(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :15/02/2024

(21) Application No.202411010686 A
(43) Publication Date : 23/02/2024

(54) Title of the invention : DYNAMIC INCIDENT RESOLUTION SYSTEM AND METHOD THEREOF

(51) International classification	:G06N0020000000, G06N0007000000, G06N0005040000, G06N0005000000, H04L0041160000
(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, 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, Vivek
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
A dynamic incident resolution system for enhancing data security is disclosed, the system 102 monitors network traffic, system logs, and user activities on computing devices 104 within a network 106. The system 102 identifies and categorizes security threats, utilizing machine learning and artificial intelligence techniques for real-time analysis. The system 102 further includes continuous training of a model, anomaly detection to identify deviations from behavioral patterns, and the integration of natural language processing techniques for comprehensive analysis. Severity identification and response initiation based on the identified severity are additional features of the disclosed system. The remediation routine includes the generation of detailed reports on identified security threats. The integration of machine learning, artificial intelligence, threat intelligence, and remediation routines contributes to a dynamic and adaptive cybersecurity framework, ensuring the identification, categorization, and mitigation of security threats in a networked environment.

No. of Pages : 27 No. of Claims : 10