(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :09/08/2023

(21) Application No.202311053442 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR BLOCKING SCAMMING ATTACKS IN A NETWORK

(51) International classification	:A61B0005000000, H04W0028020000, G06F0016230000, G16H0040670000, G06T0011600000
(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)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, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------
2)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India Pune ----------- -----------
3)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India Patiala ----------- -----------

(57) Abstract :
Embodiments of the present disclosure relates to a system (100) and method (300) for blocking scamming attacks in a network. In an aspect, the present disclosure discloses a system (102) for blocking scamming attacks in a network. The system (102) comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to collect data from a plurality of sources in real-time. Further, the processor (202) is configured to process the collected data to extract information. Next, the processor (202) is configured to identify patterns in the processed network data. In the end, the processor (202) is configured to generate a scam score based on the identified patterns

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