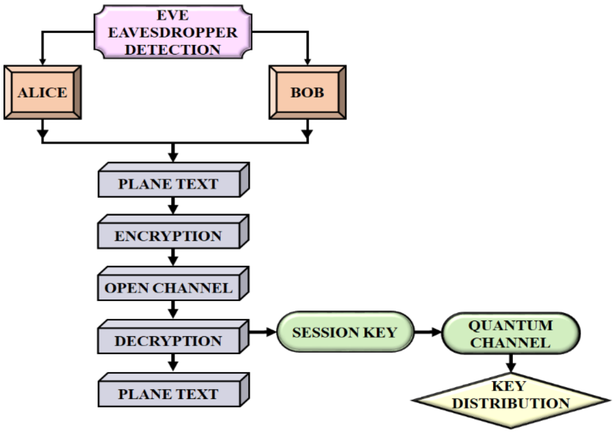


Fig.5. IQKD flow chart

However, Fig.5 certain QKD features assures that any unauthorized access on the key exchange process leads to communication errors. Significantly, highly secure key transmission is achieved only if the errors contain threshold value below the defined threshold or else, QKD drops the present process and restarts. Therefore, the system as a whole ensures enhanced and reliable performance of IoT driven HRES based smart grid system.

IQKM Protocol for Smart Grid Security

The IQKM protocol self-adapts critical refresh rates according to variation in routing stability, latency dynamics, and node trust levels obtained from the Modified BSO routing framework. This synthesis provides that secure communication routes are secured in real-time, with stronger keys being used in risk-prone transmission areas and reduced cryptographic tasks facilitated where high-speed data transfer is valued. Such synergy between key distribution and routing metrics establishes a low-latency, quantum-resilient communication backbone uniquely suited for IoT-driven HRES smart grids.

3. Results and Discussion

This section deals with performance analysis of proposed system which is implemented utilizing adafruit software.

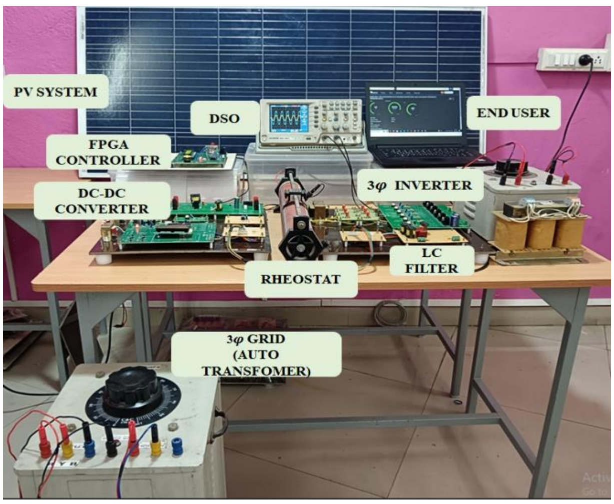


Fig.6. Hardware components of the proposed system

Fig. 6. showcases the real-world implementation of the proposed smart grid architecture, combining photovoltaic systems with IoT-based sensors and essential hardware for energy generation, control, and monitoring. This setup facilitates optimized data transmission and secure communication by leveraging Adafruit's platform, enabling seamless interaction between renewable energy inputs and grid management components within the HRES framework.

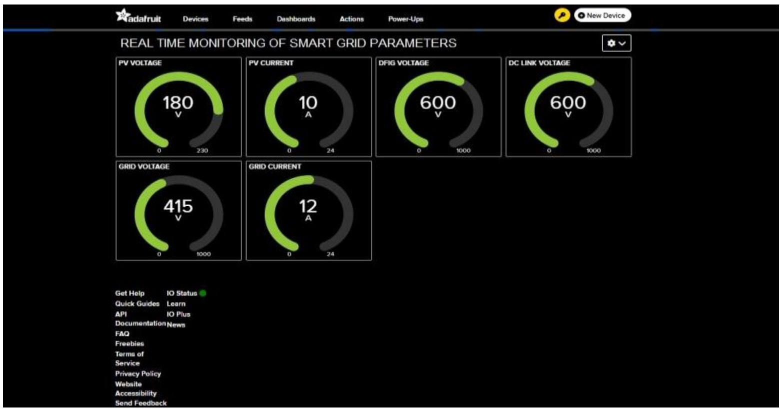


Fig.7. Real-Time monitoring of smart grid parameters

Fig. 7. showcases the Real-Time monitoring of smart grid parameters which are displayed via the Adafruit webpage comprises of proposed system metrices such as PV voltage of 180V, PV current of 10 A, DFIG voltage of 600V, DC link voltage of 600 V respectively. In addition to this, grid parameters observed shows that grid voltage is at 415 V and grid current is of 12 A respectively. Therefore, by consistent monitoring of smart grid parameters enables the system to adapt to changes, thus improving the reliability and effectiveness of proposed system.

