(12) PATENT APPLICATION PUBLICATION (21) Application No.202311058830 A

(19) INDIA

(22) Date of filing of Application :01/09/2023 (43) Publication Date : 06/10/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR MONITORING ENCRYPTED NETWORK TRAFFIC FLOW IN COMPUTER NETWORKS

(51) International classification	:H04L0045000000, H04N0021218700, H04L0041140000, H04L0043062000, H04L0041147000
(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)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 monitoring encrypted network traffic flow in computer networks. In an aspect, the present disclosure discloses a system (102) for monitoring encrypted network traffic flow in computer networks for maintaining network security, anomaly detection, and performance optimization for devices in a network. 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 extract metadata from an encrypted network traffic flow. Further, the processor (202) is configured to analyse the extracted metadata. Next, the processor (202) is configured to identify anomalous patterns in the encrypted network traffic flow based on the analysed metadata. In the end, the processor (202) is configured to generate a report of the classified network traffic flow.

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