الجمهورية العربية السورية

وزارة التعليم العالي

الجامعة السورية الخاصة

كلية الهندسة

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

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

إشراف:

د. وسيم الجنيدي

أ. يامن الحلاق

إعداد الطلّاب:

قاسم عقله

سامر رحمه

Abstract

يُعدّ تسريب البيانات من أخطر التهديدات الأمنية التي تواجه شبكات إنترنت الأشياء، نتيجة الطبيعة الموزعة لهذه الشبكات، وتعدد الأجهزة المتصلة، ومحدودية قدراتها الحاسوبية، إضافةً إلى تنوع بروتوكولات الاتصال المستخدمة ومع التوسع المتسارع في اعتماد إنترنت الأشياء ضمن القطاعات الحيوية، أصبحت الحاجة إلى آليات فعّالة لكشف التسريب في الزمن الحقيقي ضرورة ملحّة

يهدف هذا المشروع إلى دراسة مشكلة تسريب البيانات ضمن شبكات إنترنت الأشياء الذكية من منظور نظري وتطبيقي حيث يتناول الجانب النظري البنية الأساسية لهذه الشبكات، وأنماط التسريب وآثارها الأمنية، مع مراجعة منهجية لأحدث الأبحاث المعتمدة على تقنيات الذكاء الاصطناعي والتعلم الآلي أما الجانب العملي، فيقترح إطارًا متكاملًا لكشف تسريب البيانات يعتمد على محاكاة واقعية لبيئة إنترنت الأشياء، وتحليل حركة المرور الشبكية باستخدام تقنيات تعلم آلي متقدمة لاكتشاف السلوكيات الشاذة والأنشطة غير المصرح بها

تبيّن نتائج الدراسة أن دمج تقنيات الذكاء الاصطناعي مع التحليل العميق لحركة البيانات يحقق دقة كشف مرتفعة مع تقليل الإنذارات الكاذبة، مما يسهم في تعزيز أمن شبكات إنترنت الأشياء ورفع موثوقية الأنظمة الذكية.

Data leakage is one of the most critical security threats facing Internet of Things (IoT) networks due to their distributed nature, the heterogeneity of connected devices, limited computational resources, and the diversity of communication protocols. With the rapid expansion of IoT adoption in critical sectors, the need for effective real-time data leakage detection mechanisms has become increasingly essential.

This project investigates the problem of data leakage in smart IoT networks from both theoretical and practical perspectives. The theoretical part examines the fundamental architecture of IoT systems, data leakage patterns, and their security implications, while providing a systematic review of recent research based on artificial intelligence and machine learning techniques. The practical part proposes an integrated data leakage detection framework based on realistic IoT environment simulation and in-depth network traffic analysis using advanced machine learning techniques to identify anomalous and unauthorized activities.

The results demonstrate that integrating artificial intelligence techniques with deep traffic analysis achieves high detection accuracy while reducing false alarms, thereby enhancing the security and reliability of IoT networks.

فهرس المحتويات:

المقدمة(introduction) 7

المشكلة العلمية..... 7

الهدف من البحث..... 7

الدراسة المرجعية (state of the art) 8

التحديات..... 14

التطبيقات العملية..... 16

الفصل الأول (الدراسة النظرية) 16

1.1.1 البنية الأساسية لإنترنت الأشياء..... 17

1.1.2 التطبيقات لإنترنت الأشياء..... 17

1.2.1 أنماط تسريب البيانات..... 20

1.2.2 امثلة على تسريب البيانات..... 21

2.1.2 اثار تسريب البيانات..... 22

2.2.1 تحديات انترنت الأشياء..... 23

3.1.1 العواقب الرئيسية..... 24

3.2.1 نقاط الضعف في انترنت الاشياء..... 26

الفصل الثاني (بيئة العمل) 27

2.1المقدمة..... 28

2.2 مقارنة بين بيئات العمل..... 28

2.3 تبرير اختيار بيئة العمل..... 29

2.4 المراجع التقنية الرسمية لبيئة العمل والأدوات المستخدمة..... 31

2.1.1 التحقق من صحة عمل خوارزمية الذكاء الاصطناعي 34

الفصل الثالث (الحل المقترح) 37

3.1 مقدمة الفصل..... 38

3.2 المخطط الصندوقي للحل المقترح..... 38

الفصل الرابع (النتائج والتحاليل) 43

النتائج.....48

التوصيات.....50

المراجع.....52

فهرس الأشكال

الشكل1.1(التحديات).....14

الشكل 1.2(تطبيقات انترنت الأشياء) 19

الشكل 2.1 (أبرز الهجمات على انترنت الأشياء) 22

الصورة 3.1 (نتائج اختبار بيئة العمل) 34

الشكل 3.2 (المحاكاة).....35

الشكل 3.3 (كشف التسريب) 36

فهرس الجداول:

الجدول1.1 (الدراسة المرجعية) 11

الجدول 2.1 Major themes 25

الجدول 4.1 بيانات أجهزة المحاكي 45

الجدول 4.2 نتائج قياس خوارزمية الذكاء الاصطناعي 46

المقدّمة

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 أتاح 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 الجهود بذلت لتوفير آليات حماية لهذه الشبكات، فإن محدودية إمكانيات الأجهزة، وتنوع بروتوكولات الاتصال المستخدمة، تجعل 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،

يركّز 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 الأمن السيبراني وتدعم استدامة الثقة في تقنيات إنترنت الأشياء.

1- المشكلة العلمية:

مع الانتشار المتسارع لأجهزة **إنترنت الأشياء** في حياتنا اليوميّة والصناعيّة، أصبحت شبكاتها هدفاً رئيسياً للهجمات الإلكترونية وسرقة البيانات الحساسة، تعتمد هذه الأجهزة غالباً على بروتوكولات اتصال بسيطة، مما يجعلها عرضة للتسلل واستغلال الثغرات الأمنيّة، المشكلة الأساسية تكمن في عدم وجود آليات فعّالة ودقيقة لكشف تسريب البيانات في الوقت الحقيقي

الامر الذي يزيد من مخاطر فقدان المعلومات والتجسس على المستخدمين وتأثير الهجمات على استقرار الشبكات، لذلك:

هناك حاجة ملحّة لتطوير حلول تكشف هذه التسريبات بشكل مبكّر وفعّال، مع مراعاة خصوصية البيانات وأداء الشبكة.

2- الهدف من البحث:

تطوير إطار مدعوم بتقنيات الذكاء الصنعي متكامل لكشف تسريب البيانات بالسرعة اللازمة لإيقافه والتعافي منه

واستخدام أحدث الآليات والخوارزميات في أمن المعلومات وتحديد أفضلها بهدف 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 واوراق 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 انترنت الأشياء" (AI-SET)

قدمت الورقة اطارا أمنيا ذكيا لأنترنت الأشياء يعتمد على الذكاء الصنعي 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 انترنت الأشياء.

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

مقالة بعنوان: **"من السحابة الى الحافة: دمج انترنت الأشياء والذكاء الصناعي لأنظمة مستدامة وفعالة"**

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

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

أيضا 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 بيئات انترنت الأشياء موضحة اهم متطلبات الأمان والتحديات المستقبلية

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

أيضا توضح كيفية دمج الذكاء الصناعي وتقنيات البلوك تشين في تعزيز امان الوصول الى البيانات.

