(12) PATENT APPLICATION PUBLICATION (21) Application No.202311053438 A

(19) INDIA

(22) Date of filing of Application :09/08/2023 (43) Publication Date : 01/09/2023

(54) Title of the invention : SYSTEM AND METHOD FOR IDENTIFYING AND RESISTING DNS SPOOFING TROJAN THREATS

(51) International classification :G06F0021560000, H04L0061451100, G06F0021550000, H04L0051000000, G06F0021570000

(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 invention is designed to identify and resist DNS spoofing trojans, a type of malicious software that manipulates DNS settings to deceive users and compromise their security. The DNS resolver (102) intercepts DNS requests and forwards them to authoritative DNS servers. The traffic analyzer (104) inspects network traffic for anomalies and suspicious patterns, while the malware detector (106) scans the client's computer for known DNS spoofing trojans and other malware. The notification module (108) alerts users and system administrators of any detected suspicious activity, providing details, recommended actions, and instructions for removing malware. It includes a database (110) of known malicious domains and IP addresses, regularly updated to ensure it remains up-to-date against the latest threats. Machine learning algorithms (112) are employed to identify previously unknown DNS spoofing trojans and malware. The system can generate reports on detected suspicious activity, providing statistics on threats detected and recommendations for improving network security.

No. of Pages : 18 No. of Claims : 10