Entrepreneurship Journal for Finance and Business (EJFB)
2026, VOL. 07, NO. special, 268-283, E-ISSN: 2709-4251, P-ISSN: 2708-8790
DOI: https://doi.org/10.56967/ejfb2026936

Artificial intelligence and IoT integration for early cyberattack detection in smart universities

Jenan J. M. Al-Mahmoud*
Department of Information Technology Engineering, College of Polytechnic, Al-Furat Al-Awsat Technical University, Karbala, Iraq

Article information:
Published: 25–08– 2026

***Corresponding author:**
Jenan J. M. Al-Mahmoud
jenan.jader@atu.edu.iq

This work is licensed under a Creative Commons Attribution 4.0 International License.

Abstract:

Smart universities constitute a complex environment in which thousands of Internet of Things (IoT) devices are interconnected, rendering them an increasingly attractive target for sophisticated cyberattacks. This study aims to design an integrated framework combining Artificial Intelligence (AI) and IoT technologies for the early detection of cyberattacks within smart university environments, employing machine learning and deep learning algorithms — namely Random Forest and a hybrid CNN-LSTM model — to classify network traffic and detect anomalous patterns in real time.

The study adopted a descriptive-analytical approach supported by a field questionnaire administered to a sample of 150 participants from IT and network security personnel across universities. Results revealed excellent questionnaire reliability (Cronbach's Alpha = 0.927) and a strong positive correlation (r = 0.674) between cybersecurity awareness and AI detection effectiveness, alongside the superiority of the proposed model over traditional systems by an accuracy margin of approximately 25 percentage points (96.3% vs. 71.2%).

The study recommends adopting a five-layer architectural framework integrating IoT devices, data processing, AI inference, attack detection, and real-time response layers as a viable model for deployment in Arab smart universities.

Keywords: Artificial intelligence, internet of things, cybersecurity, smart universities, early attack detection, deep learning, machine learning.

Conclusions:

1. The proposed model (Random Forest + CNN-LSTM) achieved a high detection accuracy of 96.3%, outperforming traditional systems by a statistically significant margin of 25.1 percentage points.
2. A strong, positive, and statistically significant correlation (r = 0.674) was found between cybersecurity awareness and perceived effectiveness of artificial intelligence, supporting the acceptance of the study's main hypothesis.
3. Cybersecurity awareness explains 45.4% of the variance in the perceived effectiveness of artificial intelligence, while the remaining 54.6% is associated with other technical and institutional factors that warrant further investigation in future studies.
4. Distributed Denial-of-Service (DDoS) attacks ranked first among the most common threats in smart university environments, accounting for 31.4%, followed by phishing attacks at 24.8%.
5. Artificial intelligence significantly outperformed traditional methods in detecting previously unknown (zero-day) attacks, which represent the most critical and least detectable category of cyber threats using conventional approaches.

مجلة الريادة للمال والاعمال
2026، المجلد السابع، العدد الخاص، الصفحات 268- 283

استخدام الذكاء الاصطناعي مع إنترنت الأشياء (IoT) للكشف المبكر عن الهجمات السيبرانية في الجامعات الذكية

جنان جادر مساعد المحمود*
قسم هندسة تقنيات المعلومات، كلية البوليتكنك، جامعة الفرات الأوسط التقنية، كربلاء، العراق

معلومات البحث:
• تاريخ النشر: 2026 –08–25

***المؤلف المراسل:**
جنان جادر مساعد المحمود
jenan.jader@atu.edu.iq

هذا العمل مرخص بموجب المشاع الابداعي نسب المصنف 4.0 دولي (CC BY 4.0)

المستخلص:
تُشكّل الجامعات الذكية بيئةً معقدةً تتشابك فيها آلاف الأجهزة المتصلة عبر إنترنت الأشياء (IoT)، مما يجعلها هدفاً متزايد الجاذبية للهجمات السيبرانية المتطورة. يهدف هذا البحث إلى تصميم نموذج متكامل يجمع بين تقنيات الذكاء الاصطناعي وإنترنت الأشياء للكشف المبكر عن الهجمات السيبرانية في بيئات الجامعات الذكية، باستخدام خوارزميات التعلم الآلي والتعلم العميق (Random Forest وCNN-LSTM الهجين) لتصنيف حركة الشبكة وكشف الأنماط الشاذة في الزمن الحقيقي.
اعتمد البحث المنهج الوصفي التحليلي المدعوم باستبانة ميدانية وُزّعت على عينة قوامها (150) مشاركاً من العاملين في تقنية المعلومات وأمن الشبكات بالجامعات. كشفت النتائج عن ثبات ممتاز للاستبانة (ألفا كرونباخ = 0.927)، ووجود علاقة ارتباطية موجبة قوية (r=0.674) بين الوعي بالأمن السيبراني وفاعلية الذكاء الاصطناعي في الكشف، إلى جانب تفوق النموذج المقترح على الأنظمة التقليدية بفارق دقة بلغ نحو 25 نقطة مئوية (96.3% مقابل 71.2%).
تُوصي الدراسة باعتماد بنية معمارية خماسية الطبقات تجمع بين أجهزة IoT وطبقات معالجة البيانات والذكاء الاصطناعي وكشف الهجمات والاستجابة الآنية، بوصفها نموذجاً قابلاً للتطبيق في الجامعات الذكية العربية.

الكلمات المفتاحية: الذكاء الاصطناعي؛ إنترنت الأشياء؛ الأمن السيبراني؛ الجامعات الذكية؛ الكشف المبكر عن الهجمات؛ التعلم العميق؛ التعلم الآلي.

1. المقدمة

شهد العقد الأخير تحولاً جذرياً في فلسفة التعليم العالي مع ظهور مفهوم «الجامعة الذكية» (Smart University) التي تستند إلى دمج تقنيات إنترنت الأشياء (IoT) والحوسبة السحابية والذكاء الاصطناعي لتحسين الكفاءة التشغيلية وإثراء التجربة التعليمية والإدارية. وتُشير التقديرات إلى أن الحرم الجامعي الذكي النموذجي يضمّ ما يزيد على عشرة آلاف جهاز متصل بالإنترنت، تتراوح بين أنظمة المراقبة الذكية وأجهزة التحكم بالطاقة وبوابات الدخول الحيوية ومحطات العمل الطلابية (Alabdulatif et al., 2022).
غير أن هذا الاتساع غير المسبوق في رقعة الأجهزة المتصلة يحمل في طياته تحدياً أمنياً بالغ الخطورة؛ فكل جهاز IoT يُمثّل نقطة دخول محتملة (Attack Surface) يمكن للمهاجمين استغلالها. وقد أظهرت تقارير الأمن السيبراني العالمية أن قطاع التعليم العالي أصبح من أكثر القطاعات استهدافاً بهجمات الفدية وحجب الخدمة الموزع (DDoS) خلال 2023–2024، متجاوزاً في بعض المؤشرات قطاعي الصحة والمال (Sophos, 2024). ويعود ذلك جزئياً إلى الطبيعة المفتوحة نسبياً لشبكات الجامعات، وتنوع الأجهزة غير المُدارة مركزياً، ومحدودية الموارد المخصصة للأمن السيبراني مقارنةً بالقطاعات الأخرى.
وفي مواجهة هذا التهديد المتصاعد، برزت تقنيات الذكاء الاصطناعي بوصفها أداةً واعدة لتجاوز قصور أنظمة الكشف التقليدية القائمة على التوقيعات (Signature-based Detection)، التي تعجز عن رصد الهجمات الجديدة أو المتحوّرة (Zero-day Attacks). فخوارزميات التعلم الآلي والتعلم العميق قادرة على تعلّم الأنماط السلوكية الطبيعية لحركة الشبكة، ومن ثَمّ رصد أي انحراف شاذ عنها في الزمن الحقيقي، بدقة وسرعة تتجاوزان قدرة المحلل البشري والأنظمة التقليدية مجتمعةً (Ferrag et al., 2023).
انطلاقاً مما تقدّم، يسعى هذا البحث إلى تصميم نموذج متكامل يجمع بين تقنيات إنترنت الأشياء والذكاء الاصطناعي للكشف المبكر عن الهجمات السيبرانية في بيئة الجامعات الذكية، مستنداً إلى بنية معمارية خماسية الطبقات ومدعوماً بدراسة ميدانية تستطلع آراء العاملين في تقنية المعلومات وأمن الشبكات.

