

عنوان البحث

مراجعة أدبيات حديثة في أمن الشبكات تحديات الذكاء الاصطناعي الكشف عن الهجمات. وتعزيز المرونة السيبرانية (2025-2024)

اسم الطالب: عبد المعين ايمن العلي

المادة: منهجية البحث في علوم الحاسوب (A1800)

المحاضر: د. محمد عنبر

مقدمة

يشهد العالم الرقمي تطوراً متسارعاً، مما يفرض تحديات متزايدة على أمن الشبكات، ومع تزايد الاعتماد على التقنيات الحديثة كالذكاء الاصطناعي وإنترنت الأشياء، أصبحت الحاجة ملحة لفهم أعمق للتهديدات السيبرانية المتطورة والحلول المبتكرة لمواجهتها. يهدف هذا التقرير إلى تقديم مراجعة أدبية شاملة لست. أوراق بحثية حديثة (2024-2025) في مجال أمن الشبكات مع التركيز على تحليلها النقدي، تحديد نقاط القوة والضعف استكشاف الروابط والتضاربات بينها. وتقديم جدول ملخص يوضح أبرز الجوانب لكل ورقة.

مراجعة الأوراق البحثية المختارة وتحليلها النقدي

1. تحديات الأمن السيبراني في ظل تطور تقنيات الذكاء الاصطناعي: مقارنة

تحليلية واقعية

المؤلفون: جلول الخذاري

سنة النشر: 2025

الملخص: تبحث هذه الدراسة في واقع الأمن السيبراني في ظل التوسع المتزايد لاستخدام تقنيات الذكاء الاصطناعي، مسلطة الضوء على التحديات التقنية التي تواجه البنية التحتية الرقمية والتهديدات البارزة المدعومة بالخوارزميات الذكية. كما تتناول الأشكال الجديدة للهجمات السيبرانية والفجوات الأمنية التي تكشفها تطبيقات الذكاء الاصطناعي، مقدمة نماذج واقعية وتحليلية لتعقيد الفضاء السيبراني الجديد [1].

الأهداف: تحليل التهديدات الجديدة التي يفرضها الذكاء الاصطناعي على الأمن السيبراني، الكشف عن الفجوات الأمنية في تطبيقات الذكاء الاصطناعي، وتقديم استراتيجيات شاملة لمواجهة هذه التحديات.

المنهجية: اعتمد الباحث على مقارنة تحليلية أكاديمية للأدبيات الحديثة، مع التركيز على النماذج الواقعية للفضاء السيبراني. تم تحليل المقالات والتقارير المتعلقة بتأثير الذكاء الاصطناعي على الأمن السيبراني.

النتائج الرئيسية: خلصت الدراسة إلى أن تحقيق الأمن السيبراني لا يمكن أن يتم دون استراتيجيات شاملة تتضمن الجوانب التكنولوجية والتشريعية والبشرية. وأكدت أن الذكاء الاصطناعي يمثل سلاحاً ذا حدين، حيث يزيد من تعقيد الهجمات وقوة الدفاع في آن واحد.

نقاط القوة: تقدم الدراسة نظرة شاملة وتحليلية لتأثير الذكاء الاصطناعي على الأمن السيبراني، وتبرز أهمية الاستراتيجيات المتكاملة. كما أنها حديثة وتتناول موضوعاً حيوياً.

نقاط الضعف القيود: تفتقر الدراسة إلى الجانب التجريبي أو التطبيقي، حيث تعتمد بشكل أساسي على المراجعة التحليلية للأدبيات. قد لا تقدم حلولاً عملية مباشرة.

مصادر البيانات: الأدبيات العلمية والتقارير المنشورة حول الذكاء الاصطناعي والأمن السيبراني.