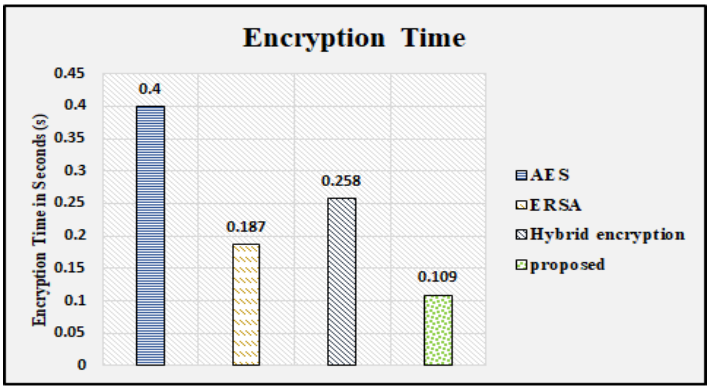


Fig.8. Comparison of encryption time

Fig.8. represents encryption time comparison among various encryption algorithms, highlighting effectiveness of proposed model integrated with improved quantum key management protocol. The proposed system demonstrates a significantly reduced encryption time, showcasing its optimized quantum-aided encryption and dynamic key generation capabilities. In comparison, prevailing algorithms such as Advanced Encryption Standard (AES) [24], Enhanced Rivest–Shamir–Adleman (ERSA) [23], and Hybrid Encryption [22] recorded higher encryption times of 0.4s, 0.187s, and 0.258s respectively, indicating slower performance due to conventional static key structures and increased computational overhead. The faster encryption achieved by the proposed IQKM model emphasizes its suitability for real-time, secure communication within IoT-based HRES environments.

Fig. 9. illustrates the decryption time comparison across multiple models, further validating the proposed system's performance. The proposed model achieved a notably reduced decryption time of 0.015s, enabled by IQKM's lightweight cryptographic operations and adaptive key refresh mechanisms. This is substantially lower than the times recorded for AES, ERSA, and Hybrid Encryption algorithms, which exhibited relatively higher decryption latencies due to conventional decryption complexity. These results affirm that IQKM enhances both security and system responsiveness, making it highly suitable for dynamic IoT energy grid applications that demand low-latency data.

Fig. 10. shows PDR comparison between Intersection-based Routing using Q-learning (IQR) [25], Adaptive Equilibrium Optimizer (AEO) [26], Modified Grasshopper Optimization Algorithm (MGOA) [28] and proposed model, attaining higher PDR ensures enhanced network reliability. This chart states the improved communication efficiency of the proposed model which attained higher PDR of 92%, While, [25], [26] and [28] show reduced PDR of 84.10%, 86% and 83% respectively, which is low when compared with the proposed model.

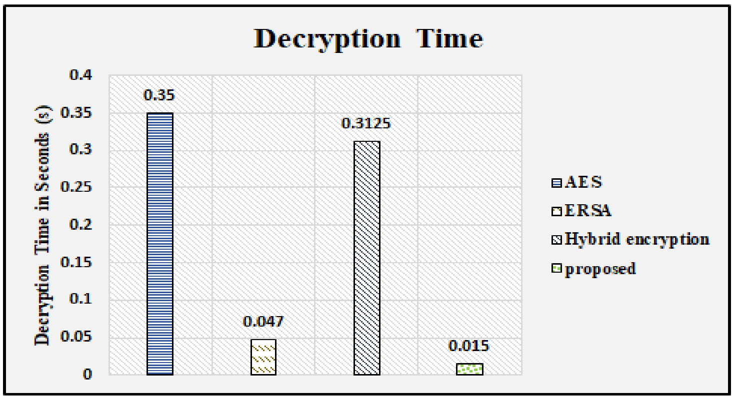
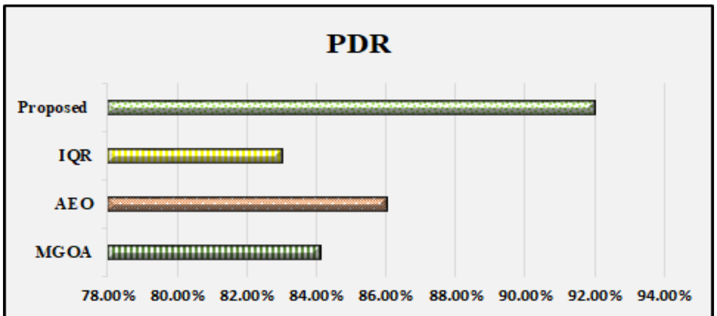


