

جامعة ميداو شن
كلية علوم الحاسوب

مراجعة الأدبيات حول الأمن السيبراني في إنترنت الأشياء الطبية
(IoMT)

تقييم فعالية خوارزميات التعلم الآلي في كشف الاختراق ضمن شبكات
إنترنت الأشياء الطبية

اسم الطالب : عبدالله الفيفي

اسم المادة : منهجية البحث في علوم الحاسوب

اسم المحاضر : د. محمد عنبر

جدول المحتويات

1. المقدمة
2. ملخص الأوراق البحثية
3. التحليل النقدي
4. الروابط والتضاريات
5. مصفوفة التوليف (جدول ملخص الأبحاث)
6. المناقشة
7. الخاتمة
8. المراجع

1- المقدمة

يهدف هذا البحث إلى دراسة دور تقنيات التعلم الآلي في تعزيز أمن شبكات إنترنت الأشياء الطبية، وتحليل أهم الدراسات العلمية التي تناولت هذا الموضوع خلال السنوات الأخيرة.

فقد شهدت تقنيات إنترنت الأشياء الطبية (Internet of Medical Things - IoMT) تطورًا كبيرًا خلال السنوات الأخيرة، حيث أصبحت الأجهزة الطبية الذكية مثل أجهزة مراقبة القلب وأجهزة قياس السكر وأجهزة الاستشعار القابلة للارتداء قادرة على الاتصال بالإنترنت وتبادل البيانات مع الأنظمة الصحية المختلفة. وقد ساهم هذا التطور في تحسين جودة الرعاية الصحية من خلال تمكين الأطباء من مراقبة حالة المرضى بشكل مستمر وتوفير خدمات صحية أكثر كفاءة.

ومع ذلك، فإن هذا التوسع في استخدام الأجهزة المتصلة بالإنترنت أدى إلى ظهور العديد من التحديات الأمنية. فشيكات إنترنت الأشياء الطبية قد تكون عرضة لمجموعة واسعة من الهجمات السيبرانية مثل هجمات حجب الخدمة (DDoS) أو هجمات التلاعب بالبيانات أو اختراق الأنظمة الطبية الحساسة. وقد يؤدي نجاح هذه الهجمات إلى تعريض بيانات المرضى للخطر أو التأثير على سلامة الأجهزة الطبية.

لذلك أصبح الأمن السيبراني أحد أهم الجوانب التي يجب أخذها في الاعتبار عند تصميم أنظمة إنترنت الأشياء الطبية. وفي هذا السياق، بدأت العديد من الدراسات في استخدام تقنيات التعلم الآلي والتعلم العميق لتحسين قدرة الأنظمة على اكتشاف الهجمات السيبرانية والتعامل معها بشكل فعال. حيث يمكن لهذه التقنيات تحليل كميات كبيرة من البيانات واكتشاف الأنماط غير الطبيعية التي قد تشير إلى وجود اختراق أو نشاط ضار داخل الشبكة.

يهدف هذا البحث إلى مراجعة مجموعة من الدراسات العلمية التي تناولت استخدام خوارزميات التعلم الآلي في كشف الهجمات داخل شبكات إنترنت الأشياء الطبية، بالإضافة إلى تحليل نقاط القوة والضعف في هذه الدراسات ومناقشة أوجه التشابه والاختلاف بينها.

2- ملخص الأوراق البحثية

• الورقة الأولى: (Sharifi & Goli-Bidgoli, 2022)

اقترحت هذه الدراسة منصة تسمى ++FogLearn تعتمد على الحوسبة الضبابية (Fog Computing) من أجل تحسين عملية اكتشاف الهجمات في شبكات إنترنت الأشياء. تعتمد الفكرة الأساسية على معالجة البيانات بالقرب من مصدرها بدلاً من إرسالها إلى خوادم مركزية بعيدة. ويساعد هذا الأسلوب في تقليل زمن الاستجابة وتحسين سرعة اكتشاف التهديدات الأمنية. وقد أظهرت نتائج الدراسة أن استخدام الحوسبة الضبابية يمكن أن يحسن أداء أنظمة كشف الاختراق بشكل ملحوظ.

• الورقة الثانية: (Dey et al., 2022)

ركزت هذه الدراسة على استخدام خوارزميات اختيار الميزات (Feature Selection) المعتمدة على أساليب Meta-Heuristic من أجل تحسين أداء نماذج التعلم الآلي. ويهدف هذا الأسلوب إلى تقليل حجم البيانات المستخدمة في التدريب من خلال اختيار الخصائص الأكثر أهمية فقط. وقد أظهرت نتائج الدراسة أن تقليل أبعاد البيانات يساعد في تحسين دقة النماذج وتسريع عملية اكتشاف الهجمات.

