(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :06/02/2024

(21) Application No.202411008040 A

(43) Publication Date : 16/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR NETWORK THREAT DETECTION IN NETWORK TOPOLOGIES

(51) International classification	:G06N0020000000, G06F0021550000, G06F0021570000, G06N0003080000, G06F0021560000
(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, 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)SHARMA, Lakshay
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

The system (100) integrates distributed sensor networks, packet analysis, and a machine learning model (108) to create a robust threat detection framework. Distributed sensors strategically placed across multi-tier network topologies continuously capture and monitor network behavior. The packet analysis module (106) conducts deep inspections of data packets, identifying anomalies and potential threats. The machine learning model (108), comprising dual layers, classifies threats by recognizing existing attack vectors and identifying new ones. The innovative approach enhances the system's (100) adaptability to evolving threats. The integration of the components enables real-time detection, classification, and response to potential security incidents, providing a dynamic and proactive defense against a spectrum of cyber threats in complex network environments. The collaboration of machine-driven analytics and human security expertise further ensures a comprehensive cybersecurity strategy.

No. of Pages : 34 No. of Claims : 10