Notification No: **F. NO. COE/ Ph. D./(Notification)/557/2024**

Notification Date: **09/04/2024**

Name of Candidate: **Raju**

Name of Supervisor: **Prof. (Dr.) Rajendra Kumar**

Name of the Department: Department of Computer Science

Faculty: Faculty of Sciences

Research Topic: **Computational intelligence Based Security for IoT**

Findings

Keywords: *Internet of Things (IoT), Computational Intelligence (CI), Security, Machine Learning (ML), Deep Learning (DL), Attack Detection*

The rapid expansion of the Internet of Things (IoT) has not only simplified device management but has also amplified security concerns. Challenges such as low power and computational capabilities in IoT exacerbate the difficulty of implementing robust security algorithms. In response, we propose **"Computational intelligence Based Security for IoT"** in our research, which aims to secure IoT by analyzing data collected from smart or IoT devices. We begin by introducing various Computational Intelligence (CI) techniques, such as Fuzzy Set, Artificial Intelligence, Evolutionary Computing, and Swarm Intelligence, to identify optimal methods for IoT security. Our review of literature suggests that Artificial Intelligence techniques, particularly Machine Learning and Deep Learning, offer promising avenues for IoT security due to the abundance of literature and simulations available. To set the stage for our research, we introduce IoT fundamentals in Chapter 1, covering types, components, architecture, security issues, and data challenges. We discuss basic security requirements and conventional methods for securing IoT, alongside applications to illustrate real-world IoT scenarios. Based on our literature review, we formulate research questions and objectives aimed at identifying attack types, threats, vulnerabilities, and CI-based security techniques for IoT. In Chapter 2, we conduct a systematic literature review spanning IoT security and CI from 2015 to 2023,

followed by an exploration of related work in IoT security and AI-based security. We delve into IoT threats, privacy, security, and other concerns, as well as layered security issues within IoT architecture. Motivated by our literature findings, Chapter 3 presents a methodology for securing IoT through attack detection, with a focus on ML and DL techniques selected from various IoT security solutions. Chapter 4 addresses challenges related to high processing time and computation costs by implementing feature engineering to reduce dataset dimensionality. We explore feature selection methods in both ML and DL, achieving promising results with selected classifiers. In Chapter 5, we introduce DL techniques, specifically LSTM and CNN, for improved IoT attack detection. Using MQTTset data, we demonstrate the efficacy of CNN in feature selection and LSTM in attack detection, aiming to enhance IoT security, especially concerning extensive datasets like MQTTset.