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

(21) Application No.202311047006 A
(43) Publication Date : 04/08/2023

(54) Title of the invention : MACHINE LEARNING MODEL FOR NETWORK INTRUSION DETECTION

(51) International classification	:G06F 215500, G06N 030400, G06N 030800, G06N 200000, H04L 411400
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :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, Saket
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)KUMAR, Naveen
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 that uses machine learning models (114) for a network (102) intrusion detection (116). The machine learning models (114) include decision trees, k-nearest neighbors, support vector machines, deep learning and artificial neural networks (102) for detection (116) of any intrusion in the network (102). If any malicious activities or intrusion is detected on the network (102), the system generates an alert for the user to take any remediation actions. The system also includes a continuous monitoring feature for monitoring the network (102) for any additional intrusions or network 102 mis functionalities. The method comprises scalability measures for effectively monitoring a larger network (102) and also includes a threat hunting capability for detecting potential threats in the network (102). The system updates its machine learning model (114) to detect any new kinds of network (102) threats.

No. of Pages : 28 No. of Claims : 13