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

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

قدمت الورقة نظاما ذكيا آمنا يعتمد على تقنيات الذكاء الصناعي للكشف عن الهجمات 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 واكتشاف تسريب المعلومات في الزمن الحقيقي.

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

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

قدمت الورقة نظاما امنيا يعتمد على التعلم العميق لتصنيف وتحليل البيانات داخل شبكات انترنت الاشياء

كما استخدم الباحثون خوارزميات هجينة من الشبكات العصبية والذكاء التطوري 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.

وقبل 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 التحديات 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 التسريبات عبر تحليل السلوك وتوظيف خوارزميات دقيقة وخفيفة الموارد.

وفي نفس العام 2024 نشر الباحثين "Mani Srivastaava, Zhichao Cao, Ness Shroff, Hyunho, Shakhrul Iman"

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

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

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

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

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

"تقنيات التعلم الآلي والعميق لاكتشاف الشذوذ في شبكات انترنت الأشياء: مراجعة شاملة"

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

لخصت: ان 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.

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

بعنوان: **"استكشاف دور الذكاء الاصطناعي في أنظمة انترنت الأشياء: دراسة تحليلية منهجية"**

قدمت دراسة منهجية لدور الذكاء الاصطناعي في أنظمة انترنت الأشياء من خلال تحليل **81** بحثاً بينت اهم مهام الذكاء الاصطناعي

لخصت: الى ان دمج الذكاء الاصطناعي في انترنت الأشياء يعزز الكفاءة والأمان والتنبؤ الذكي

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

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

مقال بعنوان: **"دمج تقنيات التعلم العميق في انترنت الأشياء: مراجعة للتقنيات والتحديات في التطبيقات الواقعية"**

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

واظهرت ان 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 انترنت 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 انترنت الأشياء مراجعة للتقنيات والتحديات	2023	دراسة شاملة حول دمج تقنيات التعلم العميق في أنظمة انترنت الأشياء لتحسين الأداء في التطبيقات الذكية	أظهرت ان الشبكات العصبية العميقة ترفع دقة الكشف والتنبؤ لكن تتأثر بضعف قدرات الأجهزة الطرفية	تفيد في توضيح كيفية استخدام الذكاء الاصطناعي لتحليل البيانات وكشف التسريبات داخل شبكات انترنت الاشياء
إطار الثقة الآمن والقائم على الذكاء الاصطناعي للحافة في انترنت الاشياء	2025	اقتراح إطار أمني ذكي يعتمد على التعلم الفيدرالي والذكاء الاصطناعي للتحكم بالوصول وكشف التسلل عند الحافة	حقق النظام دقة كشف بلغت 94% مع تقليل استهلاك الموارد وزمن الاستجابة	يوضح كيفية دمج الذكاء الاصطناعي والأمان لتحسين كشف التسريب وتعزيز ثقة انترنت الاشياء
نماذج التحكم في الوصول لإنترنت الأشياء مراجعة شاملة واتجاهات مستقبلية	2025	استعراض شامل لنماذج التحكم بالوصول في انترنت الأشياء وتحليل التوجهات المستقبلية لتعزيز الأمان والمرونة	اثبتت ان النماذج الحديثة القائمة على السمات والبلوك تشين أكثر اماناً لكنها تستهلك قدرات حسابية مرتفعة	تساعد في تحديد آلية تحكم آمنة ومرنة للبيانات ضمن نظام كشف التسريب وتعزز حماية الوصول في الشبكات الذكية
من السحابة الى الحافية: دمج انترنت الأشياء والذكاء الاصطناعي لأنظمة مستدامة وفعالة	2025	تبحث التكامل بين إنترنت الأشياء والحوسبة السحابية والطرفية لتحسين الاداء والاستدامة وتقليل زمن المعالجة	أظهرت ان الأنظمة الهجينة بين السحابة والطرف تحقق توازناً أفضل بين الأمان والكفاءة وسرعة الاستجابة	تفيد في ابراز أهمية المعالجة الطرفية لتحليل البيانات وكشف التسريب في الزمن الحقيقي دون ابطاء النظام
إطار أمني قائم على التعلم العميق لشبكات انترنت الأشياء: تقنيات ذكية هجينة لاكتشاف التهديدات	2025	تطوير نموذج أمني يعتمد على التعلم العميق والشبكات العصبية لاكتشاف التهديدات السيبرانية في انترنت الاشياء	حقق النموذج دقة عالية في الكشف وتقليل الإنذارات الخاطئة بفضل الدمج بين التعلم العميق والتطور الذكي	يدعم توظيف الذكاء الاصطناعي العميق للكشف الدقيق عن التسريبات وتحليل البيانات بفعالية اكبر

الكشف عن الهجمات السيبرانية في انترنت الأشياء باستخدام الذكاء الاصطناعي	2025	عرضت نظاماً ذكياً للكشف عن الهجمات في انترنت الأشياء باستخدام خوارزميات التعلم العميق	حقق النظام دقة عالية واستطاع التكيف مع أنواع متعددة من الهجمات وتقليل الإنذارات الكاذبة	تفيد في تصميم نموذج ذكي يكشف تسريب البيانات في الزمن الحقيقي ضمن البيئات الصناعية الذكية
الكشف عن التسلل ومنع تسريب البيانات باستخدام الذكاء الاصطناعي في أنظمة انترنت الاشياء	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 الاخطاء	تدعم تطوير نظام يعتمد على التحليل السلوكي للكشف المبكر عن التسريب باستخدام الذكاء الاصطناعي
الذكاء الاصطناعي لإنترنت الأشياء (AIOT): رؤية نحو أنظمة ذكية ومتصلة	2024	تناولت مفهوم الذكاء الاصطناعي لإنترنت الأشياء ودوره في الاستشعار، الحوسبة، الاتصال ضمن الأنظمة الحديثة	اشارت الى ان دمج الذكاء الاصطناعي يعزز التحليل في الزمن الحقيقي مع مواجهة تحديات الخصوصية والمعايير الموحدة	توضح أهمية دمج الذكاء الاصطناعي وانترنت الأشياء لتحسين سرعة ودقة كشف تسريب البيانات
تقنيات التعلم الآلي والعميق لاكتشاف الشذوذ في شبكات انترنت الأشياء: مراجعة شاملة	2024	مراجعة لأحدث أساليب الذكاء الاصطناعي في كشف الشذوذ والهجمات في شبكات انترنت الاشياء	بينت أن دمج خوارزميات التعلم الآلي والعميق يحقق دقة كشف تتجاوز 99% مع تحديات في الموارد	تساعد في اختيار خوارزميات فعالة للكشف المبكر عن التسريبات
استكشاف دور الذكاء الاصطناعي في أنظمة إنترنت الأشياء: دراسة تحليلية منهجية	2024	تحليل منهجي ل 81 دراسة توضح تطبيقات الذكاء الاصطناعي في التنبؤ، القرار وإدارة البيانات ضمن انترنت الاشياء	اشارت الى ان الذكاء الاصطناعي يعزز الأداء والأمان ويزيد قدرة الأنظمة على اتخاذ القرار الذاتي	تدعم فهم توظيف الذكاء الاصطناعي لتحسين دقة كشف التسريب وتعزيز امان شبكات انترنت الأشياء الذكية

