

A PROJECT REPORT ON
Phishing Detection Tool: Using AI/ML

Submitted in partial fulfillment of the requirement of
BACHELOR OF TECHNOLOGY
IN
INFORMATION TECHNOLOGY

Submitted By:
Aarti Kumari(21036102)
Sunita(21036156)

Under the supervision of
Mrs. Akanksha Gupta
(Assistant Professor)



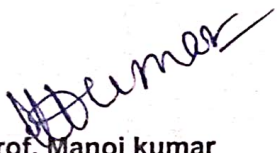
DEPARTMENT OF INFORMATION TECHNOLOGY
INSTITUTE OF TECHNOLOGY,
GURU GHASIDAS VISHWAVIDYALAYA BILASPUR, INDIA
(CENTRAL UNIVERSITY)
SESSION: 2024-2025

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

CERTIFICATE



This is to certify that the project report entitled "Phishing Detection Tool: Using AI/ML" submitted by Aarti kumari, Sunita (Roll No. 21036102, 21036156) 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 3, 2025.


Prof. Manoj kumar

Head of Department
Department of Information Technology
Guru Ghasidas Vishwavidyalaya


Mrs. Akanksha Gupta

Department of Information Technology
Guru Ghasidas Vishwavidyalaya
Bilaspur - 495009, India

Abstract

Name of the Students: Aarti Kumari, Sunita

Roll No: 21036102, 21036156

Degree Program: Bachelor of Technology Department:

Department of Information Technology Thesis Title: *Phishing*

Detection Tool: *Using AI/ML* **Thesis Supervisor:** Mrs.

Akanksha Gupta

Month and Year of Submission: April 3, 2025

In today's digital landscape, phishing attacks have become one of the most common and dangerous cybersecurity threats. Phishing is a technique used by attackers to trick individuals into revealing sensitive information such as usernames, passwords, and credit card details, often by impersonating trustworthy entities in electronic communications.

This thesis presents the development of a **Phishing Detection Tool** powered by **Artificial Intelligence (AI)** and **Machine Learning (ML)**. The objective is to design a system that can accurately distinguish between legitimate and malicious URLs or websites by analyzing various features extracted from input data.

The proposed system uses supervised machine learning models, such as **Random Forest**, **Decision Tree**, and **Logistic Regression**, trained on publicly available phishing datasets. These models evaluate features like URL structure, presence of suspicious keywords, SSL certificate usage, domain age, and more. The tool is implemented with a user- friendly interface, allowing users to input a URL and receive an instant risk evaluation along with a confidence score.

Our experiments demonstrate high accuracy in phishing detection, showing the potential of AI/ML-based solutions in enhancing cybersecurity. The tool can be integrated into browsers, email clients, or used as a standalone application to protect users from phishing threats in real-time.