2. إطار عمل قابل للتوسع لتحليل حركة مرور أمن الشبكة واكتشاف الهجمات في الوقت الفعلي باستخدام التعلم الآلي والعميق

المؤلفون: Zineb Maasaoui, Mheni Merzouki, Abdella Battou, Ahmed bath

سنة النشر: 2025

الملخص: تقدم هذه الورقة إطار عمل متقدماً (منصة NSTAP) للمراقبة والتحليل في الوقت الحقيقي لحركة مرور الشبكة وأمان النقاط النهائية في المؤسسات الكبيرة، وذلك لمعالجة التعقيد المتزايد وتكرار الهجمات السيبرانية. تستخدم المنصة مجموعة تقنيات شاملة تتضمن Elastic Stack ZEEK. Osquery. Kafka، وبيانات تحديد الموقع الجغرافي، ومن خلال دمج نماذج التعلم الآلي Random Forest (RF) (تم تقييم UNSW-NB15 الخاضعة للإشراف المدربة على مجموعة بيانات Random Forest حيث حقق مصنف 99.32% [2] Decision Trees (DT) Support Vector Machines (SVM) دقة ملحوظة بلغت

الأهداف تقديم إطار متقدم للمراقبة والتحليل في الوقت الحقيقي لحركة مرور الشبكة، تقييم أداء نماذج التعلم الآلي، وتطبيق نماذج معالجة اللغات الطبيعية (BERT) لتحسين الكشف عن الهجمات في أنظمة إنترنت الأشياء (IoT).

المنهجية استخدمت الدراسة منصة NSTAP التي تعتمد على تقنيات Elastic Stack. Zeek GeoLocationg Oiquery. Kafka لجمع ومعالجة البيانات في الوقت الحقيقي تم تدريب نماذج تعلم

الي مشرف على مجموعة بيانات UNSW-NB15، وتطبيق نماذج NLP مثل BERT مع تقنية Byte Level Byte Pair Weighted لتحويل بيانات سجلات الشبكة. تم تقييم الأداء باستخدام مقاييس مثل F1 والدقة

النتائج الرئيسية تحقيق دقة تصل إلى 99.32% باستخدام نموذج Random Forest على مجموعة بيانات UNSW-NB15 تفوق النموذج على الطرق التقليدية في تصنيف متعدد الفئات مع نتائج عالية على مجموعات بيانات Edge-IoT. أظهرت نماذج BERT أداء ممتازاً في تصنيف أنواع الهجمات المختلفة.

نقاط القوة: تقدم حلاً عملياً وقابلاً للتوسع المراقبة أمن الشبكات في الوقت الفعلي. تستخدم تقنيات حديثة ومتعددة (ML, DL (NLP)) وتظهر نتائج تجريبية قوية بدقة عالية.

نقاط الضعف القيود قد يكون تنفيذ وتشغيل هذه المنصة مكلفاً ومعقداً للمؤسسات الصغيرة والمتوسطة. تحتاج إلى كميات كبيرة من البيانات للتدريب الفعال.

مصادر البيانات مجموعات بيانات TON-IoT. Edge-IoT UNSW-NB15.

3 تعزيز مرونة الأمن السيبراني من خلال تمارين الفريق الأحمر المتقدمة ودمج MITRE ATT&CK إطار

المؤلفون: Semi Yulianto, Benfano Soewito, Ford Lumban Gaol, Aditya Kurniawan

سنة النشر: 2025

الملخص: مع التطور المقلق للتهديدات السيبرانية، أصبحت استراتيجيات الدفاع التقليدية غير فعالة بشكل متزايد. تستعرض هذه الدراسة نهجاً تحويلياً لتمرين الفريق الأحمر من خلال دمج إطار عمل MITRE ATT&CK يستفيد هذا الدمج المبتكر من تكتيكات وسلوكيات المهاجمين الواقعية لإنشاء سيناريوهات واقعية تختبر الدفاعات بدقة وتكشف عن نقاط الضعف غير المحددة سابقاً (3).

الأهداف تحسين واقعية وفعالية تمارين الفريق الأحمر، تحديد الثغرات غير المكتشفة سابقاً.

و تقديم رؤى قابلة للتنفيذ لتعزيز الدفاع الاستباقي.

المنهجية تعتمد المنهجية على دمج إطار عمل MITRE ATT&CK في تمارين الفريق الأحمر. يتم استخدام نهج يعتمد على البيانات الربط الدفاعات الحالية بتكتيكات التهديدات الناشئة، مما يعزز القدرة على الصمود السيبراني.

