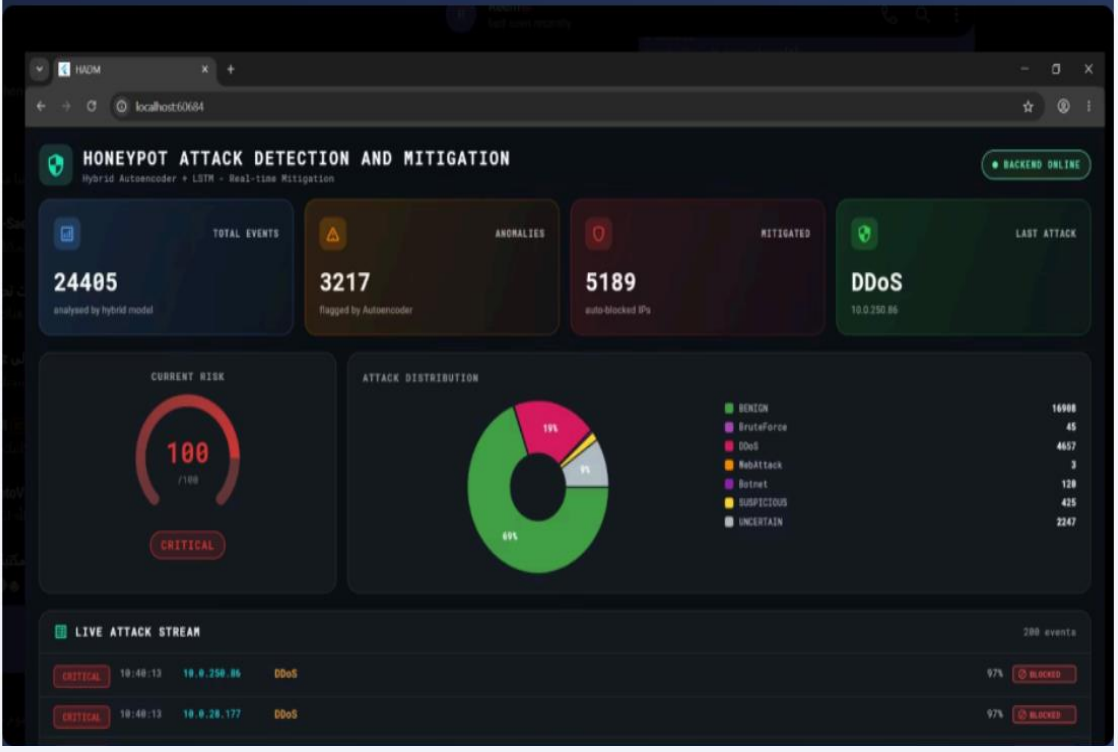
AL-SAEED UNIVERSITY

جامعة السعيد

Effective Detection and Real-Time Mitigation of Honeypot Attacks Using Deep Learning

Walid Waad, Shahd Adel, Farah Zaki, Roaa Saleh, Reem Abdul Razzaq, Farah Jalal, Mogeeb Al-Hakimi

Department of Cybersecurity, Faculty of Engineering and IT, Al-Saeed University, Taiz, Yemen



Innovation Concept

An intelligent, real-time cybersecurity system that analyzes network traffic and security logs from Honeypot environments. It combines Deep Learning for anomaly detection and attack classification with an automated Real-Time Mitigation layer that instantly translates findings into defensive measures without human delay.

Problem Statement

· Legacy detection fails against modern complex threats · Overwhelming volume of security logs and zero-day attacks · High False Positive/Negative rates overwhelming SOC teams · Time lag between detection and manual mitigation

How It Works

① Data Preprocessing (CIC-IDS2017): Cleaning & feature extraction ② Anomaly Detection (Autoencoder): Identifying unusual patterns ③ Classification (LSTM): Categorizing attack types (DoS, DDoS, Brute Force, Botnet, etc.) ④ Real-Time Mitigation: Dynamic Blocking, Rate Limiting, Traffic Redirection

Technical Feasibility

· Hybrid Architecture: Autoencoder + LSTM for maximum accuracy · Low-latency real-time processing pipeline · Integration-ready with Firewalls, IPS, and SIEM systems

Expected Impact

· Bridges the gap between passive detection and active mitigation · Drastic reduction in false positives and alert fatigue · Autonomous, proactive defense for critical digital infrastructure

AL-SAEED UNIVERSITY

جامعـة السعيـد

الكشف الفعّال والتخفيف الفوري من هجمات الـ Honeypot باستخدام تقنيات التعلم العميق

وعد وليد، شهد عادل، فرح زكي، رؤى صالح، ريم عبد الرازق، فرح جلال، مجيب الحكيمي
قسم الأمن السيبراني، كلية الهندسة وتقنية المعلومات، جامعة السعيد، تعز، اليمن

فكرة الابتكار

منظومة دفاع سيبراني ذكية ومباشرة تُحلل حركة مرور البيانات الشبكية والسجلات الأمنية المرتبطة بمصايد المخترقين (Honeypots)، حيث تُزاوج بين قدرات التعلم العميق للكشف عن التهديدات وتصنيفها، وطبقة استجابة وتخفيف أوتوماتيكية فوريّة تُترجم نتائج الكشف إلى إجراءات دفاعية لحظية دون تدخل بشري.

المشكلة

• عجز الأنظمة التقليدية عن مواكبة الهجمات الحديثة المعقدة • صعوبة معالجة السجلات الأمنية الضخمة والهجمات غير المعروفة • ارتفاع نسب الإنذارات الكاذبة • الفجوة الزمنية بين اكتشاف الهجوم واتخاذ القرار الدفاعي

آلية العمل

① الجمع والمعالجة (CIC-IDS2017): تنظيف سجلات الشبكة واستخراج السمات ② الكشف الذكي (Autoencoder): رصد الأنماط الشاذة ③ التصنيف الدقيق (LSTM): تصنيف نوع الهجوم ④ التخفيف اللحظي: تنفيذ آلي للحظر والتحويل وتقييد المعدل

الجدوى التقنية

• نموذج هجين: Autoencoder + LSTM لأعلى دقة تصنيف • معالجة فورية بدون تأخير أو إبطاء للشبكة • قابلية التكامل مع جدران الحماية وأنظمة SIEM

الأثر والفائدة المتوقعة

• تحويل الكشف إلى دفاع فعلي وآلي • تقليل الإنذارات الكاذبة ورفع موثوقية المراقبة • استجابة استباقية وذاتية لحماية البنى التحتية الحساسة