(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :07/03/2024

(21) Application No.202441016551 A
(43) Publication Date : 22/03/2024

(54) Title of the invention : DETECTION OF PHISHING WEBSITES USING MACHINE LEARNING MODEL

(51) International classification :G06N0020000000, G06F0021550000, G06F0040205000, H04L0051000000, H04L0009120000
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)**Name of Applicant :**
1)Dr. Ramesh K
Address of Applicant :Professor, Department of CSE, Sri Krishna College of Engineering and Technology ---------- ----------
2)Dr. Sasi Kala Rani K
3)Mr Vengateshwaran M
4)Lakshan Balaji R K
5)Dhinakaran V
6)Sruthi R
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr. Ramesh K
Address of Applicant :Professor, Department of CSE, Sri Krishna College of Engineering and Technology ---------- ----------
2)Lakshan Balaji R K
Address of Applicant :UG students, Department of CSE, Sri Krishna College of Engineering and Technology ---------- ----------
3)Dhinakaran V
Address of Applicant :UG students, Department of CSE, Sri Krishna College of Engineering and Technology ---------- ----------
4)Sruthi R
Address of Applicant :UG students, Department of CSE, Sri Krishna College of Engineering and Technology ---------- ----------

(57) Abstract :
4. DETECTION OF PHISHING WEBSITES USING MACHINE LEARNING MODEL 5. ABSTRACT 6. Now a days there has been an overall increase in the total number of phishing websites. It is now a widespread issue since attackers trick naive users by designing fake websites with some real elements. These websites are designed to steal personal information such as email ids, usernames, passwords, financial information, etc. Attackers deploy these fake websites that somewhat imitate their original counterparts by incorporating some realistic elements. By Using and Utilizing secure methods to proactively identify phishing websites is imperative to impede the rapid development of phishing techniques because of advancing techniques and technology. A great tool for defending against phishing assaults is machine learning algorithms. Attackers often prefer to use phishing because it is easier and simpler to fraud a victim into accessing a malicious link that looks genuine than to try to bypass a computer's security measures. The malevolent links inside the body of the message appear like links intended to direct the users to the official pages but are intended to direct the user to the spoofed company utilizing that official company's logos and other genuine information. In the methodology that is being presented here, machine learning algorithms are used to create a comprehensive approach for identifying phishing websites. Multiple models were compiled and utilized in our proposed strategy to identify phishing websites based on various parts of the URL specification. The various characteristics of the URLs of both phishing and legitimate websites can be compared by extracting the properties of them. The proposed method uses the combined model to identify the URLs if the phishing websites. This study demonstrates the performance of the suggested approach and successfully identify the legitimate websites from fake ones in real-time.

No. of Pages : 10 No. of Claims : 3