(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :21/07/2023

(21) Application No.202311049342 A
(43) Publication Date : 11/08/2023

(54) Title of the invention : A SYSTEM FOR DETECTING AND MITIGATING NETWORK SCANS

(51) International classification :A61B 050550, B24B 491000, G01R 332800, H04B 150000, H04L 121000
(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)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 present disclosure relates to a system and method for detecting and mitigating network scans. The method (200) begins with collecting, by a processor (102), a network traffic data from a network of devices. Next, the method scans, by the processor (102), the collected network traffic data to extract a network traffic information. Next, the method detects, by the processor (102), patterns and trends in the extracted network traffic information. Next, the method identifies, by the processor (102), anomalies in the detected patterns and trends in the extracted network traffic information. Next, the method mitigates, by the processor (102), the identified anomalies in the network of devices. Thereafter, the method ends with receiving, by the processor (102), a feedback from a user.

No. of Pages : 23 No. of Claims : 10