(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311054633 A

(19) INDIA

(22) Date of filing of Application :14/08/2023

(43) Publication Date : 08/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR DETECTING NETWORK INTRUSION IN REAL-TIME

(51) International classification	:H04L0043087000, H04L0043026000, A61B0005055000, G06F0016230000, H04L0043040000
(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 :

Embodiments of the present disclosure relates to a system (100) and method (300) for detecting network intrusion in real-time. In an aspect, the present disclosure discloses a system (102) for detecting network intrusion in real-time by applying packet sampling and flow-based analysis techniques. The system (102) comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to capture a plurality of packets from a network flow. Further, the processor (202) is configured to classify the captured sample of packets from the network flow. Next, the processor (202) is configured to analyse the classified sample of packets. In the end, the processor (202) is configured to detect network intrusion based on the analysed sample of packets.

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