

الجمهورية العربية السورية

وزارة التعليم العالي

جامعة السورية الخاصة

كلية الهندسة



كشف تسريب البيانات ضمن شبكات انترن特 الأشياء الذكية

باستخدام تقنيات الذكاء الصناعي

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

إشراف:

د. وسيم الجنيدى

أ. يامن الحلاق

إعداد الطالب:

قاسم عقله

سامر رحمة

Abstract

كشف تسريب البيانات ضمن شبكات إنترنت الأشياء

يهدف هذا البحث إلى دراسة التحديات الأمنية المرتبطة بتسريب البيانات في شبكات إنترنت الأشياء والتي أصبحت هدفاً رئيسياً للهجمات الإلكترونية مع التوسع الهائل في استخدامها. من الجانب النظري، يحلل البحث أسباب تسريب البيانات عبر القنوات المختلفة ويستعرض أحدث الأبحاث في المجال، لا سيما تلك التي تستخدم تقنيات التعلم الآلي والذكاء الاصطناعي للكشف عن السلوكيات الشاذة أما من الجانب العملي، فيركز المشروع على تطوير إطار متكامل يكشف عن تسريب البيانات في الوقت الفعلي، من خلال استخدام أدوات تحليلية متقدمة لمراقبة حركة البيانات وتحديد الأنشطة غير المصرح بها ويختتم البحث بالتأكيد على أن مواجهة مخاطر التسريب تتطلب نهجاً أمنياً شاملاً يدمج بين التحليل العميق واستخدام التقنيات الحديثة، لضمان حماية البنية التحتية الحيوية.

Detecting Data Leakage in Internet of Things (IoT) Networks

This research aims to study the security challenges associated with data leakage in Internet of Things (IoT) networks, which have become a primary target for cyberattacks due to their massive expansion. From a theoretical perspective, the research analyzes the causes of data leakage through various channels and reviews the latest studies in the field, especially those using machine learning and artificial intelligence to detect anomalous behaviors. From a practical standpoint, the project focuses on developing an integrated framework for real-time data leakage detection by using advanced analytical tools to monitor data traffic and identify unauthorized activities. The research concludes by emphasizing that confronting leakage risks requires a comprehensive security approach that integrates deep analysis with modern techniques to ensure the protection of critical infrastructure.

فهرس المحتويات:

7	المقدمة (introduction)
7	المشكلة العلمية
7	المهدف من البحث
8	الدراسة المرجعية (state of the art)
14	التحديات
16	التطبيقات العملية
17	الفصل الأول (الدراسة النظرية)
18	1.1.1 البنية الأساسية لإنترنت الأشياء
18	1.1.2 التطبيقات لإنترنت الأشياء
21	1.2.1 أنماط تسرير البيانات
22	1.2.2 أمثلة على تسرير البيانات
23	2.1.2 اثار تسرير البيانات
24	2.2.1 تحديات إنترنت الأشياء
25	3.1.1 العواقب الرئيسية
27	3.2.1 نقاط الضعف في إنترنت الأشياء
28	الفصل الثاني (بيئة العمل)
29	2.1 المقدمة
29	2.2 البيئة التحتية البرمجية
30	2.2.2 بيئة التطوير
31	2.2.4 أدوات التحليل
31	3.1 الحاسوب المستخدم
32	3.3 البروتوكولات الأساسية في بيئة العمل
33	4.1 المكونات البرمجية للمشروع
36	4.2 التحديات والقيود

38.....	الفصل الثالث.....
43.....	5.1 بعض نماذج تسريب.....
44.....	5.2 العلاقة بين النماذج والحل المقترن.....
45.....	5.3 الأدوات المستخدمة في تحليل المور والتسريب.....
46.....	5.4 امثلة لتسريب البيانات الكارثية.....
47.....	5.5 خطوات للحل المقترن.....
48.....	الفصل الرابع.....
55.....	النتائج.....
57.....	التوصيات.....
59.....	المراجع.....

فهرس الأشكال

11.....	الشكل 1 (تضخم لأنترنت الأشياء)
15.....	الشكل 1.1(التحديات).....
20.....	الشكل 1.2(تطبيقات انترنت الأشياء)
23.....	الشكل 2.1 (ابرز المهمات على انترنت الأشياء)
44.....	الشكل 1.3 (هجوم الرجل في المنتصف)
52.....	الشكل 1.1 العلاقة بين عدد الحزم و زمن الاستجابة.....
52.....	الشكل 2.2 يوضح نسبة استخدام المعالج مع الزمن.....

فهرس الجداول:

12.....	الجدول 1.1 (الدراسة المرجعية)
26.....	الجدول 2.1 Major themes
50.....	الجدول 2.2 مقارنة بين الدراسات النظرية
51.....	الجدول 3.1 مقارنة لبيئات العمل وأدوات التنفيذ
53.....	الجدول 3.2 المشاكل مع الحلول

المقدمة

شهد العالم في العقود الأخيرة ثورة رقمية هائلة، ترافقت مع تطور سريع في تقنيات الاتصالات والشبكات، مما أسهم في بروز إنترنت الأشياء كأحد أبرز المجالات الحديثة، وقد أتاحت هذا المجال فرصاً واسعة في مجالات متعددة مثل الصناعة، الزراعة، الصحة، والعسكرية، إضافة إلى الحياة اليومية، حيث أصبح الاعتماد على الأجهزة المتصلة بالإنترنت جزءاً أساسياً من البنية التحتية الرقمية، إن ازدياد عدد الأجهزة المتصلة أدى بطبيعة الحال إلى تضخم حجم البيانات المتبادلة عبر الشبكات، بما في ذلك البيانات الحساسة مثل البيانات الطبية والعسكرية والصناعية، وهو ما جعل شبكات إنترنت الأشياء هدفاً رئيسياً للهجمات الإلكترونية ومحاولات تسريب البيانات، ورغم أن الكثير من الجهد بذلت لتوفير آليات حماية لهذه الشبكات، فإن محدودية إمكانيات الأجهزة، وتنوع بروتوكولات الاتصال المستخدمة، يجعل تحقيق مستوى أمني مرتفع أمراً معقداً وصعباً، من هنا تبرز أهمية التعمق في مجال كشف تسريب البيانات ضمن شبكات إنترنت الأشياء، كونه يمثل ركيزة أساسية لحماية المعلومات وضمان أمن الأجهزة المتصلة ولا يقتصر ذلك على منع الهجمات فحسب، بل يشمل أيضاً تقليل المخاطر التشغيلية، والامتثال للمعايير والقوانين الدولية المتعلقة بالخصوصية، إضافة إلى تعزيز ثقة المستخدمين في تقنيات إنترنت الأشياء.

يركز هذا التقرير على دراسة بعض

التحديات الأمنية المرتبطة بكشف تسريب البيانات في شبكات إنترنت الأشياء، وتحليل البروتوكولات والآليات المستخدمة حالياً، مع مراجعة الحلول المقترحة في الدراسات السابقة، كما يسعى إلى استعراض الاتجاهات البحثية الحديثة التي توظف تقنيات مثل التعلم الآلي والذكاء الاصطناعي لتطوير حلول أكثر كفاءة وفعالية، وبذلك يشكل البحث إطاراً علمياً يمكن الاعتماد عليه لتطوير أنظمة مستقبلية تعزز الأمان السيبراني وتدعم استدامة الثقة في تقنيات إنترنت الأشياء.

١- المشكلة العلمية:

مع الانتشار المتزايد لأجهزة إنترنت الأشياء في حياتنا اليومية والصناعية، أصبحت شبكاتها هدفاً رئيسياً للهجمات الإلكترونية وسرقة البيانات الحساسة، تعتمد هذه الأجهزة غالباً على بروتوكولات اتصال بسيطة، مما يجعلها عرضة للتسلل واستغلال التغرات الأمنية، المشكلة الأساسية تكمن في عدم وجود آليات فعالة ودقيقة لكشف تسريب البيانات في الوقت الحقيقي الأمر الذي يزيد من مخاطر فقدان المعلومات والتجسس على المستخدمين وتأثير الهجمات على استقرار الشبكات، لذلك: هناك حاجة ملحة لتطوير حلول تكشف هذه التسريبات بشكل مبكر وفعال، مع مراعاة خصوصية البيانات وأداء الشبكة.

٢- الهدف من البحث:

تطوير إطار مدعوم بتقنيات الذكاء الصنعي متكملاً لكشف تسريب البيانات بالسرعة اللازمة لإيقافه والتعافي منه واستخدام أحدث الآليات والخوارزميات في أمن المعلومات وتحديد أفضلها بمدف الحد من تسريب البيانات ضمن شبكات إنترنت الأشياء

كما يهدف البحث إلى تقديم إطار علمي منهجي يمكن استخدامه كأساس لتطوير الأنظمة أمان مستقبلية والمساهمة في رفع مستوى الحماية السيبرانية للأجهزة الذكية المتصلة، بما يضمن استدامة الثقة في تقنيات إنترنت الأشياء.

سنقوم بدراسة مرجعية لأحدث التقارير ووراق البحث التي تتعلق بمشروعنا والتي يمكن الاستفادة منها:

"State of the art" -3

"google scholar"

في عام 2025 نشر الباحثان " Padmavathi and saminathan" مقال بعنوان:

"إطار الثقة الآمن القائم على الذكاء الصناعي للحافة في إنترنت الأشياء" (AI-SET)

قدمت الورقة اطراً أمنياً ذكرياً لأنترنت الأشياء يعتمد على الذكاء الصناعي والتعلم الفيدرالي يدمج كشف التسلل عند الحافة والتحكم بالوصول وفق مستوى الثقة وسلوك الأجهزة وأثبتت النتائج فعاليته بدقة كشف بلغت 94%

تفيد الورقة مشروعنا في تطوير نظام كشف تسريب البيانات من خلال توضيح أهمية التعلم الفيدرالي والذكاء الاصطناعي في تأمين شبكات إنترنت الأشياء.

وفي عام 2025 كتب الباحثون " Llenia Ficili, Maurizio, Giuseppe Tricomi, Antonio puliafito"

مقالة بعنوان: "من السحابة إلى الحافة: دمج إنترنت الأشياء والذكاء الصناعي لأنظمة مستدامة وفعالة"

ناقشت الورقة التكامل بين تقنيات إنترنت الأشياء والحوسبة السحابية والحوسبة الطرفية مع الذكاء الصناعي لتحويل البيانات إلى قرارات آنية

تفيد الورقة مشروعنا في توضيح كيفية استخدام الذكاء الصناعي عند الحافة لتحليل بيانات أجهزة إنترنت الأشياء في الزمن الحقيقي وأكتشاف التسريبات بسرعة.

أيضاً في عام 2025 نشر الباحثان "Mohammad Shamim, AL-Sakib khan" ورقة بحث بعنوان:

"نماذج التحكم في الوصول لإنترنت الأشياء: مراجعة شاملة واتجاهات مستقبلية"

قدمت الورقة دراسة شاملة لنماذج التحكم بالوصول في بيانات إنترنت الأشياء موضحة أهم متطلبات الأمان والتحديات المستقبلية

تفيد الورقة مشروعنا في تحديد أفضل نماذج التحكم بالوصول المناسبة لاكتشاف تسريب البيانات ضمن شبكات إنترنت الأشياء

أيضاً توضح كيفية دمج الذكاء الصناعي وتقنيات البلوك تشين في تعزيز أمان الوصول إلى البيانات.

وفي عام 2025 نشر الباحثون " Ali M, Eltamaly, Mashael S Maashi, Tarek S Sobh, Ahmed A " ورقة بحث بعنوان:

"الكشف عن المجمات السيبرانية في انترنت الأشياء الصناعي باستخدام الذكاء الصناعي"

قدمت الورقة نظاماً ذكرياً آمناً يعتمد على تقنيات الذكاء الصناعي للكشف عن المجمات السيبرانية في شبكات انترنت الأشياء الصناعية

قام الباحثون باستخدام خوارزميات التعلم العميق لتصنيف الأنماط الضارة وتحليل حركة البيانات بدقة عالية

نستفيد من دراسة ورقة البحث هذه تعزيز فكرة استخدام الذكاء الصناعي لتحليل البيانات الشبكية وأكتشاف تسريب المعلومات في الزمن الحقيقي.

"Hossam Magdy, Ahmed Mostafa, Hossam Faris, Aboul Ella Hassaneien" نشر 2025 أيضاً في عام
الباحثون

ورقة بحثية بعنوان: " إطار أمني قائم على التعلم العميق لشبكات انترنت الأشياء: تقنيات ذكية هجينة لاكتشاف التهديدات "

قدمت الورقة نظاماً آمنياً يعتمد على التعلم العميق لتصنيف وتحليل البيانات داخل شبكات انترنت الأشياء

كما استخدم الباحثون خوارزميات هجينة من الشبكات العصبية والذكاء التطورى لاكتشاف التهديدات والتسللات بدقة عالية

واظهرت النتائج الموجودة في الورقة البحثية تفوق النموذج في سرعة الكشف

تفيدنا هذه الورقة البحثية في دعم فكرة استخدام الذكاء الاصطناعي العميق لكشف تسريب البيانات بفعالية عالية مع توازن الأداء والسرعة.

و قبل ذلك في عام 2024 نشر الباحثون " Lotfi abdennebi, Mohamed bouchoucha, Ezzeddine" ورقة بحثية بعنوان:

"الكشف عن التسلل ومنع تسريب البيانات باستخدام الذكاء الاصطناعي في أنظمة انترنت الأشياء"

ناقشت الورقة التهديدات الأمنية في شبكات انترنت الأشياء، خاصة كشف التسلل وتسريب البيانات عبر الذكاء الاصطناعي

واستعرضت تقنيات حديثة مثل التعلم الآلي والعميق لتحليل حركة البيانات والتعرف على الأنماط المشبوهة

تفيد الورقة البحثية في مشروعنا في تحسين منهجية كشف التسربات عبر تحليل السلوك وتوظيف خوارزميات دقيقة وخفيفة الموارد.

وفي نفس العام 2024 نشر الباحثين " Mani Srivastaava, Zhichao Cao, Ness Shroff, Hyunho, Shahrul Iman" ورقة بحثية بعنوان:

مقالة بعنوان: " الذكاء الاصطناعي لإنترنت الأشياء (AIOT) : رؤية نحو أنظمة ذكية ومتصلة "

استعرضت الورقة مفهوم AIOT الذي يجمع بين الذكاء الاصطناعي وانترنت الأشياء مع توضيح اركانه الأساسية (الاستشعار، الحوسنة، الاتصال)

تناولت تطبيقاته في الرعاية الصحية والطاقة والمركبات الذاتية، لخصت على ان النماذج التوليدية والتعلم العميق تفتح آفاقاً جديدة للتحليل في الزمن الحقيقي

مع تحديات المخصوصية

نستفيد من هذه المقالة بناءً إطار يعتمد الذكاء الاصطناعي عند الحافة لتحسين سرعة ودقة كشف التسريب.

