(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :23/02/2023

(21) Application No.202311012462 A
(43) Publication Date : 17/03/2023

(54) Title of the invention : DETECTING ABNORNMAL BEHAVIOUR OF ENTERPRISES NETWORK USING MACHINE LEARNING

(51) International classification	:G06N 030400, G06N 030800, G06N 070000, G06N 200000, H04L 411600
(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)SINGH, Jaiteg
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------

(57) Abstract :
A system 100 and method 300 for monitoring malicious traffic in enterprises network include a server 108 configured with a plurality of modules for monitoring malicious traffic, in particular distributed denial-of-service using machine learning approach in a network 120. The server 108 include one or more processors 202 configured to receive external and internal network traffic data to identify Internet protocol address and hostile programme for one or more malicious traffic attacks, enable firewall logging of accepted and denied traffic to determine origination of attack, and generate warning to the network administrator. The method 300 further define strict transmission control protocol keep alive and maximum connection configuration on all perimeter devices 102.

No. of Pages : 19 No. of Claims : 10