

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

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

2025/2026

إشراف:

د. وسيم الجندي

أ. يامن الحلاق

إعداد الطلاب:

قاسم عقله

سامر رحمه



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

تم الاعتماد والعمل على بيئة العمل التالية :

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

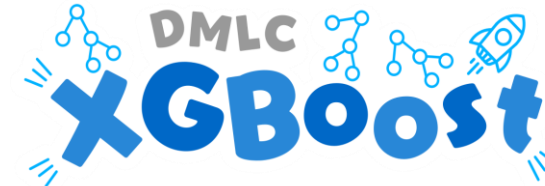
نظام التشغيل: ubuntu (افتراضي)

المحاكي: NS-3

ثم ان نظام ubuntu يتيح بيئة تطويرية متقدمة داعمة لمحاكيات الشبكات

خوارزمية الذكاء الصناعي: XGBoost

تم الاعتماد على XGBoost لما توفره من توافقية عالية واستقرار



## النتائج الأولية لتنفيذ بيئة العمل

تم انشاء نموذج محاكاة لمنزل ذكي يحوي 10 عقد (أجهزة)

تم وضع أجهزة طبيعية (8) ، وأجهزة مخترقة (2)

بالإضافة الى 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

10 أجهزة  
عدد أجهزة IoT

8 أجهزة  
أجهزة عادية

2 أجهزة  
أجهزة مخترقة

100 ثانية  
مدة المحاكاة

### البيانات المُولدة

~15%

حزم خبيثة

~85%

حزم عادية

~2,000

إجمالي الحزم

### أنواع البيانات الحساسة المُسرَّبة

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 المُستخرجة

حجم الحزم

13

خصائص زمنية

6

بروتوكول

12

المحتوى

5

+36

إجمالي الخصائص

## ملخص الكشف

15.2s

وقت التدريب

4

إنذارات خاطئة

2

مفقودة

295

مكتشفة

تحليل نتائج أداء تدريب خوارزمية الذكاء  
الصنعي

أظهر تدريب النموذج جودة ممتازة في الكشف

بلغت 0.94%