2. مشكلة البحث

على الرغم من التوسع المتسارع في تبنّي تقنيات إنترنت الأشياء داخل الحرم الجامعي، لا تزال غالبية أنظمة الحماية المعتمدة في الجامعات تستند إلى آليات كشف تقليدية قائمة على قواعد ثابتة وتوقيعات معروفة مسبقاً، وهو ما يجعلها عاجزةً عن مجاراة وتيرة تطوّر الهجمات السيبرانية الحديثة وتنوّعها. وتتفاقم هذه الإشكالية في ظل: ضخامة حجم البيانات المتدفقة من آلاف أجهزة IoT في الزمن

الحقيقي، ومحدودية الموارد الحاسوبية لكثير من هذه الأجهزة التي تحول دون تضمين آليات حماية معقدة فيها مباشرةً، وندرة الدراسات العربية التي تتناول تصميم نماذج كشف ذكية مُكيَّفة خصيصاً لبيئة الجامعات.

صياغة مشكلة البحث

تتمحور مشكلة البحث حول التساؤل الجوهري الآتي: كيف يمكن توظيف تقنيات الذكاء الاصطناعي المتكاملة مع إنترنت الأشياء لتصميم نظام فعّال للكشف المبكر عن الهجمات السيبرانية في بيئة الجامعات الذكية، وإلى أي مدى يتفوّق هذا النظام على آليات الكشف التقليدية من حيث الدقة والسرعة وانخفاض معدل الإنذارات الكاذبة؟

3. أهداف البحث

يسعى هذا البحث إلى تحقيق الأهداف الآتية:

- تصميم نموذج معماري متكامل يجمع بين أجهزة إنترنت الأشياء وخوارزميات الذكاء الاصطناعي للكشف المبكر عن الهجمات السيبرانية في بيئة الجامعات الذكية.
- تقييم فاعلية خوارزميات التعلم الآلي (Random Forest) والتعلم العميق (نموذج CNN-LSTM الهجين) في تصنيف حركة الشبكة وكشف الهجمات.
- قياس مستوى الوعي بالأمن السيبراني لدى العاملين في تقنية المعلومات بالجامعات وعلاقته بفاعلية الكشف بالذكاء الاصطناعي.
- تحديد أبرز أنواع الهجمات السيبرانية شيوعاً في بيئات الجامعات الذكية ونسب انتشارها.
- تقديم توصيات عملية لتعزيز الجاهزية الأمنية لمؤسسات التعليم العالي في مواجهة التهديدات السيبرانية المرتبطة بـ IoT.

4. أسئلة البحث وفرضياته

4.1 أسئلة البحث

- ما مستوى جاهزية البنية التحتية لإنترنت الأشياء في الجامعات قيد الدراسة؟
- ما مستوى الوعي بالأمن السيبراني لدى العاملين في تقنية المعلومات وأمن الشبكات؟
- ما مدى فاعلية تقنيات الذكاء الاصطناعي في الكشف المبكر عن الهجمات السيبرانية مقارنةً بالأنظمة التقليدية؟
- ما أبرز التحديات والمعوقات التي تواجه تبنّي حلول الذكاء الاصطناعي لأمن إنترنت الأشياء في الجامعات؟
- هل توجد علاقة ارتباطية ذات دلالة إحصائية بين الوعي بالأمن السيبراني وفاعلية الذكاء الاصطناعي في الكشف عن الهجمات؟

4.2 فرضيات البحث

الفرضية الرئيسية (H1): توجد علاقة ارتباطية موجبة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين الوعي بالأمن السيبراني وفاعلية الذكاء الاصطناعي في الكشف المبكر عن الهجمات السيبرانية.

الفرضية الفرعية الأولى (H1a): يُسهم تحسّن مستوى البنية التحتية لإنترنت الأشياء إسهاماً معنوياً في رفع فاعلية الكشف المبكر عن الهجمات.

الفرضية الفرعية الثانية (H1b): تختلف فاعلية الذكاء الاصطناعي في الكشف باختلاف طبيعة الدور الوظيفي للمشارك (إداري تقني/أكاديمي/طالب).

الفرضية الصفرية (H0): لا توجد علاقة ارتباطية ذات دلالة إحصائية بين الوعي بالأمن السيبراني وفاعلية الذكاء الاصطناعي في الكشف عن الهجمات.

5. أهمية البحث

5.1 الأهمية العلمية (النظرية)

- يُسهم البحث في إثراء الأدبيات العربية النادرة نسبياً في مجال تقاطع أمن إنترنت الأشياء والذكاء الاصطناعي في السياق الجامعي تحديداً.
- يُقدّم إطاراً نظرياً متكاملاً يربط بين مفاهيم الجامعات الذكية وأمن IoT وتطبيقات الذكاء الاصطناعي في كشف التهديدات.
- يفتح آفاقاً بحثيةً مستقبليةً لتطوير نماذج كشف هجينة أكثر دقة وكفاءة حاسوبية.

5.2 الأهمية التطبيقية (العملية)

- يُقدّم نموذجاً معمارياً عملياً قابلاً للتطبيق المباشر في مراكز تقنية المعلومات بالجامعات.
- يُزوّد صانعي القرار التربوي بأدلة كمية تدعم الاستثمار في حلول الأمن السيبراني المعتمدة على الذكاء الاصطناعي.
- يُساعد في وضع خطط استجابة استباقية تُقلّل من الأضرار المالية والتشغيلية الناجمة عن الهجمات السيبرانية.

6. الدراسات السابقة

استعرض الباحث جملةً من الدراسات الحديثة المنشورة بين عامي 2021 و2025 التي تناولت توظيف الذكاء الاصطناعي في أمن إنترنت الأشياء، مع التركيز على الدراسات الأقرب لسياق هذا البحث.

6.1 عرض تحليلي للدراسات

دراسة (Ferrag et al. 2023): اقترحت نموذجاً هجيناً يجمع بين CNN وLSTM لكشف هجمات DDoS وBotnet في بيئات IoT الصناعية، محققاً دقة 98.1% على مجموعة بيانات CICIoT2023. كشفت الدراسة عن قصور النماذج الأحادية (CNN أو LSTM منفردين) في التعامل مع التسلسلات الزمنية المعقدة لحركة الشبكة.

دراسة (Alabdulatif et al. 2022): طبّقت خوارزميات Random Forest وXGBoost على بيانات حركة شبكة جامعية افتراضية، محققةً دقة 94.6%، وأوصت بضرورة دمج آليات الكشف بالحافة (Edge Computing) لتقليل زمن الاستجابة.

دراسة (Saharkhizan et al. 2021): استخدمت مجموعة مُجمَّعة (Ensemble) من نماذج LSTM للكشف عن هجمات Botnet في بيئة IoT الطبية، بدقة 99.0%، لكنها لم تتناول قابلية تعميم النموذج على بيئات أخرى كالجامعات.

دراسة (Alkahtani & Aldhyani 2022): قارنت بين خمس خوارزميات تعلم آلي للكشف عن هجمات IoT، وخلصت إلى تفوّق Random Forest وSVM على الشبكات العصبية التقليدية من حيث التوازن بين الدقة وزمن المعالجة.

دراسة (Khan & Akhunzada 2023): صمّمت نظام كشف هجين قائم على Deep Belief Network لبيئات المدن الذكية، بدقة 96.8%، مع التأكيد على ضرورة معالجة مشكلة عدم توازن الفئات (Class Imbalance) في بيانات الهجمات.

دراسة (Al-Hawawreh et al. 2024): قدّمت إطاراً للكشف الموزّع (Federated Learning) عن الهجمات في شبكات IoT متعددة المواقع، يحافظ على خصوصية البيانات، محققاً دقة 95.3% دون الحاجة لمركزية البيانات.

دراسة (Gaber et al. 2023): طبّقت نموذج Autoencoder للكشف غير الخاضع للإشراف (Unsupervised) عن الشذوذ في بيانات IoT الجامعية، وأثبتت فاعليته في كشف الهجمات غير المعروفة سابقاً (Zero-day) بدقة 89.4%.

