(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :19/09/2023

(21) Application No.202311062923 A
(43) Publication Date : 13/10/2023

(54) Title of the invention : HEURISTIC BOTNET DETECTION MECHANISM

(51) International classification :G06N0020000000, G06F0021550000, G06F0021560000, H04L0041140000, G06N0005040000
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :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 introduces a heuristic botnet detection mechanism designed for computer networks, offering real-time identification and mitigation of botnet activities. Departing from conventional signature-based methods, the mechanism incorporates machine learning algorithms, network traffic analysis, and behavioral scrutiny. The system encompasses modules for data collection, preprocessing, machine learning-based detection, behavioral analysis, decision-making, counteraction, and continuous adaptation. This comprehensive approach allows for detection of known botnet patterns while remaining adaptive to emerging threats, ensuring enhanced security and resilience against evolving malicious activities in computer networks.

No. of Pages : 25 No. of Claims : 10