

# **Phishing Attack Detection using AI/ML**

**A PROJECT REPORT**

*Submitted by,*

**MANJUNATH A C  
DINESH KUMAR K  
AKASH S  
PRAJWAL KANTHAN T**

**20211CAI0124  
20211CAI0074  
20211CAI0110  
20211CAI0075**

*Under the guidance of,*

**Ms. KAYALVIZHI**

—— Assistant Professor  
School of Computer Science and Engineering  
Presidency University, Bengaluru

*in partial fulfillment for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

**At**



**PRESIDENCY UNIVERSITY, BENGALURU**

**MAY 2025**

# **PRESIDENCY UNIVERSITY**

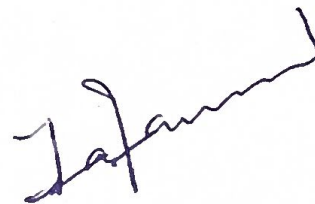
## **PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING**

### **CERTIFICATE**

This is to certify that the Project report “Phishing Attack Detection using AI/ML” being submitted by “MANJUNATH A C (20211CAI0124)”, “DINESH KUMAR K (20211CAI0074)”, “AKASH S (20211CAI0110)”, “PRAJWAL KANTHAN T(20211CAI0075)”, in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a Bonafide work carried out under my supervision.



**Ms. KAYALVIZHI**  
Assistant Professor  
School of Computer Science and  
Engineering  
Presidency University, Bengaluru



**Dr. ZAFAR ALI KHAN**  
Prof & Hod  
Dept. of Computer Science  
Engineering  
Presidency University, Bengaluru



**Dr. MYDHILI NAIR**  
Professor & Associate Dean  
School of CSE  
Presidency University, Bengaluru



**Dr. SAMEERUDDIN KHAN**  
Pro-Vice Chancellor - Engineering  
Dean – School of CSE & IS  
Presidency University, Bengaluru

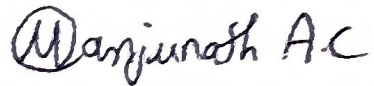
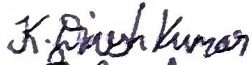
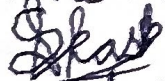

# PRESIDENCY UNIVERSITY

## PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

### DECLARATION

I hereby declare that the work, which is being presented in the report entitled **“Phishing Attack Detection using AI/ML”** in partial fulfillment for the award of Degree of **Bachelor of Technology in Computer Science and Engineering**, is a record of my own investigations carried under the guidance of **Ms. Kayalvizhi, Assistant Professor, Presidency School of Computer Science and Engineering, Presidency University, Bengaluru.**

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NUMBER	SIGNATURE
MANJUNATH A C	20211CAI0124	
DINESH KUMAR K	20211CAI0074	
AKASH S	20211CAI0110	
PRAJWAL KANTHAN T	20211CAI0075	



## ABSTRACT

Phishing has become a major cybersecurity challenge due to the fact that attackers continue to innovate the methods of luring individuals into revealing sensitive information like passwords, financial details, and login credentials. The sophistication of deception in phishing attacks in today's world renders conventional rule-based security mechanisms inadequate. Hence, our contribution extends further to investigate an even better solution—utilize artificial intelligence (AI) and machine learning (ML) to effectively detect phishing attacks based on website URL analysis.

The model used in this research utilizes empirical data gathered from two reliable sources, the UCI Machine Learning Repository and Kaggle's phishing data set. After going through data cleansing and integration activities, a balanced data set containing over 21,000 records was developed. We derived useful features from the combined data that assist in the identification of phishing URLs, including URL length, number of special characters, presence of suspicious keywords, subdomain patterns, and the domain structure.

Some algorithms were employed in comparing the performance of the top-performing model, wherein the Random Forest classifier excelled against such counterparts as Logistic Regression and Decision Trees. At a performance rate of more than 99%, the model has an exceptionally high capacity to distinguish between phishing and safe URLs with extremely high accuracy. In order to cater to an enhanced user experience, an interactive dashboard was built based on Streamlit. The web interface makes it possible for a user to enter a URL, which is parsed by the system and tagged as secure or suspicious. To maintain your model current with evolving phishing trends, a retrain feature has been included. This allows the system to learn and improve its detection accuracy in sync with evolving attack tactics employed by attackers. The tool has been made lightweight and user-friendly to allow its deployment on local systems and cloud services such as AWS and Heroku. This project shows the efficacy of using properly designed features coupled with high-speed machine learning algorithms in providing efficient and scalable protection against phishing attacks. It not only safeguards a single user against internet frauds but also displays the real-time usage of artificial intelligence in securing cybersecurity measures.