أيضاً في عام 2024 نشر الباحثون "Amira, Saida Hafsa Rafique, Nura Shifa Musa, Abdallah" مقال بعنوان:

"**تقنيات التعلم الآلي والعميق للكشف الشذوذ في شبكات إنترنت الأشياء: مراجعة شاملة**"

استعرض المقال أحدث الاتجاهات في استخدام التعلم الآلي والعميق لكشف الشذوذ في شبكات إنترنت الأشياء، راجحت أكثر من 60 دراسة تضمنت خوارزميات مثل الشجر العشوائي والشبكة العصبية و XGBoost

لخصت: أن الذكاء الاصطناعي يرفع دقة الكشف لكنه يواجه تحديات في البيانات الواقعية واستهلاك الموارد

تفيد مشروعنا في اختيار الخوارزميات الأنسب لبناء نظام دقيق وفعال للكشف المبكر عن التسريب

بالفعل تم اختيار خوارزمية من هذه المقالة للعمل عليها في تقريرنا.

أيضاً في عام 2024 نشر الباحثون "Umair Khadam, Paul Davidsson, Romina Spalazzese" ورقة بحثية

عنوان: "استكشاف دور الذكاء الاصطناعي في أنظمة إنترنت الأشياء: دراسة تحليلية منهجية"

قدمت دراسة منهجية لدور الذكاء الاصطناعي في أنظمة إنترنت الأشياء من خلال تحليل 81 بحثاً بيّنت أهم مهام الذكاء الاصطناعي

لخصت: إلى أن دمج الذكاء الاصطناعي في إنترنت الأشياء يعزز الكفاءة والأمان والتنبؤ الذكي

تفيدنا هذه المقالة في تحديد كيفية توظيف الذكاء الاصطناعي لتحسين دقة كشف التسريب وتعزيز أمان الشبكات الذكية.

وفي عام 2023 نشر الباحثون "Abdussalam Elhanashi, Pierpaolo Dini, Sergio Saponara, Qinghe Zheng" مقال بعنوان:

"**دمج تقنيات التعلم العميق في إنترنت الأشياء: مراجعة للتقنيات والتحديات في التطبيقات الواقعية**"

تناولت دمج تقنيات التعلم العميق في إنترنت الأشياء لتحليل البيانات وتحسين الأداء في تطبيقات المدن الذكية والرعاية الصحية والمراقبة

واظهرت أن الشبكات العصبية ترفع دقة الكشف والتنبؤ، لكن تواجه تحديات في استهلاك الموارد وضعف الأجهزة الطرفية

تفيد المقالة مشروعنا في توضيح دور الذكاء الاصطناعي في كشف التسريبات وتحليل البيانات الحية ضمن شبكات إنترنت الأشياء الذكية،

وتبرز أهمية تصميم نماذج فعالة منخفضة الاستهلاك.

وفيما يلي ملخص مما سبق:

الجدول 1.1

(الدراسة المرجعية)

المقالة	التاريخ	الموضوع	النتائج	العلاقة مع المشروع
دمج تقنيات التعلم العميق في إنترنت الأشياء مراجعة للتقنيات والتحديات	2023	دراسة شاملة حول دمج تقنيات التعلم العميق في أنظمة إنترنت الأشياء لتحليل البيانات وتحسين الأداء في الأجهزة الطرفية	أظهرت ان الشبكات العصبية العميقه ترفع دقة الكشف والتنبؤ لكن تأثير بعض قرارات داخل شبكات إنترنت الأشياء تفید في توضیح کیفیة استخدام	تفید ان الشبکات العصبیّة أظهرت ان الشبکات العصبیّة العمیقة ترفع دقة الكشاف والتنبؤ لكن تأثیر بعض قرارات الأجهزة الطرفیّة
إطار الفقة الآمن والقائم على الذكاء الاصطناعي للحافة في إنترنت الأشياء	2025	اقتراح إطار أمني ذكي يعتمد على التعلم الفيدرالي والذكاء الاصطناعي للتحكم بالوصول الموارد و زمن الاستجابة وكشف التسلل عند الحافة	حقن النظام دقة كشف بلغ 94% مع تقليل استهلاك الموارد و زمن الاستجابة وكشف التسلل عند الحافة	يوضح کیفیة دمج الذکاء الاصطناعی والأمان لتحسين کشف التسرب وتعزیز ثقة إنترنت الأشياء
نماذج التحكم في الوصول لإنترنت الأشياء مراجعة شاملة واتجاهات مستقبلية	2025	استعراض شامل لنماذج التحكم بالوصول في إنترنت الأشياء وتحليل التوجهات المستقبلية لتعزيز الأمان والمرونة	ثبتت ان النماذج الحديثة القائمة على السمات والبلوك تشين أكثر اماناً لكنها تستهلك قدرات حساسية مرتفعة	تساعد في تحديد آلية تحكم آمنة ومرنة للبيانات ضمن نظام كشف التسرب وتعزیز حماية الوصول في الشبکات الذکیّة
من السحابة الى الحاوية: دمج إنترنت الأشياء والذكاء الاصطناعي لأنظمة مستدامة وفعالة	2025	تحث التكامل بين إنترنت الأشياء والحوسبة السحابية والطيفية لتحسين الاداء والاستدامة وتقليل زمن المعالجة	أظهرت ان الأنظمة المهجينة بين السحابة والطرف تحقق توازناً أفضل بين الأمان والكافأة وسرعة الاستجابة	تفید في ابراز أهمية المعالجة الطيفية لتحليل البيانات وكشف التسرب في الزمن الحقيقي دون ابطاء النظام
إطار أمني قائم على التعلم العميق لشبکات إنترنت الأشياء: تقنيات ذكية هجينة لاكتشاف التهديدات	2025	تطوير نموذج أمني يعتمد على التعلم العميق والشبکات العصبية لاكتشاف التهديدات السيبرانية في إنترنت الأشياء	تحقق النموذج دقة عالية في الكشف وتقليل الإنذارات الخاطئة بفضل الدمج بين التعلم العصبي والتطور الذکی	يدعم توظيف الذكاء الاصطناعي العميق للكشف الدقيق عن التسربات وتحليل البيانات بفعالية أكبر

الكشف عن الهجمات السيبرانية في إنترنت الأشياء باستخدام الذكاء الاصطناعي	2025	عرضت نظاماً ذكيّاً للكشف عن الهجمات عن الهجمات في إنترنت الأشياء متعددة من المجمّمات وتقليل الأشياء باستخدام خوارزميات التعلم العميق	حقن النظام دقة عالية واستطاع التكيف مع أنواع متنوعة من المجمّمات وتقليل الإنذارات الكاذبة الصناعية الذكية
إنترنت الأشياء الذكاء الاصطناعي في أنظمة ذكية ومتصلة	2024	تناولت استخدام الذكاء الاصطناعي لتحليل سلوك الشبكات وكشف التسللات ومنع تسريب البيانات	أظهرت ان الدمج بين التحليل السلوكي وخوارزميات التعلم العميق يرفع دقة الكشف ويقلل الأخطاء
الذكاء الاصطناعي لإنتernet الأشياء (AIOT): رؤية نحو أنظمة ذكية ومتصلة	2024	تناولت مفهوم الذكاء الاصطناعي لإنترنت الأشياء ودوره في الاستشعار، الحوسنة، الاتصال ضمن الأنظمة الحديثة	توضّح أهمية دمج الذكاء الاصطناعي وإنترنت الأشياء لتحسين سرعة ودقة كشف تسرب البيانات الموحدة
إنترنت الأشياء: مراجعة شاملة	2024	مراجعة لأحدث أساليب الذكاء الاصطناعي في كشف الشذوذ والهجمات في شبكات إنترنت الأشياء	تساعد في اختيار خوارزميات التعلم الآلي والعميق لاكتشاف الشذوذ في شبكات إنترنت الأشياء
دراسة تحليلية منهجية	2024	تحليل منهجي ل 81 دراسة توضح تطبيقات الذكاء الاصطناعي في التنبؤ، القرار وإدارة البيانات ضمن إنترنت الأشياء	توضّح فهم توظيف الذكاء الاصطناعي لتحسين دقة كشف فعالة للكشف المبكر عن التسريبات

تواجه إنترنت الأشياء العديد من التحديات، نذكر منها:

4- التحديات [1]

1- تنوّع الأجهزة والأنظمة:

تتميز أجهزة إنترنت الأشياء بتنوعها الكبير من حيث الأنواع، الشركات المصنعة، والأنظمة التشغيلية هذا التنوّع يجعل من الصعب تطبيق حلول أمنية موحدة وفعالة عبر جميع الأجهزة.

2- محدودية القدرات الحسابية والتخزينية:

تفتقر العديد من أجهزة إنترنت الأشياء إلى المعالجة القوية والذاكرة الكافية، مما يحد من قدرتها على تنفيذ خوارزميات الكشف المتقدمة أو تخزين سجلات الأمان بشكل فعال.

3- غياب التحديثات الأمنية المنتظمة:

الكثير من الأجهزة لا تتلقى تحديثات أمنية دورية، مما يجعلها عرضة للثغرات الأمنية المعروفة والهجمات المستهدفة.

4- نقص التشفير القوي للبيانات:

ترسل البيانات بين أجهزة إنترنت الأشياء والحوادم بدون تشفير قوي في بعض الأحيان، مما يعرضها للاعتراض والتلاعب أثناء النقل.

5- التكامل المعقد بين البروتوكولات:

ما يزيد من تعقيد عملية مراقبة البيانات وكشف التسريبات. (MQTT، CoAP مثل) تستخدم أجهزة إنترنت الأشياء بروتوكولات اتصال متعددة

6- التهديدات المتزايدة والمجمّمات المستهدفة:

مع تزايد عدد الأجهزة المتصلة، تزداد فرص الهجمات مثل تسريبات البيانات، البرمجيات الخبيثة، أو المجمّمات على البنية التحتية للشبكة.

7- التحديات في التحليل والتعلم الآلي:

تواجه تقنيات التحليل والتعلم الآلي صعوبة في التعامل مع البيانات غير المنظمة والمضوضاء الناجمة عن الأجهزة المتنوعة، مما يؤثر على دقة الكشف.

8- محدودية الوعي الأمني لدى المستخدمين:

قلة الوعي الأمني لدى المستخدمين النهائيين تؤدي إلى تكوين كلمات مرور ضعيفة أو عدم تحديث الأجهزة، مما يزيد من احتمالية التسريبات.

9- التحديات في الحوسية الطرفية:

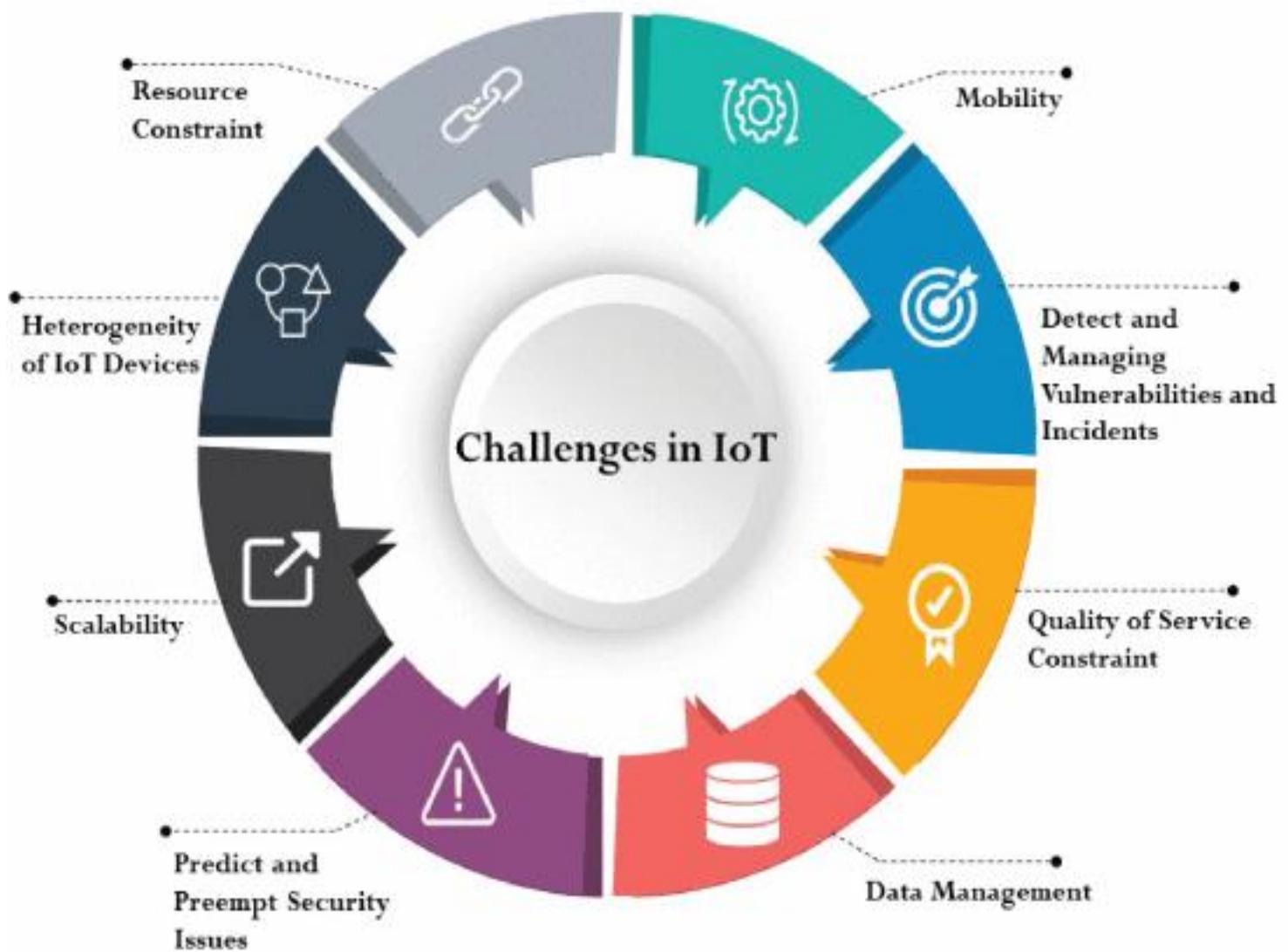
تواجه الحوسية الطرفية صعوبة في تطبيق تقنيات الأمان المتقدمة بسبب محدودية الموارد، مما يعرض البيانات للتسريب أثناء المعالجة المحلية.