تواجه انترنت الأشياء العديد من التحديات، نذكر منها:

4- التحديات [1]

1- تنوع الأجهزة والأنظمة:

تتميز أجهزة إنترنت الأشياء بتنوعها الكبير من حيث الأنواع، الشركات المصنعة، والأنظمة التشغيلية هذا التنوع يجعل من الصعب تطبيق حلول أمنية موحدة وفعّالة 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:

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

5- التكامل المعقد بين البروتوكولات:

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

6- التهديدات المتزايدة والهجمات المستهدفة:

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

7- التحديات في التحليل والتعلم الآلي:

تواجه تقنيات التحليل والتعلم الآلي صعوبة في التعامل مع البيانات غير المنظمة والضوضاء الناتجة 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 الحوسبة الطرفية:

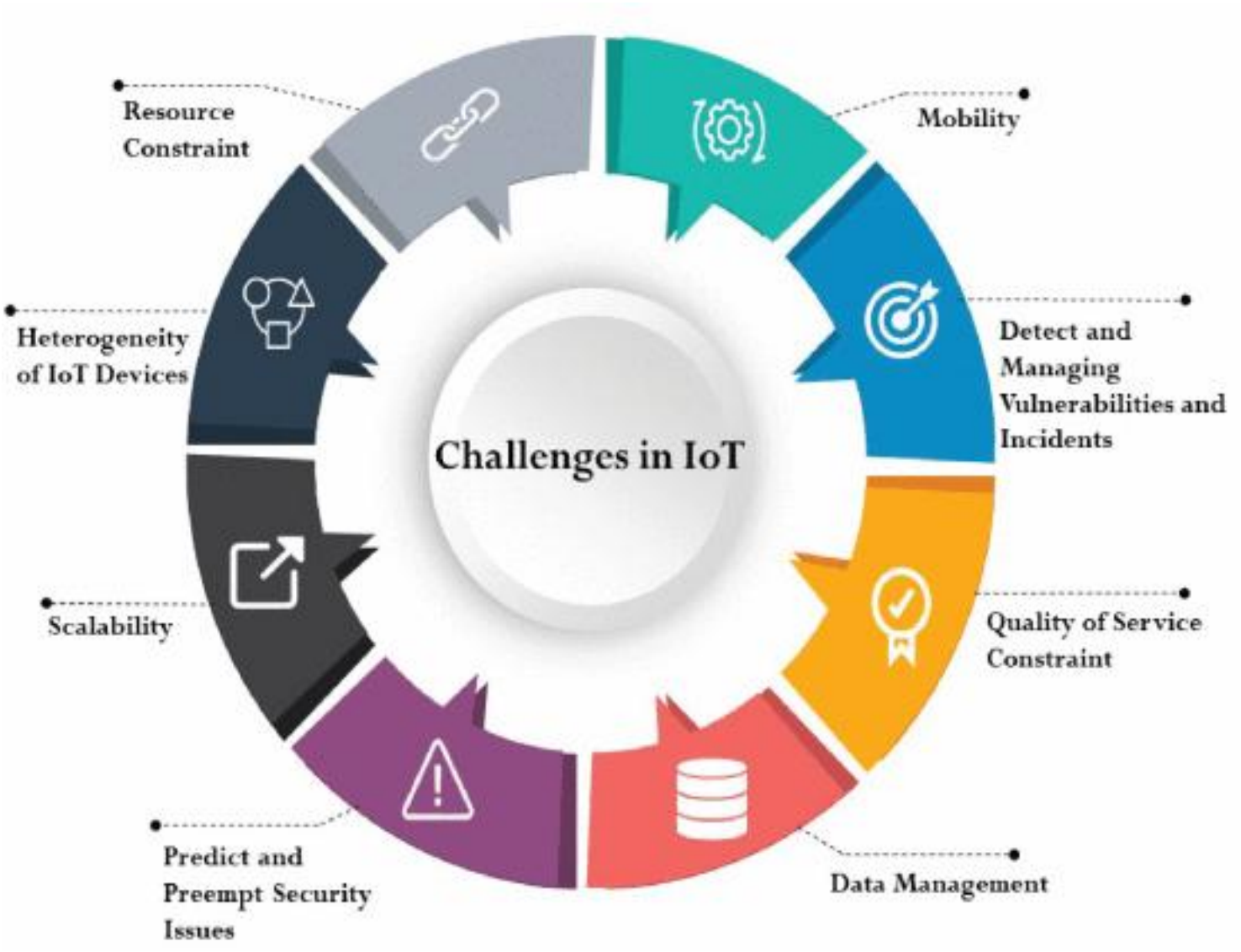
تواجه الحوسبة الطرفية صعوبة في تطبيق تقنيات الأمان المتقدمة بسبب محدودية الموارد، مما يعرض البيانات للتسريب أثناء المعالجة المحلية.

10- الامتثال للمعايير واللوائح:

تختلف 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:

الشكل1.1:


Challenges in IoT
Resource Constraint
Mobility
Heterogeneity of IoT Devices
Detect and Managing Vulnerabilities and Incidents
Scalability
Quality of Service Constraint
Predict and Preempt Security Issues
Data Management

نبين فيما يلي أبرز التطبيقات العملية للبحث:

5-التطبيقات العمليّة [2]

استخدام خوارزميات التعلم الآلي للكشف عن التسريبات:

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 تسريبات بيانات محتملة.

تطبيقات الكشف عن التسريبات في الصناعات:

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

أنظمة الكشف المبكر في المنازل الذكية:

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

تحليل البيانات الشبكية للكشف عن التسريبات:

تُستخدم تقنيات تحليل البيانات الشبكية لمراقبة حركة البيانات عبر الشبكات. من خلال تحليل هذه البيانات، يمكن اكتشاف أي تسريبات 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 بُعد. تُساعد هذه الأجهزة في الكشف عن أي تسريبات 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 التسريبات، مما يساهم في تحسين كفاءة الخدمات وتقليل الفاقد.

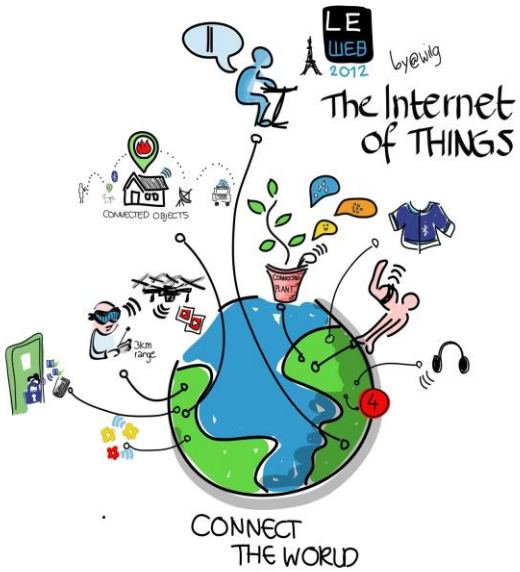
تحليل سلوك الأجهزة للكشف عن التسريبات:

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

مراقبة الشبكات للكشف عن التسريبات: تُستخدم تقنيات مراقبة الشبكات لمتابعة حركة البيانات عبر الشبكات. من خلال هذه المراقبة، يمكن اكتشاف أي تسريبات 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 يمكّنها من تبادل البيانات والمعلومات بصورة ذاتية دون تدخل مباشر من الإنسان وقد أحدث هذا المفهوم تحولًا جذريًا في أنماط التفاعل بين الإنسان والآلة، كما فتح آفاقًا واسعة لتطوير الخدمات في مجالات عديدة تشمل الصحة والصناعة والنقل والزراعة والمدن الذكية

اكاديمياً:

يمكن تعريف إنترنت الأشياء بأنه شبكة مترابطة 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 السُحب 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 بتخزين 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 المستفيدين من إنترنت الأشياء، إذ تُستخدم المستشعرات لربط خطوط الإنتاج ومراقبتها بشكل آني، الأمر الذي يتيح 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.