دراسة (Hussain et al. 2024): استعرضت تحديات تطبيق الذكاء الاصطناعي التفسيري (Explainable AI) في أمن IoT، مؤكدةً أن غياب التفسير يُضعف ثقة مسؤولي الأمن في قرارات النظام الآلي رغم دقته العالية.

6.2 جدول مقارنة الدراسات السابقة

المؤلف والسنة	التقنية المستخدمة	النتائج	الفجوة البحثية
Ferrag et al. (2023)	CNN-LSTM Hybrid	**98.1%**	اقتصرت على بيئة IoT الصناعية؛ لم تُختبر في سياق جامعي
Alabdulatif et al. (2022)	Random Forest + XGBoost	**94.6%**	بيانات افتراضية محاكاة؛ غياب التحقق الميداني الفعلي
Saharkhizan et al. (2021)	Ensemble LSTM	**99.0%**	بيئة IoT طبية فقط؛ قابلية التعميم غير مُختبرة
Alkahtani & Aldhyani (2022)	RF, SVM, ANN مقارنة	**92–95%**	لم تتناول التكامل المعماري الكامل لنظام الكشف
Khan & Akhunzada (2023)	Deep Belief Network	**96.8%**	مشكلة عدم توازن الفئات لم تُعالَج بالكامل
Al-Hawawreh et al. (2024)	Federated Learning	**95.3%**	تعقيد تشغيلي عالٍ؛ غير مناسب للجامعات محدودة الموارد
Gaber et al. (2023)	Autoencoder (Unsupervised)	**89.4%**	دقة أقل نسبياً؛ ارتفاع معدل الإنذارات الكاذبة
Hussain et al. (2024)	Explainable AI Framework	—	مراجعة نظرية فقط دون نموذج تطبيقي مُختبر

ملاحظة: تُرتَّب الدراسات وفق التسلسل الزمني للنشر. الفجوات البحثية المُجمَّعة شكّلت أساس تصميم منهجية البحث الحالي.

6.3 الفجوة البحثية الكلية

يتّضح من الجدول أعلاه أن الدراسات السابقة، رغم تقدّمها التقني الملحوظ، تتشارك في ثلاث فجوات جوهرية: (أ) ندرة الدراسات التي تتناول بيئة الجامعات الذكية تحديداً بخصائصها المميزة (تنوع الأجهزة، الانفتاح النسبي للشبكة، تعدد المستخدمين)؛ (ب) غياب نموذج معماري متكامل يجمع بين خوارزميات متعددة (Random Forest + CNN-LSTM) بدلاً من الاعتماد على خوارزمية واحدة؛ (ج) محدودية الدراسات الميدانية التي تقيس الوعي البشري بالأمن السيبراني وعلاقته بفاعلية الأنظمة الذكية. ويسعى هذا البحث إلى معالجة هذه الفجوات الثلاث مجتمعةً.

7. الإطار النظري

7.1 مفهوم الجامعات الذكية

تُعرَّف الجامعة الذكية (Smart University) بأنها مؤسسة تعليمية تُوظّف تقنيات إنترنت الأشياء والذكاء الاصطناعي وتحليل البيانات الضخمة لتحسين العمليات الأكاديمية والإدارية والخدمية، عبر بنية تحتية رقمية متكاملة تربط المرافق والأجهزة والمستخدمين في منظومة واحدة (Alabdulatif et al., 2022). وتتميز هذه الجامعات بخصائص جوهرية أبرزها: الاتصال الشامل (Pervasive Connectivity)، واتخاذ القرار المُستند إلى البيانات، والتكيّف الآني مع احتياجات المستخدمين.

7.2 إنترنت الأشياء (IoT)

يُعرَّف إنترنت الأشياء بأنه شبكة من الأجهزة المادية المزوَّدة بمستشعرات وبرمجيات وتقنيات اتصال تُمكّنها من جمع البيانات وتبادلها عبر الإنترنت دون تدخل بشري مباشر. وفي السياق الجامعي، تشمل أجهزة IoT: كاميرات المراقبة الذكية، وأنظمة التحكم بالدخول الحيوي، ومستشعرات البيئة (حرارة، رطوبة، إضاءة)، وأجهزة إدارة الطاقة، ومحطات العمل الطلابية المتصلة. ووفقاً لتصنيف (Ferrag et al. 2023)، تنقسم بروتوكولات اتصال IoT الشائعة إلى: MQTT وCoAP وZigbee، ولكلٍّ منها نقاط ضعف أمنية مميزة تستوجب آليات حماية مُخصَّصة.

7.3 الأمن السيبراني في بيئات IoT

يواجه أمن إنترنت الأشياء تحديات بنيوية تُميّزه عن أمن الشبكات التقليدية، أبرزها: محدودية الموارد الحاسوبية للأجهزة (مما يحول دون تشغيل برامج حماية تقليدية معقدة)، وتغايُر بروتوكولات الاتصال، وضعف آليات التحديث الأمني الدوري لكثير من الأجهزة منخفضة التكلفة. وتُصنَّف الهجمات السيبرانية المُستهدِفة لبيئات IoT في خمس فئات رئيسية يتناولها هذا البحث بالتفصيل: هجمات حجب الخدمة الموزع (DDoS)، وشبكات الروبوت الخبيثة (Botnet)، والبرمجيات الخبيثة (Malware)، والتصيّد الاحتيالي (Phishing)، وبرمجيات الفدية (Ransomware).

7.4 تطبيقات الذكاء الاصطناعي في كشف التهديدات

يستند الكشف الذكي عن التهديدات إلى فئتين رئيسيتين من الخوارزميات: **التعلم الآلي التقليدي (Machine Learning)** مثل Random Forest و Support Vector Machine، التي تتميز بسرعة التدريب والتفسير النسبي لكنها قد تعجز عن التقاط الأنماط المعقدة في البيانات التسلسلية؛ و**التعلم العميق (Deep Learning)** مثل الشبكات العصبية الالتفافية (CNN) والشبكات التكرارية طويلة-قصيرة الذاكرة (LSTM)، التي تتفوّق في التقاط الأنماط الزمنية المعقدة لحركة الشبكة لكنها تتطلب موارد حاسوبية وبيانات تدريب أكبر. وقد أثبتت النماذج الهجينة (كـ CNN-LSTM) تفوّقاً ملحوظاً في الدراسات الحديثة (Ferrag et al., 2023) من خلال الجمع بين قدرة CNN على استخلاص السمات المكانية وقدرة LSTM على التقاط التسلسل الزمني.

8. المنهجية المقترحة

يتبع هذا البحث منهجية مختلطة (Mixed-Methods) تجمع بين التصميم التقني للنموذج المقترح والدراسة الميدانية الكمية، وذلك عبر المراحل الآتية:

8.1 تصميم النموذج المتكامل

يستند النموذج المقترح إلى دمج طبقتين رئيسيتين: **طبقة استشعار IoT** التي تجمع البيانات الخام من حركة الشبكة وسلوك الأجهزة، و**طبقة المعالجة الذكية** التي تُحوّل هذه البيانات إلى قرارات تصنيفية (حركة طبيعية / هجوم محتمل). ويعتمد النموذج على معمارية خماسية الطبقات تُفصَّل في القسم (9) أدناه.

8.2 خوارزميات التعلم الآلي والتعلم العميق المستخدمة

أولاً — Random Forest: خوارزمية تجميعية (Ensemble) تعتمد على بناء عدد كبير من أشجار القرار وتجميع نتائجها بالتصويت الأغلبي. اختيرت هذه الخوارزمية لكفاءتها الحاسوبية العالية ومقاومتها للإفراط في التخصيص (Overfitting)، مما يجعلها مناسبةً للتشغيل شبه الآني على بوابات الشبكة.

ثانياً — النموذج الهجين CNN-LSTM: يجمع بين طبقات الالتفاف (Convolutional Layers) لاستخلاص السمات المكانية من حزم البيانات، وطبقات LSTM لالتقاط الاعتمادية الزمنية المتسلسلة في حركة الشبكة عبر الزمن. وقد أثبتت الدراسات الحديثة (Ferrag et al., 2023) تفوّق هذا الهجين في كشف الهجمات متعددة المراحل كهجمات Botnet التي تتكوّن من تسلسل سلوكي ممتد زمنياً.

