(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :29/08/2023

(21) Application No.202311057924 A
(43) Publication Date : 29/09/2023

(54) Title of the invention : ADAPTIVE ANOMALY-BASED INTRUSION DETECTION SYSTEM

(51) International classification :G06N0020000000, G06F0021550000, H04L0041147000, H04W0012121000, H04L0041142000
(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 adaptive anomaly-based intrusion detection system (100) is a comprehensive defense framework encompassing several interconnected modules. The data collection module (104), which accumulates network traffic data and user activity logs. The feature extraction module (106) preprocesses this data, distilling pertinent features that encapsulate network traffic nuances and user behaviors. The training module (108) leverages machine learning algorithms to construct normal behavior patterns grounded in the extracted features. Subsequently, the Anomaly detection module (110) springs into action, scrutinizing real-time extracted features against established norms. It skillfully identifies anomalies that could potentially signify security breaches, triggering timely alerts through the Alert generation module (114). The system remains ever-vigilant through the adaptive learning mechanism (112), dynamically refreshing normal behavior patterns to harmonize with evolving network conditions and user actions. When anomalies arise, the Response mechanism (116) takes charge, initiating automated responses that neutralize detected intrusion attempts

No. of Pages : 28 No. of Claims : 10