Fig.9. Comparison of decryption time



	MGOA	AEO	IQR	Proposed
PDR	84.10%	86%	83%	92%

Fig.10. Comparison of packet delivery ratio (PDR)

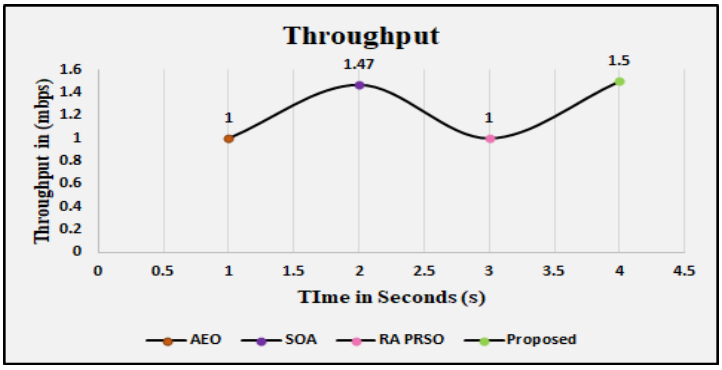


Fig.11. Throughput comparison

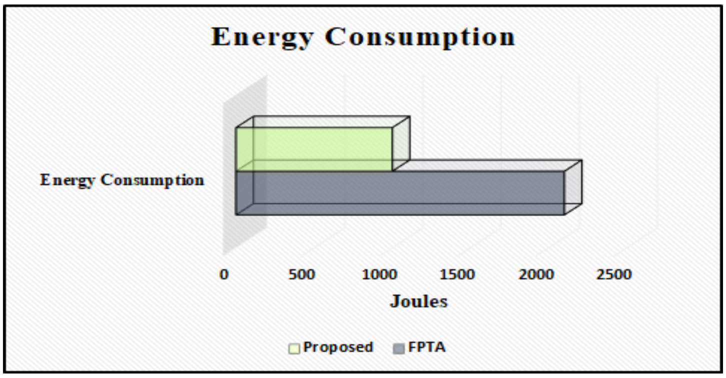


Fig.12. Energy consumption comparison

The throughput comparison of proposed model with various conventional topologies such as AEO [26], SOA [27] and RS PRSO [16] is depicted in Fig. 11. Where, increased throughput indicates the ability of the model to handle large amount of data. This chart showcases the reliability of the proposed model in terms of throughput by acquring higher throughput of 1.5 mbps respectively. Conversly, [26], [27] and [16] attained mildly reduced thruoghput.

Fig. 12. demonstrates Energy consumption comparison between FPTA and proposed model, where proposed model relatively consumed less energy of 1000 J than FPTA which consumed 2100 J, indicating that, proposed model attains enhanced performance with optimum routing, thereby, reducing the amount of total energy consumed and increases the overall system efficiency.

