(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :08/09/2023

(21) Application No.202311060596 A
(43) Publication Date : 13/10/2023

(54) Title of the invention : INTRUSION ATTACK DETECTION SYSTEM AND METHOD FOR INTERNET OF VEHICLES

(51) International classification :G06F0021550000, H04W0012122000, H04L0043062000, G08B0013196000, H04L0043000000
(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 :
The present disclosure relates to an intrusion attack detection system (100) for an Internet of Vehicles (IoV) (112). The system (100) includes a monitoring unit (114) configured to monitor traffic patterns associated with one or more computing devices (104) associated with the intrusion attack detection system (100) and a server (108) operatively coupled to the monitoring unit (114). The server (108) is configured to receive the monitored traffic pattern from the monitoring unit (114) and predict a behavior of one or more users by processing the received traffic pattern. Further, the server (108) is configured identify deviations of the predicted behavior from a normal behavior and correspondingly detect potential intrusion attacks using an intrusion detection unit (118) and generate an alert to notify concerned authorities about potential intrusion attacks. Furthermore, the server (108) is configured to initiate counter-response measures upon receiving notification of the potential intrusion attacks on the Internet of Vehicles (IoV) (112)

No. of Pages : 24 No. of Claims : 10