VISVESVARAYA TECHNOLOGICAL UNIVERSITY,

BELAGAVI

A PROJECT REPORT ON

"PHISHING URL DETECTION USING MACHINE LEARNING"

Submitted in partial fulfillment for the award of Degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE & ENGINEERING

By

MAYYA MADHUSUDHAN	**4AL20CS072**
MOHAMMED SHOAIB	**4AL20CS077**
MOHITH S SHETTY	**4AL20CS079**
PRATHEEK PRAMOD SHETTY	**4AL20CS097**

Under the Guidance of

Dr. Bramha Prakash H P

Associate Professor

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MOODBIDRI-574225, KARNATAKA

2023-24

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K. -574225, KARNATAKA

ALVA'S
Education Foundation

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"PHISHING URL DETECTION USING MACHINE LEARNING"** has been successfully completed by

MAYYA MADHUSUDHAN	**4AL20CS072**
MOHAMMED SHOAIB	**4AL20CS077**
MOHITH S SHETTY	**4AL20CS079**
PRATHEEK PRAMOD SHETTY	**4AL20CS097**

the bonafide students of **DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY** of the **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the year 2023–24. It is certified that all corrections/suggestions indicated for Internal Assessmenthave been incorporated in the report deposited in the departmental library. The project reporthas been approved as it satisfies the academic requirements in respect of Project work prescribed for the Bachelor of Engineering Degree.

BP 13/5/24.

Dr. Bramha Prakash H P
Project Guide

13/5/24

Dr. Manjunath Kotari
Head Of the Department

Head of the Department
Dept. of Computer Science & Engineering
Alva's Institute of Engineering and Technology
Mijar, Moodubidire - 574 225, D.K. Karnataka, India

Dr. Peter Fernandes
Principal

PRINCIPAL
Alva's Institute of Engg. & Technology,
Mijar, MOODBIDRI - 574 225, D.K

External Viva

Name of the Examiners	Signature with Date
1. Dr. Manjunath Kotari	
2. Dr. Prabhakara B.K	

ABSTRACT

Phishing attacks continue to pose a significant threat to internet security, deceiving users into divulging personal and financial information through sophisticated social engineering tactics. This project addresses the urgent need for effective phishing detection by developing a machine learning-based system capable of accurately distinguishing between phishing and legitimate URLs. Utilizing a combination of advanced algorithms including Decision Trees, Support Vector Machines (SVM), XGBoost, Multilayer Perceptions (MLPs), Auto Encoder Neural Networks, and Random Forest, the system analyzes various features extracted from URLs to identify potential phishing attempts. The effectiveness of these models was rigorously tested and integrated into a user-friendly web application, allowing users to verify URLs in real-time. The best performing model, the Random Forest, demonstrated high accuracy and robustness, making it the backbone of the detection system. The project not only improves individual and organizational cybersecurity but also offers insights into phishing tactics and countermeasures. Future work will focus on refining these models, expanding the dataset to include newer phishing techniques, and enhancing the system's adaptability to continually evolve in response to emerging threats. This initiative marks a significant step forward in the ongoing battle against cybercrime, providing a scalable and reliable tool for phishing detection.