(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :09/01/2024

(21) Application No.202411001605 A
(43) Publication Date : 02/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR NETWORK DNS FLOOD PROTECTION USING ANOMALY DETECTION AND TRAFFIC ANALYSIS

(51) International classification	:H04L0061451100, G06N0020000000, G06F0021550000, H04L0043026000, G06F0021570000
(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 :
The present invention discloses a system (100) and method (200) to safeguard a network against Domain Name System (DNS) flooding attacks. The system includes a processor for DNS traffic collection and analysis through a traffic analyzer to identify patterns and trends, and an anomaly detector to detect anomalous behavior indicative of DNS flood attacks. Upon detection, the system performs actions like diverting traffic or applying rate-limiting techniques and notifies network administrators while generating a comprehensive report with attack details. The method includes steps for DNS traffic collection and analysis, anomaly detection, action implementation, notification, and report generation. Additional features include statistical analysis, machine learning algorithms, flow-based analysis for DDoS detection, and GeoIP filtering to block attacks from specific regions.

No. of Pages : 22 No. of Claims : 10