(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :14/08/2023

(21) Application No.202311054611 A

(43) Publication Date : 08/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR BLOCKING MALICIOUS APPLICATIONS BY AGENTS IN DEVICES OF A NETWORK

(51) International classification	:G06F0021560000, G06F0021550000, H04W0004800000, H04L0012280000, A61B0005000000
(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)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 malicious applications by agents in devices of a network. In an aspect, the present disclosure discloses a system (102) for blocking malicious applications by agents in devices of 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 the installed agents. Further, the processor (202) is configured to analyse the collected data to detect patterns of malicious application activity. Next, the processor (202) is configured to compare the detected patterns of malicious application activity with known malicious application activities in a database (220). In the end, the processor (202) is configured to block the detected patterns of malicious application activity.

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