(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :24/06/2023

(21) Application No.202311042459 A

(43) Publication Date : 21/07/2023

(54) Title of the invention : SYSTEM AND METHOD TO ANALYZE REMOTE SSL CERTIFICATES

(51) International classification	:B01L 030000, F21K 099000, H04M 150000, H04R 030000, H04W 040290
(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 :

The system (100) in the present disclosure analyses remote Secure Socket Layer (SSL) certificates. The system checks for various features of the SSL certificate including its digital signature, encryption algorithms, domain name, publication by a Certificate Authority (CA), Common name (CN), any revocations among other information. The system is capable of analysing several SSL certificates at once and also decrypting it using the public key provided by the certificate. The method comprises checking a Certificate Transparency logs for the SSL certificate and also generating a final report (114) that consists of all relevant information about the security configurations and other important data of the SSL certificate. It is capable of breaking down a connection if the remote SSL certificate is found to be unauthorized or fraudulent.

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