النتائج الرئيسية: أظهرت الدراسة تحسناً كبيراً في واقعية وفعالية تمارين الفريق الأحمر، مما أدى إلى تحسين تحديد الثغرات وتوليد رؤى قابلة للتنفيذ للمعالجة الاستباقية تساهم هذه الدراسة في توفير منهجية منظمة لتعزيز مرونة الأمن السيبراني.

نقاط القوة تقدم منهجية مبتكرة لتقييم وتحسين الدفاعات السيبرانية من خلال محاكاة واقعية للتهديدات تركز على النهج الاستباقي بدلاً من رد الفعل.

نقاط الضعف القيود قد يتطلب تطبيق هذه المنهجية موارد وخبرات عالية، وقد يكون صعباً على المؤسسات ذات الميزانيات المحدودة تعتمد فعاليتها على التحديث المستمر الإطار MITRE مصادر البيانات بيانات مستمدة من تمارين الفريق الأحمر، وإطار عمل MITRE ATT&CK، وتحليل تكتيكات المهاجمين الواقعية.

4. التعلم الآلي والشبكات العصبية للكشف عن التصيد الاحتيالي: مراجعة منهجية (2024-2017)

المؤلفون: Jacek Lukasz Wilk-Jakubowski, Lukasz Pawlik, Grzegorz Wilk-Jakubowski

سنة النشر: 2025

الملخص: لا يزال التصيد الاحتيالي يمثل تهديداً سيبرانياً مستمراً ومتطوراً، حيث يكيف تكتيكاته باستمرار لتجاوز إجراءات الأمان التقليدية. لقد عزز ظهور التعلم الآلي (ML) والشبكات العصبية (NN) بشكل كبير من قدرات أنظمة الكشف الآلي عن التصيد الاحتيالي تستعرض هذه المراجعة الشاملة بشكل منهجي المشهد العام الأساليب الكشف عن التصيد الاحتيالي القائمة على التعلم الآلي والشبكات العصبية (4).

الأهداف: فحص المشهد العام الأساليب الكشف عن التصيد الاحتيالي، تصنيف الأبحاث الحالية حسب قنوات التسليم مواقع الويب البريد الإلكتروني والشبكات الاجتماعية)، وتحديد التحديات الرئيسية والاتجاهات المستقبلية.

المنهجية مراجعة منهجية صارمة للأدبيات المنشورة بين عامي 2017 و 2024 في قواعد بيانات علم الحاسوب والرياضيات ذات الصلة مثل (Scopus). تم تحليل المقالات بناءً على قنوات التسليم. نماذج التعلم الآلي والتقنيات المستخدمة، والممارسات المنهجية.

النتائج الرئيسية أشارت النتائج إلى تحول جذري نحو النماذج المعتمدة على البيانات لمواجهة هجمات "اليوم الصفر". ثم تحديد التحديات الرئيسية مثل جودة البيانات مخاطر تسريب البيانات بين مجموعات التدريب والاختبار، والتحقق الزمني

نقاط القوة: مراجعة شاملة ومنهجية توفر نظرة عامة ممتازة على أحدث التطورات في الكشف عن التصيد الاحتيالي باستخدام ML و NN تحدد الفجوات البحثية والاتجاهات المستقبلية بوضوح.

نقاط الضعف القيود كونها مراجعة أدبية، فإنها لا تقدم نتائج تجريبية جديدة. تعتمد جودتها على دقة وشمولية عملية البحث عن الأدبيات.

مصادر البيانات: قواعد بيانات أكاديمية (مثل Scopus) تحتوي على مقالات منشورة بين 2017 و 2024

5 تحليل حركة مرور الشبكة المشفرة لتعزيز الأمن السيبراني في البيئات الديناميكية

المؤلفون: Faciz Alserhani

سنة النشر: 2024

الملخص: يمثل التشفير حجر الزاوية في اتصالات الإنترنت الحديثة، حيث يوفر أقصى درجات الخصوصية والأمان للبيانات المنقولة، ومع ذلك، فإن تطبيق البيانات المشفرة يطرح مشكلات خطيرة لأنظمة الكشف والوقاية، خاصة وأن فحص الحزم العميق (DPI) هو الطبقة الأساسية للدفاع ضد العديد من الهجمات السيبرانية. تعالج هذه الورقة تحديات أنظمة كشف التسلل (IDS) في التعامل مع البيانات المشفرة في بيئات ديناميكية مثل إنترنت الأشياء (1)