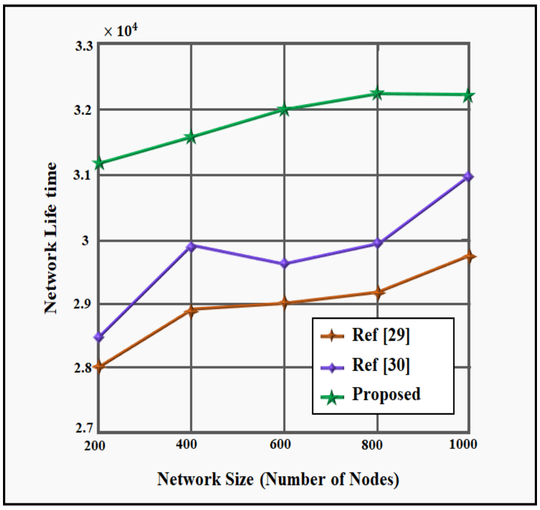


Fig.13. Network lifetime comparison

Fig. 13. shows a comparative analysis of network lifetime for increasing node numbers with respect to three routing protocols Energy-Aware Trust algorithm based on AODV protocol and Multi-path Routing strategy (EATMR) [29], Deep Belief Network (DBN) routing protocol [30], and the Proposed Model. As network size increases from 200 to 1000 nodes, the proposed model always exhibits the longest functioning lifetime, far outperforming both EATMR and DBN-based methods. This enhanced longevity is attributed to the dynamic routing adaptation and energy-efficient transmission control of the proposed protocol, providing optimized resource allocation throughout the HRES smart grid.

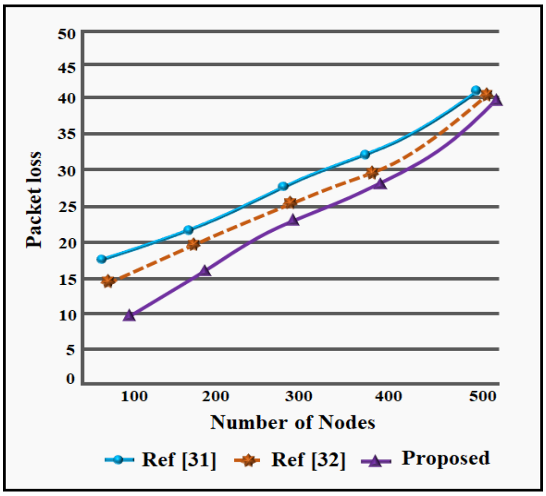


Fig.14. Packet loss ratio comparison

Fig. 14. represents the comparative analysis of packet loss against number of nodes (100 to 500 nodes) for various protocols such as Ad Hoc On-Demand Distance Vector–Packet Drop Battling Mechanism (AODV–PDBM) [31], Multipath Multimedia Dynamic Source Routing (MMDSR) [32], and the proposed IQKM-modified BSO Model. As the node density, all the protocols show increasing packet loss, but the proposed model shows consistently lower drop values. Conversely, AODV–PDBM and MMDSR exhibit sharper packet loss rates, indicating lower flexibility and congestion control. The outperformance of the proposed model indicates its solid packet processing and optimal route optimization under scalability restrictions in the HRES communication scenario.

Fig. 15. displays the comparison between node density and average latency of the Proposed model and the ML-Fresh protocol [33]. The x-axis measures node density in the range of 100 to 1000, and the y-axis measures average latency in milliseconds. The ML-Fresh protocol [33] illustrates high initial latency in sparse node conditions, which then decreases as node density rises. On the other hand, the Proposed model has uniformly low latency throughout the densities, reflecting its high scalability and lower delay even in heavy network conditions.

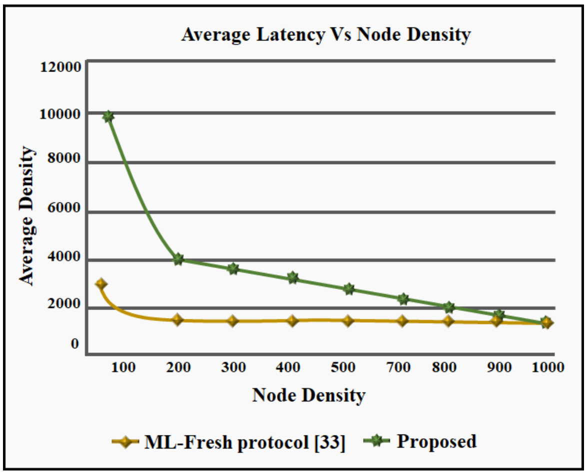


Fig.15. Latency comparison

4. Conclusions

The proposed Iot_based HRES smart grid system, integrated with Modified BSO algorithm and IQKM, ensures improved energy management and secure information transmission. The implementation of modified BSO algorithm into cloud environment effectively assures to find the optimum shortest routing path with minimized transmission losses. Significantly, the deployment of IQKM ensures secured and protected system functioning against possible cyber threats by allowing improved encryption process. The utilization IoT sensors and cloud platforms, enables real-time monitoring, control and optimization of HRES parameters. Furthermore, the incorporation of PV and WES allows stable power supply, thus improving the system reliability. In addition to this, Adafruit implementation results shows that, proposed system achieved reduced encryption and decryption time with increased PDR of 92%, indicating highly reliable and sustainable monitoring of HRES with protected and secured data transmisson within the smard grid architecture. Nonetheless, the computational requirements of the Modified BSO method and IQKM protocol could be imposing in terms of deployment on low-power IoT devices with limited memory and computational capabilities. Scaling the system to different heterogeneous energy infrastructures might also face interoperability and cost limitations. Optimizing the algorithms to run lightweight and testing them across wider deployment settings will be focus of future research.