10- الامتثال للمعايير واللوائح:

تحتفي مختلف معايير الأمان والخصوصية عبر المناطق الجغرافية، مما يجعل من الصعب ضمان الامتثال الكامل لجميع اللوائح المتعلقة بحماية البيانات.

يبين الشكل الآتي بعض تحديات إنترنت الأشياء:

الشكل 1.1:



5-التطبيقات العلمية [2]

استخدام خوارزميات التعلم الآلي للكشف عن التسربات:

تم تطوير نماذج تعتمد على خوارزميات التعلم الآلي لتحليل البيانات المجمعة من أجهزة إنترنت الأشياء. تُستخدم هذه الخوارزميات لاكتشاف الأنماط الشاذة التي قد تشير إلى تسربات بيانات محتملة.

تطبيقات الكشف عن التسربات في الصناعات:

في قطاع النفط والغاز، تم تطبيق حلول تعتمد على إنترنت الأشياء للكشف المبكر عن التسربات في الأنابيب. تُستخدم أجهزة استشعار لقياس التغيرات في الضغط ودرجة الحرارة، مما يساعد في تحديد موقع التسربات بدقة عالية.

أنظمة الكشف المبكر في المنازل الذكية:

في المنازل الذكية، تُستخدم أجهزة استشعار للكشف عن التسربات في شبكات المياه. تُرسل هذه الأجهزة تبيهات فورية إلى المستخدمين عبر تطبيقات الهواتف الذكية، مما يسمح باتخاذ إجراءات سريعة للحد من الأضرار.

تحليل البيانات الشبكية للكشف عن التسربات:

تُستخدم تقنيات تحليل البيانات الشبكية لمراقبة حركة البيانات عبر الشبكات. من خلال تحليل هذه البيانات، يمكن اكتشاف أي تسربات محتملة أو أنشطة غير مصرح بها، مما يساعد في تعزيز أمان الشبكة.

تطبيقات الكشف في القطاع الصحي:

في القطاع الصحي، تُستخدم أجهزة إنترنت الأشياء لمراقبة المرضى عن بعد. تُساعد هذه الأجهزة في الكشف عن أي تسربات في البيانات الطبية، مما يضمن حماية خصوصية المرضى.

أنظمة الكشف في المدن الذكية:

في المدن الذكية، تُستخدم أجهزة استشعار لمراقبة البنية التحتية مثل شبكات المياه والكهرباء. تُساعد هذه الأنظمة في الكشف المبكر عن التسربات، مما يساهم في تحسين كفاءة الخدمات وتقليل الفاقد.

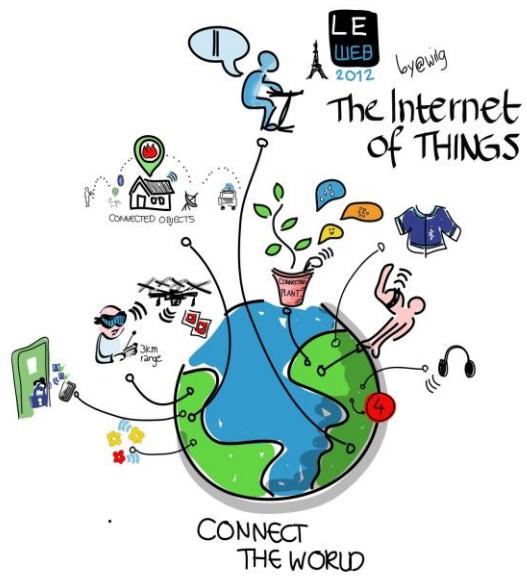
تحليل سلوك الأجهزة للكشف عن التسربات:

يتم تحليل سلوك الأجهزة المتصلة بشبكات إنترنت الأشياء للكشف عن أي أنماط غير طبيعية قد تشير إلى تسربات بيانات. يساعد هذا التحليل في تحديد الأجهزة المشتبه بها واتخاذ الإجراءات المناسبة.

مراقبة الشبكات للكشف عن التسربات: تُستخدم تقنيات مراقبة الشبكات لمتابعة حركة البيانات عبر الشبكات. من خلال هذه المراقبة، يمكن اكتشاف أي تسربات محتملة أو أنشطة غير مصرح بها، مما يساعد في تعزيز أمان الشبكة.

الفصل الأول

الدراسة النظرية



يمثل إنترنت الأشياء أحد أبرز مظاهر التطور التقني في العصر الرقمي المعاصر، حيث يقوم على ربط الأشياء المادية بمختلف أنواعها عبر شبكات الاتصال، بما يمكنها من تبادل البيانات والمعلومات بصورة ذاتية دون تدخل مباشر من الإنسان وقد أحدث هذا المفهوم تحولاً جذرياً في أنماط التفاعل بين الإنسان والآلة، كما فتح آفاقاً واسعة لتطوير الخدمات في مجالات عديدة تشمل الصحة والصناعة والنقل والزراعة والمدن الذكية

أكاديمياً:

يمكن تعريف إنترنت الأشياء بأنه شبكة متراقبة من الأجهزة المادية التي تضم المستشعرات وأدوات التحكم، والتي تعمل على جمع البيانات ومشاركتها عبر بروتوكولات اتصال قياسية، بهدف معالجتها وتحويلها إلى معلومات ذات قيمة تشغيلية أو خدمية ويتميز هذا النظام بقدرته على توفير الاتصال الذاتي بين الأجهزة دون الاعتماد الكامل على العنصر البشري

1.1.1 البنية الأساسية لإنترنت الأشياء:

يتكون إنترنت الأشياء من ثلاث طبقات رئيسية، هي:

1- طبقة الأجهزة الطرفية:

تضم جميع الحساسات والمستشعرات التي تلتقط البيانات البيئية أو التشغيلية، إضافة إلى المشغلات التي تنفذ الأوامر تتميز هذه الأجهزة بقدرات محدودة من حيث الطاقة والمعالجة، مما يجعلها عرضة للمخاطر الأمنية.

2- طبقة الشبكات:

تشكل حلقة الوصل بين الأجهزة الطرفية والخوادم المركزية أو السحب الحاسوبية، حيث يتم نقل البيانات عبر بروتوكولات متعددة مثل بروتوكولات الرسائل الخفيفة وبروتوكولات التطبيقات الموجهة للأجهزة محدودة القدرات. وتعد هذه الطبقة من أكثر المراحل حساسية، إذ يمكن استغلالها لتنفيذ هجمات تهدف إلى تسريب البيانات.

3- طبقة التطبيقات والمنصات :

تتضمن نظم المعالجة المركزية التي تقوم ب تخزين البيانات وتحليلها، إضافة إلى التطبيقات التي تقدم الخدمات للمستخدم النهائي. وتتطلب هذه الطبقة حماية قوية ضد الاختراقات لضمان سرية البيانات وسلامتها.

1.1.2 التطبيقات لأنترنت الأشياء:

القطاع الصناعي (الصناعة الذكية) :

يمثل القطاع الصناعي أحد أهم المستفيدن من إنترنت الأشياء، إذ تُستخدم المستشعرات لربط خطوط الإنتاج ومراقبتها بشكل آلي، الأمر الذي يتبع التنبؤ بالأعطال قبل وقوعها فيما يعرف بالصيانة التنبؤية هذا الأسلوب يقلل من التوقفات المفاجئة ويرفع من كفاءة التشغيل ويخفض التكاليف كما تتيح هذه الأنظمة مراقبة جودة المنتجات وتحسين استهلاك الموارد، بما يعزز القدرة التنافسية للمؤسسات الصناعية.

أحدثت إنترنت الأشياء نقلة نوعية في المجال الصحي من خلال الأجهزة الطبية القابلة للارتداء، مثل أجهزة قياس ضغط الدم ونبض القلب ومستويات الأوكسجين تقوم هذه الأجهزة بإرسال البيانات بشكل فوري إلى الأطباء أو مراكز المراقبة، مما يساعد على متابعة حالة المرضى واتخاذ قرارات سريعة في حالات الطوارئ غير أن هذه البيانات الصحية تُعد من أكثر أنواع البيانات حساسية، وبالتالي فإن أي تسريب لها قد يشكل تهديداً مباشرًا لخصوصية المرضى وسلامتهم.

المدن الذكية:

تُعد المدن الذكية نموذجاً متطوراً لتطبيقات إنترنت الأشياء، حيث يتم من خلالها إدارة البنية التحتية بشكل ذكي وفعال. فعلى سبيل المثال، تُستخدم المستشعرات في تنظيم حركة المرور وتحفييف الازدحام، كما تُوظف في إدارة شبكات الطاقة والمياه والإضاءة العامة. وقد أدى هذا النوع من التطبيقات إلى تحسين جودة الحياة وخفض التكاليف التشغيلية في العديد من المدن المتقدمة. إلا أن هذه الأنظمة تتعرض لهجمات إلكترونية قد تؤدي إلى تعطيل الخدمات الحيوية.

الزراعة الذكية:

ساهمت إنترنت الأشياء في تعزيز الأمان الغذائي عبر أنظمة تعتمد على مراقبة التربة والمناخ ورطوبة الهواء للتحكم في الري والتسميد بشكل آلي. كما يتم استخدام طائرات مسيرة مزودة بمستشعرات لمتابعة صحة النباتات ورصد الآفات مبكراً هذه التقنيات أدت إلى رفع كفاءة الإنتاج الزراعي، وتقليل استهلاك المياه والأسمدة، بما يحقق استدامة الموارد الطبيعية.

نقل والمركبات المتصلة:

أدخلت إنترنت الأشياء تحسينات كبيرة في قطاع النقل من خلال أنظمة تتبع المركبات والشحنات في الزمن الحقيقي. كما تُستخدم في إدارة الموانئ والمطارات وتسهيل العمليات اللوجستية، مما يقلل من الفاقد ويرفع من مستوى الأمان. إضافة إلى ذلك، فإن المركبات ذاتية القيادة تعتمد بشكل رئيسي على تقنيات إنترنت الأشياء لتتبادل البيانات مع البنية التحتية المحيطة وضمان سلامة التنقل.

الأمن والدفاع:

تمثل إنترنت الأشياء أداة مهمة في تعزيز القدرات الأمنية والعسكرية، حيث تُستخدم في أنظمة المراقبة الذكية والطائرات بدون طيار، إضافة إلى حماية المنشآت الحيوية إلا أن هذا المجال من أكثر القطاعات حساسية، حيث إن أي تسريب للبيانات قد يؤدي إلى مخاطر جسيمة على الأمن القومي.

يوضح الشكل الآتي البعض من تطبيقات انترنت الأشياء:

الشكل 1.2



تسريب البيانات وهو ما بني عليه هذا التقرير، يُعد من أخطر التهديدات التي تواجه أنظمة إنترنت الأشياء، نظرًا لطبيعة عمل هذه الشبكات التي تعتمد على أجهزة متصلة ذات قدرات محدودة تعمل في بيئات قد تكون غير آمنة، ما يجعلها بيئة خصبة للهجمات الإلكترونية.

أكاديمياً:

يعرف تسريب البيانات بأنه انتقال غير مشروع للمعلومات من داخل النظام إلى جهات خارجية غير مخولة بالاطلاع عليها، سواء كان ذلك نتيجة هجمات متعمدة، أو بسبب ثغرات في التصميم، أو من خلال ضعف إجراءات الحماية أثناء تخزين البيانات أو نقلها.

1.2.1 أخطاء تسريب البيانات:

التسريب المباشر (الاختراق الكامل للأنظمة):

يُعد هذا النمط من أكثر أشكال التسريب وضوحاً وخطورة، حيث يقوم المهاجم باختراق الجهاز أو الخادم والوصول إلى البيانات المخزنةداخله في هذه الحالة، يمكن نسخ الملفات الحساسة أو تعديلها أو حذفها بالكامل وغالباً ما يستهدف هذا النوع من التسريب الأجهزة الطبية المتصلة أو الكاميرات الذكية أو الخوادم الصناعية، على سبيل المثال، قد يؤدي اختراق مضخة أنسولين متصلة إلى تسريب بيانات المريض الطبية أو حتى التلاعب في عمل الجهاز نفسه، مما يشكل خطراً مباشراً على حياة الأفراد.

التسريب عبر القنوات الجانبية (تحليل البيانات الثانوية):

حتى في حال تشفير البيانات الأساسية، يمكن للمهاجمين تحليل البيانات الوصفية (مثل حجم الحزم، زمن الإرسال، أو تردد الاتصال) للتوصول إلى معلومات حساسة يُعرف هذا النمط بـ "التسريب عبر القنوات الجانبية"، وهو يعتمد على مراقبة الأنماط السلوكية للتواصل بدلاً من محتوى البيانات نفسها فمثلاً، في المنازل الذكية يمكن تحديد أوقات وجود السكان أو غيابهم من خلال مراقبة تشغيل وإطفاء الأجهزة الكهربائية، حتى دون معرفة البيانات الفعلية ورغم أن هذا النمط غير مباشر، إلا أنه يمثل تحديداً بالغ الخطورة لأنه يتجاوز الحماية التقليدية القائمة على التشفير.

التسريب أثناء النقل (اعتراض البيانات):

تُعتبر مرحلة انتقال البيانات بين الأجهزة الطرفية والخوادم المركزية من أكثر المراحل عرضة للتسريب، خاصة عند استخدام بروتوكولات اتصال ضعيفة أو غياب التشفير الكامل في هذا النمط، يعرض المهاجم البيانات أثناء انتقالها، سواء عبر شبكات الاتصال اللاسلكية أو عبر الإنترن特 ويزداد هذا الخطر مع الاعتماد الواسع على شبكات 20LoRaWAN اي العامة، أو عند استخدام بروتوكولات خفيفة مثل بروتوكول الرسائل في إنترنت الأشياء من الأمثلة العملية، اعتراض البيانات المرسلة من أجهزة استشعار في خطوط أنابيب النفط والغاز، مما قد يؤدي إلى كشف موقع الأعطال أو طبيعة الإنتاج، وهي بيانات حساسة ذات قيمة استراتيجية.

التسريب الناتج عن التغرات البرمجية والتصميمية:

غالباً ما تحتوي الأجهزة الذكية على برمجيات وتطبيقات معقدة، وقد تترك بعض التغرات الأمنية دون معالجة نتيجة لغياب التحديثات الدورية أو استخدام إصدارات قديمة من البرمجيات في هذا النمط، يستغل المهاجم هذه التغرات لزرع برمجيات خبيثة داخل الجهاز، ما يتيح له الحصول على البيانات أو التحكم في سلوك الجهاز على سبيل المثال، قد يؤدي استغلال ثغرة في برمجيات كاميرا مراقبة صناعية إلى الوصول المباشر إلى البيت المركزي والتحكم في إعداداته ويعتبر هذا النمط من أكثر أشكال التسريب شيوعاً في بيئات إنترنت الأشياء، نظراً لاعتماد كثير من الأجهزة على برمجيات غير مدروسة أو محدودة الموارد.