الأهداف: تطوير نظام IDS محسن يعتمد على نماذج التعلم العميق لتحليل أنماط حركة المرور المشفرة دون الحاجة لفك التشفير الكامل، وبالتالي الحفاظ على الخصوصية. التنبؤ بالهجمات السيبرانية ومنعها.

المنهجية: تم استخدام منهجية Tree-based Spider-Net Multipath (TBSN) مع تقنيات التعلم التعزيزي العميق (DRL-TS) لتحسين اختيار القنوات والمسارات تم دمج شبكة عصبية عميقة خفيفة الوزن مع خوارزميات تحسين (LDNN-HGS-ROA) لإنشاء نظام IDS محسن.

النتائج الرئيسية: أظهرت نتائج التقييم أن بنية النظام المقترحة فعالة في اكتشاف الهجمات. محققة معدلات أداء محسنة لنظام IDS تفوق النظام على الطرق التقليدية في التعامل مع حركة المرور المشفرة.

نقاط القوة: تقدم حلاً مبتكراً لمشكلة حرجية في الأمن السيبراني تحليل حركة المرور المشفرة) دون المساس بالخصوصية. تستخدم تقنيات تعلم عميق متقدمة وتظهر نتائج تجريبية واعدة.

مصادر البيانات؛ بيانات حركة مرور الشبكة المشفرة من بيئات IoT وبيانات محاكاة لاختبار النظام.

6. مستقبل أمن الشبكات والاتجاهات والابتكارات في عام 2024

المؤلفون: مستخلص من مراجعة الاتجاهات العامة لعام 2024، بناء على تقارير عالمية

سنة النشر: 2024

الملخص: تستكشف هذه الورقة التحليلية الاتجاهات الناشئة والابتكارات الضرورية التي تشكل مستقبل أمن الشبكات في عام 2024 تتضمن هذه الاتجاهات أمن الحوسبة السحابية. مبدأ الثقة الصفريّة (Zero Trust) ، وأمن سلاسل التوريد الرقمية، بالإضافة إلى دور الذكاء الاصطناعي في تعزيز الدفاعات السيبرانية [6] [7].

الأهداف: تحديد الابتكارات التقنية اللازمة لمواجهة تطور الجرائم السيبرانية المنظمة، وتقديم رؤى حول كيفية بناء استراتيجيات أمنية مستقبلية.

المنهجية: اعتمدت الدراسة على تحليل شامل للتقارير العالمية الصادرة عن منظمات مثل المنتدى الاقتصادي العالمي ((6) WEF) والأبحاث التقنية الرائدة لعام 2024 بالإضافة إلى مراجعة أدبيات حول الاتجاهات المستقبلية في الأمن السيبراني (7).

النتائج الرئيسية: خلصت الدراسة إلى أن المستقبل يتطلب الانتقال نحو نماذج أمنية مرنة تعتمد بشكل كلي على الأتمتة والذكاء الاصطناعي لتقليل زمن الاستجابة للحوادث الأمنية. كما أكدت على أهمية تبني مبدأ الثقة الصقرية لحماية البنية التحتية الحيوية.

نقاط القوة: تقدم نظرة استشرافية للتهديدات والحلول المستقبلية في أمن الشبكات. تستند إلى تقارير موثوقة من منظمات عالمية.

نقاط الضعف القيود: قد تكون عامة بعض الشيء ولا تتعمق في تفاصيل تقنية محددة. تعتمد على التنبؤات التي قد تتغير مع تطور التكنولوجيا والتهديدات.

