HYBRID APPROACH FOR NETWORK INTRUSION DETECTION SYSTEM USING MACHINE LEARNING

ABSTRACT

IDS plays a crucial role in network security by detecting malicious activities. Traditional signature-based IDS is effective against known attacks but fails to detect anomalies and novel threats. Machine learning classifiers offer a more robust solution but often struggle with rare and uncommon attack types, such as Remote-to-Local (R2L) and User-to-Root (U2R), due to the diversity in attack patterns. We are introducing an improved Double Layered Hybrid Approach(DLHA) which is the hybrid model of the enhanced Bidirectional Long Short Term Memory(BLSTM),and its ability to detect attack performance will be enhanced.

Our method employs Principal Component Analysis (PCA) to capture key features and variance across attack categories, revealing that R2L and U2R exhibit behaviour similar to normal users. DLHA has Naive Bayes as Layer 1 that classifies the Denial of Service (DoS) and Probe attacks quite effectively, and Layer 2 combines Support Vector Machines (SVM) with BLSTM that differentiates the R2L and U2R attacks from normal instances accurately. The introduction of BLSTM allows DLHA to learn the temporal and sequential patterns in the network traffic for better detection of rare attacks.

IOMP ID:IT-25-12

Name 1: Suragani Revathi

Roll No:22261A1253

Name 2: Patloori Durga

Roll No:22261A1246

(Mrs.Ch.Sudha)

Internal Supervisor

(Mrs. U.Chaitanya)

IOMP Supervisor