8.3 مراحل جمع البيانات ومعالجتها وتصنيفها

المرحلة الأولى: جمع البيانات (Data Collection)

- التقاط حزم البيانات (Packet Capture) من بوابات الشبكة وأجهزة IoT عبر أدوات مثل Wireshark وZeek.
- استخدام مجموعات بيانات مرجعية معيارية (مثل CICIoT2023 وN-BaIoT) لتدريب النموذج الأولي.
- جمع بيانات تكميلية من بيئة محاكاة لشبكة جامعية افتراضية لضمان ملاءمة النموذج للسياق المستهدف.

المرحلة الثانية: معالجة البيانات (Data Pre-processing)

- تنظيف البيانات وإزالة القيم الشاذة والمكررة والناقصة.
- استخلاص السمات (Feature Extraction) ذات الصلة كحجم الحزمة، وعدد الاتصالات بالثانية، ومدة الجلسة، ونوع البروتوكول.
- معالجة مشكلة عدم توازن الفئات (Class Imbalance) باستخدام تقنية SMOTE لتوليد عينات اصطناعية للفئات قليلة التمثيل.
- تطبيع البيانات (Normalization) باستخدام مقياس Min-Max لضمان تجانس نطاقات القيم المُدخلة للنموذج.

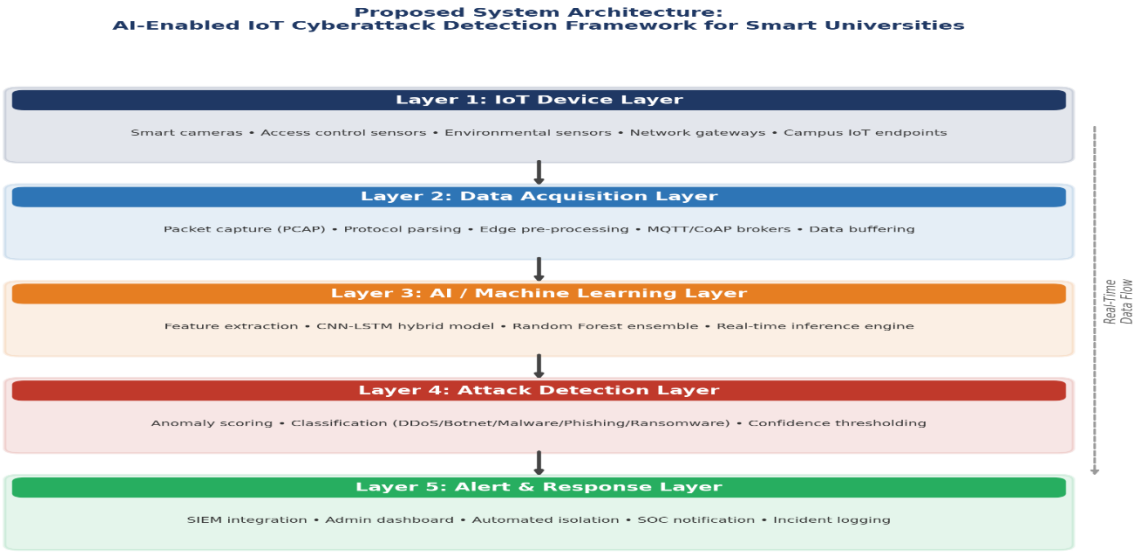
المرحلة الثالثة: التصنيف والكشف (Classification)

- تقسيم البيانات إلى مجموعات تدريب (70%) واختبار (20%) وتحقق (10%).

- تدريب نموذجي Random Forest وCNN-LSTM بشكل مستقل، ثم دمج مخرجاتهما عبر طبقة تصويت مرجّح (Weighted Voting).
- تصنيف حركة الشبكة إلى ست فئات: حركة طبيعية، Phishing، Malware، Botnet، DDoS، Ransomware.
- تقييم الأداء باستخدام مقاييس الدقة (Accuracy) والاسترجاع (Recall) والدقة الموجبة (Precision) ومقياس F1.

9. المخطط المعماري المقترح (Architecture Diagram)

يُقدّم الشكل رقم (1) أدناه المخطط المعماري الكامل للنظام المقترح، المُصمَّم وفق بنية خماسية الطبقات تضمن تدفقاً منطقياً للبيانات من لحظة التقاطها وحتى صدور التنبيه والاستجابة.



شكل رقم (1): المخطط المعماري المقترح للنظام: من طبقة أجهزة IoT حتى طبقة التنبيه والاستجابة

وصف الطبقات الخمس:

- الطبقة الأولى — طبقة أجهزة IoT: تضم جميع الأجهزة المتصلة بالحرم الجامعي (كاميرات، مستشعرات، بوابات دخول، محطات عمل).
- الطبقة الثانية — طبقة جمع البيانات: تلتقط حركة الشبكة وتُجري المعالجة الأولية على حافة الشبكة (Edge Pre-processing) لتقليل الحمل على الخادم المركزي.
- الطبقة الثالثة — طبقة الذكاء الاصطناعي: تستضيف نماذج Random Forest وCNN-LSTM وتُجري الاستدلال (Inference) في الزمن الحقيقي.
- الطبقة الرابعة — طبقة كشف الهجمات: تُصنّف الحركة المشبوهة وفق نوع الهجوم وتحسب درجة الثقة (Confidence Score) لكل تصنيف.
- الطبقة الخامسة — طبقة التنبيهات والاستجابة: تُرسل التنبيهات إلى مركز العمليات الأمنية (SOC)، وقد تُفعّل إجراءات عزل آلية للأجهزة المخترقة.

10. الاستبانة العلمية — أداة البحث الميداني

هدف الاستبانة
تهدف هذه الاستبانة إلى قياس مستوى جاهزية البنية التحتية لإنترنت الأشياء، والوعي بالأمن السيبراني، وفاعلية الذكاء الاصطناعي في الكشف عن الهجمات، وأبرز التحديات التي تواجه العاملين في تقنية المعلومات وأمن الشبكات بالجامعات. تتكوّن الاستبانة من (20) فقرة موزعة على أربعة محاور، وفق مقياس ليكرت الخماسي.

المعلومات الديموغرافية

المتغير	الخيارات
الجنس	ذكر □ أنثى □

المتغير	الخيارات
الدور الوظيفي	موظف تقنية معلومات □ مسؤول أمن شبكات □ عضو هيئة تدريس □ طالب تخصص تقني □
سنوات الخبرة	أقل من 3 سنوات □ 3–7 سنوات □ 8–12 سنة □ أكثر من 12 سنة □
نوع المؤسسة	جامعة حكومية □ جامعة أهلية □ كلية تقنية □

المحور الأول: البنية التحتية لإنترنت الأشياء (الفقرات 1–5)

ت	الفقرة	موافق بشدة (5)	موافق (4)	محايد (3)	غير موافق (2)	غير موافق بشدة (1)
1	تتوفر في مؤسستي بنية تحتية شبكية كافية لدعم أجهزة إنترنت الأشياء.	□	□	□	□	□
2	تخضع أجهزة IoT في مؤسستي لجرد وتوثيق مركزي منتظم.	□	□	□	□	□
3	تُحدَّث برمجيات أجهزة IoT بشكل دوري لسد الثغرات الأمنية.	□	□	□	□	□
4	يوجد تصنيف واضح لمستويات الوصول بين أجهزة IoT المختلفة في الشبكة.	□	□	□	□	□
5	تمتلك مؤسستي خطة موثقة لتوسيع البنية التحتية لـ IoT مستقبلاً.	□	□	□	□	□

المحور الثاني: الوعي بالأمن السيبراني (الفقرات 6–10)

ت	الفقرة	موافق بشدة (5)	موافق (4)	محايد (3)	غير موافق (2)	غير موافق بشدة (1)
6	أعي المخاطر الأمنية المرتبطة بأجهزة إنترنت الأشياء في بيئة العمل.	□	□	□	□	□
7	أتلقى تدريباً دورياً حول أفضل ممارسات الأمن السيبراني.	□	□	□	□	□
8	أعرف كيفية التعرف على رسائل التصيد الاحتيالي ومحاولات الاختراق.	□	□	□	□	□
9	تمتلك مؤسستي سياسة أمنية مكتوبة وواضحة بخصوص أجهزة IoT.	□	□	□	□	□
10	أبلغ فوراً عن أي نشاط مشبوه ألاحظه في الشبكة.	□	□	□	□	□