الرعاية الصحية والطب عن بُعد:

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 تهديدًا مباشرًا لخصوصية المرضى وسلامتهم.

المدن الذكية:

تُعد المدن الذكية نموذجًا متطورًا لتطبيقات إنترنت الأشياء، حيث يتم من خلالها إدارة البنية التحتية بشكل ذكي وفعال. فعلى سبيل المثال، تُستخدم المستشعرات في تنظيم حركة المرور وتخفيف 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 تظل عرضة لهجمات إلكترونية قد تؤدي إلى تعطيل الخدمات الحيوية.

الزراعة الذكية:

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

لنقل 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 لتبادل 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.

اكاديمياً:

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 أنماط تسريب البيانات:

التسريب المباشر (الاختراق الكامل للأنظمة):

يُعد هذا النمط من أكثر أشكال التسريب وضوحًا وخطورة، حيث يقوم المهاجم باختراق الجهاز أو الخادم والوصول إلى البيانات المخزنة داخله في هذه الحالة، يمكن نسخ الملفات الحساسة أو تعديلها أو حذفها بالكامل وغالبًا ما يُستهدف 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، ما يشكل خطرًا مباشرًا 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) للتوصل إلى معلومات حساسة يُعرف هذا النمط بـ "التسريب عبر القنوات الجانبية"، وهو يعتمد على مراقبة الأنماط السلوكية للتواصل بدلاً من محتوى البيانات نفسها فمثلًا، 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 تهديدًا 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، يعترض المهاجم البيانات أثناء انتقالها، سواء عبر شبكات الاتصال اللاسلكية أو عبر الإنترنت ويزداد هذا الخطر مع الاعتماد الواسع على شبكات 20لوايف 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 مواقع الأعطال أو طبيعة الإنتاج، وهي بيانات حساسة ذات قيمة استراتيجية.

التسريب الناتج عن الثغرات البرمجية والتصميمية:

غالبًا ما تحتوي الأجهزة الذكية على برمجيات وتطبيقات معقدة، وقد تُترك بعض الثغرات الأمنية دون معالجة نتيجة لغياب التحديثات الدورية أو استخدام إصدارات قديمة من البرمجيات في هذا النمط، يستغل المهاجم هذه الثغرات 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 البث المرئي والتحكم في إعداداته ويُعتبر هذا النمط من أكثر أشكال التسريب شيوعًا في بيئات إنترنت الأشياء، نظرًا لاعتماد كثير من الأجهزة على برمجيات غير مدعومة 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 مثلًا، 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 المتعمدة 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 البث المرئي المباشر والتحكم في الإعدادات.

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

استغلال بروتوكولات الاتصال الخفيفة: نتيجة ضعف آليات التحقق والمصادقة

المدن الذكية والبنية التحتية:

مثل: أنظمة إشارات المرور الذكية وأجهزة الاستشعار

تثبيت الأجهزة دون تغيير اعدادات المصنع الأمنية

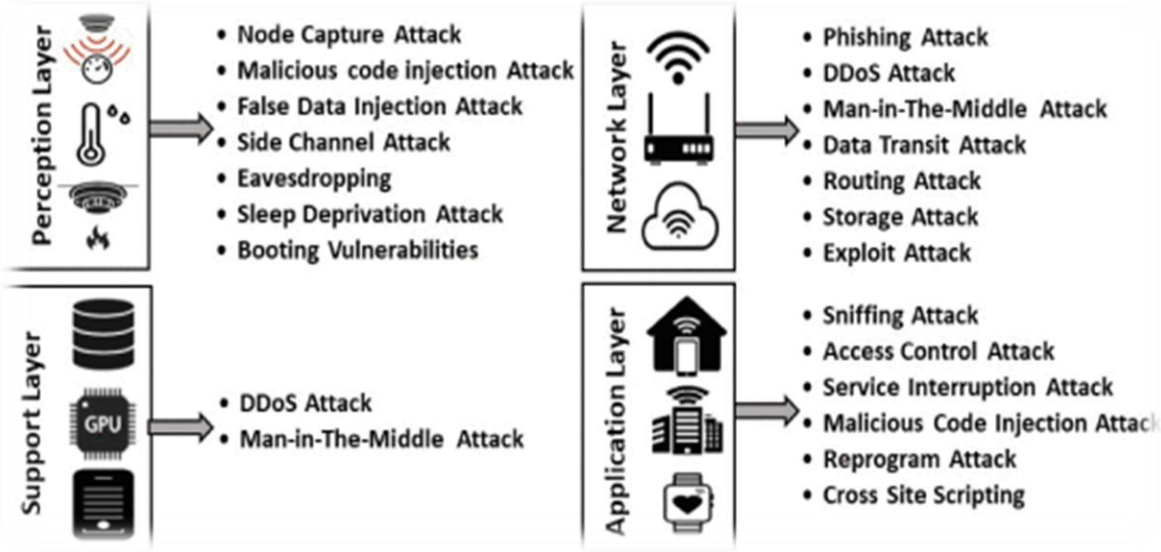
التصنيع والصناعة:

مثل: الروبوتات

السبب عدم تجزئة الشبكة والبروتوكولات القديمة المستخدمة

2.1.2 آثار تسريب البيانات :

تُعدُّ آثار تسريب البيانات في شبكات إنترنت الأشياء بالغة التعقيد والخطورة، حيث تمتد تداعياتها عبر مستويات متعددة، بدءًا من انتهاك الخصوصية الفردية بشكل غير مسبوق، نظرًا لطبيعة البيانات الحساسة التي تجمعها هذه الأجهزة من الحياة اليومية للأفراد، مما يهدد أمنهم الشخصي ويجعلهم عرضة للابتزاز والمراقبة ولا تقتصر الآثار على الجانب الشخصي فحسب، بل تمتد إلى خسائر اقتصادية كبرى تنجم عن الغرامات المالية الباهظة، وتراجع ثقة العملاء، وما يتبع ذلك من ضرر بالغ في السمعة المؤسسية علاوة على ذلك، فإن البيانات المسربة لا تقف عند حد الاستغلال المباشر، بل تُستغل كأداة خطيرة لتمكين هجمات إلكترونية أوسع نطاقًا وأكثر تطورًا، مثل الهجمات الإلكترونية المستهدفة، مما يهدد البنية التحتية الحيوية للمؤسسات والدول كما أن اختراق الأجهزة الطبية المتصلة يشكل خطرًا مباشرًا على حياة المرضى، في حين أن اختراق أنظمة المدن الذكية والصناعية يمكن أن يؤدي إلى شل الحركة المرورية، وتعطيل خطوط الإنتاج، والتسبب في كوارث مادية وبيئية وبالتالي، يصبح أمن إنترنت الأشياء مسألة مصيرية تتطلب نهجًا أمنيًا شاملاً يتجاوز الحلول التقليدية لضمان حماية البيانات، واستمرارية الخدمات، والحفاظ على الثقة في التحول الرقمي.



