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

(21) Application No.202311047013 A
(43) Publication Date : 04/08/2023

(54) Title of the invention : DISTRIBUTED DENIAL OF SERVICE

(51) International classification	:E05B 730000, G06F 094800, H04J 031600, H04L 451200, H04L 671000
(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)PANDA, Surya Narayan
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present subject matter discloses a system and method for effectively handling distributed denial of service (DDoS) attacks in a computer network. The system comprises a network traffic monitoring module, a traffic analysis module, and a traffic blocking module, all coupled to a processor. The network traffic monitoring module intercepts the network traffic, allowing for thorough visibility into the communication within the network. The traffic analysis module detects trends and abnormalities in the network traffic, serving as indicators of potential DDoS attacks. It utilizes advanced techniques, including statistical analysis and machine learning, to identify patterns associated with different types of attacks. The traffic blocking module blocks the DDoS attack based on the information obtained from the traffic analysis, utilizing criteria such as IP addresses, port numbers, and protocol types. This integrated approach ensures effective detection and mitigation of DDoS attacks, preserving the reliability and availability of the computer network.

No. of Pages : 27 No. of Claims : 10