التسريب عبر التكامل غير الآمن بين الأنظمة:

مع تزايد الاعتماد على تكامل الأجهزة والتطبيقات عبر منصات مختلفة، تظهر مخاطر جديدة ناجمة عن ضعف الربط أو غياب المعايير الموحدة ففي المدن الذكية مثلاً، قد يؤدي دمج أنظمة المرور مع أنظمة الإضاءة أو الطاقة دون تأمين كافٍ إلى تسريب بيانات حساسة بين المنصات هذا النمط لا يعتمد على اختراق جهاز محدد، بل يستغل نقاط الضعف في عملية التكامل بين الأنظمة المتعددة.

التسريب غير المقصود (أخطاء بشرية أو إدارية):

لا تقتصر أنماط التسريب على الهجمات المعمدة فقط، بل قد يحدث التسريب نتيجة إهمال أو ضعف في الإجراءات الأمنية على سبيل المثال، إبقاء كلمات المرور الافتراضية دون تغيير، أو مشاركة بيانات الدخول مع أطراف غير مختصة، أو تثبيت الأجهزة الذكية دون تفعيل خصائص الأمان ورغم أن هذا النمط غير مقصود، إلا أن آثاره قد تكون كارثية، خاصة في الأنظمة الصحية والعسكرية.

1.2.2 بعض الأمثلة العملية لتسريب البيانات:

اختراق الكاميرات المنزلية الذكية: للوصول إلى البيت المركزي المباشر والتحكم في الإعدادات.

استهداف الأجهزة الطبية المتصلة: مثل مضخات الأنسولين وأجهزة مراقبة القلب، مما يشكل خطراً على حياة المرضى

استغلال بروتوكولات الاتصال الخفية: نتيجة ضعف آليات التحقق والمصادقة

المدن الذكية والبنية التحتية:

مثل: أنظمة إشارات المرور الذكية وأجهزة الاستشعار

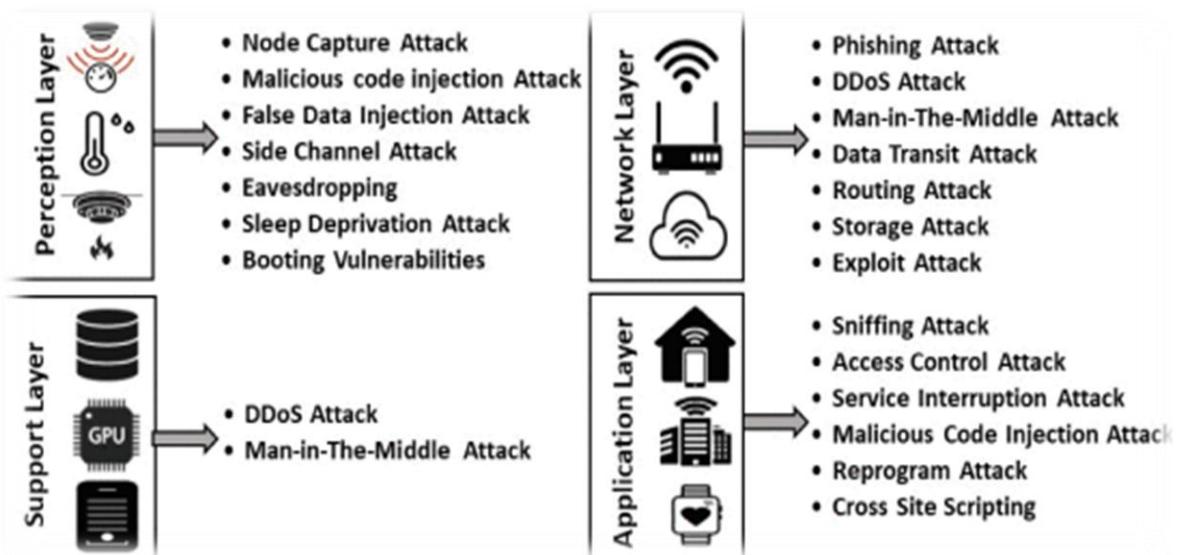
تثبيت الأجهزة دون تغيير اعدادات المصنع للأمنية

التصنيع والصناعة:

مثل: الروبوتات

السبب عدم تجزئة الشبكة والبروتوكولات القديمة المستخدمة

تُعد آثار تسريب البيانات في شبكات إنترنت الأشياء باللغة التعقيد والخطورة، حيث تمتدد تداعياتها عبر مستويات متعددة، بدءاً من انتهاك الخصوصية الفردية بشكل غير مسبوق، نظراً لطبيعة البيانات الحساسة التي تجمعها هذه الأجهزة من الحياة اليومية للأفراد، مما يهدد أنفسهم الشخصي و يجعلهم عرضة للابتزاز والمراقبة ولا تقتصر الآثار على الجانب الشخصي فحسب، بل تمتدد إلى خسائر اقتصادية كبيرة تstem عن الغرامات المالية الباهظة، وتراجع ثقة العملاء، وما يتبع ذلك من ضرر بالغ في السمعة المؤسسية علاوة على ذلك، فإن البيانات المسرقة لا تقف عند حد الاستغلال المباشر، بل تستغل كأدلة كما خطيرة لتمكين هجمات إلكترونية أوسع نطاقاً وأكثر تطوراً، مثل المجموعات الإلكترونية المستهدفة، مما يهدد البنية التحتية الحيوية للمؤسسات والدول كما أن اختراق الأجهزة الطبية المتصلة يشكل خطراً مباشراً على حياة المرضى، في حين أن اختراق أنظمة المدن الذكية والصناعية يمكن أن يؤدي إلى شل الحركة المائية، وتعطيل خطوط الإنتاج، والتسبب في كوارث مادية وبيئية وبالتالي، يصبح أمن إنترنت الأشياء مسألة مصرية تتطلب نهجاً أمنياً شاملًا يتجاوز الحلول التقليدية لضمان حماية البيانات، واستمرارية الخدمات، والحفاظ على الثقة في التحول الرقمي.



الشكل 2.1 يبين أبرز الهجمات السيبرانية على إنترنت الأشياء

2.2.1 فيما يلي بعض من التحديات مع امثلة مع بعض الحلول:

تبعد نقاط الضعف في إنترنت الأشياء من مجموعة من العوامل التقنية والتشغيلية والمعمارية، ويمكن تصنيفها على النحو الآتي:

أولاً: التحديات التقنية

ضعف آليات التشفير: حيث تفتقر العديد من الأجهزة إلى استخدام تقنيات تشفير قوية، مما يجعل البيانات عرضة للاعتراض

محدودية الموارد الحاسوبية: مما يمنع من تطبيق بروتوكولات حماية متقدمة

غياب التحديثات الأمنية: يترك الأجهزة عرضة للثغرات المكتشفة بمراور الوقت

ثانياً: التحديات التشغيلية

قصور الوعي الأمني لدى المستخدمين: يؤدي إلى أخطاء شائعة مثل الإبقاء على كلمات المرور الافتراضية

تعدد الشركات المصنعة: يخلق فجوة في معايير الحماية، ويحول دون توحيد آليات الأمان

ثالثاً: التحديات التصميمية والمعمارية

البيانات الكبير في بروتوكولات الاتصال: يزيد من صعوبة تأمين عمليات التكامل بين الأنظمة المختلفة

لاعتماد على نماذج الشبكات التقليدية: يجعل إنترنت الأشياء أقل توافقاً مع متطلبات الأمان الحديثة

لمواجهة هذه الثغرات، تبنت بعض الابحاث عدة مسارات للحماية، من أبرزها:

التعلم الآلي لرصد الهجمات: للكشف المبكر عن الأنماط غير الطبيعية في حركة البيانات

تقنية السجلات الموزعة (سلسلة الكتل): لتأمين نقل البيانات والتحقق من الهوية بشكل لا مركزى

النماذج القائمة على انعدام الثقة: والتي تفترض تحققًا دائمًا من الهوية وعدم منح الثقة المسبقة لأي جهاز

تعزيز الحوسبة الطرفية الآمنة: من خلال تنفيذ عمليات التشفير والمعالجة بالقرب من الأجهزة لتقليل نقاط الضعف أثناء النقل

هذه التوجهات لا تمثل خياراً تكميلياً، بل أصبحت ضرورة حتمية لضمان استمرارية استخدام إنترنت الأشياء ضمن بيئه آمنة ومستدامة.

تسريب البيانات ومخاطر الخصوصية:

برز تسريب البيانات ومخاطر الخصوصية كأحد الموضوعات الرئيسية فيما يتعلق بعواقب خروقات أمن إنترنت الأشياء في حالة تسريب البيانات، يمكن أن تتعرض المعلومات الحساسة للخطر، مما يهدد خصوصية الأفراد والأسرار الأخرى تحدث مخاطر اختراق المعلومات الحساسة عندما يكون هناك احتمال للتلاعب بأجهزة إنترنت الأشياء لجمع الأسرار التشفيرية أو تعديل البرمجيات على الرغم من الفوائد العديدة لتكنولوجيا إنترنت الأشياء مثل توفير الطاقة والراحة، فإن العديد من الأجهزة المتصلة بالإنترنت تفتقر إلى إجراءات أمنية مدمجة، مما يجعلها عرضة للهجمات السيبرانية. يمكن أن يؤدي اختراق كاميرات الويب أو أجهزة مراقبة الصحة إلى وصول غير مصرح به من قبل أطراف ضارة تؤكد الدراسات على ضرورة وجود إجراءات أمنية قوية لمواجهة هذه التهديدات الجديدة.

اختراق البنية التحتية الحرجة:

يشكل اختراق البنية التحتية الحرجة موضوعاً آخر حيث يمكن أن تؤدي خروقات الأمان في إنترنت الأشياء إلى تعطيل البنية الهامة تشمل المخاطر هجمات حجب الخدمة التي تؤثر سلباً على قدرة التشغيل لهذه الأجهزة يمكن أن يؤدي الاختراق إلى دخول غير مصرح به إلى شبكات أنظمة إنترنت الأشياء، مما يعرض أنها وسلامتها للخطر تُعد هذه السيناريوهات مقلقة بشكل خاص لأن أجهزة إنترنت الأشياء يمكن استخدامها لاختراق شبكات أوسع. قد يكون هذا الضعف كبيراً في الأنظمة الحرجة التي تتطلب تشغيلاً مستمراً، مثل المعدات الطبية أو برامج التحكم الصناعي يحذر تقرير منتدى الاقتصاد العالمي لعام 2023 من أن الهجمات السيبرانية على البنية التحتية الحرجة هي واحدة من أكبر خمسة مخاطر عالمية تواجه العالم في العقد القادم

مخاطر السلامة والأمن:

برزت مخاطر السلامة والأمن كموضوع آخر من خلال التحليل يمكن أن تؤدي خروقات الأمان إلى عواقب وخيمة في التطبيقات العسكرية أو أنظمة الرعاية الصحية، مثل الإصابات أو تعريض بيانات صحية سرية للخطر تشمل القضايا الأمنية النظام البيئي الكامل وإنترنت الأشياء وليس فقط أجهزة محددة في عام 2020، استهدفت هجنة سيبرانية محطة معالجة مياه في فلوريدا من خلال استغلال نقاط الضعف في نظام يعمل بتقنية إنترنت الأشياء يسلط هذا الحادث الضوء على إمكانية تعطيل البنية التحتية الحرجة بعواقب تحدد الحياة.

Major themes

Author(s)	Major themes
Meneghelli, et al (2019); Arias, et al (2015); Sivaraman, et al (2018), Li, et al (2016); Neshenko, et al (2019) and chen, et al (2018)	Data and privacy vulnerabilities
Zhou, et al. (2018) Neshenko, et al (2019) And tankard, (2015)	Com promised critical infrastructure
Butun, et al. (2019) Zhou, et al (2018) Ling et al (2017) Neshenko, et al (2019) And tankard, (2015)	Safety and security risk

آليات أمنية ضعيفة :

على الرغم من أن التهديدات الأمنية لإنترنت الأشياء رقمية في الغالب، إلا أنها تشمل أيضًا مخاطر مادية، خاصة فيما يتعلق بالمنازل الذكية والاستخدامات الصناعية. تكمن المشكلة في أن الأتمتة والكفاءة التي توفرها أجهزة إنترنت الأشياء تأتي على حساب ضعف الأمان المدمج، مما يؤدي إلى وصول غير مصرح به يمكن أن يؤثر اختراق كاميرات الويب أو أجهزة مراقبة الصحة على الخصوصية، من التجسس البسيط إلى الكشف عن معلومات طبية سرية. يُعد الوصول غير المصرح به إلى الشبكات أحد أهم نقاط الضعف التي تقوض الأمان والسلامة في الأنظمة الذكية.

النطاق والتتنوع :

يتميز انتشار إنترنت الأشياء بنقاط ضعف كبيرة يمكن أن تعرّض المستخدمين لمخاطر مختلفة يجعل النطاق الواسع والتتنوع إنترنت الأشياء أكثر عرضة وتكنولوجياً في إنترنت الأشياء أكثر عرضة للخطر تُعد (WSNs) ثروقات الأمان مع هذه الخصائص، يصبح دمج شبكات الاستشعار اللاسلكية إنترنت الأشياء منصات محددة تستخدم في مجالات حرجية مثل التطبيقات العسكرية أو أنظمة الرعاية الصحية، مما يجعلها بيئة مثالية للمخاطر الأمنية وفقاً للدراسات، فإن النشر السريع لإنترنت الأشياء يؤدي إلى ظهور تهديدات جديدة وحرجة لأمن إنترنت الأشياء، مما يجعل الأنظمة أكثر عرضة للاختراق.

نقص المعايير للأجهزة محدودة الموارد :

ثانيةً، لا توجد معايير محددة عند تنفيذ وإدارة إنترنت الأشياء، مما يجعلها عرضة لثروقات الأمان. تُعد أحد نقاط الضعف الرئيسية هي عدم وجود بروتوكولات أمنية عامة لأجهزة إنترنت الأشياء ذات الموارد المحدودة والتقنيات غير المتجانسة نظرًا لأن أجهزة إنترنت الأشياء لا تمتلك قوة معالجة غير محدودة ومساحة ذاكرة وسعة اتصال، فإنها تصبح عرضة للتهديدات السيبرانية. يؤدي نقص المعايير المحددة لهذه الأجهزة إلى جعل أنظمة إنترنت الأشياء عرضة للاستغلال، مما يجعل ضمان الأمان القوي أكثر تعقيدًا.

