(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :01/09/2023

(21) Application No.202311058831 A
(43) Publication Date : 06/10/2023

(54) Title of the invention : PROACTIVE EXPLOIT DETECTION SYSTEM AND METHOD USING MACHINE LEARNING AND BEHAVIORAL ANALYSIS TECHNIQUES FOR IMPROVED NETWORK SECURITY

| | |
|---|---|
| (51) International classification | :G06F0021550000, G06N0020000000, G06N0005040000, G06F0021560000, G06N0020200000 |
| (86) International Application No<br>Filing Date | :NA<br>:NA |
| (87) International Publication No | : NA |
| (61) Patent of Addition to Application Number<br>Filing Date | :NA<br>:NA |
| (62) Divisional to Application Number<br>Filing Date | :NA<br>: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 :
Presented is a proactive exploit detection system (100) that enhances network security by fusing machine learning, behavioral analysis, and threat intelligence. The system collects data from network sources (102) and analyzes it behaviorally (104) and historically (106). It detects anomalies (108) by comparing real-time network behavior with statistical models and integrates current threat intelligence (110). Real-time alerts (112) notify administrators of potential threats, while automated countermeasures (114) mitigate risks. Comprehensive reporting (116) offers insights for refined defenses. This paradigm shift (100) advances network security by precluding threats before damage occurs.

No. of Pages : 26 No. of Claims : 10