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

(21) Application No.202311056226 A
(43) Publication Date : 22/09/2023

(54) Title of the invention : SYSTEM AND METHOD FOR DETECTING AND RESPONDING TO AI-BASED ATTACKS

(51) International classification :G06N0020000000, G06N0003080000, G06F0021550000, H04L0041160000, H04L0051000000
(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 invention describes a system (100) and method (300) for detecting and responding to artificial intelligent (AI)-based attacks by using machine learning (ML) techniques. The proposed system (100) includes an AI-based attack detection unit (210) that analyzes network traffic and identifies patterns consistent with AI-based attacks. The system (100) also includes an AI-based attack response unit (212) that responds to detected AI-based attacks by modifying network traffic, applying access control rules, and triggering alerts for further analysis. Furthermore, the AI-based attack detection unit (212) uses a variety of ML techniques, including supervised and unsupervised learning, to identify patterns consistent with AI-based attacks. However, the ML techniques can be implemented as a standalone device or integrated into existing security measures. The system (100) can be trained using historical data to improve accuracy and reduce false positives.

No. of Pages : 24 No. of Claims : 6