(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :16/08/2023

(21) Application No.202311054814 A
(43) Publication Date : 15/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR DETECTING NETWORK INTRUSION IN REAL-TIME

(51) International classification :G06F0021550000, A61B0005000000, G06F0016230000, H04W0012121000, A61B0005055000
(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 :
Embodiments of the present disclosure relates to a system (100) and method (300) for detecting network intrusion in real-time. In an aspect, the present disclosure discloses a system (102) for detecting network intrusion in real-time by correlating data from multiple intrusion detection systems (IDS) distributed throughout a network. The system (102) comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to scan network traffic data. Further, the processor (202) is configured to identify patterns of network security breaches in the scanned network traffic data. Next, the processor (202) is configured to compare the identified patterns of network security breaches to known patterns of network security breaches in a database (220). In the end, the processor (202) is configured to generate a report of the identified patterns of network security breaches based on the comparison.

No. of Pages : 26 No. of Claims : 10