مصادر البيانات: تقارير المنتدى الاقتصادي العالمي (WEF) لعام 2024 (6). تقارير [7] CERT-FR ومقالات بحثية حول الاتجاهات المستقبلية في الأمن السيبراني

الروابط والتضاربات بين الأوراق البحثية

تظهر الأوراق البحثية المختارة ترابطاً قوياً في معالجتها للتحديات الأمنية الحديثة، خاصة فيما يتعلق بدور الذكاء الاصطناعي والتعلم الآلي الورقة الأولى (1) والورقة السادسة (6) (7) تقدمان نظرة عامة وتحليلية التأثير الذكاء الاصطناعي على الأمن السيبراني والاتجاهات المستقبلية، مؤكدين على أن الذكاء الاصطناعي يمثل فرصة وتحدياً في آن واحد. بينما تتعمق الأوراق الأخرى في جوانب تطبيقية محددة لهذه التقنيات.

الورقة الثانية (2) والورقة الخامسة (5) تكملان بعضهما البعض في معالجة مشكلة الكشف عن الهجمات في الشبكات الورقة الثانية تقدم إطار عمل شاملاً للكشف في الوقت الفعلي باستخدام ML و DL، بينما تركز الورقة الخامسة على التحدي الأكثر تعقيداً وهو تحليل حركة المرور المشفرة، مقدمة حلولاً مبتكرة للحفاظ على الخصوصية. كلاهما يبرز فعالية التعلم الآلي والعميق في تحسين دقة الكشف عن التهديدات.

الورقة الثالثة (3). التي تتناول دمج إطار MITRE ATTACK في تمارين الفريق الأحمر، ترتبط بشكل وثيق بالهدف العام لتعزيز المرونة السيبرانية الذي أشارت إليه الورقة السادسة (6) (7). فتمارين الفريق الأحمر هي تطبيق عملي للاستراتيجيات الاستباقية التي تدعو إليها الورقة السادسة لمواجهة التهديدات المتطورة.

أما الورقة الرابعة (4) وهي مراجعة منهجية للكشف عن التصيد الاحتيالي، فتوفر الأساس النظري والتصنيفي للتقنيات التي يمكن تطبيقها في إطار عمل مثل NSTAP المذكورة في الورقة الثانية (2). كما أنها تسلط الضوء على تحديات جودة البيانات وتسريبها، وهي قضايا حاسمة يجب مراعاتها عند بناء أنظمة الكشف القائمة على التعلم الآلي.

لا توجد تضاريات جوهرية بين الأوراق، بل هي متكامل لتقديم صورة شاملة لتحديات وحلول أمن الشبكات الحديثة الاختلافات تكمن في مستوى التفصيل والتركيز على جوانب معينة تحليلي مقابل تطبيقي، عام مقابل خاص).

جدول ملخص الأوراق البحثية المراجعة

نقاط الضعف/القيود	النتائج الرئيسية	المنهجية المستخدمة	المؤلفون	سنة النشر	عنوان الورقة البحثية
تفتقر للجانب التجريبي/التطبيقي، تعتمد على المراجعة النظرية	ضرورة الاستراتيجيات الشاملة (تقنية، تشريعية، بشرية) لمواجهة الذكاء الاصطناعي كسلح نو حدين	تحليلية أكاديمية للأدبيات	جلول لخذاري	2025	تحديات الأمن السيبراني في ظل تطور تقنيات الذكاء الاصطناعي
تكلفة وتعقيد التنفيذ، الحاجة لكميات كبيرة من بيانات التدريب	دقة 99.32% باستخدام Random Forest، في BERT تفوق نماذج تصنيف الهجمات المعقدة	تقنية (منصة NSTAP، Elastic Stack، Kafka، ML/DL)	Zineb Maasaoui et al.	2025	إطار عمل قابل للتوسع لتحليل حركة مرور أمن الشبكة واكتشاف الهجمات في الوقت الفعلي باستخدام التعلم الآلي والعميق
تتطلب موارد وخبرات عالية، تعتمد على التحديث المستمر لـ MITRE ATT&CK	تحسين واقعية تمارين الفريق الأحمر، تحديد الثغرات، تعزيز الصمود السيبراني	MITRE ATT&CK في تمارين الفريق الأحمر، تحليل بيانات	Semi Yulianto et al.	2025	تعزيز مرونة الأمن السيبراني من خلال تمارين الفريق الأحمر المتقدمة MITRE ATT&CK ودمج إطار عمل
كونها مراجعة أدبية لا تقدم نتائج تجريبية جديدة، تعتمد على دقة البحث عن الأدبيات	تحول جذري نحو النماذج المعتمدة على البيانات لمواجهة هجمات "اليوم الصفر"	مراجعة منهجية (Scopus)	Jacek Lukasz Wilk-Jakubowski et al.	2025	التعلم الآلي والشبكات العصبية للكشف عن التصيد الاحتيالي: مراجعة منهجية (2017-2024)
تعقيد الخوارزميات، متطلبات حاسوبية كبيرة، تحديات قابلية التوسع	فعالية عالية في اكتشاف الهجمات داخل حركة المرور المشفرة دون فك التشفير	تعلم تعزيزي عميق (TBSNM, DRL-TS, LDNN-HGS-ROA)	Faeiz Alserhani	2024	تحليل حركة مرور الشبكة المشفرة لتعزيز الأمن السيبراني في البيئات الديناميكية
عامة بعض الشيء، تعتمد على التنبؤات التي قد تتغير	حتمية الانتقال نحو نماذج أمنية مرنة تعتمد على الأتمتة والذكاء الاصطناعي ومبدأ الثقة الصفرية	تحليل شامل للتقارير العالمية والأبحاث التقنية الرائدة	مستخلص من تقارير (عالمية)	2024	مستقبل أمن الشبكات: الاتجاهات والابتكارات في عام 2024

