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

(21) Application No.202311054281 A
(43) Publication Date : 08/09/2023

(54) Title of the invention : SYSTEM AND METHOD FOR IDENTIFYING AND BLOCKING MALICIOUS CHATBOT ACTIVITIES

(51) International classification	:H04L0051020000, G06N0020000000, G06F0021560000, H04L0067020000, G06Q0050000000
(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, 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 :
The present invention discloses a system (100) and method (200) for identifying and blocking malicious chatbots on a computing device (110). The system includes a processor (102) configured to receive a plurality of chatbot activities from one or more platforms on the associated computing device. By applying one or more techniques, such as neural networks, decision trees, and support vector machines, the system determines whether any of the received chatbot activities are malicious. Upon detection of malicious chatbot activities, the system takes appropriate action to block the identified malicious chatbots, which may include blocking their IP addresses, domain names, or associated accounts. Additionally, the system may be deployed in various environments, including social media platforms, messaging applications, and customer service systems. It is capable of adapting to new threats and can be updated with machine learning algorithms to enhance its effectiveness over time

No. of Pages : 22 No. of Claims : 10