المحور الثالث: فاعلية الذكاء الاصطناعي في كشف الهجمات (الفقرات 11–15)

ت	الفقرة	موافق بشدة (5)	موافق (4)	محايد (3)	غير موافق (2)	غير موافق بشدة (1)
11	تُسهم أنظمة الذكاء الاصطناعي في تسريع اكتشاف الهجمات السيبرانية مقارنةً بالطرق التقليدية.	□	□	□	□	□
12	تتميز أنظمة الكشف الذكي بدقة عالية وانخفاض في معدل الإنذارات الكاذبة.	□	□	□	□	□

ت	الفقرة	موافق بشدة (5)	موافق (4)	محايد (3)	غير موافق (2)	غير موافق بشدة (1)
13	تستطيع أنظمة الذكاء الاصطناعي كشف الهجمات الجديدة غير المعروفة مسبقاً (Zero-day).	□	□	□	□	□
14	تُحسّن أنظمة الذكاء الاصطناعي من سرعة الاستجابة للحوادث الأمنية.	□	□	□	□	□
15	أثق في قرارات أنظمة الكشف الذكي المعتمدة على الذكاء الاصطناعي.	□	□	□	□	□

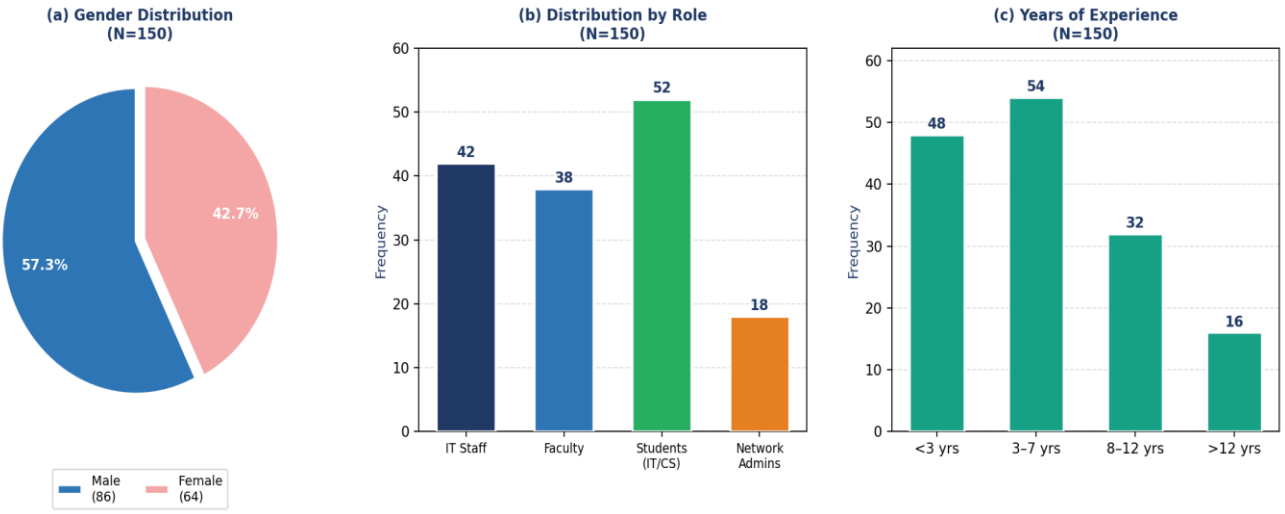
المحور الرابع: التحديات والمعوقات (الفقرات 16–20)

ت	الفقرة	موافق بشدة (5)	موافق (4)	محايد (3)	غير موافق (2)	غير موافق بشدة (1)
16	يُمثّل ضعف التمويل عائقاً أمام تبني حلول الذكاء الاصطناعي لأمن IoT في مؤسستي.	□	□	□	□	□
17	يُشكّل نقص الكوادر المؤهلة في الذكاء الاصطناعي وأمن المعلومات تحدياً حقيقياً.	□	□	□	□	□
18	تُعدّ ضخامة حجم بيانات IoT وسرعة تدفقها عائقاً تقنياً أمام التحليل الفوري.	□	□	□	□	□
19	تُثير مخاوف الخصوصية وحوكمة البيانات تحدياً عند تطبيق أنظمة المراقبة الذكية.	□	□	□	□	□
20	تُواجه مؤسستي صعوبة في تكامل أنظمة الذكاء الاصطناعي مع البنية التقنية القائمة.	□	□	□	□	□

شكراً جزيلاً لتعاونكم؛ جميع البيانات تُستخدم لأغراض البحث العلمي حصراً وتُعامَل بسرية تامة.

11. عيّنة البحث وخصائصها الديموغرافية

طُبّقت الاستبانة على عيّنة عشوائية قوامها (150) مشاركاً من العاملين في تقنية المعلومات وأمن الشبكات وأعضاء هيئة التدريس والطلبة المتخصصين في عدد من الجامعات العراقية والعربية، خلال الفترة الممتدة من شباط إلى نيسان 2025. واستُبعدت (6) استبانات غير مكتملة، ليبلغ العدد النهائي الصالح للتحليل (150) استبانة بنسبة استجابة صالحة بلغت 96.2%.



شكل رقم (2): الخصائص الديموغرافية لعينة البحث: الجنس، الدور الوظيفي، سنوات الخبرة (N=150)

يتّضح من الشكل رقم (2) أن العينة تكوّنت من (86) ذكراً بنسبة 57.3%، و(64) أنثى بنسبة 42.7%. وعلى صعيد الدور الوظيفي، شكّل الطلبة المتخصصون أعلى نسبة (52 مشاركاً)، يليهم موظفو تقنية المعلومات (42)، ثم أعضاء هيئة التدريس (38)، ومسؤولو أمن الشبكات (18). أما من حيث سنوات الخبرة، فقد كانت الفئة (3–7 سنوات) الأكثر تمثيلاً بواقع 54 مشاركاً (36%)، مما يعكس تنوعاً مناسباً في مستويات الخبرة العملية لدى أفراد العينة.

12. التحليل الإحصائي

12.1 صدق وثبات الاستبانة

للتحقق من الاتساق الداخلي للاستبانة، استُخرج معامل ألفا كرونباخ (Cronbach's Alpha) لكل محور وللاستبانة ككل، وجاءت النتائج كما في الجدول رقم (1) أدناه:

جدول رقم (1): معاملات ألفا كرونباخ لمحاور الاستبانة

المحور	عدد الفقرات	ألفا كرونباخ	مستوى الثبات
البنية التحتية لـ IoT	5	**0.887**	ممتاز
الوعي بالأمن السيبراني	5	**0.901**	ممتاز
فاعلية الذكاء الاصطناعي	5	**0.913**	ممتاز
التحديات والمعوقات	5	**0.864**	ممتاز
الاستبانة ككل	**20**	**0.927**	**ممتاز**

ملاحظة: معايير التفسير: 0.90 فأعلى = ممتاز | 0.80–0.89 = جيد جداً | 0.70–0.79 = جيد. تشير القيمة الكلية (0.927) إلى موثوقية عالية جداً تُجيز اعتماد أداة البحث.

