(12) PATENT APPLICATION PUBLICATION	(21) Application No.202311063673 A
(19) INDIA	
(22) Date of filing of Application :22/09/2023	(43) Publication Date : 13/10/2023

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

(51) International classification	:G06F0021550000, G06N0020000000, G06F0021560000, G16H0050200000, G06F0040300000
(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 artificial intelligence (AI) based activities on a computing device (110). The system (100) includes a processor (102) configured to receive a plurality of AI-based activities on the associated computing device. The system applies one or more techniques to the received AI-based activities to determine if the intent of at least one of the AI-based activities is malicious. Upon identifying malicious activities, the system proceeds to block the malicious activities to prevent harm to the associated computing device. Additionally, the system identifies patterns in the malicious AI-based activities and transmits an alert signal to an entity associated with the computing device (110).

No. of Pages : 24 No. of Claims : 10