F.NO.COE/Ph.D./(Notification)/595/2026 **Notification Date: 26/02/2026**

Student's Name: Shikha Kuchhal

Supervisor's Name: Prof. Ikbal Ali

Co-Supervisor's Name: Prof. Ibraheem

Name of the Department: Department of Electrical Engineering

Name of the topic: Secure and Efficient Information Communication for Smart Grid

Findings:

Key Words: Smart Grid Communication, Cybersecurity in Smart Grids, Advanced Encryption Standard (AES), Wireless Communication Networks, Smart Meter Security, Game Theory in Cybersecurity, Electric Vehicle (EV) Communication, Vehicle-to-Grid (V2G) Technology, Renewable Energy Integration, Solar–Wind Hybrid Energy Systems

The research identifies several important findings related to communication security, smart grid infrastructure, electric vehicle integration, and renewable energy management. It highlights that modern smart grids depend heavily on wireless communication technologies such as ZigBee, Wi-Fi, LoRaWAN, and 5G for real-time data exchange between smart meters, control centres, and energy resources. However, these communication channels are vulnerable to various cyber threats such as eavesdropping, spoofing, and denial-of-service attacks. The study finds that implementing the Advanced Encryption Standard (AES) significantly improves the security of data transmission while maintaining low latency and efficient performance. This makes AES suitable for devices with limited computing capacity such as smart meters and IoT devices used in smart grids.

Another important finding of the research relates to the security of smart metering systems. Smart meters are essential for monitoring electricity consumption and enabling demand response, but they can be targeted by cyber attackers who may manipulate energy data. The study introduces game-theoretic security models such as Stackelberg, Bayesian, and evolutionary games to analyze the strategic interaction between attackers and defenders. The results show that these models allow the system to dynamically adjust security strategies such as encryption strength and authentication frequency, thereby improving the resilience of smart grid networks against cyber threats.

The research also finds that electric vehicles (EVs) play an increasingly important role in smart grids through vehicle-to-grid (V2G) communication. However, EV networks are exposed to cyber risks including identity spoofing and data manipulation. The proposed lightweight security protocols and predictive defense mechanisms improve the reliability and safety of EV communication systems.

Finally, the study concludes that integrating renewable energy sources such as solar and wind with advanced communication technologies, energy storage systems, and intelligent grid management can enhance sustainability, reliability, and overall efficiency of modern power systems.