(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :19/12/2025

(21) Application No.202541129120 A
(43) Publication Date : 02/01/2026

(54) Title of the invention : NETWORK TRAFFIC ANALYSIS FOR SECURITY ANOMALY

(51) International classification	:H04L 29/06, G06N 20/00, H04L 12/26, G06F 21/55, H04L 12/24
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(86) International Application No Filing Date	: :01/01/1900
(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)Dr Poornima Raikar
Address of Applicant :Department of Computer Science AIML KLS VDIT Haliyal Karnataka India
(72)**Name of Inventor :**
1)Ekata S Shanbhag
2)Dr Poornima Raikar
3)Anusha J Poojari
4)Khushi Poojary
5)Shravya A Bangera
6)Sneha B Karlawad

(57) Abstract :
This invention proposes a real-time, machine-learning-based Network Traffic Analysis System capable of detecting security anomalies in large-scale network environments. Modern networks generate massive volumes of traffic, making traditional rule-based IDS ineffective against newly emerging and unknown cyber-attacks. The system preprocesses raw network data, performs statistical analysis, and selects significant features using Random Forest feature importance, as referenced in the project methodology The anomaly detection model, trained on the WEB-IDS23 dataset containing over twelve million records and multiple attack categories, achieves an accuracy of 94.15% and a ROC-AUC of 0.987, demonstrating strong classification performance . The invention integrates this model into a Flask-based web application that processes uploaded or live network logs to identify malicious traffic in real time. The system provides visual dashboards, attack summaries, browser alerts, and automated email notifications to ensure immediate incident awareness. By combining scalable preprocessing, intelligent classification, and real-time alerting, the invention offers a proactive, efficient, and deployable solution for modern cybersecurity needs, enabling early detection of threats and reducing risks associated with network intrusions.

No. of Pages : 8 No. of Claims : 3