(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :07/09/2023

(21) Application No.202311060127 A
(43) Publication Date : 06/10/2023

(54) Title of the invention : SYSTEM AND METHOD FOR FLOW-BASED PACKET SAMPLING FOR NETWORK INTRUSION DETECTION

(51) International classification :G06F0021550000, H04L0043026000, H04L0043000000, H04L0061000000, H04L0043160000
(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 discloses a network intrusion detection system (100) involves that safeguard against cyber threats. The system receives incoming network traffic and identifies distinct network flows. A subset of packets from these flows is sampled, with a predefined set of attack signatures being employed to detect and mitigate threats. Further, behavioral analysis is applied to remaining packets to identify abnormal patterns indicative of intrusion attempts. By establishing historical traffic-based normal behavior profiles, the system compares the behavioral attributes of remaining packets against these profiles and generates intrusion alerts if deviations are detected. These alerts are transmitted to a network administrator's computing device. The system operates on various network devices, employs advanced packet analysis techniques, and can dynamically update its threat detection mechanisms.

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