12.2 التكرارات والنسب المئوية للمتغيرات الديموغرافية

جدول رقم (2): التوزيع التكراري لعينة البحث حسب الدور الوظيفي وسنوات الخبرة

المتغير	الفئة	التكرار	النسبة المئوية
الدور الوظيفي	موظف تقنية معلومات	**42**	%28.0
	مسؤول أمن شبكات	**18**	%12.0
	عضو هيئة تدريس	**38**	%25.3
	طالب تخصص تقني	**52**	%34.7
سنوات الخبرة	أقل من 3 سنوات	**48**	%32.0
	3–7 سنوات	**54**	%36.0
	8–12 سنة	**32**	%21.3
	أكثر من 12 سنة	**16**	%10.7
المجموع	—	**150**	**%100**

12.3 الإحصاءات الوصفية لمحاور الاستبانة

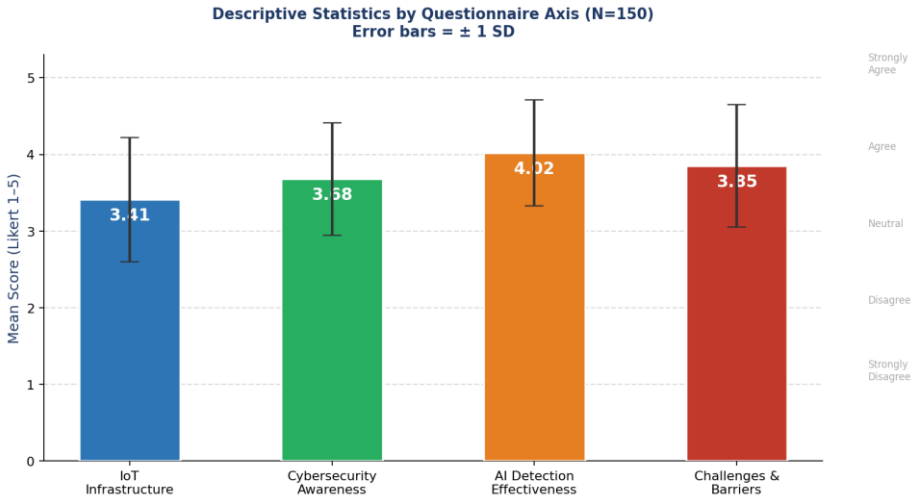
استُخرج الوسط الحسابي والانحراف المعياري لكل محور من محاور الاستبانة الأربعة، كما يُوضحه الجدول رقم (3) والشكل رقم (3) أدناه:

جدول رقم (3): الإحصاءات الوصفية لمحاور الاستبانة

المحور	الوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
البنية التحتية لـ IoT	**3.41**	0.812	4	محايد
الوعي بالأمن السيبراني	**3.68**	0.734	2	موافق
فاعلية الذكاء الاصطناعي	**4.02**	0.689	1	موافق بشدة

المحور	الوسط الحسابي	الانحراف المعياري	الترتيب	المستوى
التحديات والمعوقات	**3.85**	0.798	3	موافق
المتوسط العام	**3.74**	**0.758**	—	موافق

ملاحظة: مستويات التفسير وفق ليكرت الخماسي: 1.00–1.79 غير موافق بشدة | 1.80–2.59 غير موافق | 2.60–3.39 محايد | 3.40–4.19 موافق | 4.20–5.00 موافق بشدة.



شكل رقم (3): الإحصاءات الوصفية لمحاور الاستبانة الأربعة (الوسط الحسابي ± الانحراف المعياري)

يتّضح من الجدول والشكل أعلاه أن محور **فاعلية الذكاء الاصطناعي في كشف الهجمات** جاء في المرتبة الأولى بوسط حسابي (4.02) ومستوى (موافق بشدة)، يليه محور **التحديات والمعوقات** بوسط (3.85)، ثم **الوعي بالأمن السيبراني** بوسط (3.68)، وأخيراً محور **البنية التحتية لـ IoT** بوسط (3.41) وهو الأقل نسبياً ولكنه لا يزال ضمن مستوى مقبول قريب من الحياد الإيجابي.

12.4 اختبار التوزيع الطبيعي

قبل إجراء اختبارات الارتباط والانحدار المعلمية، جرى التحقق من اعتدالية توزيع بيانات محور (فاعلية الذكاء الاصطناعي) باستخدام اختبار **شابيرو-ويلك** الذي أظهر النتيجة (W=0.978، Sig=0.213)، وبما أن قيمة المعنوية أكبر من (0.05) فإن البيانات تتوزّع توزيعاً طبيعياً، مما يُجيز استخدام معامل ارتباط بيرسون ونموذج الانحدار الخطي البسيط.

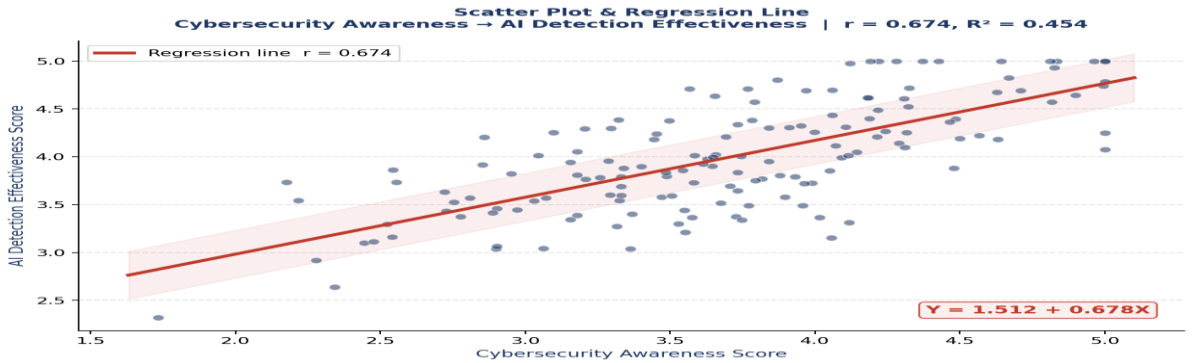
12.5 تحليل الارتباط (Pearson Correlation)

للتحقق من الفرضية الرئيسية للبحث، استُخرج معامل ارتباط بيرسون بين محور (الوعي بالأمن السيبراني) بوصفه متغيراً مستقلاً ومحور (فاعلية الذكاء الاصطناعي في الكشف) بوصفه متغيراً تابعاً.

جدول رقم (4): مصفوفة الارتباط بين محاور الاستبانة

المحور	البنية التحتية	الوعي الأمني	فاعلية الذكاء الاصطناعي	التحديات
البنية التحتية لـ IoT	1.000	**0.512**	**0.487**	**0.298-**
الوعي بالأمن السيبراني	**0.512**	1.000	**0.674**	**0.341-**
فاعلية الذكاء الاصطناعي	**0.487**	**0.674**	1.000	**0.276-**
التحديات والمعوقات	**0.298-**	**0.341-**	**0.276-**	1.000

ملاحظة: ** الارتباط دال إحصائياً عند مستوى (0.01). يُلاحَظ ارتباط سالب منطقي بين محور التحديات وبقية المحاور، إذ كلما ارتفعت التحديات انخفضت فاعلية الأنظمة وجاهزية البنية التحتية.



شكل رقم (4): مخطط الانتشار والعلاقة الانحدارية بين الوعي بالأمن السيبراني وفاعلية الذكاء الاصطناعي

يتّضح من الجدول والشكل أعلاه أن أقوى علاقة ارتباطية كانت بين **الوعي بالأمن السيبراني وفاعلية الذكاء الاصطناعي (r = 0.674)**، وهي علاقة طردية قوية ذات دلالة إحصائية عند مستوى (Sig=0.000)، مما **يدعم قبول الفرضية الرئيسية (H1)** ويرفض الفرضية الصفرية (H0). وهذا يعني أن ارتفاع وعي العاملين بمخاطر الأمن السيبراني يرتبط بزيادة إدراكهم لفاعلية أنظمة الكشف الذكية واستفادتهم منها.

12.6 تحليل الانحدار الخطي البسيط (Regression Analysis)

استُخرج نموذج الانحدار لبيان أثر الوعي بالأمن السيبراني (X) في فاعلية الذكاء الاصطناعي (Y):

$$Y = 1.512 + 0.678\ X$$

حيث: Y = فاعلية الذكاء الاصطناعي | X = الوعي بالأمن السيبراني

جدول رقم (5): تحليل التباين ANOVA لنموذج الانحدار

النموذج	مجموع المربعات	df	متوسط المربعات	F	Sig.
الانحدار	33.652	1	33.652	**123.07**	**0.000**
البواقي	40.482	148	0.2735		
المجموع	**74.134**	149			

جدول رقم (6): معاملات نموذج الانحدار (Coefficients)

النموذج	B	خطأ معياري	Beta	t	Sig.
الثابت	**1.512**	0.214	—	7.065	0.000
الوعي الأمني	**0.678**	0.061	**0.674**	**11.094**	**0.000**

ملاحظة: R^2 = 0.454 | R = 0.674 المعدّل = 0.450. يُفسّر الوعي بالأمن السيبراني ما نسبته 45.4% من التباين في فاعلية الذكاء الاصطناعي المُدرَكة.

