Notification No: 566/2024
Date of Award: 06/09/2024

Name of Scholar: Mahsa Mirlashari
Name of Supervisor: Prof. S.A.M Rizvi
Department: Department of Computer Science, Faculty of Natural Science, Jamia Millia Islamia

Topic of Research: Designing IoT security framework for organizations

Key Finding

The rapid growth of IoT adoption has introduced significant challenges in securing devices, networks, and data. Key findings from this study emphasize the critical need for robust IoT security frameworks addressing vulnerabilities across various layers, including devices, communication protocols, and system architecture.

The study highlights four primary challenges: **authentication**, **authorization and access control**, **privacy**, and **secure architecture**.

- Authentication issues arise from inefficient key management and the absence of a reliable Certificate Authority.

- Authorization and access control face difficulties due to the heterogeneity of IoT nodes, requiring diverse mechanisms for ensuring secure access.

- Privacy concerns stem from the collection of sensitive data, necessitating user-centric, content-oriented, and context-oriented privacy models.

- A secure architecture must integrate IoT, Software-Defined Networks (SDN), and cloud infrastructure while combating malicious traffic and attacks.

- Machine Learning (ML), Neural Networks (NN), and Graph Neural Networks (GNN) have been identified as promising technologies to enhance IoT security frameworks.

- The above methods can mitigate threats like eavesdropping, denial-of-service attacks, and unauthorized access by enabling dynamic authentication, real-time intrusion detection, and adaptive access control.

- The proposed framework focuses on addressing existing gaps and designing a system that ensures scalability, reliability, and compliance with organizational needs, thereby enhancing IoT security posture.