INTERNATIONAL CONFERENCE ON RESEARCHES IN ENGINEERING, SCIENCE, MANAGEMENT AND HUMANITIES (ICRESMH – 2025)

Delhi, India on 27th April, 2025

CERTIFICATE NO : ICRESMH /2025/C0425422

A Study of Detect Intrusion from Network Traffic in Real Time

Dogiparthy Sravankumar

Research Scholar, Department of Computer Science, Mansarovar Global University,
Sehore M.P., India.

ABSTRACT

Real-time intrusion detection from network traffic is a crucial aspect of modern cybersecurity, as organizations must identify and respond to threats the moment they occur. Real-time systems continuously monitor incoming and outgoing network packets, analyzing patterns, behaviors, and anomalies to detect suspicious activities instantly. This approach relies on advanced algorithms, machine learning models, and deep packet inspection techniques that can quickly differentiate between normal and malicious traffic. By processing data at high speed, real-time intrusion detection can identify threats such as malware infections, unauthorized access attempts, data exfiltration, and distributed denial-of-service (DDoS) attacks before they cause significant damage. The system uses automated alerts and adaptive response mechanisms to block or mitigate attacks immediately, minimizing the risk to the organization. Real-time monitoring also enables security teams to detect zero-day attacks and previously unknown vulnerabilities by flagging abnormal behavior rather than depending solely on predefined signatures. To achieve high accuracy, such systems must handle large volumes of data, maintain low latency, and continuously update their detection models. Overall, real-time intrusion detection from network traffic enhances the resilience of networks by providing faster threat identification, reducing potential downtime, and strengthening overall security against evolving cyber threats.