الفصل الثاني

بيئة العمل

تُعد بيئة العمل الإطار الذي تُنفَذ ضمنه الدراسات البحثية والتجارب العملية، حيث تحدد هذه البيئة الموارد البرمجية وأدوات التحليل الازمة لتحقيق أهداف البحث وفي سياق هذا المشروع، الذي يركز على كشف تسريب البيانات في شبكات إنترنت الأشياء باستخدام تقنيات الذكاء الاصطناعي، كان من الضروري بناء نموذج عمل متكامل يمزج بين الجانب النظري المتعلق بفهم طبيعة البروتوكولات الشبكية، والجانب العملي المتمثل في نموذج محاكاة منزل ذكي.

2.2 مقارنة بين بيئات العمل

المساوئ	المزايا	البيئة
يحتاج خبرة قوية في الطرفية Terminal	دعم قوي لمحاكيات الشبكات (وهو المطلوب) ودعم قوي للذكاء الصنعي مستقر، خفيف	Ubuntu
غير مناسب لمحاكيات مثل: Ns3	سهل الاستخدام يدعم البرامج الرسومية	windows
مكلف دعم محدود لبعض المحاكيات	أداء جيد مستقر	macOS

المساوئ	المزايا	المحاكي
غير رسومي ويحتاج خبرة كافية	دقيق واعي مناسب ل IOT	Ns-3
محدود واقل مرونة	واجهة سهلة مناسب لعقد IOT الصغيرة	Cooja
غير مناسب ل IOT اللاسلكي	خفيف مناسب ل SDN	mininet

الخوارزمية	المزايا	المساوى
XGBoost	دقة عالية سرعه متناز للكشف عن الشذوذ (وهو المطلوب)	يحتاج تجهيز بيانات جيدة
Scikit-learn	سهل متعدد الخوارزميات	اقل أداء مع البيانات الكبيرة
Neural networks	دقة عالية جداً	تحتاج موارد كبيرة ووقت للتدريب

2.3 تبرير اختيار بيئة العمل:

تم اعتماد بيئة العمل القائمة على نظام **Ubuntu** ضمن منصة **VMware** ضمن منصة **NS-3** وخوارزمية التعلم الآلي **XGBoost** لما توفره من توافقية عالية واستقرار وثبات يتطلبها هذا النوع من الأبحاث، إذ يتيح **Ubuntu** بيئة تطويرية متقدمة داعمة لمحاكيات الشبكات، بينما يوفر **VMware** عرلاً منهجياً يضمن إعادة إنتاج التجارب بدقة عبر نقاط الاسترجاع، وبعد **NS-3** الخيار الأمثل لمحاكاة أنظمة وأنترنت الأشياء بفضل دقه و واقعيته في توليد حركة مرور قابلة للتحليل، اما استخدام **XGBoost** فجاء استناداً إلى كفاءته العالية في مهام الكشف عن الشذوذ والتسلسلي وقدرتها على التعامل مع البيانات الناتجة عن المحاكاة بكفاءة. وبذلك تلبي هذه البيئة متطلبات المشروع البحثية بأعلى مستوى من الدقة والموثوقية.

٤.٢ المراجع التقنية الرسمية لبيئة العمل والأدوات المستخدمة:

اعداد منصة العمل الافتراضية (VMware workstation) :

١- تحميل VMware workstation (pro) من الموقع الرسمي www.vmware.com (نسخة pro)

٢- تثبيت البرنامج على الجهاز المضيف: next →Accept →Install →Finish

٣- فتح التطبيق و اختيار: Create new virtual machine

٤- تحديد ملف تثبيت النظام (ubuntu ISO)

٥- اختيار نوع النظام Linux →Ubuntu 64-bit

٦- تحصيص موارد الجهاز الافتراضي:

يفضل RAM 4-8 GB

٧- عدد الأنيوية: 2-4

نوع التخزين: Split

حجم القرص 40 GB فما فوق

٨- تثبيت نظام **ubuntu** داخل VMware

عند تشغيل الجهاز الافتراضي نختار **Normal Installation** ثم اختيار **Install Ubuntu**

ومن ثم متابعة التثبيت مع إعادة تشغيل النظام

بعد الدخول الى النظام نقوم بفتح لوحة الأوامر Terminal

ومن ثم ننفذ الأوامر التالية:

تحديث النظام بالأمر:

```
sudo apt update && sudo apt upgrade -y
```

1- تنصيب الأدوات الأساسية للعمل على الشبكات:

تنصيب الأدوات التطويرية الأساسية:

```
sudo apt install build-essential git python3 python3-pip cmake g++ -y
```

2- تنصيب وإعداد محاكي الشبكات NS-3

تحميل NS-3 الإصدار 3.39:

```
git clone https://gitlab.com/nsnam/ns-3-dev.git ns3  
cd ns3
```

تنصيب المتطلبات:

```
sudo apt install gcc g++ python3 python3-pip qt5-default  
mercurial \  
cmake libc6-dev libc6-dev-i386 gdb valgrind \  
gsl-bin libgsl-dev libsdlite3-dev python3-setuptools \  
libxml2 libxml2-dev -y
```

: NS-3 بناء

```
. ./ns3 configure --enable-examples --enable-tests  
. ./ns3 build
```

اختبار نجاح التثبيت:

```
./ns3 run hello-simulator
```

3- تنصيب مكتبات الذكاء الصنعي : Python+XGBoost

تنصيب بيئة Python الافتراضية

```
sudo apt install python3-venv -y  
python3 -m venv ml-env  
source ml-env/bin/activate
```

تنصيب المكتبات العلمية

```
pip install numpy pandas scikit-learn xgboost  
matplotlib
```

4- ربط NS-3 مع Python لمعالجة البيانات

تجهيز مجلد للنتائج داخل مجلد NS-3

```
mkdir results
```

تعديل سكريبتات NS-3 لتصدير بيانات الشبكة

انشاء كتابة السيناريو يتم تفعيل التتبع:

```
AsciiTraceHelper ascii;  
csmma.EnableAsciiAll(ascii.CreateFileStream("results/traffic.tr"));
```

```
cd ns3/scratch
```

```
touch smart_home.cc
```

تنفيذ السيناريو:

```
./ns3 run scratch/smart_home.cc
```

5- تدريب نموذج التعلم الآلي للكشف عن تسريب البيانات:

```
from xgboost import XGBClassifier
```

```
model = XGBClassifier()
```

```
model.fit(X_train, y_train)
```

اختبار النموذج:

```
predictions =  
model.predict(X_test)
```

بعد تنفيذ الخطوات السابقة سيتم تثبيت الأدوات والمكتبات التي تحتاجها لبيئة العمل، ثم تشغيل محاكي وبناء سيناريوهات شبكات إنترنت أشياء، وتصدير البيانات ومعالجتها باستخدام بايثون، ثم تطبيق خوارزمية التعلم الآلي للكشف عن تسريب البيانات

2.1.1 التحقق من صحة عمل خوارزمية XGBoost باستخدام تطبيق معياري مرجعي:

لإثبات ان الخوارزمية تعمل بشكل صحيح ضمن بيئة العمل المعتمد، تم تطبيقها على مجموعة بيانات معيارية مستخدمة في الادبيات العلمية، ثم قمت مقارنة نتائجها مع القيم المنشورة في الأبحاث الأصلية.

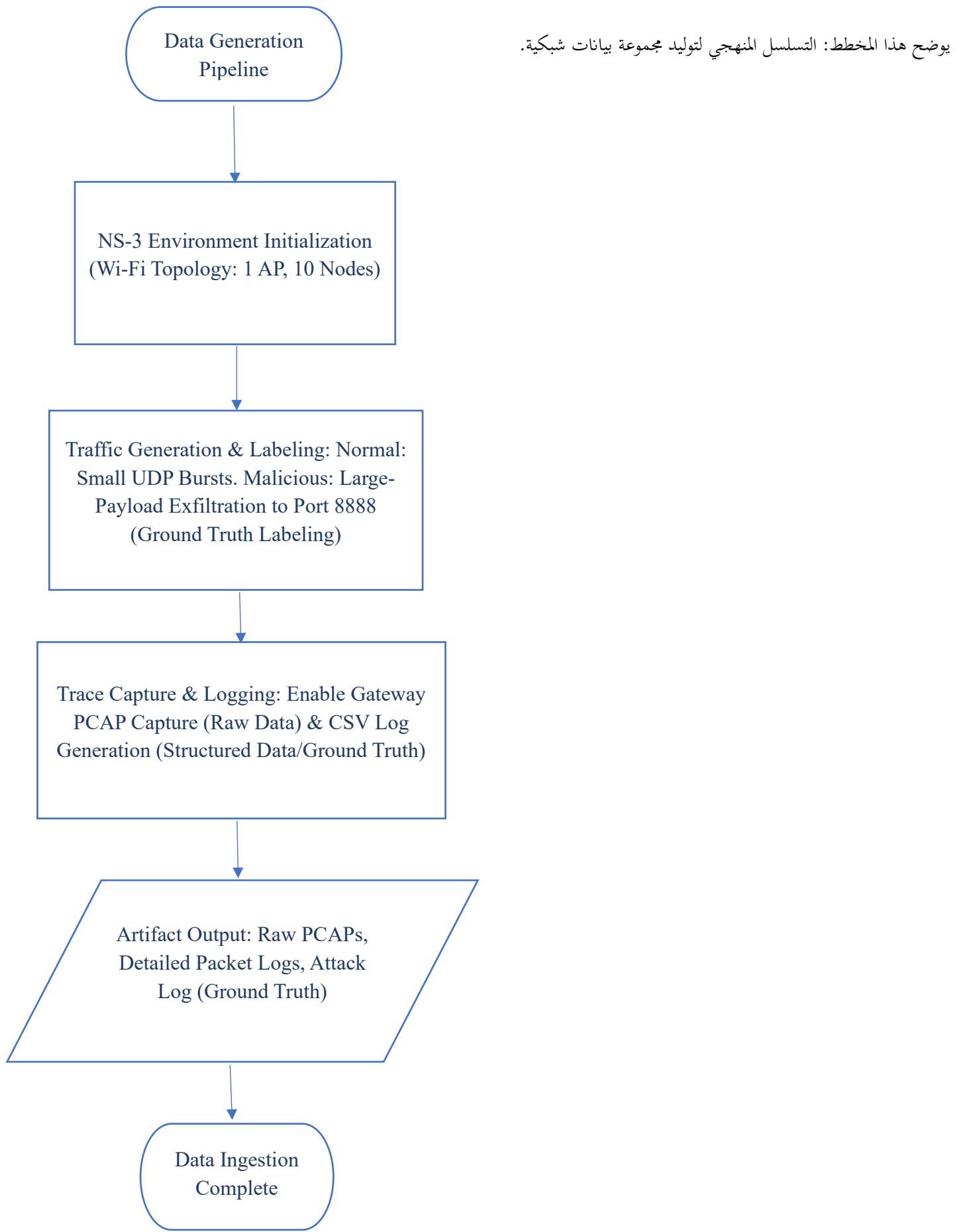
أظهرت النتائج المتحصل عليها تقارباً واضحاً في مؤشرات الأداء مثل: الدقة والاستدعاء مع النتائج المرجعية، مما يدل على صحة تنفيذ الخوارزمية وسلامة بيئة العمل، وبما أن خوارزمية XGBoost

خوارزمية موثوقة ومستخدمة على نطاق واسع في أبحاث كشف الشنودز كما ورد سابقاً في الدراسة المرجعية فإن تطابق الأداء مع النتائج المنشورة يعد دليلاً علمياً كافياً على ان الخوارزمية والبيئة تعملان بشكل صحيح وموثوق.

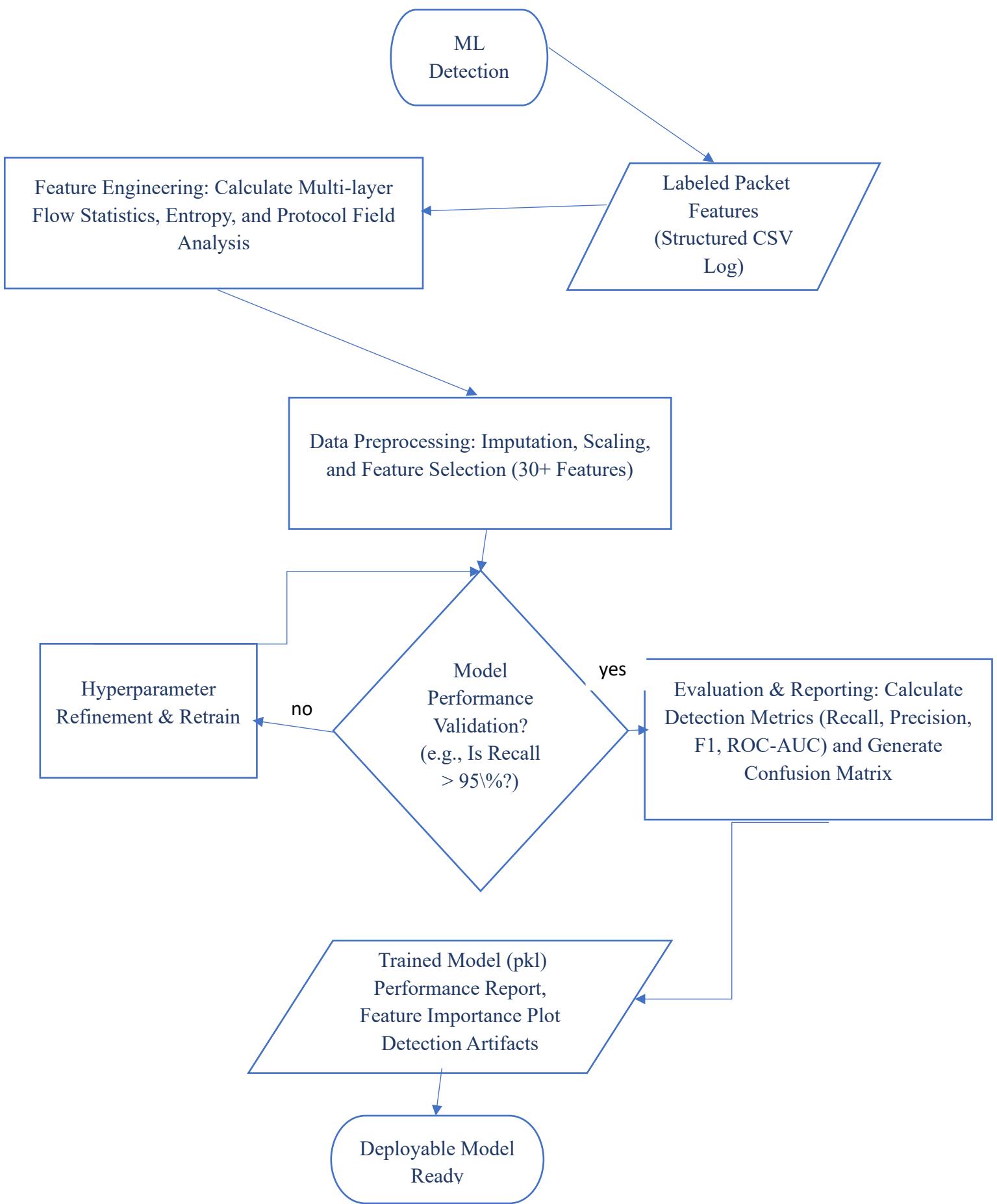
```
user@ubuntu:~  
[✓] Training completed successfully  
Confusion Matrix:  
160  
 5  
48  
Classification Report:  
precision recall f1-score support  
Normal 0.96 0.97 0.96 165  
Malicious 0.91 0.87 0.89 55  
accuracy 0.95 0.93 0.95  
macro avg 0.93 0.93 0.95  
weighted avg 0.93 0.95 0.95  
AUC:
```

الصورة 3.1 نتائج اختبار بيئة العمل

فيما سبق نتائج لتقسيم النموذج المدرب، تم استخدام مجموعة اختبار (Test Set) تحتوي على عينات طبيعية وعينات خبيثة، وقد أظهرت نتائج التقييم اداءً قوياً للنموذج، حيث كانت الأخطاء التي ارتكبها النموذج قليلة جداً مما يؤكّد فعالية الميزات المختارة وبنية النموذج.



