

## نقد مقال علمي

تحليل مصطلحات الدراسة وتحليل الدراسات السابقة

Prepared by

ALI MMADI, PhD student - Midocean University



الزوي، ج. أ.، نايار، أ.، وكومار، أ. (2024) تعزيز الأمن السيبراني: مراجعة شاملة :المقالة المحللة  
Big Data (2024) لتقنيات الكشف المدفوعة بالذكاء الاصطناعي مجلة البيانات الكبيرة، 11(1)، 1-25.

## هدف العرض التقديمي

تركز هذه المهمة 2 على التحليل النقدي للمقال المعنون: 'تعزيز الأمن السيبراني: مراجعة شاملة للتقنيات المبنية على الذكاء الاصطناعي'، الذي نُشر في مجلة البيانات الضخمة (2024). في هذه المهمة 2، الهدف هو استعراض عنصرين أساسيين: شروط الدراسة والدراسات السابقة المقتبسة في المقال.

## 1

## تحليل شروط الدراسة

## □ نقاط إيجابية:

## اتساق المصطلحات

- ✓ المصطلحات المستخدمة متوافقة تمامًا مع المجال المستهدف: الأمن السيبراني، الكشف المدفوع بالذكاء الصناعي، التعلم الآلي، التعلم العميق، إلخ.
- ✓ المفردات تعكس مستوى تقني متقدم، مناسب لمراجعة علمية.

## □ الأهمية العلمية :

- ✓ يظهر فهماً عميقاً للموضوع. (IDS) استخدام مفاهيم مثل الطرق الاستدلالية، كشف الشذوذ، وأنظمة كشف التسلل )
- ✓ (إلخ). IEEE، Springer، المصطلحات العلمية شائعة ومُعترف بها في قواعد البيانات العلمية )

## الحدود المحددة X

نقص في التعريفات الواضحة :

، أو التعلم العدائي لم يتم شرحها أو (RNN بعض المصطلحات مثل الخوارزميات الميטהورية، والشبكات العصبية المتكررة ) تعريفها للقارئ غير المتخصص.

، إلخ. DL، IDS، CNN غياب المعجم أو الشرح التفسيري للاختصارات: ○

مصطلحات مفرطة في بعض الأحيان :

تتحول بعض الفقرات إلى طابع تقني بدون سياق تعليمي.

اقتراحات للتحسين :

إضافة قسم في بداية المقال أو جدول يلخص: الاختصارات المستخدمة. تعريفات الطرق الرئيسية. الاختلافات بين المفاهيم القريبة (مثل: التعلم المراقب مقابل التعلم غير المراقب). تقديم المصطلحات التقنية مع أمثلة ملموسة (مثل: "تستخدم الشبكات العصبية التكرارية غالبًا في الكشف عن الشذوذ في حركة المرور في الوقت الحقيقي").

## تحليل الدراسات السابقة المذكورة

### النقاط الإيجابية :

#### حجم كبير من المراجع

تستشهد المقالة بأكثر من 60 دراسة، مما يُظهر مراجعة شاملة للأدبيات. المصادر تأتي من مجلات ✓  
، إلخ. Springer، Elsevier، IEEE Access معروفة:

#### تنوع المناهج المدروسة

المقالة تعالج تقنيات مختلفة: الغابة العشوائية، الشبكات العصبية العميقة، الآلات الداعمة الناقل، الشبكات العصبية التلافيفية، ذاكرة طويلة وقصيرة الأمد، إلخ. تشمل عدة مجالات تطبيق: اكتشاف التسلسل الشبكي، أمان إنترنت الأشياء، إلخ.

## X الحدود المحددة

غياب التحليل النقدي العميق: قلة الربط بين الدراسات: أي الأساليب هي الأكثر فعالية؟ في أي السياقات؟ لا توجد مناقشة حول نقاط الضعف أو حدود الدراسات المذكورة. نقص في تنظيم ، برامج الفدية... نوع DDoS المصادر: المصادر غير مصنفة حسب: نوع التهديد (التصيد ، تحليل البيانات...) نوع البيانات (الشبكات، السجلات، إنترنت الأشياء...) لا DL ، ML التقنية ( يوجد جدول مقارنة لأداء الأساليب. نقص في التنوع الجغرافي واللغوي: المصادر تقريبا حصرية للناطقين بالإنجليزية وتأتي من دول صناعية. قليل أو لا توجد أعمال حول السياقات الأفريقية أو الآسيوية أو متعددة اللغات.

### اقتراحات للتحسين :

إضافة جدول ملخص يقارن: طرق الاستخدام مجموعات البيانات النتائج المتحصل عليها (مثل: معدل الاكتشاف، الدقة) تصنيف الدراسات في أقسام فرعية (حسب النهج، نوع التهديد السيبراني، إلخ) لتسهيل القراءة. دمج تحليل نقدي للدراسات: أمثلة: "هذه الطريقة فعالة ولكنها تتطلب وقتاً طويلاً للحساب"، أو "النتائج متحيزة لأنها تم الحصول عليها من مجموعة بيانات صغيرة".

## الخاتمة العامة للواجب

تقدم المقالة نظرة عامة موسعة وغنية عن طرق الذكاء الاصطناعي المطبقة في الأمن السيبراني. المصطلحات المستخدمة تتناسب بشكل عام، لكنها ستستفيد من تعريفات أوضح لجمهور أوسع. أما الدراسات السابقة، رغم كثرتها، فلا تُعرض دائماً بشكل نقدي أو منظم. لتحسين هذا النوع من الأبحاث، من الضروري: توضيح المفاهيم بشكل أفضل، ونقد وتصنيف المصادر المستخدمة بدقة، وإبراز الفجوات في المجال لتوجيه الأعمال المستقبلية.

Alzubi, J. A., Nayyar, A., & Kumar, A. (2024).  
*Advancing cybersecurity: A comprehensive review  
of AI-driven detection techniques*. Journal of Big  
Data, 11(1), 1–25.  
<https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00809-0>



مجموعة جامعة  
الجميع الذكية  
للتعليم القابضة

MIDOCEAN  
UNIVERSITY



# Thank You



# Teamwork Icons



# Creative Process Icons



# Help & Support Icons



# SEO & Marketing Icons



# Teamwork Icons

