(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :17/07/2023

(21) Application No.202311048049 A
(43) Publication Date : 11/08/2023

(54) Title of the invention : SYSTEM AND METHOD FOR DETECTING INCOMING MALICIOUS TRAFFIC USING BLACKLIST IP

(51) International classification	:G06F 215600, H04L 614511, H04L 690800, H04W 120800, H04W 881800
(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, Saket
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)SINGH, Jaiteg
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present invention discloses a system (100) and a method (200) for detecting malicious network traffic. The system includes a processor (102) configured to monitor network traffic in real-time within a predefined area where multiple computing devices are connected to a network (108). Each packet of network traffic is analyzed to determine its legitimacy or maliciousness, and suspicious activities are identified using a combination of machine learning algorithms and a rule-based system. Further, preventive measures, such as blocking IP addresses, terminating network connections, and activating firewall rules, are initiated to prevent the success of detected attacks. Additionally, notifications are transmitted to administrators or associated computing devices, alerting them about the detected suspicious activities. The system may further include a network packet capture module for capturing network packets and associated metadata, and the processor further record details of detected suspicious activities and the corresponding preventive measures.

No. of Pages : 24 No. of Claims : 9