References

[1] P. K. Udayaprasad, J. Shreyas, N. N. Srinidhi, S. D. Kumar, P. Dayananda, S. S. Askar, and M. Abouhawwash, “Energy Efficient Optimized Routing Technique with Distributed SDN-AI to Large Scale I-IoT Networks”, *IEEE Access,* vol. 12, pp.2742-2759, 2024, doi: https://doi.org/10.1109/ACCESS.2023.3346679.

[2] A. K. Soma, “Weighted Graph Clustering with PaCCo”, *In 2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, pp. 815-818. 2025, doi: https://doi.org/10.1109/ESIC64052.2025.10962723.

[3] C. L. D. Santos, A. M. Mezher, J. P. A. León, J. C. Barrera, E. C. Guerra and J. Meng, “ML-RPL: Machine Learning-Based Routing Protocol for Wireless Smart Grid Networks”, *in IEEE Access*, vol. 11, pp. 57401-57414, 2023, doi: 10.1109/ACCESS.2023.3283208.

[4] M. A. Islam, R. Atat and M. Ismail, “Software-Defined Networking-Based Resilient Proactive Routing in Smart Grids Using Graph Neural Networks and Deep Q-Networks”, *in IEEE Access*, vol. 12, pp. 111169-111186, 2024, doi: 10.1109/ACCESS.2024.3438938.

[5] Soma, Arun Kumar. "Enhancing Supply Chain Transparency and Integrity: A Permissioned Blockchain Framework." In 2025 International Conference on Emerging Systems and Intelligent Computing (ESIC), pp. 819-826. IEEE, 2025.

[6] A. K. Al Mhdawi, H. Al-Raweshidy, W. J. Al-Karkhi and A. Jaleel Humaidi, “Micro Software Defined Control (μSDC): Empowering Smart Grids with Enhanced Control and Optimization”, *in IEEE Access*, vol. 12, pp. 95750-95761, 2024, doi: 10.1109/ACCESS.2024.3421947.

[7] C. L. D. Santos, A. M. Mezher, J. P. A. León, J. C. Barrera, E. C. Guerra, and J. Meng, “Ml-rpl: Machine learning-based routing protocol for wireless smart grid networks”, *IEEE Access,* vol. 11, pp. 57401-57414, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3283208.

[8] A. K. Soma, “Building Aether Sensor Network using LoRaWAN Network”, *In 2025 International Conference on Emerging Systems and Intelligent Computing (ESIC),* pp. 807-814, 2025, doi: https://doi.org/10.1109/ESIC64052.2025.10962750.

[9] A. Khan, S. H. Shirazi, M. Adeel, M. Assam, Y. Y. Ghadi, H. G. Mohamed, and Y. Xie, “A QoS-Aware Data Aggregation Strategy for Resource Constrained IoT-Enabled AMI Network in Smart Grid”, *in IEEE Access*, vol. 11, pp. 98988-99004, 2023, doi: 10.1109/ACCESS.2023.3312552.

[10] A. kumar Soma, “Hybrid RNN-GRU-LSTM Model for Accurate Detection of DDoS Attacks on IDS Dataset”, Journal of Modern Technology, vol. 2, no. 01, pp. 283-291, 2025, doi: https://doi.org/10.71426/jmt.v2.i1.pp283-291.

[11] M. U. Saleem, M. R. Usman, M. A. Yaqub, A. Liotta and A. Asim, “Smarter Grid in the 5G Era: Integrating the Internet of Things with a Cyber-Physical System”, *in IEEE Access*, vol. 12, pp. 34002-34018, 2024, doi: 10.1109/ACCESS.2024.3372379.

[12] B. Priyanka, P. Udayaraju, C. S. Koppireddy, and A. Neethika "Developing a region-based energy-efficient IoT agriculture network using region-based clustering and shortest path routing for making sustainable agriculture environment", Measurement: Sensors, vol. 27, pp. 100734, 2023, doi: https://doi.org/10.1016/j.measen.2023.100734.

