(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :11/10/2023

(21) Application No.202311068271 A
(43) Publication Date : 27/10/2023

(54) Title of the invention : SYSTEM AND METHOD FOR BLOCKING CYBER SECURITY THREATS BY APPLYING THREAT INTELLIGENCE-ENABLED DNS PROTOCOL

(51) International classification	:H04L0061451100, G06N0020000000, G06F0021550000, G06Q0040020000, H04W0024080000
(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)PANDEY, Sakshi
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 (102) and method (200) for blocking cyber security threats by applying a threat intelligence-enabled DNS protocol. The system (102) comprises a processor (104) coupled to a memory (106). The memory (106) stores processor-executable instructions. The processor (104) is configured to analyse DNS resolution requests in real-time. Next, the processor (104) is configured to identify suspicious behaviours exhibited by the analysed DNS resolution requests. Thereafter, the processor (104) is configured to assign a score to domains, IP addresses, and URLs based on the identified suspicious behaviours. In the end, the processor (104) is configured to take appropriate actions to mitigate cybersecurity risks based on the score.

No. of Pages : 17 No. of Claims : 10