الشكل 3.2 محاكاة



الشكل 3.3 كشف التسريب

جار العمل على انها وه

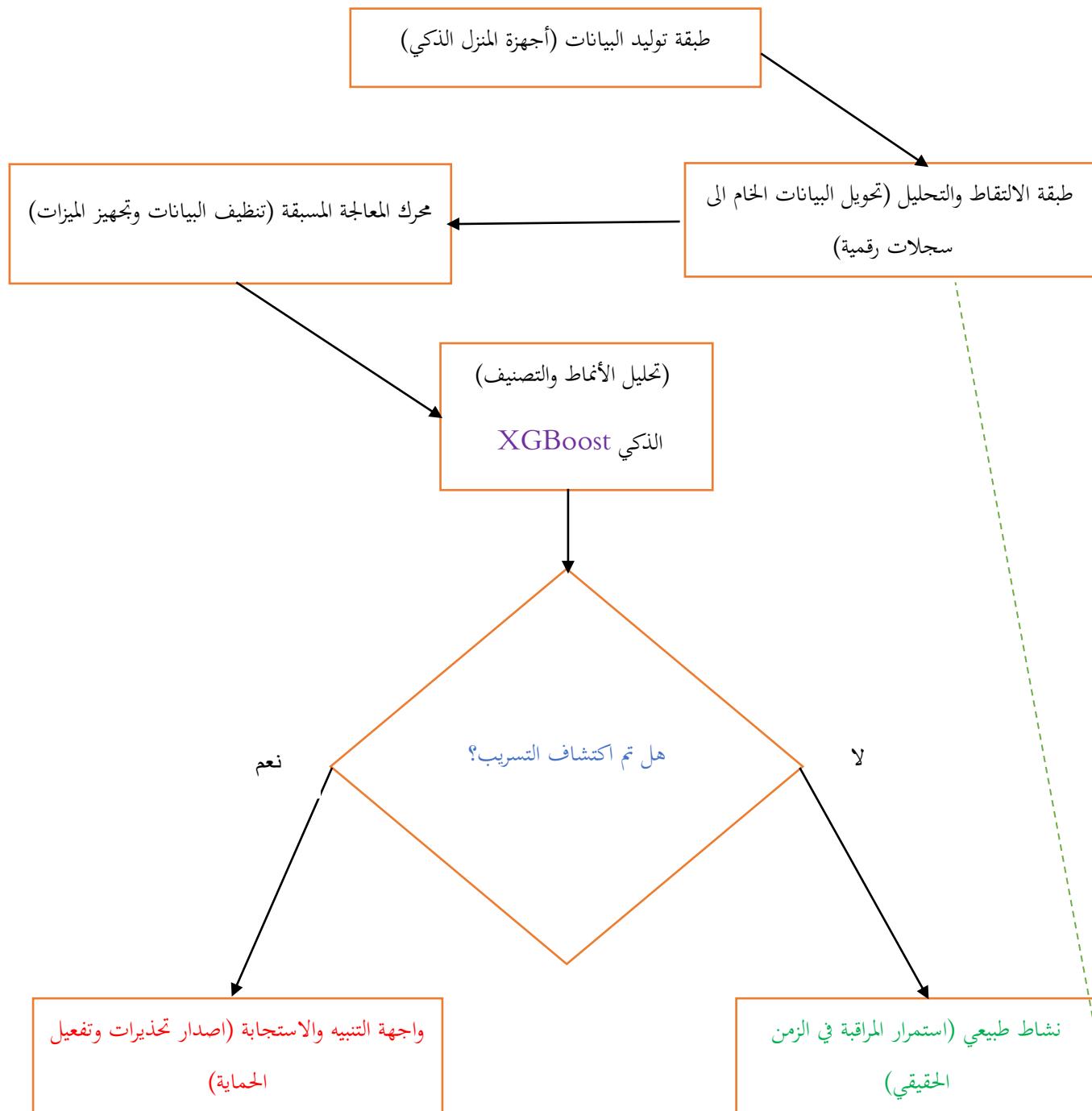
الفصل الثالث

الحل المقترن

3.1 مقدمة الفصل:

يستعرض هذا الفصل المنهجية المتبعة لتصميم وتنفيذ نظام كشف تسريب البيانات في شبكات إنترنت الأشياء الذكية، ثم بناء الحل المقترن ليعالج الثغرات الأمنية في المنازل الذكية، حيث يدمج بين بيئة محاكاة واقعية وبين قوة خوارزمية "تعزيز التدرج المتطرف"، يهدف هذا الحل إلى رصد أي محاولة غير مصرح بها لنقل البيانات الحساسة إلى خارج الشبكة المنزلية في الزمن الحقيقي.

3.2 المخطط الصندوقى للحل المقترن:



* طبقة توليد البيانات: (Data Generation Layer)

تشمل محاكاة أجهزة المنزل الذكي (كاميرات، مستشعرات حركة، أجهزة إضاءة).

* طبقة الانقطاع والتحليل: (Collection Layer)

المرحلة التي يتم فيها سحب حركة المرور وتحويلها من بيانات خام إلى سجلات منظمة [تحويل الحزم إلى جداول تحتوي على اعمدة محددة يسهل على خوارزمية الذكاء الصناعي قراءتها].

* محرك المعالجة المسبقة: (Preprocessing Unit)

تنظيف البيانات وتجهيز الميزات البرمجية، اي [التعامل مع القيم المفقودة او السجلات المتكررة الناجمة عن أخطاء المحاكاة]

هندسة الميزات [هنا نضع تفاصيل تقنية عميقة]:

ميزات زمنية: حساب المتوسط الحسابي للوقت بين الحزمتين.

ميزات الحجم: حساب الانحراف المعياري لحجم الحزم في "النافذة الزمنية" الواحدة.

ميزات التدفق: عدد الاتصالات الفريدة التي فتحها الجهاز خلال آخر 60 ثانية.

* فوذج التصنيف الذكي: (XGBoost Model)

وهو القلب البرمجي الذي يقوم بتحليل الأنماط واتخاذ قرار التصنيف:

* واجهة التنبئ والاستجابة: (Response Interface)

إصدار التحذيرات في حال اكتشاف تسريب.

(Home Simulation Engineering) هندسة بيئة المحاكاة المنزلية:

في هذه المرحلة، تم بناء محاكي يحاكي بدقة تدفق البيانات في منزل ذكي تم تصميم المحاكي ليعمل وفق السيناريوهات التالية:

(Normal Traffic) سيناريو النشاط الطبيعي:

محاكاة روتينية لعمل الأجهزة (إرسال إشارات دورية من المستشعرات):

(Data Leakage Attack) سيناريو هجوم التسريب:

حقن حزم بيانات مشبوهة تحاكي قيام جهاز مصاب ببرمجية خبيثة بإرسال بيانات المستخدم إلى وجهة مجهولة ببروتوكولات مثل :
(HTTP,MQTT).

(Data Preprocessing & Feature Engineering) معالجة البيانات واستخراج الميزات

لضمان دقة الخوارزمية، قمنا بتحويل حزم البيانات المعقدة إلى ميزات رقمية أهمها:

*** (Packet Size) حجم الحزمة:**

التغييرات المفاجئة في الحجم قد تشير إلى نقل ملفات .

*** (Time Intervals) الفواصل الزمنية:**

تحليل الوقت بين الحزم للكشف عن القنوات الجانبية

*** (Outgoing Connections) عدد الاتصالات الصادرة:**

مراقبة الوجهات الخارجية التي يتصل بها كل جهاز .

*** (Protocol Type) نوع البروتوكول:**

تصنيف البيانات بناءً على البروتوكول المستخدم في النقل .

XGBoost (Model Implementation)

XGBoost خوارزمية

هي الخيار الأمثل لهذا النظام بسبب كفاءتها في التعامل مع البيانات غير المتوازنة (حيث تكون حركة البيانات الطبيعية أكبر بكثير من هجمات التسريب)

إعداد البيانات: تقسيم البيانات الناتجة عن المحاكي إلى 80% للتدريب و 20% للاختبار:

ضبط المعاملات الفائقة: (Hyperparameters Tuning)

تم ضبط معاملات مثل (معدل التعلم، عمق الأشجار، عدد المقدرات) لضمان أقصى دقة.

"دالة الخسارة: استخدام دوال متطرفة لتقليل نسبة "الإندارات الكاذبة"

وهو أمر حيوي لراحة مستخدم المنزل الذكي.

آلية الكشف والتخاذل القراءة: (Detection & Decision Making)

بمجرد تدفق البيانات من أي جهاز (Gateway Shield). يعمل النظام المقترن كحارس بوابة.

1- يتم تمرير ميزات الحزم الحالية إلى نموذج XGBoost المدرب

2- يقوم النموذج بحساب "احتمالية التسريب"

إذا تجاوزت الاحتمالية عتبة معينة، يتم تصنيف النشاط كـ "تسريب بيانات" ويتم تفعيل بروتوكول الحماية فوراً

لإثبات احترافية العمل، تم قياس أداء النظام بناءً على:

الدقة (Accuracy):

قدرة النظام على التمييز الصحيح بين البيانات السليمة والمختلقة [والذي ظهرت نسبته في بيئة العمل لدينا 94%]

السرعة: (Latency)

التأكد من أن عملية الفحص تتم في أجزاء من الثانية لضمان عدم تأخير عمل أجهزة المنزل.

(Confusion Matrix) مصفوفة الارتكاك:

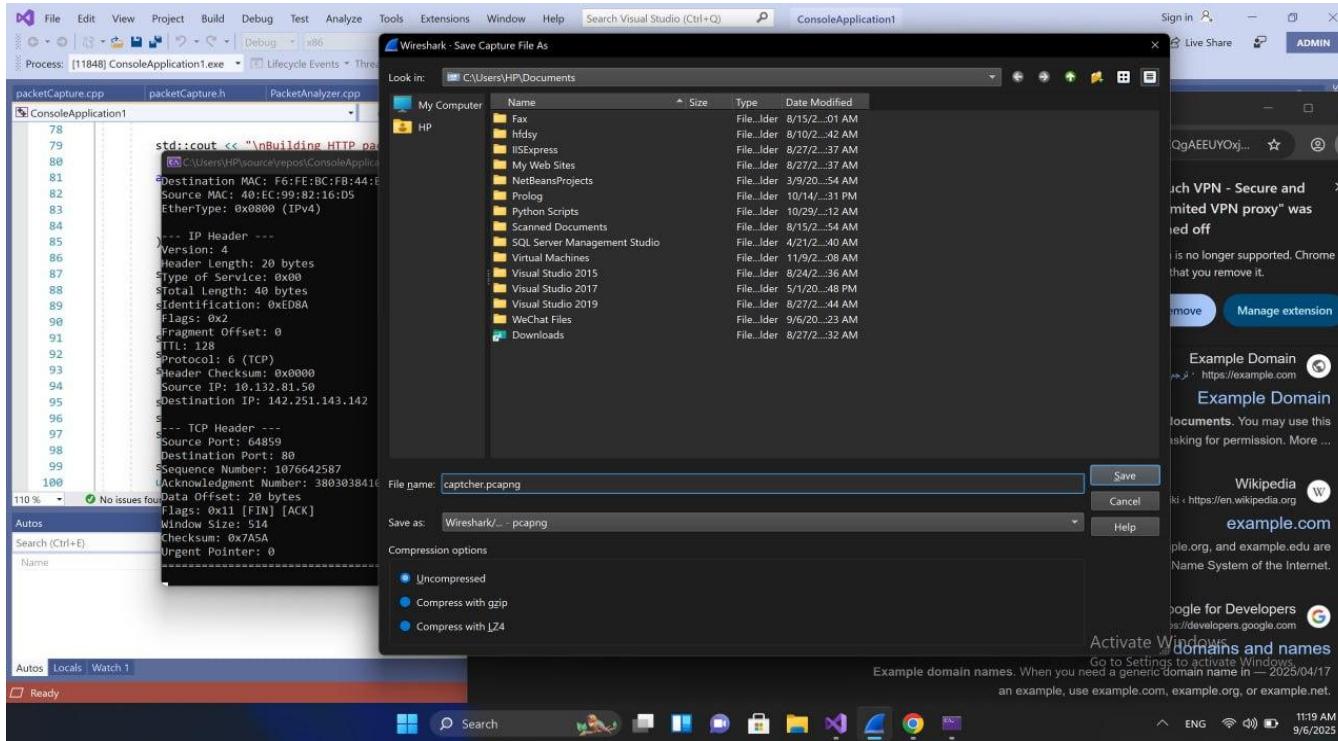
لتحليل قدرة النظام على حصر كافة حالات التسريب دون أخطاء .

