(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :30/08/2023

(21) Application No.202311058225 A

(43) Publication Date : 29/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR PROACTIVE THREAT DETECTION AND RESPONSE IN A COMPUTER NETWORK

(51) International classification	:A61B0005000000, G06F0021550000, G06F0021560000, H04W0024080000, H04W0004020000
(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)PANDEY, Sakshi
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 proactive threat detection and response in a computer network using distributed deception techniques. The system comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to collect network traffic data from a plurality of sources. Further, the processor (202) is configured to analyse the collected network traffic data. Next, the processor (202) is configured to detect one or more threat patterns in the analysed network traffic data. In the end, the processor (202) is configured to block the detected one or more threat patterns.

No. of Pages : 26 No. of Claims : 10