الشكل 2.1 يبين أبرز الهجمات السيبرانية على انترنت الاشياء

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

تنبع 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 بمرور الوقت

ثانيًا: 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

ثالثًا: التحديات التصميمية والمعمارية

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

لاعتماد على نماذج الشبكات التقليدية: يجعل إنترنت الأشياء أقل توافقًا 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 مركزي

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 خيارًا تكميليًا، بل أصبحت ضرورة حتمية لضمان استمرارية استخدام **إنترنت الأشياء** ضمن بيئة آمنة ومستدامة.

3.1.1 العواقب الرئيسية:

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 موضوعًا آخر حيث يمكن أن تؤدي خروقات الأمن في إنترنت الأشياء إلى تعطيل البنية التحتية الهامة تشمل المخاطر هجمات حجب الخدمة التي تؤثر سلبًا على قدرة التشغيل لهذه الأجهزة يمكن أن يؤدي الاختراق إلى دخول غير مصرح به إلى شبكات أنظمة إنترنت الأشياء، مما يعرض أمنها وسلامتها للخطر تُعد هذه السيناريوهات مقلقة بشكل خاص لأن أجهزة إنترنت الأشياء يمكن استخدامها لاختراق شبكات أوسع. قد يكون هذا الضعف كبيرًا في الأنظمة الحرجة التي تتطلب تشغيلًا مستمرًا، 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 الأمن إلى عواقب وخيمة في التطبيقات العسكرية أو أنظمة الرعاية الصحية، مثل الإصابات أو تعريض بيانات صحية سرية للخطر تشمل القضايا الأمنية النظام البيئي الكامل لإنترنت الأشياء وليس فقط أجهزة محددة في عام 2020، استهدفت هجمة 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 تهدد الحياة.

Major themes

Author(s)	Major themes
Meneghello, 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

3.2.1 نقاط الضعف في إنترنت الأشياء

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 الأمن والسلامة في الأنظمة الذكية.

النطاق والتنوع :

يتميز انتشار إنترنت الأشياء بنقاط ضعف كبيرة يمكن أن تعرض المستخدمين لمخاطر مختلفة يجعل النطاق الواسع والتنوع إنترنت الأشياء أكثر عرضة وتكنولوجيا في إنترنت الأشياء أكثر عرضة للخطر تُعد (WSNs) لخروقات الأمن مع هذه الخصائص، يصبح دمج شبكات الاستشعار اللاسلكية إنترنت الأشياء منصات محددة تستخدم في مجالات حرجة مثل التطبيقات العسكرية أو أنظمة الرعاية الصحية، مما يجعلها بيئة مثالية للمخاطر الأمنية وفقًا 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 :

ثانيًا، لا توجد معايير محددة عند تنفيذ وإدارة إنترنت الأشياء، مما يجعلها عرضة لخروقات الأمن. 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

المقدمة 2.1

تُعد بيئة العمل الإطار الذي تُنفّذ ضمنه الدراسات البحثية والتجارب العملية، حيث تحدد هذه البيئة الموارد البرمجية وأدوات التحليل اللازمة 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

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

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

الخوارزمية	المزايا	المساوئ
XGBoost	دقة عالية سريع ممتاز 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**باستخدام محاكي الشبكات **NS-3** وخوارزمية التعلم الآلي XGBoost**لما** توفره من توافقية عالية واستقرار وثبات يتطلبه هذا النوع من الأبحاث، إذ يتيح **Ubuntu** بيئة تطويرية متقدمة داعمة لمحاكيات **الشبكات**، بينما يوفر **VMware**عزلاً منهجياً يضمن إعادة انتاج التجارب بدقة عبر نقاط الاسترجاع، ويعد NS-3 الخيار الأمثل لمحاكاة **انظمة** وأنترنت الأشياء بفضل دقته و واقعيته في توليد حركة مرور قابلة للتحليل، اما استخدام **XGBoost** فجاء استناداً الى كفاءته العالية في **مهام** الكشف عن الشذوذ والتسريب وقدرته على التعامل مع البيانات الناتجة عن المحاكاة بكفاءة

وبذلك تلبي هذه البيئة متطلبات المشروع البحثية بأعلى مستوى من الدقة والموثوقية.

2.4 المراجع التقنية الرسمية لبيئة العمل والأدوات المستخدمة:

اعداد منصة العمل الافتراضية (VMware workstation):

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

2– تثبيت البرنامج على الجهاز المضيف: next →Accept →Install →Finish

3– فتح التطبيق واختيار: Create new virtual machine

4– تحديد ملف تثبيت النظام (ubuntu ISO)

5– اختيار نوع النظام Linux →Ubuntu 64-bit

6– تخصيص موارد الجهاز الافتراضي:

يفضّل RAM 4-8 GB

عدد الأنوية: **2–4**

نوع التخزين: Split

حجم القرص 40 GB فما فوق

تثبيت نظام ubuntu داخل VMware

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

ومن ثم متابعة التثبيت مع إعادة تشغيلا 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:

تثبيت 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
```

تثبيت المتطلبات:

```
sudo apt install gcc g++ python3 python3-pip qt5-default mercurial \
cmake libc6-dev libc6-dev-i386 gdb valgrind \
gsl-bin libgsl-dev libsqlite3-dev python3-setuptools \
libxml2 libxml2-dev -y
```

بناء NS-3 :

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

اختبار نجاح التثبيت:

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

3-تنصيب مكتبات الذكاء الصنعي Python+XGBoost :

تثبيت بيئة Python الافتراضية

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

تثبيت 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 سكربتات NS-3 لتصدير بيانات الشبكة

اثناء كتابة السيناريو يتم تفعيل التتبع:

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

تشغيل سيناريو محاكاة المنزل الذكي:

```
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 نحتاجها لبيئة العمل، ثم تشغيل محاكي وبناء سيناريوهات شبكات انترنت 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 تمت مقارنة نتائجها مع القيم المنشورة في الأبحاث الاصلية.

