(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :06/10/2023

(21) Application No.202311067004 A
(43) Publication Date : 27/10/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR DETECTING CYBER DECEPTION BY APPLYING FUZZY LOGIC TECHNIQUES

(51) International classification :G06F0021550000, A61B0005000000, A61B0005160000, G06N0020000000, G06F0021560000
(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 (102) and method (200) for detecting cyber deception by combining fuzzy logic principles, adaptive learning, and pattern matching techniques to improve the accuracy and efficiency of detecting and identifying cyber threats. The system (102) comprises a processor (104) coupled to a memory (106). The memory (106) stores processor-executable instructions. The processor (104) is configured to collect cyber data from a plurality of sources. Next, the processor (104) is configured process the collected cyber data. Thereafter, the processor (104) is configured to analyse the processed cyber data to detect cyber deception patterns. In the end, the processor (104) is configured to trigger an alert to mitigate cyber deception.

No. of Pages : 19 No. of Claims : 10