(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :13/09/2023

(21) Application No.202311061495 A
(43) Publication Date : 13/10/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR DETECTING AND BLOCKING MALWARE BY SIMILARITY ANALYSIS

(51) International classification :G06F0021560000, A61B0005000000, G06F0016230000, H04L0043062000, G06F0021550000
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :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 detecting and blocking malware by similarity analysis. In an aspect, the present disclosure discloses a system (102) for detecting and blocking malware by similarity analysis. 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 scan files and network traffic in real-time. Further, the processor (202) is configured to compare the scanned files and network traffic with known malware samples in a database. Next, the processor (202) is configured to predict a likelihood of the files and the network traffic to be infected with malware based on the comparison. In the end, the processor (202) is configured to generate a report of the files and the network traffic infected with malware.

No. of Pages : 26 No. of Claims : 10