الخاتمة

تؤكد هذه المراجعة الأدبية على أن مجال أمن الشبكات يشهد تحولات جذرية، مدفوعة بالتقدم في الذكاء الاصطناعي والتعلم الآلي وتزايد تعقيد التهديدات السيبرانية. تبرز الأوراق البحثية المختارة الحاجة الماسة إلى تبني استراتيجيات دفاعية استباقية، وأنظمة كشف متطورة قادرة على التعامل مع البيئات الديناميكية والبيانات المشفرة، بالإضافة إلى تعزيز مرونة الأنظمة من خلال التقييم المستمر. يتضح أن الحلول الفعالة تتطلب تكاملاً بين الابتكارات التكنولوجية، الأطر التشريعية، وتطوير الوعي البشري، لضمان فضاء سيبراني آمن ومستدام في المستقبل.

(1) جلول لخذاري (2025) تحديات الأمن السيبراني في ظل تطور تقنيات الذكاء الاصطناعي: مقارنة تحليلية واقعية واقع الأمن السيبراني في ظل تنامي استعمالات الذكاء الاصطناعي، جامعة ميله الجزائر.

Maasaoui, Z., Merzouki, M., Battou, A., & Lbath, A. (2025). A Scalable Framework for Real- [2] Time Network Security Traffic Analysis and Attack Detection Using Machine .and Deep Learning

Platforms, 3(2), 7. <https://doi.org/10.3390/platforms3020007>

Yulianto, S., Soewito, B., Gaol, F. L., & Kurniawan, A. (2025). Enhancing cybersecurity 3 resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration: A paradigm shift in cybersecurity assessment. Cyber Security and .Applications, 3, 100077

<https://doi.org/10.3390/electronics14183744>

Wilk-Jakubowski, J. L., Pawlik, L., Wilk-Jakubowski, G., & Sikora, A. (2025). Machine [4] Learning and Neural Networks for Phishing Detection: A Systematic Review (2017- .2024)

Electronics, 14(18), 3744. <https://doi.org/10.3390/electronics14183744>

Alserhani, F. (2024). Analysis of Encrypted Network Traffic for Enhancing Cyber-security in [5] Dynamic Environments. *Applied Artificial Intelligence*, 38(1). 2381882

<https://doi.org/10.1080/08839514-2024.2381882>

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. [6]
[https://www3.weforum.org/docs/WEF_Global Cybersecurity Outlook 2024.pdf](https://www3.weforum.org/docs/WEF_Global%20Cybersecurity%20Outlook%202024.pdf)

CERT-FR (2024). CYBER THREAT OVERVIEW 2024. [7]

<https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CT1-004.pdf>