(12) PATENT APPLICATION PUBLICATION (21) Application No.202411008918 A

(19) INDIA

(22) Date of filing of Application :09/02/2024 (43) Publication Date : 16/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR DYNAMICALLY IDENTIFYING AND THWARTING PHISHING WEBSITES

(51) International classification	:H04L0051000000, G06F0021550000, G06N0020000000, G06F0021560000, G06N0003040000
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**

1)Chitkara University

Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

2)Bluest Mettle Solutions Private Limited

Name of Applicant : NA

Address of Applicant : NA

(72)**Name of Inventor :**

1)MISHRA, Saket

Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------

2)PANDEY, Sakshi

Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------

3)VANSHIKA

Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

The present disclosure relates to system (100) and a method (300) for dynamically identifying and thwarting phishing websites involves simulating, via a website interaction engine, user engagement with suspicious websites on one or more computing devices; observing and documenting via a behavior monitoring engine, the behavior of the suspicious websites throughout simulated interactions; scrutinizing, via an anomaly detection engine (216), the documented behavior to determine abnormal patterns indicative of phishing or malicious activities; extracting, via a feature extraction engine (218) integrated within a machine learning integration module, a plurality of pertinent features from the documented behavior; and evaluating, via a classifier engine (220) trained on historical data, the extracted features to classify the suspicious website as benign, suspicious, or malicious.

No. of Pages : 29 No. of Claims : 9