• الورقة الثالثة: (Yang et al., 2023)

تناولت هذه الدراسة مفهوم التعلم الفيدرالي (Federated Learning) كحل لتعزيز الخصوصية في أنظمة إنترنت الأشياء. يسمح هذا الأسلوب بتدريب النماذج على الأجهزة المحلية دون الحاجة إلى إرسال البيانات الحساسة إلى خادم مركزي. وبهذه الطريقة يمكن حماية بيانات المرضى مع الحفاظ على كفاءة النماذج المستخدمة في كشف الاختراق.

• الورقة الرابعة: (Ma et al., 2023)

اقترحت هذه الدراسة استخدام تقنية التعلم قليلة اللقطات (Few-Shot Learning) للكشف عن الهجمات السيبرانية في الحالات التي تكون فيها بيانات التدريب محدودة. ويعتمد هذا النموذج على شبكات Meta Residual Networks القادرة على التعلم من عدد صغير من الأمثلة. وأظهرت النتائج أن هذا الأسلوب يمكن أن يكون فعالاً في اكتشاف الهجمات الجديدة أو غير المعروفة.

• الورقة الخامسة: (Vu et al., 2020)

ركزت هذه الدراسة على استخدام التعلم بالنقل (Transfer Learning) لتحسين أمن شبكات إنترنت الأشياء. يعتمد هذا الأسلوب على استخدام نماذج مدربة مسبقاً وتكييفها مع بيانات جديدة. ويساعد هذا النهج في تقليل وقت التدريب وتحسين كفاءة النظام خاصة في الأجهزة ذات الموارد المحدودة.

• الورقة السادسة: (Türkoğlu et al., 2022)

هدفت هذه الدراسة إلى تحسين أداء أنظمة كشف الهجمات من خلال ضبط المعلمات الفائقة (Hyperparameters) في نماذج التعلم الآلي. وقد أظهرت النتائج أن اختيار المعلمات المناسبة يمكن أن يساعد في تحقيق توازن جيد بين سرعة النظام ودقة الكشف عن الهجمات.

3- التحليل النقدي

تشير الدراسات السابقة إلى أن تقنيات التعلم الآلي أصبحت أداة فعالة في تحسين أمن شبكات إنترنت الأشياء الطبية. حيث يمكن لهذه التقنيات تحليل البيانات الضخمة واكتشاف الأنماط غير الطبيعية التي قد تشير إلى وجود هجمات سيبرانية. كما تساعد هذه التقنيات في تحسين سرعة اكتشاف الهجمات مقارنة بالطرق التقليدية.

ومن خلال مراجعة هذه الدراسات يمكن ملاحظة وجود اتجاه واضح نحو استخدام الحلول الموزعة مثل الحوسبة الضبابية والتعلم الفيدرالي. تساعد هذه الحلول في تقليل زمن الاستجابة وتحسين حماية خصوصية البيانات، وهو أمر مهم جدًا في الأنظمة الطبية التي تتعامل مع بيانات حساسة.

ومع ذلك، لا تزال هناك بعض التحديات التي تواجه هذه الأنظمة. فمعظم الدراسات تعتمد على بيانات محاكاة أو مجموعات بيانات محدودة، ولا يتم اختبار النماذج المقترحة على أجهزة طبية حقيقية. كما أن بعض الخوارزميات قد تتطلب موارد حسابية كبيرة، مما قد يجعل تطبيقها على الأجهزة الطبية الصغيرة أمرًا صعبًا.

من وجهة نظر الباحث، فإن استخدام تقنيات التعلم الآلي في أنظمة إنترنت الأشياء الطبية يمثل خطوة مهمة نحو تحسين مستوى الأمن السيبراني، إلا أن نجاح هذه الحلول يعتمد بشكل كبير على جودة البيانات المستخدمة في تدريب النماذج، بالإضافة إلى ضرورة اختبار هذه الأنظمة في بيئات تشغيل حقيقية.

4- الروابط والتضاربات

- **الروابط:** جميع الأوراق تتفق على هشاشة بروتوكولات التوجيه المعتمدة في إنترنت الأشياء وهناك حاجة ملحة لنظام تشخيص ذكي وأنظمة كشف شبكية ذكية. لذا يتفق الباحثون على أن "التعلم الآلي" هو الطريقة الأكثر فعالية لإدارة كميات كبيرة من البيانات.
- **التضاربات:** هناك تضاربات حول كيفية إدارة هذه البيانات؛ بعض الدراسات تدعو إلى "التحكم المركزي" لإدارة المراقبة بشكل شامل، بينما يؤكد آخرون أن "التدريب الموزع" (أي التعلم الفيدرالي) هو الحل الوحيد القابل للتوسع والقابل لحماية الخصوصية.

