(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :12/09/2023

(21) Application No.202311061202 A
(43) Publication Date : 13/10/2023

(54) Title of the invention : A SYSTEM AND METHOD OF CREATING A TRUSTED OPERATING ENVIRONMENT FOR MALWARE DETECTION

(51) International classification	:G06F0021560000, G06F0021570000, A61B0005000000, G06F0021530000, A61B0005055000
(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 creating a trusted operating environment for malware detection. The system comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to establish a trusted operating environment. Further, the processor (202) is configured to isolate the trusted operating environment from a main operating system of the device. Next, the processor (202) is configured to scan one or more files in the device to detect malware. In the end, the processor (202) is configured to trigger an action against the detected malware.

No. of Pages : 25 No. of Claims : 10