[13] Z. Ning, H. Chen, X. Wang, S. Wang, and L. Guo, "Blockchain-enabled electrical fault inspection and secure transmission in 5G smart grids", *IEEE Journal of Selected Topics in Signal Processing,* vol. 16, no. 1, pp. 82-96, 2021,doi: https://doi.org/10.1109/JSTSP.2021.3120872.

[14] T. Vaiyapuri, V. S. Parvathy, V. Manikandan, N. Krishnaraj, D. Gupta, and K. Shankar, "A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing", *Wireless Personal Communications,* vol. 127, no. 1, pp. 39-62, 2022,doi: https://doi.org/10.1007/s11277-021-08088-w.

[15] H. Mohapatra, and A. K. Rath "A fault tolerant routing scheme for advanced metering infrastructure: an approach towards smart grid", *Cluster computing,* vol. 24, no. 3, pp. 2193-2211, 2021, doi: https://doi.org/10.1007/s10586-021-03255-x.

[16] M. Elshrkawey, H. Al-Mahdi, and W. Atwa, "An enhanced routing algorithm based on a re-position particle swarm optimization (RA-RPSO) for wireless sensor network", *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 10304-10318, 2022,doi: https://doi.org/10.1016/j.jksuci.2022.10.022.

[17] S. Prithi, and S. Sumathi. "Automata based hybrid PSO–GWO algorithm for secured energy efficient optimal routing in wireless sensor network", *Wireless personal communications*, vol. 117, pp. 545-559, 2021, doi: https://doi.org/10.1007/s11277-020-07882-2.

[18] M. Sohal, and S. Sharma, "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing", *Journal of King Saud University-Computer and Information Sciences,* vol. 34, no. 1, pp. 1417-1425, 2022, doi: https://doi.org/10.1016/j.jksuci.2018.09.024.

[19] B. Alaya, and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks", *Journal of Information Security and Applications*, vol. 58, pp. 102779, 2021, doi: https://doi.org/10.1016/j.jisa.2021.102779.

[20] X. Li, S. Shang, S. Liu, K. Gu, M. A. Jan, X. Zhang, and F. Khan, "An identity-based data integrity auditing scheme for cloud-based maritime transportation systems", *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, no. 2, pp. 2556-2567, 2022, doi: https://doi.org/10.1109/TITS.2022.3179991.

[21] P. Du, X. Yan, and P. Feng, "Design of information security transmission scheme and related authentication services based on Kerberos", *Highlights in Science, Engineering and Technology,* vol. 60, pp. 266-273, 2023.

[22] A. Orobosade, T. A. Favour-Bethy, A. B. Kayode, and A. J. Gabriel, "Cloud application security using hybrid encryption", *Communications on Applied Electronics,* vol. 7, no. 33, pp. 25-31, 2020, doi: 10.5120/cae2020652866.

[23] R. Imam, F. Anwer, and M. Nadeem, "An effective and enhanced RSA based public key encryption scheme (XRSA)", *International Journal of Information Technology*, vol. 14, no. 5, pp. 2645-2656, 2022, doi: https://doi.org/10.1007/s41870-022-00993-y.

[24] Z. Lu, and H. Mohamed, "A complex encryption system design implemented by AES", *Journal of Information Security*, vol. 12, no. 2, pp. 177-187, 2021, doi: https://doi.org/10.4236/jis.2021.122009.

[25] M. U. Khan, M. Hosseinzadeh, and A. Mosavi, "An intersection-based routing scheme using Q-learning in vehicular ad hoc networks for traffic management in the intelligent transportation system", *Mathematics,* vol. 10, no. 20, pp. 3731, 2022, doi: https://doi.org/10.3390/math10203731.

[26] R. Hemalatha, R. Umamaheswari, and S. Jothi. "Optimal route maintenance based on adaptive equilibrium optimization and GTA based route discovery model in MANET", *Peer-to-Peer Networking and Applications*, vol. 14, no. 6, pp. 3416-3430, 2021, doi: https://doi.org/10.1007/s12083-021-01186-3.

[27] S. Vadivel, S. Konda, K. R. Balmuri, A. Stateczny and B. D. Parameshachari, "Dynamic route discovery using modified grasshopper optimization algorithm in wireless Ad-Hoc visible light communication network", *Electronics,* vol. 10, no. 10, pp. 1176, 2021, doi: https://doi.org/10.3390/electronics10101176.

