URL PHISHING ATTACK DETECTION USING MACHINE LEARNING

A project report submitted in partial fulfillment of the requirements For the award of the degree of

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING

Submitted by

K NISCHALA DEVI
(18811A0527)

L SASIPRIYA
(18811A0539)

B TEJA
(18811A0505)

S NEELIMA
(18811A0553)

K TEJASWI
(18811A0533)

Under the Esteemed Guidance of

Mr. J. GANESH SIR
Assistant Professor

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING

AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY
(Permanently Affiliated to Jawaharlal Nehru Technological University, Kakinada, AP)
(Accredited by NAAC,UGC & NBA,AICTE)
Tamaram, Narsipatnam, Visakhapatnam-
531113
(2018-2022)

AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

(Permanently Affiliated to Jawaharlal Nehru Technological University,Kakinada, AP)

(An NAAC Accredited Institution)

Tamaram,Narsipatnam,Visakhapatnam-531113

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project report entitled **"URL PHISHING ATTACK DETECTION USING MACHINE LEARNING"** in partial fulfillment for the of degree of Bachelor of Technology in COMPUTER SCIENCE AND ENGINEERING at AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY, MAKAVARAPALEM, VISAKHAPATNAM is an bonafied work carried out by the **K NISCHALA DEVI (18811A0527), L SASI PRIYA (18811A0539), B TEJA (18811A0505), S.NEELIMA(18811A0553), K.TEJASWI(18811A0533)** under the guidance and supervision during 2021-2022.Project Guide Head of the Department External Examiner

J. Ganesh

Internal Guide

Head of the Department

External Examiner

Abstract

Phishing are one of the most common and most dangerous attacks among cybercrimes. The aim of these attacks is to steal the information used by individuals and organizations to conduct transactions. Phishing websites contain various hints among their contents and web browser-based information. The purpose of this study is to perform Extreme Learning Machine (ELM) based classification for 30 features including PhishingWebsites Data in UC Irvine Machine Learning Repositorydatabase. For results assessment, ELM was compared with other machine learning methods such as Support Vector Machine (SVM), Naïve Bayes (NB) and detected to have the highest accuracy of95.34%.

Existing System

The main objective of the phisher is to deceive the user by designing an exact image of legitimate site such that the user does not get any suspicion on the phishing site. Hence, the anti-phishing techniques compare suspicious website image with legitimate image database to get the similarity ratio, used for the classification of suspicious websites. The website is classified as phishing when the similarity score is greater than a certain threshold else it is treated as legitimate.

- Imagecomparison of suspicious website with entire legitimatedatabase store takes more time complexity.
- Morespace to store legitimate image database.
- Web pagewith animated website compared with phishing websiteleads to the low percentage of similarity that leads tohigh false negative rate. This