

كشف تسريب البيانات ضمن شبكات انترنت الأشياء الذكية باستخدام تقنيات الذكاء الصنعي

Data Leakage Detection in Smart Internet of things (IOT) Networks

2025/2026

إعداد الطّلاب:

قاسم عقله

سامر رحمة

إشراف:

د. وسيم الجندي

أ. يامن الحلاق



الجامعة السورية الخاصة
SYRIAN PRIVATE UNIVERSITY



الخيار الأمثل لمحاكاة أنظمة وانترنت الأشاء بفضل دقته وواقعته في توليد حركة مرور قابلة للتحليل NS-3

بعد البحث والمقارنة بين بيئات العمل المتاحة (من بين أنظمة التشغيل والمحاكيات وخوارزميات الذكاء الصنعي ولغات البرمجة)

تم الاعتماد والعمل على بيئة العمل التالية :

نظام التشغيل: ubuntu (افتراضي)

المحاكي: NS-3

ثم ان نظام ubuntu يتيح بيئة تطويرية متقدمة داعمة لمحاكيات الشبكات

خوارزمية الذكاء الصنعي: XGBoost

تم الاعتماد على XGBoost لما تتوفره من توافقية عالية واستقرار



النتائج الأولية لتنفيذ بيئة العمل

تم إنشاء نموذج محاكاة منزل ذكي يحوي **10** عقد (أجهزة)

تم وضع **أجهزة طبيعية (8)** ، وأجهزة مختربة (2)

بالإضافة إلى توليد حزم بيانات تتبادلها الأجهزة

%85 من الحزم طبيعية

%15 من الحزم خبيثة

سيناريو الهجوم !

الجهاز المخترق

Device 9 (Camera)

نوع الهجوم

Data Exfiltration

المنفذ المستهدف

Port 8888

حجم الحزمة

8K - 15K bytes

بيئة المحاكاة

عدد أجهزة IoT

10 أجهزة

أجهزة عادية

8 أجهزة

أجهزة مختربة

2 أجهزة

مدة المحاكاة

100 ثانية

البيانات المولدة

15%~

حزم خبيثة

85%~

حزم عادية

2,000~

إجمالي الحزم

أنواع البيانات الحساسة الممسرة

سجلات طبية

مفاتيح API

رقم الضمان

بطاقات ائتمان

كلمات المرور

مقاييس الأداء

0.995

ROC-AUC

الجودة

99.2%

Recall

الكشف

97.8%

Precision

التصنيف

98.5%

Accuracy

الدقة

أهم 5 خصائص

28%

max_packet_size

22%

suspicious_port

18%

packets/second

15%

ttl_suspicious

12%

size_entropy

الخصائص المستخرجة

13

حجم الحزم

6

خصائص زمنية

12

بروتوكول

5

المحتوى

+36

إجمالي الخصائص

تحليل نتائج أداء تدريب خوارزمية الذكاء الصنعي

أظهر تدريب النموذج جودة ممتازة في الكشف

%0.94

ملخص الكشف

15.2s

وقت التدريب

4

إنذارات خاطئة

2

مفقودة

295

مكتشفة