(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :06/09/2023

(21) Application No.202311059990 A
(43) Publication Date : 06/10/2023

(54) Title of the invention : SYSTEM FOR DETECTING AND CLASSIFYING DNS TUNNELING BEHAVIOURS IN A NETWORK AND METHOD THEREOF

(51) International classification :H04L0061451100, G06N0020000000, A61K0031000000, G06N0005040000, G06N0005020000
(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, Saket
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)SINGH, Gurjinder
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present disclosure relates generally to field of network security and more particularly to a behavior analysis-based DNS tunneling detection and classification framework for network security. More specifically the present invention relates to a system for detecting and classifying DNS tunneling behaviours in a network. The system (100) includes a DNS traffic analyzer (102), a behavior analyzer (104), a classifier (106), a feedback unit (108), a reporting device (110) and a policy enforcement device (112). The behavior analyzer (104) is configured to analyze the behavior of DNS traffic and detect tunneling behaviours. The classifier (106) is configured to classify the detected tunneling behaviours into different types. Further the present invention relates to a method for detecting and classifying DNS tunneling behaviours in a network. Advantageously, the present invention relates to a system which helps the network administrators to improve security of their networks and protect against new and unknown attacks.

No. of Pages : 21 No. of Claims : 10