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**

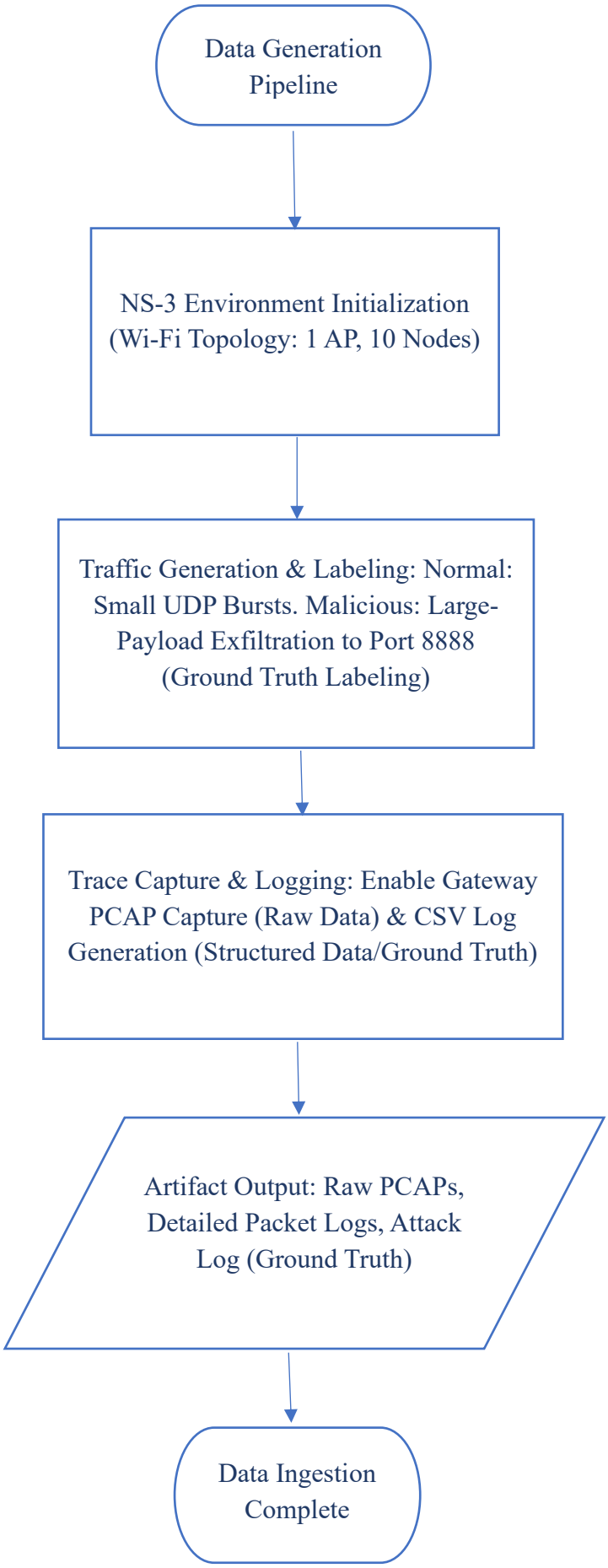
خوارزمية موثوقة ومستخدمة على نطاق واسع في أبحاث كشف الشذوذ كما ورد سابقا في الدراسة المرجعية فإن تطابق الأداء مع النتائج المنشورة يعد دليلاً علميا كافياً على ان الخوارزمية والبيئة تعملان بشكل صحيح وموثوق.

```
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:
```

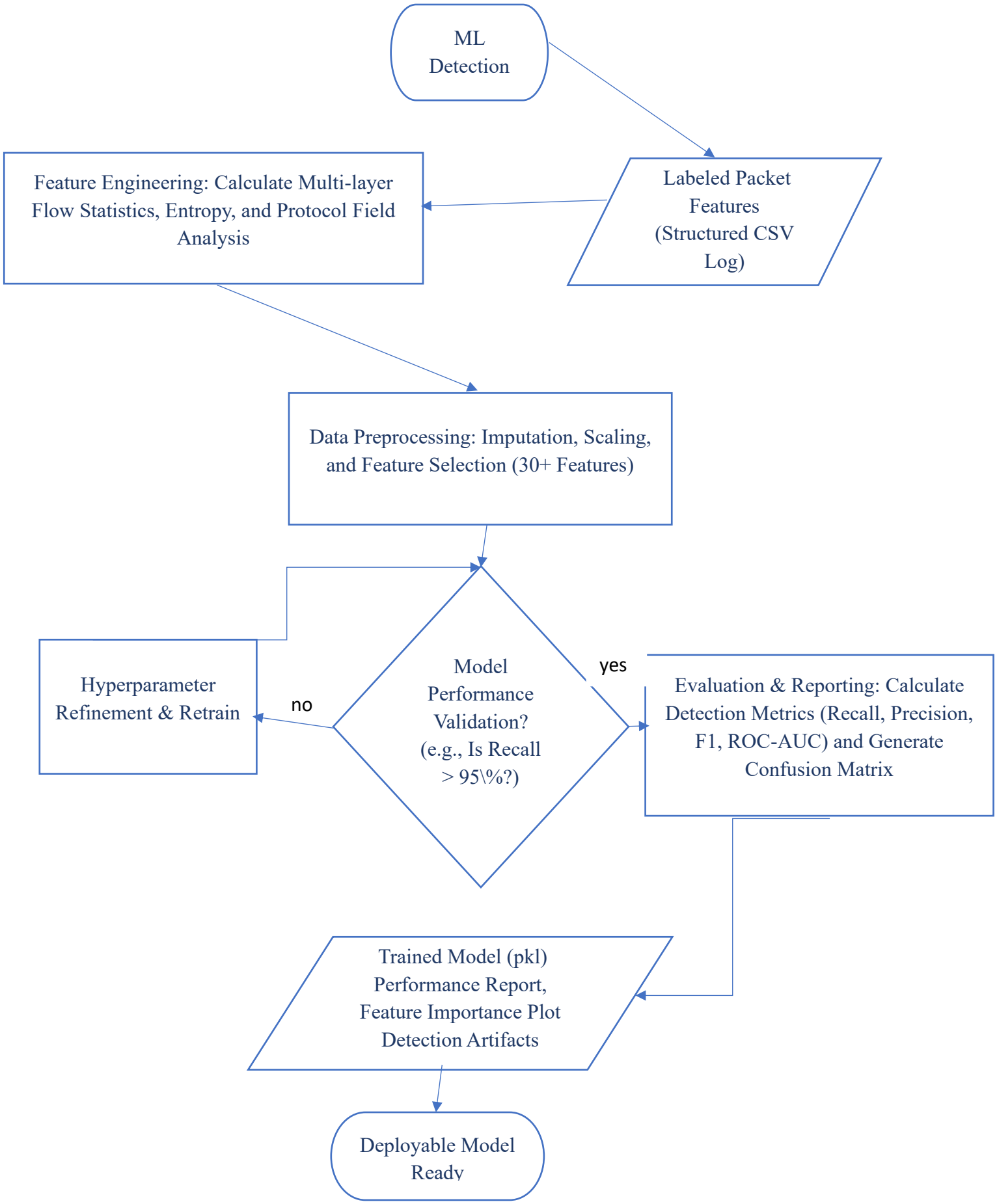
الصورة 3.1 نتائج اختبار بيئة العمل

فيما سبق نتائج لتقييم 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 يؤكد فعالية الميزات المختارة وبنية النموذج.

يوضح هذا المخطط: التسلسل المنهجي لتوليد مجموعة بيانات شبكية.