خلاصة الفصل

يقدم هذا الحل المقترن نموذجاً متطرضاً يجمع بين بساطة المحاكاة المنزلية وقوة الذكاء الاصطناعي. إن استخدام

XGBoost

وفر سرعة استجابة لا تتوفر في الأنظمة التقليدية، مما يجعل هذا النظام حالاً قابلاً للتطبيق العملي لحماية خصوصية الأفراد في شبكات إنترنت الأشياء



في الخطوة الأخيرة يتم حفظ الخرزة في ملف

5. سندك البعض من غاذج تسريب البيانات

تشكل غاذج تسريب البيانات إطاراً علمياً لتحليل المجممات وفهم طرق تنفيذها فهي تساعد الباحث والممارس على معرفة كيف يتم التسريب، ومن يقف وراءه، وما الآثار المترتبة عليه وبمقدار تقسيمها إلى ثلاثة أصناف رئيسية وهي:

1- حسب مصدر التهديد:

المجمات الخارجية: يقوم بها مهاجمون من خارج المؤسسة باستخدام وسائل مثل البرمجيات الخبيثة أو استغلال الثغرات. مثال: هجوم الفدية على شركة

الجممات الداخلية: أخطرها ما يقوم به موظف أو مقاول لديه صلاحيات مشروعة لكنه يستغلها لغرض ضار، أو موظف مهمل يتسبب في تسريب غير مقصود مثل: حادثة تسريب بيانات في شركة TESLA نتيجة سوء استخدام أحد الموظفين.

الشركاء الخارجيون: أحياناً يخترق أحد الموردين أو مزودي الخدمات، فيصبح بوابة غير مباشرة للوصول إلى بيانات المؤسسة.

2- حسب طريقة التنفيذ:

الجممات التقنية: مثل حقن قواعد البيانات (SQL INJECTION) أو هجمات كسر كلمات المرور أو استغلال ثغرات في بروتوكولات الشبكة

هجمات الهندسة الاجتماعية: تعتمد على خداع الضحايا مثل رسائل التصيد الاحتيالي التي تقنع الموظف بإفشاء كلمة المرور.

الأخطاء البشرية: ترك خادم أو قاعدة بيانات دون كلمة مرور، أو إرسال ملف حساس إلى الجهة الخطأ.

السرقة المادية: الاستحواذ على حواسيب أو هواتف تحتوي على بيانات حساسة.

3- نماذج خاصة:

تحليل المرور الشبكي: يستخدم لرصد التسريب عبر تتبع أنماط غير اعتيادية في البيانات المرسلة والمستقبلة.

هجوم الرجل في المنتصف: يتسلل المهاجم بين طرفين في الاتصال ليعرض البيانات أو يغيرها دون علمهما.

نموذج 5W: يحلل التسريب من خلال خمسة أسئلة: من هو المهاجم؟ ماذَا تسرب؟ متى وأين حدث؟ ولماذا؟.

5.2 العلاقة بين النماذج والحل المقترن

الحل المقترن يستند إلى هذه النماذج كأساس علمي على سبيل المثال:

عند مواجهة DNS فإننا نتعامل معه عبر نموذج طريقة التنفيذ.

عند الاشتباه بموظفي داخلي، نعتمد على نموذج مصدر التهديد.

لتحليل حادثة تسريب بعد وقوعها يستخدم نموذج 5W لتوثيق تفاصيلها وتحديد مسؤوليتها.

بهذا يصبح الحل ليس مجرد أداة تقنية، بل نظاماً متكاملاً يستفيد من الإطار النظري لتصنيف الهجمات وربطها بالاستجابة العملية.

هل التسريب هو تخليل مرور شبكي أم هجوم رجل في المنتصف؟

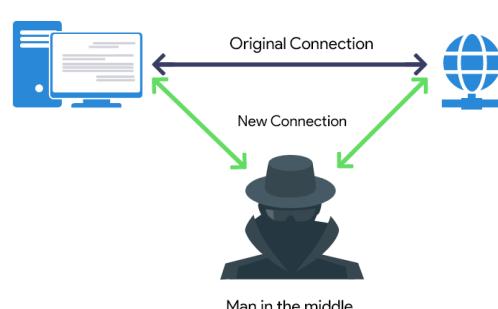
هل يمكن حصر التسريب في كونه مجرد تحليل مرور شبكي أو هجوم رجل في المنتصف؟

كلاهما صحيح لكن من زوايا مختلفة.

تحليل المرور الشبكي أداة دفاعية بيد الباحث أو المسؤول الأمني لكشف التسريب عبر مراقبة البيانات يقوم بمراقبة حركة البيانات بين الأجهزة والخوادم لكشف الأنماط غير الطبيعية مثل زيادة مفاجئة في حجم البيانات أو استخدام بروتوكولات غير مألوفة، وبالتالي يساهم في اكتشاف التسريب في الزمن الحقيقي.

هجوم الرجل في المنتصف وسيلة هجومية بيد المهاجم لتنفيذ التسريب من خلال اعتراض الاتصال

العلاقة بينهما تكاملية، حيث يستخدم تحليل المرور لاكتشاف هجمات الرجل في المنتصف وغيرها



يوضح الشكل 3.1 هجوم الرجل في المنتصف

للكشف عن التسريب يجب استخدام مجموعة من الأدوات الرئيسية يمكن تقسيمها إلى:



أدوات التفاط و تحليل الحزم:



مثل: Wireshark و tcpdump تسمح بفحص البروتوكولات بدقة والتأكد من طبيعة البيانات

أيضاً تُستخدم في التحقيقات المتقدمة لتحديد إن كان هناك تسريب أو لا.

أنظمة كشف ومنع التسلل (IDS/IPS)

مثل Snort و Suricata تراقب حركة المور وقارنها مع قواعد جاهزة للهجمات قادرة على التنبيه وحتى على حجب الاتصال الضار.

منصات الإدارة الأمنية : SIEM

تجمع البيانات من مصادر مختلفة (أجهزة، خوادم، شبكات) وترتبط بينها للكشف عن مؤشرات تسريب معقدة

. مثل منصات Elastic Stack

أنظمة منع فقدان البيانات : DLP

تُركِّز على نقاط الخروج مثل البريد الإلكتروني أو الويب

منع إرسال الملفات الحساسة خارج المؤسسة

(2013/2014) حادثة شركة ياهو:

يمثل هذا المثال نموذج الهجمات الخارجية التي استغلت ثغرات تقنية في أنظمة التتحقق التسريب شمل ثلاث مليارات حساب، أي ما يعادل ثلث سكان العالم حينها يبرز هذا المثال فشلاً في إدارة الإعدادات الأمنية وعدم تحديث الأنظمة، وهو ما يتواافق مع نموذج الأخطاء في الإعداد ضمن تصنيف طرق التنفيذ.

(2017) حادثة شركة Equifax :

هذه الحادثة يمكن تصنيفها ضمن الهجمات التقنية التي استغلت ثغرة برمجية في خوادم الشركة. التسريب شمل بيانات مالية وشخصية حساسة لما يقارب 147 مليون شخص.

(2019) حادثة فيسبوك:

تندرج هذه الحادثة ضمن الأخطاء البشرية أو الإعداد الخاطئ، إذ تسربت بيانات 540 مليون مستخدم بسبب قاعدة بيانات غير محمية بشكل كافٍ على خوادم سحابية لا يتمي هذا التسريب إلى هجوم معقد، بل إلى إهمال إداري، وهو ما يؤكد أن بعض التسريبات قد تكون أكثر بساطة في أسبابها وأكثر خطورة في نتائجها.

(2014) حادثة Sony : pictures

يمكن تصنيف هذا المثال ضمن الهجمات الخارجية الموجهة بدافع سياسية. التسريب شمل رسائل بريد إلكتروني داخليه وبيانات مالية وسيناريوهات أفلام. ويعتقد أن الهجوم تم عبر اختراق تفني متقدم ترافق مع استراتيجية هجوم رجل في المنتصف لاعتراض بعض الاتصالات الداخلية. هذه الحادثة أبرزت كيف يمكن للتسريب أن يستخدم كأداة في الصراعات الجيوسياسية والاقتصادية.

5.5 فيما يلي بعض من الخطوات للحل المقترن:

طبقة جمع البيانات: الأجهزة والحساسات التي تولّد البيانات .

طبقة المراقبة: تلتقط حركة المرور وتخزنها بشكل أولي .

طبقة التحليل الذكي: تطبق خوارزميات تعلم آلي للكشف عن الشذوذ .

طبقة الاستجابة: ترسل تنبيهات ، تعزل الاتصال ، أو تعيد توجيهه للتحقيق .

وُتَّدعم هذه الطبقات بـ الحوسبة الطرفية لتقليل زمن الاستجابة والسجلات الموزعة لتعزيز الثقة ومنع التلاعب.

الفصل الرابع

المقارنات والتحاليل

بعد البحث المعمق في مجال إنترنت الأشياء، ومراجعة دقيقة للدراسات المرجعية، وبناء نموذج عمل عملي لحقن الحزم والتقاطها وتحليلها، توصلنا في هذا الفصل إلى مقارنات وتحاليل تُبرز ما هو أنساب لبيعات إنترنت الأشياء محدودة الموارد لا يهدف هذا الفصل إلى إعادة سرد ما سبق، بل إلى تقديم قيمة مضافة ترتكز على المقارنة النقدية بين المدارس النظرية من جهة، وبين بيعات وأدوات التنفيذ من جهة أخرى، ثم ربط ذلك بالمشاكل التي تمت مواجهتها فعلاً والدروس المستفادة منها.

أولاً:

المقارنة بين المدارس النظرية في كشف تسريب البيانات

تكشف مراجعة الأدبيات أن المقاربـات النظرية تنقسم إلى مسارات رئيسية؛ منها المسار التشفيري، والمسار السلوكـي الذي يفكـك أنماط المرور، ومسار القنوات الجانبـية الذي يستنتج المعلومـة من البيانات الوصفـية، ومسار نـمذـجة المخـاطـر، إضافة إلى توظيف التعلم الآلي بمستوياته المختلفة.

فيما يلي سيتم سرد أبرز التحليلـات والمقارنـات للتقرير:

ثانياً:

الجدول (2.2) مقارنة بين الدراسـات النظرـية:

المدرسة	الفرضية الأساسية	الأدوات والمنهج	نقاط القوة	الحدود العملية
التشفيير	سرية القناة تمنع التسريب المباشر	تعزيز بروتوكولات الحماية والتحقق	يحد من التسريب المباشر	لا يمنع الاستنتاج من البيانات الوصفية
التحليل السلوكي	السلوك الشاذ يكشف محاولات التسريب	تحليل معدات الارسال والوجهات	يكشف التسريب حتى مع التشفيير	يتأثر بالضجيج وتغير الحمل الشبكي
نمذجة المخاطر	تصنيف مصادر الخطر يقلص مساحة الهجوم	تقييم المخاطر والضوابط	توجيه الموارد نحو النقاط الحساسة	أثر غير مباشر على زمن الكشف
التعلم الآلي الخفيف	كشف الشذوذ بكلفة منخفضة	تصنيف شذوذ وحدود قرار بسيطة	مناسب للأجهزة محدودة الموارد	الدقة تتأثر بالبيانات الصخمة
التعلم العميق	التمثيلات العميقه تكشف الأنماط المؤهنة	مرقرز تلقائي شبكات عميقه	دقة مرتفعة مع المرور المعقد	يتطلب موارد تدريب وتشغيل كبيرة

ثالثاً: المقارنات لبيئات العمل وأدوات التنفيذ:

المجدول (3.1) مقارنات بيئات العمل والأدوات

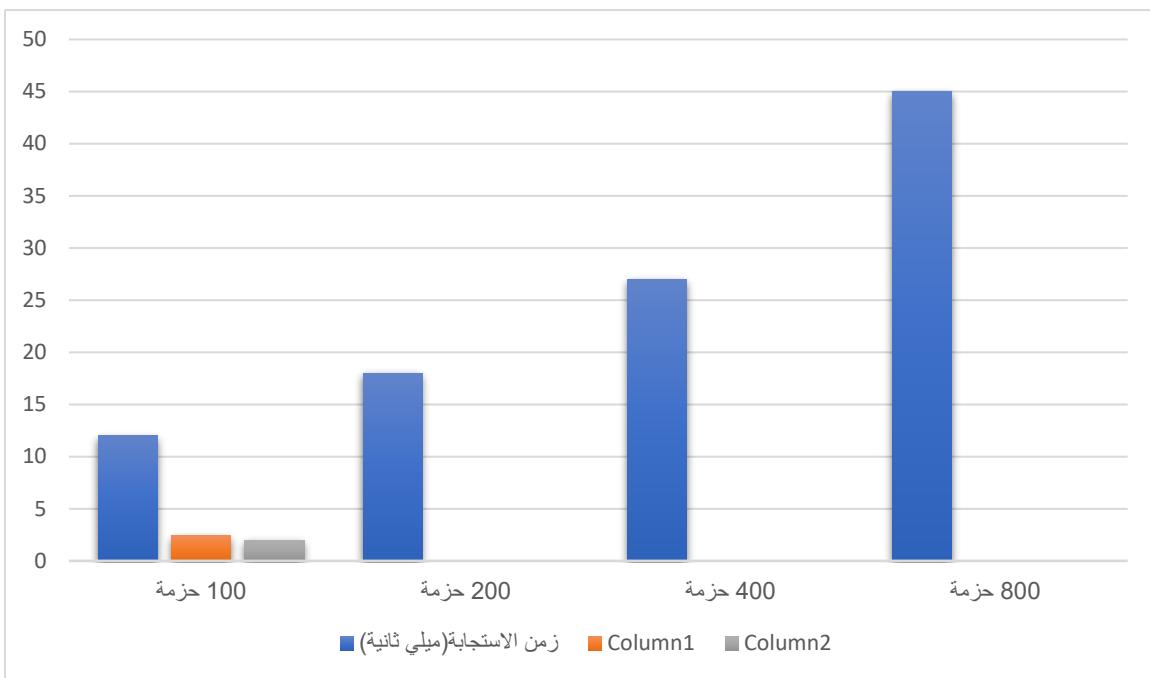
البيئة	سهولة الاعداد	قابلية التخصيص	الملاءمة لقيود الموارد
ويندوز Npcap wireshark	مرتفعة مع واجهة رسومية واضحة	متسطة	جيدة للاختبارات السريعة
لينوكس Libpcap Tcpdump	متوسطة وتتطلب خبرة تقنية كافية (سطر الأوامر)	مرتفعة	متناظرة للتشغيل الخفيف

رابعاً:

