Enhancing Intrusion Detection in Wireless Sensor Networks Using Machine Learning

Project-III (IT208PPC31) report submitted to

Guru Ghasidas Vishwavidyalaya

in partial fulfilment for the award of the degree of

Bachelor of Technology

in

Information Technology

by

Shantanu S Srivastava , Siri Varsha Puli, Lokesh kumar Haldkar

(21036169, 21036153, 21036132)

Under the supervision of

Dr.Pankaj Chandra

Department of Information Technology

Guru Ghasidas Vishwavidyalaya

April,2025

April 03, 2025

DEPARTMENT OF INFORMATION TECHNOLOGY
GURU GHASIDAS VISHWAVIDYALAYA
BILASPUR - 495009, INDIA

CERTIFICATE

This is to certify that the project report entitled "**Enhancing Intrusion Detection in Wireless Sensor Networks Using Machine Learning** " submitted by **Shantanu S Srivastava , Siri Varsha Puli, Lokesh kumar Haldkar** (Roll No. 21036169, 21036153, 21036132) to Guru Ghasidas Vishwavidyalaya towards partial fulfilment of requirements for the award of degree of Bachelor of Technology in Information Technology is a record of bonafide work carried out by him under my supervision and guidance during April,2025.

Prof.Manoj Kumar
Head of Department
Department of IT
Guru Ghasidas Vishwavidyalaya

Dr.Pankaj Chandra
Department of Information Technology
Guru Ghasidas Vishwavidyalaya
Bilaspur - 495009, India

Abstract

Name of the student: **Shantanu S Srivastava , Siri Varsha Puli, Lokesh kumar Haldkar**

Roll No: **21036169, 21036153, 21036132**

Degree for which submitted: **Bachelor of Technology**

Department: **Department of Information Technology**

Thesis title: **Enhancing Intrusion Detection in Wireless Sensor Networks Using Machine Learning**

Thesis supervisor: **Dr.Pankaj Chandra**

Month and year of thesis submission: **April 03, 2025**

The growth of internet use has created more cybersecurity risks, making existing security systems less effective against new types of attacks. This research presents a comprehensive evaluation of machine learning approaches for network intrusion detection using the CICIDS2017 dataset containing diverse attack scenarios. We implement an advanced feature selection methodology combining Mutual Information with Random Forest Regressor analysis to optimize detection capabilities.This project helps in demonstrating strong performance in identifying both known and novel zero-day attack patterns while maintaining operational efficiency. Experimental results validate the effectiveness of these methods, with Decision Trees achieving 95.256 % accuracy, K-Nearest Neighbors 98.09 %, Random Forest 96.70 %, and Support Vector Machines 83.25 %. These findings establish machine learning as a powerful framework for next-generation adaptive security systems.