F.NO. COE/ Ph. D/(Notification)/578/2025 **Notification Date:08/05/2025**

Student's Name: Abdul Mazid

Supervisor's Name: Prof. Manaullah

Name of the Department: Department of Electrical Engineering

Name of the Topic: IoT Enabled Framework for Smart Automation with Enhanced Security Using Machine Learning

Key Words: Internet of Things, Smart Home Automation, Machine Learning, Blockchain Technology, Privacy-Preserving

Findings

The Internet of Things (IoT) is transforming modern life by connecting devices and enabling intelligent automation across domains such as smart homes, healthcare, and urban management. Despite its benefits, IoT faces challenges like cybersecurity risks, privacy threats, and scalability issues. This research addresses these gaps by developing advanced frameworks integrating machine learning, federated learning, blockchain, and ensemble learning to enhance smart home automation, intrusion detection, and smart city development.

A novel IoT-enabled smart home automation framework is proposed, leveraging AI and blockchain technology for real-time control, user preference learning, and secure data exchange. Smart contracts automate tasks like device authentication and billing, while a user-friendly interface ensures ease of access and control.

For network security, an intrusion detection framework using PCA, Pearson correlation, and CNNs (1D, 2D, 3D) is developed. Evaluated on datasets like Edge-IIoTset and NSL-KDD, it achieves up to 99.76% accuracy in binary classification and strong multiclass performance, significantly improving threat detection in IoT networks.

To preserve privacy, the FL-IDPP framework is introduced, combining federated learning and ensemble methods. It uses bidirectional RNNs for anomaly detection and maintains data on local devices, ensuring secure, decentralized model training with reduced communication overhead.

Finally, for smart cities, a decentralized, privacy-preserving framework is proposed, integrating blockchain, federated learning, and IPFS for secure data sharing, efficient storage, and scalable intrusion detection. Experimental results validate the frameworks' robustness, scalability, and privacy guarantees.

This research contributes significantly to secure, efficient, and scalable IoT ecosystems, laying the foundation for intelligent, trustworthy infrastructures that enhance quality of life and drive sustainable innovation.