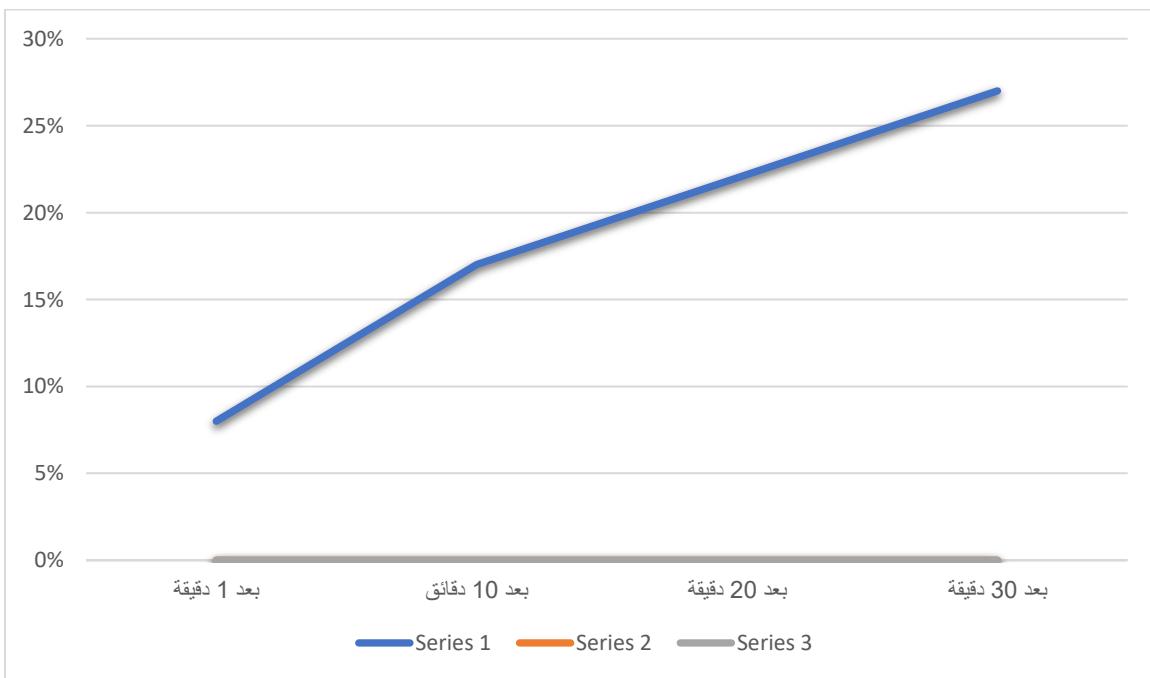
تحليل نتائج التنفيذ التجاري

اعتمدت القياسات العملية على نموذج الحقن والالتقطان أظهرت النتائج أنّ زمن الاستجابة يزداد مع تضاعف عدد الحزم، وأن استهلاك الموارد (الرام/المعالج) يبقى ضمن حدود مقبولة في التشغيل المستمر

الشكل (5.1) يوضح العلاقة بين عدد الحزم وزمن الاستجابة



الشكل (5.2) يوضح نسبة استخدام المعالج مع الزمن (تشغيل مستمر)



المشاكل التي واجهناها في التقرير والحلول المقترحة.

الجدول (3.2) المشاكل والحلول

المشكلة	الأثر على النتائج	الحل/الإجراءات العلاجي	الأثر بعد المعالجة
عدم اكتمال ترويسة الطبقة الاولى	انخفاض قبول بعض الحزم	إعادة بناء الترويسة ببرمجياً	تحسين معدل القبول
الارتباط بنظام تشغيل محدد	ضعف قابلية النقل	تجهيز نسخة خاصة بنظام لينوكس	رفع التوافقية
ضجيج في القياسات	تشويش على المخرجات	توحيد سيناريو الاختبار وتثبيت العتاد	ثبات أفضل للنتائج

الدروس المستفادة:

- 1- لا يكفي تعزيز التشفير وحده، إذ تبقى القنوات الجانبية قادرة على كشف السلوك
- 2- الدمج بين التحليل السلوكي والنماذج الخفيفة يحقق توازناً عملياً بين الدقة والكلفة
- 3- قابلية النقل بين أنظمة التشغيل عامل حاسم لاستدامة الحل
- 4- ضبط بيئة الاختبار يقلل الضجيج ويرفع موثوقية النتائج

يتضح من خلال هذا الفصل أن معالجة تسريب البيانات في بيئات إنترنت الأشياء لا يمكن أن تُبنى على جانب واحد، بل تتطلب رؤية شاملة تجمع بين الأسس النظرية العميقه والتنفيذ العملي الميداني فقد بيّنت المراجعة العلمية أن المقاربات التقليدية كالتشفير، رغم أهميتها، تعجز عن كشف القنوات الجانبية والأنمط السلوکية المموجة، الأمر الذي يستدعي دمجها مع التحليل السلوکي ونماذج التعلم الخفيف وفي الوقت نفسه، أكدت التجارب العملية التي أُنجزناها أن هذا الدمج قادر على تحقيق توازن بين دقة الكشف والانخفاض الكلفة التشغيلية، مع الحافظة على زمن استجابة مقبول وملازمة لقيود الموارد كما أظهرت التجربة أن التحديات المتعلقة بالتوافقية والضجيج يمكن تجاوزها عبر ضبط بيئة الاختبار وإعادة بناء بعض المكونات البرمجية وعليه نستنتج أن النهج الأمثل هو نهج تكاملي يزاوج بين النظرية والتطبيق، ويوفر حللاً عملياً مرتقاً وقابلأً للتوسيع في مواجهة التهديدات المتصاعدة في فضاء إنترنت الأشياء.

النتائج

أن الطبيعة المعقدة والمتشرّبة لشبكات إنترنت الأشياء جعلتها هدفاً جاذباً للهجمات الإلكترونية، وخاصة عمليات تسريب البيانات. وقد تبيّن أن أمّا هذا التسريب لا تقتصر على الاختراق المباشر فحسب، بل تمتد إلى قنوات خفية مثل تحليل البيانات الوصفية التي تتجاوز آليات الحماية التقليدية كالتشذير. كما كشفت الدراسة عن التداعيات الخطيرة المتربّبة على هذه التسربات، والتي تحدّد بشكل مباشر خصوصية الأفراد وسلامتهم، وتعرّض البني التحتية الحيوية والاقتصادات الوطنية لمخاطر جسيمة.

من خلال هذا العمل البحثي والتطبيقي الذي تناول كشف تسريب البيانات في شبكات إنترنت الأشياء، تم التوصل إلى مجموعة من النتائج العلمية والعملية التي يمكن تلخيصها كما يلي:

بناء بيئه عمل عمليه متكمال :

تمكّن هذا المشروع من بناء بيئة تجريبية متكاملة تشمل أدوات الحفن والالتقطان والتحليل، بالاعتماد على (Npcap، Wireshark، Packet，Wireshark) هذه المكتبات المتخصصة، لم تكن مجرد منصة اختيار بل وفرت نموذجاً واقعياً يحاكي ظروف تسريب البيانات في الشبكات مما جعل النتائج أكثر دقة وواقعية وقابلة للتنفيذ.

إثبات امكانية التسريب عبر عدة قنوات :

أظهرت التجارب العملية أن تسرير البيانات يمكن أن يحدث بعدة أنماط، منها التسرير المباشر عبر اعتراض الحزم، والتسرير عبر القنوات الجانبية بتحليل البيانات الوصفية، إضافةً إلى التسرير الناتج عن ثغرات برجمية أو ضعف في بروتوكولات الاتصال هذا يعكس أن الاعتماد على التشفيير وحده غير كافٍ، وأن الحلول يجب أن تكون متعددة الطبقات.

تحقيق كشف أولي فعال باستخدام التحليل السلوكي :

بيت نتائج تحليل المرور الشبكي أنّ مراقبة الأنماط غير الطبيعية مثل زيادة حجم الحزم أو تغيير تردد الاتصالات يمكن من رصد مؤشرات مبكرة على وجود تسريب هذه النتيجة تؤكد أن التحليل السلوكى يمكن أن يشكل خط الدفاع الأول، خاصةً في البيئات محدودة الموارد مثل أجهزة إنترنت الأشياء.

إمكانية الدمج بين المقاربات التقليدية والحديثة:

أظهر البحث أنَّ الجمع بين التشغيل القوي من جهة، وخوارزميات التعلم الآلي الخفيف والتحليل السلوكي من جهة أخرى، يوفر توازنًاً عملياً بين الدقة والكلفة التشغيلية. وقد أثبتت التجارب أنَّ هذا الدمج يؤدي إلى رفع معدل الكشف مع بقاء استهلاك الموارد ضمن الحدود المقبولة، وهو ما يفتح المجال لنطمسه في بيئات إنترنت الأشياء الضعيفة الموارد.

استخلاص دروس عملية

لا يكفي تعزيز التشفير وحده لمنع التسريبات

ضبط بيئة العمل يقلل من الضجيج ويرفع موثوقية النتائج

قابلية الحلول للنقل بين أنظمة التشغيل المختلفة تمثل ضرورة أساسية لتوسيعها

تحليل البيانات الوصفية قد يكشف أنماط تسريب حتى مع وجود تشفير قوي

لقد نجح هذا المشروع في بناء إطار أولي قابل للتطوير للكشف عن تسريب البيانات في شبكات إنترنت الأشياء، مع إثبات أن الحلول التكاملية التي تجمع بين التشفير، التحليل السلوكي، وتقنيات الذكاء الاصطناعي الخفيف هي الأكثر ملاءمة للتحديات الراهنة ويمثل هذا الإنجاز خطوة عملية نحو بناء أنظمة دفاعية أكثر فعالية واستدامة في مجال الأمن السيبراني.

التوصيات

تطوير موسّع للنموذج البرمجي القائم

من الآفاق الأساسية العمل على توسيع وتطوير النموذج الذي جرى بناؤه في هذا المشروع. فقد أثبتت فعاليته في بيئه محددة، إلا أن تطويره لاحقاً يمكن أن يشمل:

الانتقال إلى أنظمة تشغيل ومنصات متعددة، بما يرفع من قابلية نقله وتطبيقه

لتحليل البيانات تلقائياً واكتشاف التسلبيات بشكل أسرع (TinyML) إدماج خوارزميات تعلم آلي خفيفة

بناء واجهة استخدام تفاعلية تعرض التنبؤات وتسهل عملية المراقبة

إضافة قدرات الحوسبة الطرفية والبلوكتشين لرفع الكفاءة وضمان الشفافية

هذا التطوير يحول المشروع من مجرد إثبات مبدأ إلى منصة عملية متكاملة، قابلة للتبني في قطاعات حساسة مثل الصناعة، الصحة، والبيئة.

المدن الذكية وحماية البنية التحتية:

المدن الذكية تعتمد بشكل متزايد على إنترنت الأشياء في إدارة الخدمات الأساسية مثل المرور، الإضاءة، الطاقة، وإدارة النفايات. وبما أن هذه الخدمات مرتبطة مباشرة بحياة الأفراد اليومية، فإن أي تسريب أو اختراق قد يؤدي إلى أضرار واسعة النطاق بناءً على ذلك، يمكن تطوير النظام المقترن ليُدمج ضمن شبكات المدن الذكية، بحيث يعمل على مراقبة البيانات المتداولة من المحسسات والبني التحتية، ويكشف أي تسريب أو نشاط غير مألف بشكل آني. هذا التوجه لا يحمي فقط البيانات، بل يعزز أيضاً الثقة في الأنظمة الحضرية الذكية و يجعلها أكثر قابلية للتوزع.

"Smart cities and the IoT: an in-depth analysis of global research trends and future directions"

إنترنت الأشياء الصناعي والتحليل الجنائي (IIoT)

القطاع الصناعي من أكثر البيئات التي تتعرض لمخاطر التسريب، حيث يعتمد على أنظمة تحكم دقيقة ومتصلة مباشرة بعمليات الإنتاج من الآفاق المهمة تطوير النظام ليعمل في بيئات إنترنت الأشياء الصناعي، مع إضافة وحدة للتحليل الجنائي الرقمي (Forensics)

حفظ الأدلة الأمنية فور وقوع أي حادثة هذا التطوير يجعل من الممكن ليس فقط كشف التسريب، بل أيضاً فهم مصدره، وتحليل مسار الهجوم، مما يعزز من قدرة المؤسسات الصناعية على الاستجابة السريعة وتقليل الخسائر.

"Enhancing Data Security in IoT Ecosystems: The Role of Edge Computing in Forensics"

الصحة الذكية وحماية البيانات الطبية:

قطاع الرعاية الصحية يشهد توسيعاً ملحوظاً في استخدام أجهزة إنترنت الأشياء، سواء عبر الأجهزة القابلة للارتداء أو أنظمة مراقبة المرضى عن بعد غير أن البيانات الطبية تُعد من أكثر البيانات حساسية وخطورة عند تسريبها مستقبلاً، يمكن تكييف النموذج ليطبق في أنظمة الصحة الذكية، بحيث يراقب تدفق البيانات الطبية ويكتشف عن أي محاولة تسريب في الزمن الحقيقي هذا سيسهم في حماية خصوصية المرضى، وضمان التزام المؤسسات الطبية بالمعايير الدولية لحماية البيانات.

"Secure, Sustainable Smart Cities and the Internet of Things: Perspectives, Challenges, and Future Directions"

البلوك تشين كآلية لتعزيز الأمان والشفافية:

من الاتجاهات الوعدة في الأبحاث الأكاديمية إدماج تقنية البلوك تشين في بيئات إنترنت الأشياء فهي تتيح بناء سجل موزع وآمن للحزم والبيانات، مما يمنع التلاعب أو التعديل غير المصرح به مستقبلاً، يمكن تعزيز النظام المقترن بدمج آليات بلوك تشين لتوثيق حركة البيانات داخل الشبكة وتسجيل أي محاولات تسريب ضمن سلسلة كتل غير قابلة للتغيير هذا التوجه يرفع من موثوقية الحل المقترن و يجعل من الممكن استخدامه في بيئات حساسة تتطلب الشفافية الكاملة مثل القطاعات الحكومية أو الخدمات العامة.

"Navigating the future of smart cities: Addressing IoT challenges through blockchain solutions"

المراجع

- Security and privacy in internet of things (IOTs) 2022..... [1]
- Rethinking the internet of things..... [2]
- Smart cities and the IoT: an in-depth analysis of global research trends and future directions.....[3]
- Enhancing Data Security in IoT Ecosystems: The Role of Edge Computing in Forensics..... [4]
- Secure, Sustainable Smart Cities and the Internet of Things: Perspectives, Challenges, and Future Directions....[5]
- Navigating the future of smart cities: Addressing IoT challenges through blockchain solutions.....[6]