5- مصفوفة التوليف لمراجعة الأدبيات

يوضح الجدول التالي ملخصاً لأهم الدراسات التي تم تحليلها في هذه المراجعة، مع بيان المنهجيات المستخدمة والنتائج الرئيسية لكل دراسة .

الدراسة	المؤلفون	السنة	المنهجية	النتائج الرئيسية	القيود والضعف
FogLearn++	Sharifi et al.	2022	تعلم آلي في طبقة الضباب	تحسين سرعة الكشف عن الهجمات	مقتصر على طبقة الضباب
آلية اختيار الميزات	Dey et al.	2022	خوارزميات-Meta Heuristic	زيادة دقة النماذج	تكلفة حسابية عالية للاختيار
التعلم الفيدرالي	Yang et al.	2023	تدريب موزع ومحلي	حماية خصوصية البيانات	عبء المزامنة بين العقد
التعلم بلبقات قليلة	Ma et al.	2023	Meta Residual Networks	اكتشاف الهجمات الجديدة	احتمالية الإفراط في الملاءمة
التعلم بالنقل	Vu et al.	2020	نماذج مدربة مسبقاً	تقليل تكلفة التدريب	الاعتماد على جودة بيانات المصدر
تحسين المعلمات	Türkoğlu et al.	2022	تحسين Hyperparameters	توازن مثالي بين السرعة والدقة	مجهود حسابي كبير للتحسين

6- المناقشة

يمكن القول إن دمج تقنيات الذكاء الاصطناعي مع أنظمة إنترنت الأشياء الطبية يمثل اتجاهًا واعدًا لتحسين الأمن السيبراني في القطاع الصحي. فمع تزايد عدد الأجهزة المتصلة بالشبكات، تصبح الحاجة إلى أنظمة ذكية قادرة على اكتشاف الهجمات بسرعة وكفاءة أكثر أهمية من أي وقت مضى.

وبالمقارنة بين دراسة Yang et al. (2023) ودراسة Ma et al. (2023)، يمكن ملاحظة أن التعلم الفيدرالي يركز بشكل أكبر على حماية الخصوصية، بينما يركز التعلم قليل اللقطات على تحسين قدرة النظام على اكتشاف الهجمات الجديدة حتى مع توفر بيانات تدريب محدودة.

كما تشير بعض الدراسات الحديثة إلى أن استخدام تقنيات التعلم الآلي والتعلم العميق يمكن أن يعزز بشكل كبير من قدرة أنظمة إنترنت الأشياء على اكتشاف الهجمات السيبرانية وتحليل البيانات الضخمة (Al-Garadi et al., 2024).

7- الخاتمة

خلصت هذه الدراسة إلى أن تقنيات التعلم الآلي تلعب دورًا مهمًا في تعزيز أمن شبكات إنترنت الأشياء الطبية. وقد أظهرت العديد من الدراسات أن هذه التقنيات قادرة على تحسين قدرة الأنظمة على اكتشاف الهجمات السيبرانية وتحليل البيانات بشكل فعال.

ومع ذلك، لا تزال هناك حاجة إلى إجراء المزيد من الأبحاث التي تركز على تطبيق هذه التقنيات في بيئات تشغيل حقيقية، إضافة إلى تطوير خوارزميات أكثر كفاءة يمكن تشغيلها على الأجهزة الطبية ذات الموارد المحدودة. كما يجب التركيز على تطوير حلول تحقق التوازن بين مستوى الأمان وحماية خصوصية المرضى.

وبناءً على ما تم عرضه في هذه الدراسة، يمكن القول إن استخدام تقنيات التعلم الآلي في أنظمة إنترنت الأشياء الطبية يمثل اتجاهًا واعدًا، إلا أن نجاح هذه الحلول يتطلب إجراء المزيد من التجارب العملية على بيانات حقيقية لضمان فعاليتها في البيئات الطبية الواقعية.

8- المراجع

- Adhikary, K., et al. (2020). Hybrid Algorithm to Detect DDoS Attacks in VANETs.
- Sharifi, A., & Goli-Bidgoli, S. (2022). FogLearn++: A new platform for fog layer IoT attack detection.
- Yang, R., et al. (2023). Dependable Federated Learning for IoT Intrusion Detection.
- Dey, N., et al. (2022). Feature Selection Techniques for Cybersecurity Applications.
- Ma, X., et al. (2023). Few-Shot Learning for Network Intrusion Detection.
- Vu, L., et al. (2020). Transfer Learning for IoT Security.
- Türkoğlu, M., et al. (2022). Hyperparameter Optimization for DDoS Detection.
- Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2024). A Survey of Machine Learning and Deep Learning Techniques for IoT Security.