(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :04/10/2023

(21) Application No.202311066565 A

(43) Publication Date : 20/10/2023

(54) Title of the invention : TECHNIQUES TO DETECT VIDEO TRANSFER FROM NETWORK USAGE

(51) International classification	:G06N0020000000, G06F0016245500, H04L0067010000, H04L0043026000, 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 :
The system (100) for detecting video transfer from network usage consists of a network traffic analyzer (102) responsible for receiving and analyzing network traffic data to identify video transfer patterns. A processor (104) utilizes a machine learning model (108), trained using various traffic features, to recognize these patterns. An alert generator (112) then generates alerts or takes appropriate actions based on the identified patterns. This system can detect different types of video transfer, including streaming and conferencing, even in encrypted network traffic. Users can configure specific criteria through the User Configuration Interface (114), and a data processing module (106) enhances data quality through techniques like noise reduction, normalization, and aggregation before analysis.

No. of Pages : 26 No. of Claims : 10