[28] R. P. Pingale, and S. N. Shinde, "Multi-objective sunflower based grey wolf optimization algorithm for multipath routing in IoT network", *Wireless Personal Communications*, vol. 117, no. 3, pp. 1909-1930, 2021, doi: https://doi.org/10.1007/s11277-020-07951-6.

[29] H. Yin, H. Yang, and S. Shahmoradi, "EATMR: an energy-aware trust algorithm based the AODV protocol and multi-path routing approach in wireless sensor networks", *Telecommunication Systems*, vol. 81, no. 1, pp. 1-19, 2022, doi: https://doi.org/10.1007/s11235-022-00915-0.

[30] G. Arya, A. Bagwari, and D. S. Chauhan, "Performance analysis of deep learning-based routing protocol for an efficient data transmission in 5G WSN communication", *IEEE Access*, vol. 10, pp. 9340-9356, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3142082.

[31] A. F. Subahi, Y. Alotaibi, O. I. Khalaf, and F. Ajesh, "Packet Drop Battling Mechanism for Energy Aware Detection in Wireless Networks", *Computers, Materials & Continua,* vol. 66, no. 2, 2021, doi: https://doi.org/10.32604/cmc.2020.014094.

[32] E. Palacios Jara, A. Mohamad Mezher, M. Aguilar Igartua, R. P. D. Redondo, and A. Fernandez-Vilas, "QSMVM: QoS-aware and social-aware multimetric routing protocol for video-streaming services over MANETS", *Sensors,* vol. 21, no. 3, pp. 901, 2021, doi: https://doi.org/10.3390/s21030901.

[33] P. Garg, A. Dixit, and P. Sethi, "Ml-fresh: novel routing protocol in opportunistic networks using machine learning", *Computer Systems Science & Engineering, Forthcoming,* vol. 40, no. 2, pp. 703-717, 2022, doi: https://doi.org/10.32604/csse.2022.019557.

Authors' Profiles

Shriram J. B. received his B.Tech degree in Information Technology and B.E. degree in Electrical and Electronics Engineering from College of Engineering, Anna University, Guindy Campus, Chennai, Tamil Nadu, India in 2006. He obtained his M.E. degree in Computer Science and Engineering from Anna University of Technology, Tiruchirappalli, Tamil Nadu, India in 2010. He is currently working as Teaching Fellow in the Department of Information Technology at University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, Tamil Nadu, India. His research area covers Distributed Computing, Cloud Computing and Internet of Things.

Anbalagan P. received his B.E degree in Electrical engineering from Bharathiar University, Coimbatore, Tamil Nadu, India. He obtained his M.E degree in Power Systems Engineering from Anna University, Chennai, Tamilnadu, India and PhD degree in Faculty of Electrical Engineering from Anna University, Chennai, Tamil Nadu, India. He is currently working as Assistant professor in Electrical Engineering at BIT campus, University College of Engineering, Anna University, Tiruchirappalli, Tamil Nadu, India. His research area covers the application of power electronics in renewable energy systems, Power quality, Information and Communication Technologies.

A. Vegi Fernando received her Bachelor's degree in Computer Science and Engineering in 2004 from Manonmaniam Sundaranar University, Tamil Nadu, India. She obtained her Master of Engineering (M.E) in 2010 from Anna University, Chennai and Doctor of Philosophy (Ph.D) in 2023, both from Anna University, Chennai. She is currently serving as an Associate Professor in the Department of Computer Science and Engineering (AIML) at Dayananda Sagar University, Bengaluru, Karnataka, India. Her research interests include Computer Vision, Natural Language Processing and IoT.

M. Srikanth (Mylapalli Srikanth) received M.Tech degree in Computer Science and Engineering from KLEF, Vaddeswaram, Andhra Pradesh in 2011. He is currently working toward the Ph.D. degree at the Department of Computer Science Engineering, KLEF, Vaddeswaram, India. His research interests include Cloud Computing, Internet of Things and Artificial Intelligence.

How to cite this paper: J. B. Shriram, P. Anbalagan, A. Vegi Fernando, Srikanth Mylapalli, "IoT Driven HRES Smart Grid with Advanced Routing and IQKM Security Mechanism", International Journal of Information Technology and Computer Science(IJITCS), Vol.18, No.1, pp.1-13, 2026. DOI:10.5815/ijitcs.2026.01.01