

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311039078 A

(19) INDIA

(22) Date of filing of Application :07/06/2023

(43) Publication Date : 07/07/2023

(54) Title of the invention : SYSTEM AND METHOD TO DETECT CREDENTIAL PHISHING ON A URL OR EMAIL AND MITIGATE THE ATTACK

<p>(51) International classification :G06F 213100, G06F 215500, G06F 215700, H04L 510000, H04L 510800</p> <p>(86) International Application No :NA Filing Date :NA</p> <p>(87) International Publication No : NA</p> <p>(61) Patent of Addition to Application Number :NA Filing Date :NA</p> <p>(62) Divisional to Application Number :NA Filing Date :NA</p>	<p>(71)Name of Applicant : 1)Chitkara University Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----</p> <p>2)Bluest Mettle Solutions Private Limited Name of Applicant : NA Address of Applicant : NA</p> <p>(72)Name of Inventor : 1)MISHRA, Rahul Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----</p> <p>2)SINGH, Dhiraj Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----</p> <p>3)MITTAL, Ruchi Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----</p>
--	---

(57) Abstract :

The present disclosure relates to a system (100) for detection of credential phishing on a URL or email and mitigation of the attack. It involves screening of emails or data from any other website (108) for credential phishing or any other kind of phishing. A feature extraction (106) is performed on the data from the websites (108) or the received emails for extracting the DNS address, Internet Protocol (IP) address, email name and other features to determine their authenticity. Then the features are screened for any kind of malicious activity and are added to a blacklist if any phishing attempts are identified. The system (100) can identify a variety of phishing attempts such as vishing, smishing, honey pots and so on. It can also identify if the name of the user is being used maliciously and illegally for any online transactions or emails. The system (100) also includes a method for prevention of any potential attacks or malicious activity to harm the computer system (100).

No. of Pages : 25 No. of Claims : 10