(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :03/02/2023

(21) Application No.202311007092 A
(43) Publication Date : 10/02/2023

(54) Title of the invention : SECURING INTERNAL NETWORK FROM UNSECURED INTERNET TRAFFIC

(51) International classification :H04L0061451100, H04W0012128000, G06F0021550000, G06F0021570000, G06Q0040020000
(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)SHARMA, Bhanu
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------

(57) Abstract :
A method 300 for securing internal network from unsecured internet traffic includes a cloud server 108 accessed by a plurality of users 102 in a network 120, a database 110, and one or more processor to perform operations including monitoring entering of one or more security attacks in the internal network, detecting at least one such attack, assessing the one such attack for success probability limits and its associated impact parameters, assessing at least one activation impact parameter of at least one counter security measure in response to the at least one detected security attack and its associated impact parameters, deciding activation of at least one counter security program, and activating at least one counter security program to counter the security attack in the internal network. The counter security programs/application includes URL and DNS filters, a SSL scan, a TLS interception, and one or more malware protectors.

No. of Pages : 19 No. of Claims : 10