(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :07/06/2023

(21) Application No.202311039083 A
(43) Publication Date : 07/07/2023

(54) Title of the invention : SYSTEM AND METHOD TO AUTOMATICALLY CLASSIFY AND BLOCK MALICIOUS NETWORK TRAFFIC

(51) International classification	:G06F 161850, G06F 162100, G06F 215500, G06Q 300000, H04L 430620
(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)SHARMA, Bhanu
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present disclosure relates to a system (100) for scanning all incoming network traffic from various network interfaces (108) for a number of vulnerabilities and malicious activity. The system uses a firewall to screen the incoming network traffic and records all the network that passes through the firewall. It creates log records for data packets of the incoming traffic network. The data packets are inspected for any kind of malicious activity, and other suspicious behaviour. There are possibilities of various kind of network attacks that aim at disabling computer systems. The system (100) aims at discouraging such activities while identifying and reporting them in real time. The system (100) uses various behavioral analytical techniques and packet filtering methods for monitoring the incoming network traffic. The system (100) also generates real-time alerts and a report of all the details of malicious activity.

No. of Pages : 28 No. of Claims : 9