الشكل 3.2 لمحاكاة



الشكل 3.3 كشف التسريب

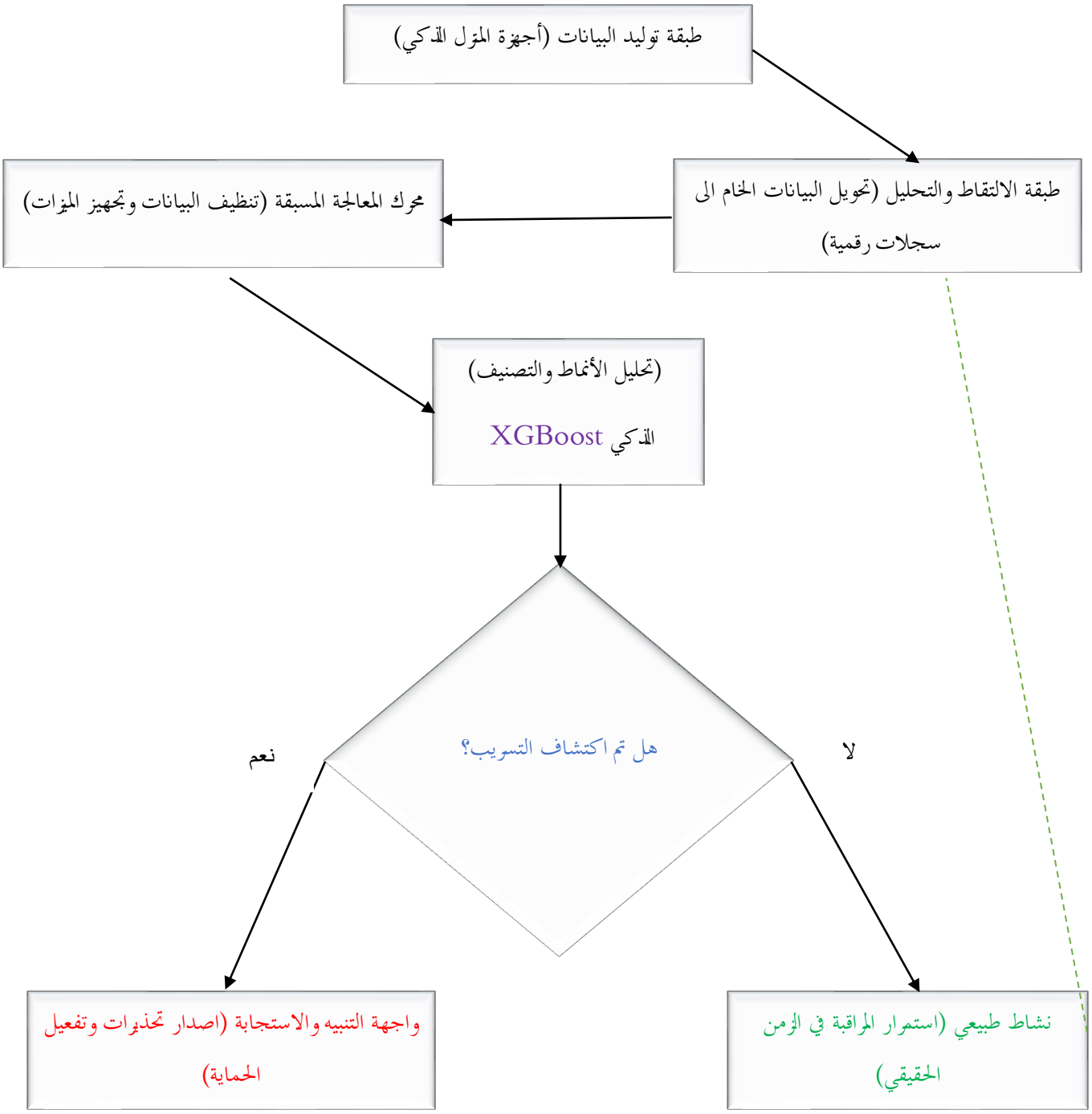
الفصل الثالث

الحل المقترح

3.1 مقدمة الفصل:

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

3.2 المخطط الصندوقي للحل المقترح:



* **(Data Generation Layer) طبقة توليد البيانات:**

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

* **(Collection Layer) طبقة الالتقاط والتحليل:**

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

* **(Preprocessing Unit) محرك المعالجة المسبقة:**

تنظيف البيانات وتجهيز الميزات البرمجية، اي [التعامل مع القيم المفقودة او السجلات المتكررة الناتجة 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 اخر 60 ثانية.

* **(XGBoost Model) نموذج التصنيف الذكي:**

وهو القلب البرمجي الذي يقوم بتحليل الأنماط واتخاذ قرار التصنيف:

* **(Response Interface) واجهة التنبيه والاستجابة:**

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:**

التغيرات 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 .

(Model Implementation) XGBoost البناء والتدريب:

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 و20% للاختبار:

(Hyperparameters Tuning) ضبط المعاملات الفائقة:

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

"دالة الخسارة: استخدام دوال متطورة لتقليل نسبة **"الإنذارات الكاذبة"**

وهو أمر حيوي لراحة مستخدم المنزل الذكي.

(Detection & Decision Making) آلية الكشف واتخاذ القرا:

بمجرد تدفق البيانات من أي جهاز .(Gateway Shield) يعمل النظام المقترح 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:

(Accuracy): الدقة

قدرة النظام على التمييز الصحيح بين البيانات السليمة والمخترقة [والذي ظهرت نسبته في بيئة العمل لدينا94%]

(Latency) السرعة:

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

(Confusion Matrix) مصفوفة الارتباك:

لتحليل قدرة النظام على حصر كافة حالات التسريب دون أخطاء .

خلاصة الفصل

يقدم هذا الحل المقترح نموذجاً متطوراً يجمع بين بساطة المحاكاة المنزلية وقوة الذكاء الاصطناعي. إن استخدام

XGBoost

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

الفصل الربع

المقارنات والتحاليل

بعد البحث المعمّق في مجال إنترنت الأشياء، ومراجعةٍ دقيقةٍ للدراسات المرجعية، وبناء نموذج عمل عملي، إنشاء نموذج محاكاة لمنزل ذكي وتدريب خوارزمية الذكاء الصنعي لكشف التسريب وتصنيفه ، توصّلنا في هذا الفصل إلى مقارنات وتحاليل تُبرز ما هو أنسب لبيئات إنترنت الأشياء محدودة الموارد لا يهدف هذا الفصل إلى إعادة سرد ما سبق، بل إلى تقديم قيمة مضافة تركّز على المقارنة النقدية بين الدراسة النظرية من جهة، وبين بيئات وأدوات التنفيذ من جهةٍ أخرى، ثم ربط ذلك بالمشاكل التي تمّت مواجهتها فعلاً والدروس المستفادة منها.

4.2 تحليل البيانات التجريبية:

تم استخدام مجموعة بيانات تحاكي حركة المرور في شبكة منزل ذكي، مع التركيز على الأنماط الشاذة التي تشير الى تسريب البيانات

تصنيف البيانات: تم تصنيف الحزم الى (طبيعية/مشبوهة) بناء على بروتوكولات **UDP/MQTT المستخدمة في بيئة العمل.**

المعالجة الأولية: تم تنظيف البيانات من الضوضاء الناتجة عن تنوع الأجهزة، وهو ما عالج التحدي التقني المذكور في الفصل الأول.

أداء خوارزمية الذكاء الاصطناعي: بناءً على اختيار الخوارزميات الأنسب مثل: **XGBoost :**

(Detection Accuracy Analysis) تحليل دقة الكشف :

حقق الإطار المقترح دقة كشف عالية بلغت94%

التعامل مع الشذوذ: أظهرت النتائج قدرة النظام على تصنيف الأنماط الضارة وتحليل حركة البيانات بدقة عالية، مما ساهم في تقليل الإنذارات الكاذبة.

