(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :09/02/2024

(21) Application No.202411008916 A
(43) Publication Date : 16/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR CYBERSECURITY EVENT DETECTION AND RESPONSE

(51) International classification :G06N0020000000, H04W0012060000, G06F0021570000, G06F0021560000, G06F0003010000
(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)SHARMA, Shubham
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present disclosure provides a system (108) for cybersecurity event detection and response. The system (108) includes primary computing devices (112) communicatively coupled to the system (108) over a network (106) via network devices (110). The system (108) is communicatively coupled to secondary computing devices (104) being operated by users (102) via the network (106). The system (108) receives a network traffic data from the network devices (110), at predefined time intervals, and extracts features from the network traffic data. The system (108) detects presence of cybersecurity events, based on the analysis of the network traffic data using techniques which may include machine learning techniques, based on the features. The system (108) initiates responses associated with the cybersecurity events detected, and sends an alert to the users (102). The system (108) transmits a report to the users (102), based on the analysis of the network traffic data.

No. of Pages : 21 No. of Claims : 10