VISVESVARAYA TECHNOLOGICAL UNIVERSITY,

BELAGAVI - 590018

A PROJECT REPORT ON

PHISHING WEBSITE DETECTION USING DEEP LEARNING

Submitted in partial fulfillment for the award of Degree of,

BACHELOR OF ENGINEERING

IN

INFORMATION SCIENCE AND ENGINEERING

By

AKASH K ACHARYA	4AL20IS003
FATHIMA THAHIBA	4AL20IS017
SHRAMIK S SHETTY	4AL20IS046
VANDAN M SHETTY	4AL20IS058

Under the Guidance of

Mr. Pradeep Nayak

Assistant Professor

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

ALVA'S
Education Foundation®

ALVA'S INSTITUTE OF ENGINEERING & TECHNOLOGY

MIJAR, MOODBIDRI, D.K, KARNATAKA - 574225

2023 – 2024

ALVA'S INSTITUTE OF ENGINEERING & TECHNOLOGY

MIJAR, MOODBIDRI, D.K, KARNATAKA - 574225

ALVA'S
Education Foundation®

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Project entitled **"PHISHING WEBSITE DETECTION USING DEEP LEARNING"** has been successfully completed by

AKASH K ACHARYA	**4AL20IS003**
FATHIMA THAHIBA	**4AL20IS017**
SHRAMIK S SHETTY	**4AL20IS046**
VANDAN M SHETTY	**4AL20IS058**

the bonafide students of **DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING, Alva's Institute of Engineering and Technology,** Moodbidri affiliated **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the year 2023–2024. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The Project report has been approved as it satisfies the academic requirements in respect of project work prescribed in partial fulfilment of awarding Bachelor of Engineering Degree.

Mr. Pradeep Nayak
Assistant Professor
Project Guide

Dr. Sudheer Shetty
Professor
HOD ISE

Dr. Peter Fernandes
Principal

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

EXTERNAL VIVA

Name of the Examiners

1. Dr Sudheer Shetty
2. Dr. Ritesh Pankala

Signature with Date

29/5/24

Pankala 29/5/24

ABSTRACT

Phishing attacks have emerged as one of the most prevalent and perilous forms of cybercrime in recent years. These malicious tactics are designed to deceive individuals and organizations into divulging sensitive information used for transactions. Typically, phishing websites are crafted with subtle clues within their content and browser-based information to mimic legitimate platforms. By employing tactics such as specially crafted emails or instant messages, attackers create replicas of existing web pages, tricking users into divulging personal, financial, or password data under the guise of legitimate service .Inresponse to this escalating threat, there is a growing need to leverage advanced technologies like Machine Learning (ML) for enhanced detection and classification of phishing websites. ML algorithms can analyze a multitude of features extracted from datasets, such as those availablein the UCI Machine Learning Repository database, to identify patterns indicative of phishing behavior Furthermore, the study aims to delve deeper into the intricate characteristics of phishing websites, exploring nuances in their design, content, and behavior. Through comprehensive analysis and feature extraction, ML algorithms can learn to discern subtle cuesthat differentiate phishing sites from legitimate ones, thereby bolstering the effectiveness of detection mechanism.