(Real-time Efficiency)كفاءة النظام في الزمن الحقيقي:

يعتبر الكشف في الزمن الحقيقي الركيزة الأساسية لهذا البحث

النظام يحافظ على سرعة معالجة عالية حتى مع زيادة تدفق البيانات.

(Discussion) مناقشة النتائج:

أثبتت النتائج أن دمج الذكاء الاصطناعي مع تقنيات إنترنت الأشياء يعزز من أمان الشبكات الذكية نجح النظام في كشف أنماط التسريب المباشر وغير المباشر (عبر القنوات الجانبية) التي تم تفصيلها في الفصل الأول كما أن النظام المقترح يساهم في الامتثال للمواصفات الدولية لحماية البيانات عبر توفير سجلات غير قابلة للتلاعب (في حال دمج البلوك تشين مستقبلاً).

السلوك	الفترة الزمنية	حجم الحزمة	الجهاز
كاميرا ذكية	2s	512	الجهاز 1
حساس حرارة	5s	256	الجهاز 2
مساعد صوتي	1s	1024	الجهاز 3
تلفاز ذكي	0.5s	4096	الجهاز 4
نظام امني	4s	3500	الجهاز 5

الأجهزة المخترقة (9و10):

الجهاز 9: يسرب بيانات حساسة (بريد الكتروني، بطاقات أتمان)

الجاهز 10: يفحص المنافذ

الجدول 4.1 بيانات أجهزة محاكي المنزل الذكي

التقييم	الفعلي	المستهدف	المقياس
اعلى قليلا	%94.53	%92-88	*Accuracy*
ممتاز	%100	%90-85	*Precision*
ضعيف جدا	%58.82	%93-87	*Recall*
اقل من المتوقع	74.07%	86-91%	*F1-score*

الجدول 4.2 نتائج قياس خوارزمية الذكاء الاصطناعي

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 يقلّل الضجيج ويرفع موثوقية النتائج

يتضح من خلال هذا الفصل أنّ معالجة تسريب البيانات في بيئات إنترنت الأشياء لا يمكن أن تُبنى على جانب واحد، بل تتطلّب رؤية شمولية تجمع بين الأسس النظرية العميقة والتنفيذ العملي الميداني فقد بيّنت المراجعة العلمية أنّ المقاربات التقليدية كالتشفير، رغم أهميتها، تعجز عن كشف القنوات الجانبية والأنماط السلوكية المموّهة، الأمر الذي يستدعي دمجها مع التحليل السلوكي ونماذج التعلّم الخفيف وفي الوقت نفسه، أكدت التجارب العملية التي أنجزناها أنّ هذا الدمج قادر على تحقيق توازن بين دقّة الكشف وانخفاض الكلفة التشغيلية، مع المحافظة على زمن استجابة مقبول وملاءمة لقيود الموارد كما أظهرت التجربة أنّ التحديات المتعلقة بالتوافقية والضجيج يمكن تجاوزها عبر ضبط بيئة الاختبار وإعادة بناء بعض المكوّنات البرمجية وعليه نستنتج أنّ النهج الأمثل هو نهج تكاملي نقدي يزاوج بين النظرية والتطبيق، ويوفّر حلاً عملياً مرناً وقابلاً للتوسّع في مواجهة التهديدات المتصاعدة في فضاء إنترنت الأشياء.

النتائج

أن الطبيعة المعقدة والمنتشرة لشبكات إنترنت الأشياء جعلتها هدفاً جاذباً للهجمات الإلكترونية، وخاصة عمليات تسريب البيانات. وقد تبيّن أن أنماط هذا التسريب لا تقتصر على الاختراق المباشر فحسب، بل تمتد إلى قنوات خفية مثل تحليل البيانات الوصفية التي تتجاوز آليات الحماية التقليدية كالتشفير. كما كشفت الدراسة عن التداعيات الخطيرة المترتبة على هذه التسريبات، والتي تهدد بشكل مباشر خصوصية الأفراد وسلامتهم، وتعرّض البنى 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 بيئة عمل عملية متكامل :

تمكّن هذا المشروع من بناء بيئة تجريبية تشمل نموذج محاكاة لمنزل ذكي وتدريب خوارزمية الذكاء الصنعي، بالاعتماد على **NS-3&XGBoost** لم تكن مجرد منصة اختيار بل وفرت نموذجاً واقعياً يحاكي ظروف تسريب البيانات في الشبكات مما جعل النتائج أكثر دقة وواقعية وقابلة للتنفيذ.

إثبات إمكانية التسريب عبر عدة قنوات :

أظهرت التجارب العملية أنّ تسريب البيانات يمكن أن يحدث بعدة أنماط، منها التسريب المباشر عبر اعتراض الحزم، والتسريب عبر القنوات الجانبية بتحليل البيانات الوصفية، إضافةً إلى التسريب الناتج عن ثغرات برمجية أو ضعف في بروتوكولات الاتصال هذا يعكس أن الاعتماد على التشفير وحده غير كافٍ، وأن الحلول يجب أن تكون متعددة الطبقات.

تحقيق كشف أولي فعّال باستخدام التحليل السلوكي :

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

إمكانية الدمج بين المقاربات التقليدية والحديثة:

أظهر البحث أنّ الجمع بين التشفير القوي من جهة، وخوارزميات التعلم الآلي الخفيف والتحليل السلوكي من جهة أخرى، يوفر توازناً عملياً بين الدقة والكلفة التشغيلية. وقد أثبتت التجارب أنّ هذا الدمج يؤدي إلى رفع معدل الكشف مع بقاء استهلاك الموارد ضمن الحدود المقبولة، وهو ما يفتح المجال لتطبيقه 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 لتوسّعها

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 التكامليّة 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 أثبت فعاليته في بيئة محددة، إلا أن تطويره لاحقاً يمكن أن يشمل:

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

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

بناء واجهة استخدام تفاعلية تعرض التنبيهات وتُسهّل عملية المراقبة

إضافة قدرات الحوسبة الطرفية **والبلوك تشين** لرفع الكفاءة وضمان الشفافية

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

المدن الذكية وحماية البنى التحتية:

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

"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 توسعاً ملحوظاً في استخدام أجهزة إنترنت الأشياء، سواء عبر الأجهزة القابلة للارتداء أو أنظمة مراقبة المرضى عن بُعد غير أن البيانات الطبية تُعد من أكثر البيانات حساسية وخطورة عند تسريبها مستقبلاً، يمكن تكييف النموذج ليُطبق في أنظمة الصحة الذكية، بحيث يراقب تدفق البيانات الطبية ويكشف عن أي محاولة تسريب في الزمن الحقيقي هذا سيُسهم 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 الواعدة في الأبحاث الأكاديمية إدماج تقنية البلوك تشين في بيئات إنترنت الأشياء فهي تتيح بناء سجل موزّع وآمن للحزم والبيانات، مما يمنع التلاعب أو التعديل غير المصرح به مستقبلاً، يمكن تعزيز النظام المقترح 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 المقترح ويجعل 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]