Secondary Objectiveso SO-1: To acquire and preprocess benchmark IoT intrusion detection datasets.5 (NSL-KDD,UNSW-NB15, CIC-IoT2023, N-BaIoT, TON-IoT) with rigorous Leave-One-Attack-Out (LOAO)zero-day evaluation protocol design.o SO-2: To design a hybrid 1D-CNN + BiLSTM + Transformer encoder architecture exploitingcomplementary features at packet, flow-temporal, and long-range behavioral abstraction levels.o SO-3: To implement NT-Xent self-supervised contrastive pre-training for zero-day anomalydetection capability without labeled attack examples.o SO-4: To develop an EWC-based continual learning mechanism for sustained detectionperformance under concept drift.o SO-5: To integrate a hierarchical four-level explainability architecture (Grad-CAM, IntegratedGradients, Attention Rollout, Cross-Attention Maps, SHAP Values).o SO-6: To conduct rigorous comparative evaluation against state-of-the-art baselines withstatistical significance testing.5.3.Primary ObjectiveTo design, implement, and rigorously evaluate a unified, zero-day-robust deep learning framework forintelligent intrusion detection in dynamic IoT network environments -- a framework capable of reliablyidentifying both known and previously unseen attack patterns while sustaining detection performanceunder concept drift, maintaining operationally viable false positive rates, and providinghuman-interpretable, actionable explanations for detection decisions.5.2.Does the hybrid 1D-CNN + BiLSTM + Transformer multi-stream encoder architecture providestatistically significant detection performance advantages -- measured by AUC-ROC, F1-Score, andzero-day detection rate -- compared to any single-stream or dual-stream encoder architectureapplied in isolation?3.Research .Objectives and Questions5.1.Research Questions1