INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	**Pradeepkumar Gajendra Bhale**
Roll Number	:	**1661001013**
Programme of Study	:	Ph.D.
Thesis Title:		**Attack Detection and Mitigation for IoT Ecosystems: Adaptive, Scalable, and Lightweight Approaches**
Name of Thesis Supervisor(s)	:	**Prof. Sukumar Nandi and Santosh Biswas (IIT Bhilai)**
Thesis Submitted to the Department/ Center	:	**Computer Science and Engineering**
Date of completion of Thesis Viva-Voce Exam	:	**17 April 2024**
Key words for description of Thesis Work	:	**Internet of Things (IoT), Intrusion Detection Systems (IDS), Edge Computing, Machine Learning (ML), Naive Bayes Classifier, Distributed Denial-of-Service (DDoS) Attack, Packet Inspection Agent (PIA), Low-Rate DDoS (LRDDoS) Attacks, Mixed-Rate DDoS (MRDDoS) Attacks, LSTM-based IDS, Wasserstein Generative Adversarial Network (WGAN), Rank attacks, Sinkhole attacks, Buffer overflow (BOF) attack, Roaming IDS, Markov Chain Analysis (MCA).**

SHORT ABSTRACT

This thesis presents innovative security solutions for IoT networks, addressing challenges such as DDoS attacks and botnet infiltration.

Edge-based ML for DDoS Detection: Introduces an edge-based ML method for Intrusion Detection Systems (IDS) using a naïve Bayes classifier. Demonstrates scalability and comparable performance in terms of memory utilization, energy usage, and response time.

Packet Inspection Agent (PIA) for LRDDoS Detection: Proposes a distributed, lightweight PIA utilizing Total Variation Metric (TVM) and Packet Flow Count (PFC) to detect and mitigate low-rate DDoS attacks efficiently in IoT networks.

IDS for MRDDoS Detection: Presents a lightweight IDS using Long Short-Term Memory (LSTM) model and optimal placement strategy to detect mixed-rate DDoS attacks. Achieves superior performance compared to existing approaches.

Roaming IDS for Mixed Attacks: Introduces roaming IDS capable of detecting and mitigating various mixed attacks in IoT networks using a lightweight shadow honeypot. Employing Markov chain analysis for attack prediction, the RENO model demonstrates improved performance compared to existing solutions.

Overall, the thesis offers insights into the development of adaptive, scalable, and lightweight security solutions for IoT ecosystems.