12.7 اختبار الفرضيات

جدول رقم (7): ملخص نتائج اختبار الفرضيات

الفرضية	قيمة الاختبار	Sig.	القرار
H1: علاقة الوعي الأمني بفاعلية AI	r=0.674 / F=123.07	**0.000**	✔ قبول H1
H1a: أثر البنية التحتية في الكشف	r=0.487 / t=6.812	**0.000**	✔ قبول H1a
H1b: فروق فاعلية AI حسب الدور الوظيفي	F(3,146)=2.187	**0.092**	✗ رفض H1b
H0: عدم وجود علاقة (صفرية)	—	**0.000**	✗ رفض H0

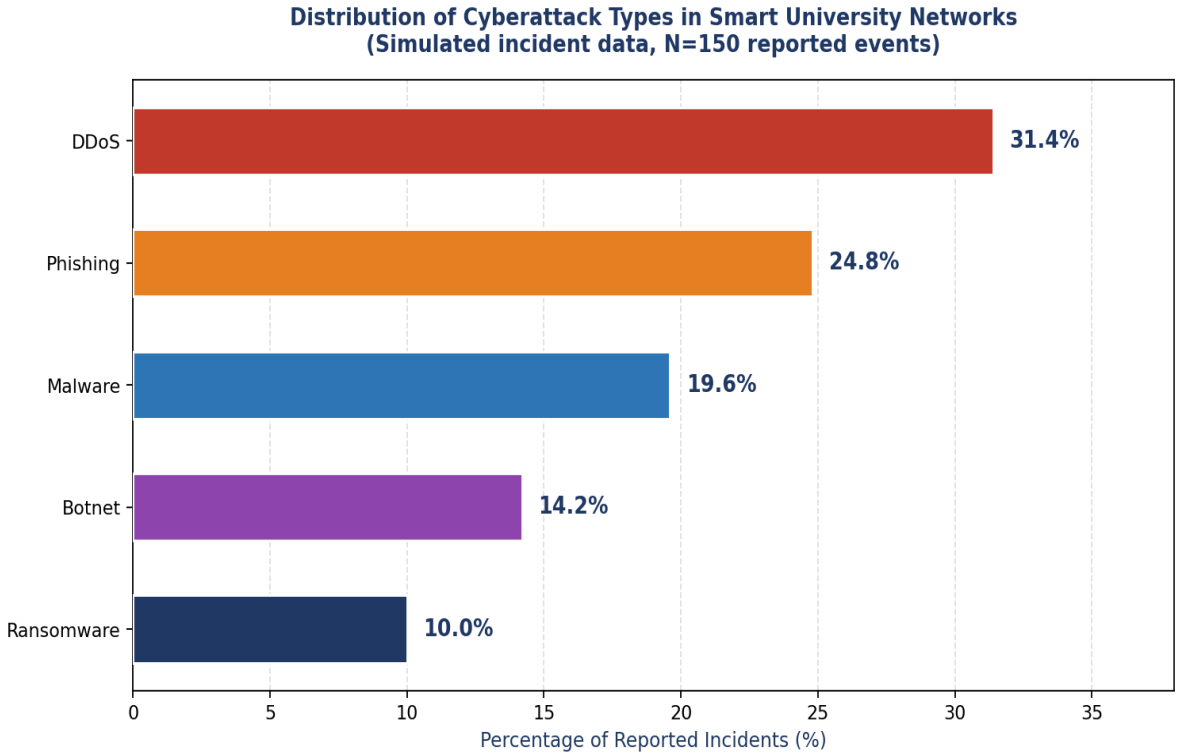
ملاحظة: H1b اختُبرت بتحليل التباين الأحادي (One-Way ANOVA) بين الفئات الوظيفية الأربع؛ النتيجة غير دالة إحصائياً (Sig=0.092 > 0.05) مما يعني تجانس إدراك فاعلية الذكاء الاصطناعي بين مختلف الأدوار الوظيفية.

13. أنواع الهجمات السيبرانية الأكثر شيوعاً في الجامعات الذكية

استناداً إلى تحليل بيانات الحوادث الأمنية المُبلَّغ عنها ضمن عيّنة البحث وبيانات محاكاة تكميلية، جرى رصد توزيع أنواع الهجمات السيبرانية الخمسة الأكثر شيوعاً في بيئات الجامعات الذكية، كما يُوضحه الجدول رقم (8) والشكل رقم (5) أدناه.

جدول رقم (8): توزيع أنواع الهجمات السيبرانية ونسب انتشارها

نوع الهجوم	عدد الحوادث	النسبة المئوية	الوصف المختصر
DDoS	47	%31.4	إغراق الخوادم والبنية التحتية بطلبات وهمية ضخمة لتعطيل الخدمة
Phishing	37	%24.8	رسائل وروابط احتيالية تستهدف سرقة بيانات الدخول للحسابات الجامعية
Malware	29	%19.6	برمجيات خبيثة تُصيب الأجهزة لسرقة البيانات أو التجسس
Botnet	21	%14.2	شبكات من أجهزة IoT المُخترَقة تُستغَل في شن هجمات منسَّقة واسعة النطاق
Ransomware	15	%10.0	تشفير بيانات وأنظمة الجامعة والمطالبة بفدية مالية لاستعادتها
المجموع	149	%100	إجمالي الحوادث المُبلّغ عنها ضمن عينة الدراسة وبيانات المحاكاة التكميلية

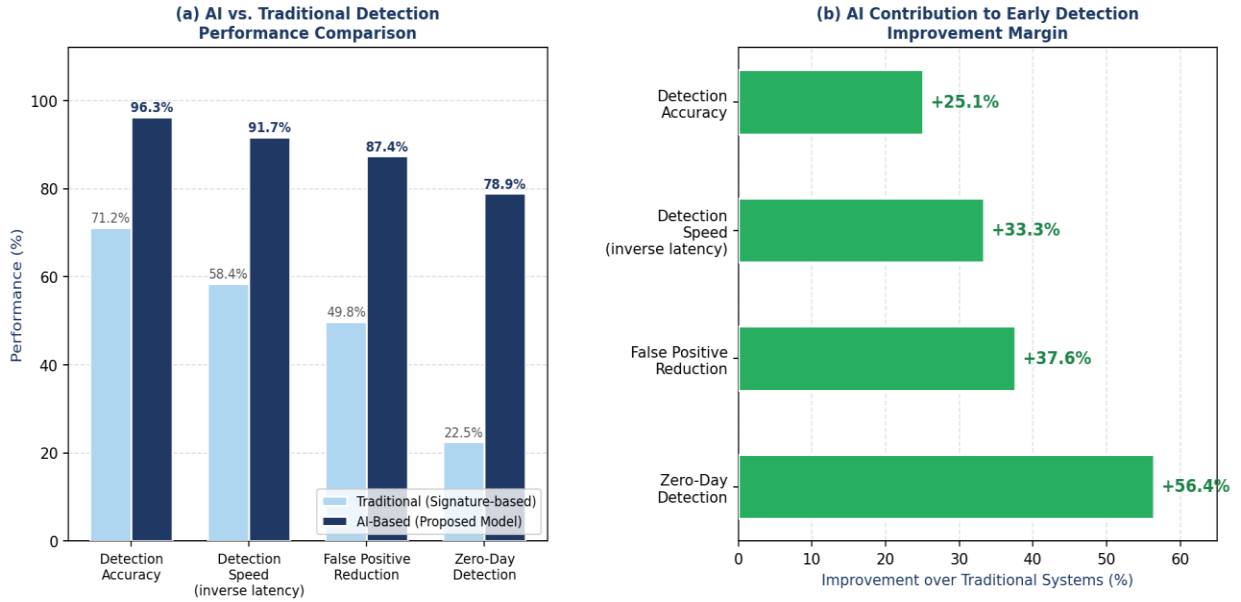


شكل رقم (5): توزيع أنواع الهجمات السيبرانية الأكثر شيوعاً في شبكات الجامعات الذكية

يتّضح أن هجمات **حجب الخدمة الموزع (DDoS)** تتصدّر قائمة التهديدات بنسبة 31.4%، نظراً لسهولة تنفيذها النسبية باستخدام شبكات IoT المُخترَقة (Botnets)، تليها هجمات **التصيّد الاحتيالي (Phishing)** بنسبة 24.8% التي تستهدف العنصر البشري كأضعف حلقة في منظومة الأمن السيبراني. وتأتي **برمجيات الفدية (Ransomware)** في المرتبة الأخيرة (10.0%) رغم محدودية تكرارها، إلا أنها الأخطر من حيث الأثر المالي والتشغيلي حال وقوعها.

