(12) PATENT APPLICATION PUBLICATION (21) Application No.202311070833 A

(19) INDIA

(22) Date of filing of Application :18/10/2023 (43) Publication Date : 24/11/2023

(54) Title of the invention : SYSTEM AND METHOD FOR DETECTING MALWARE BY APPLYING MACHINE LEARNING AND BEHAVIORAL ANALYSIS TECHNIQUES

(51) International classification	:G06F0021560000, A61B0005000000, G06N0020000000, A61B0005110000, G06N0005020000
(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 :

Embodiments of the present disclosure relates to a system (102) and method (200) for detecting malware context profiles by applying machine learning and behavioural analysis techniques. 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 data pertaining to a software execution context. Next, the processor (104) is configured to extract one or more features from the collected data. Thereafter, the processor (104) is configured to build a behavioural profile based on the extracted features. In the end, the processor (104) is configured to analyse the behavioural profile to detect malware profiles.

No. of Pages : 17 No. of Claims : 10