(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :28/09/2023

(21) Application No.202311065208 A
(43) Publication Date : 20/10/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR INLINE MALWARE DETECTION USING MACHINE LEARNING AND REAL-TIME BEHAVIORAL ANALYSIS

(51) International classification	:G06F0021560000, G06N0020000000, H04W0024080000, A61B0005000000, G06F0016245700
(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 (100) and method (300) for inline malware detection in a network using machine learning techniques and real-time behavioural 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 collect network traffic data from a plurality of sources. Next, the processor (202) is configured to analyse the collected network traffic data. Thereafter, the processor (202) is configured to identify patterns of inline malware threats. In the end, the processor (202) is configured to block the identified patterns of inline malware threats.

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