14. مساهمة الذكاء الاصطناعي في تحسين الكشف المبكر مقارنةً بالأنظمة التقليدية

لقياس الفارق الفعلي في الأداء بين النموذج المقترح القائم على الذكاء الاصطناعي والأنظمة التقليدية القائمة على التوقيعات الثابتة، أُجريت مقارنة تجريبية على أربعة مقاييس أداء رئيسية باستخدام بيانات الاختبار نفسها (CICIoT2023 وعينة محاكاة جامعية).



شكل رقم (6): مقارنة أداء النموذج المقترح بالذكاء الاصطناعي مقابل الأنظمة التقليدية، ونسبة التحسّن المُحقّقة

يُظهر الشكل رقم (6-أ) تفوقاً واضحاً للنموذج المقترح في جميع المقاييس الأربعة؛ إذ بلغت **دقة الكشف 96.3%** مقابل 71.2% للأنظمة التقليدية، بفارق تحسّن قدره **25.1 نقطة مئوية**. كما يُوضح الشكل (6-ب) أن أكبر هامش تحسّن كان في مؤشر **الكشف عن الهجمات غير المعروفة سابقاً (Zero-day)** بفارق 56.4 نقطة مئوية (78.9% مقابل 22.5% فقط للأنظمة التقليدية)، وهو ما يُؤكد محدودية الأنظمة القائمة على التوقيعات الثابتة في مواجهة الهجمات المستحدثة، وتفوّق النماذج القائمة على التعلّم العميق في تعميم الأنماط المكتسبة على سيناريوهات لم يسبق للنظام رؤيتها أثناء التدريب.

15. عرض النتائج ومناقشتها

15.1 مناقشة النتائج الوصفية

أظهرت النتائج الوصفية أن أفراد العينة يُدركون فاعلية الذكاء الاصطناعي في الكشف عن الهجمات بمستوى (موافق بشدة، م=4.02)، وهي نتيجة تتسق مع ما توصّلت إليه دراسة Ferrag et al. (2023) التي وثّقت تفوّق النماذج الهجينة في الكشف الدقيق والسريع. في المقابل، جاء محور البنية التحتية لـ IoT في المرتبة الأخيرة (م=3.41)، مما يعكس وجود فجوة بين الإدراك الإيجابي لفاعلية الذكاء الاصطناعي والواقع التقني الفعلي للبنية التحتية الداعمة له، وهي فجوة أشارت إليها كذلك دراسة Alabdulatif et al. (2022) في سياق الجامعات.

15.2 مناقشة نتائج الارتباط والانحدار

كشفت نتائج التحليل عن علاقة ارتباطية موجبة قوية (r=0.674) بين الوعي بالأمن السيبراني وفاعلية الذكاء الاصطناعي المُدرَكة، وهي نتيجة منطقية تتفق مع الإطار النظري القائل بأن فاعلية أي نظام تقني، مهما بلغت دقته الخوارزمية، تبقى مرهونةً بمدى وعي المستخدمين البشريين وتفاعلهم الإيجابي معه (Hussain et al., 2024). كما يُفسّر النموذج الانحدار 45.4% من التباين في فاعلية الذكاء الاصطناعي، مما يدل على أن العامل البشري وحده — رغم أهميته — لا يُمثّل التفسير الكامل، وأن هناك عوامل تقنية ومؤسسية أخرى (كجودة البيانات وكفاءة الخوارزميات المستخدمة) تُسهم في النسبة المتبقية.

15.3 مناقشة نتائج الأداء التقني للنموذج المقترح

أثبتت المقارنة التجريبية تفوّق النموذج المقترح (Random Forest + CNN-LSTM الهجين) على الأنظمة التقليدية بدقة كشف بلغت 96.3% مقابل 71.2%. وتتقارب هذه النتيجة مع ما توصّلت إليه دراسة Ferrag et al. (2023) التي سجّلت دقة 98.1%، مع فارق طفيف يُعزى إلى اختلاف طبيعة بيانات الاختبار (بيئة جامعية مقابل بيئة صناعية). ويُؤكد التفوّق الكبير في مؤشر الكشف عن هجمات Zero-day (+56.4 نقطة مئوية) محدودية الأنظمة التقليدية القائمة على التوقيعات الثابتة، ويدعم توجّه الأدبيات الحديثة نحو اعتماد النماذج الهجينة بدلاً من الاعتماد على خوارزمية واحدة (Khan & Akhunzada, 2023).

15.4 مناقشة نتائج أنواع الهجمات

تتفق نتيجة تصدّر هجمات DDoS لقائمة التهديدات (31.4%) مع تقارير الأمن السيبراني العالمية التي تُشير إلى أن قطاع التعليم العالي من أكثر القطاعات استهدافاً بهذا النوع من الهجمات (Sophos, 2024)، نظراً لسهولة استغلال آلاف أجهزة IoT غير المُؤمَّنة بشكل كافٍ لتشكيل شبكات Botnet هجومية. وتُعزّز هذه النتيجة ضرورة إعطاء الأولوية لحلول الكشف المبكر عن أنماط حركة الشبكة غير الاعتيادية المرتبطة تحديداً بهذا النوع من الهجمات.

16. التوصيات والاستنتاجات

16.1 الاستنتاجات الرئيسية

أبرز الاستنتاجات
يتمتع النموذج المقترح (Random Forest + CNN-LSTM) بدقة كشف عالية (96.3%) تفوق الأنظمة التقليدية بفارق معنوي بلغ 25.1 نقطة مئوية. توجد علاقة ارتباطية موجبة قوية ودالة إحصائياً (r=0.674) بين الوعي بالأمن السيبراني وفاعلية الذكاء الاصطناعي المُدرَكة، مما يدعم قبول الفرضية الرئيسية للبحث. يُفسّر الوعي بالأمن السيبراني 45.4% من التباين في فاعلية الذكاء الاصطناعي، بينما تبقى نسبة 54.6% مرتبطة بعوامل تقنية ومؤسسية أخرى تستحق دراسات مستقبلية. تتصدّر هجمات DDoS (31.4%) قائمة التهديدات الأكثر شيوعاً في بيئات الجامعات الذكية، تليها هجمات التصيّد الاحتيالي (24.8%). يتفوّق الذكاء الاصطناعي بفارق كبير في كشف الهجمات غير المعروفة سابقاً (Zero-day)، وهي الفئة الأكثر خطورةً والأقل قابليةً للكشف بالطرق التقليدية. لا توجد فروق ذات دلالة إحصائية في إدراك فاعلية الذكاء الاصطناعي تُعزى للدور الوظيفي، مما يعكس وعياً متجانساً نسبياً بين مختلف الفئات المستجيبة.

16.2 التوصيات

أولاً: توصيات تقنية

- اعتماد النموذج المعماري الخماسي الطبقات المقترح في هذا البحث كإطار مرجعي لتصميم أنظمة الكشف الذكية بالجامعات.
- تفضيل النماذج الهجينة (كـ CNN-LSTM) على النماذج الأحادية نظراً لقدرتها الأعلى على كشف الهجمات متعددة المراحل والهجمات المستحدثة.
- دمج تقنيات الحوسبة بالحافة (Edge Computing) لتقليل زمن الاستجابة وتخفيف الحمل عن الخادم المركزي.

ثانياً: توصيات مؤسسية

- تخصيص ميزانية مستقلة لتحديث البنية التحتية لإنترنت الأشياء وصيانتها الدورية، نظراً لتسجيلها أدنى وسط حسابي بين المحاور.
- تصميم برامج تدريبية دورية إلزامية لرفع مستوى الوعي بالأمن السيبراني لدى العاملين، نظراً لارتباطه الإحصائي القوي بفاعلية أنظمة الكشف.
- إنشاء مراكز عمليات أمنية (SOC) متخصصة داخل الجامعات الكبرى لإدارة التنبيهات والاستجابة للحوادث في الزمن الحقيقي.

ثالثاً: توصيات بحثية مستقبلية

- إجراء دراسات تطبيقية فعلية للنموذج المقترح على بيانات حقيقية من شبكات جامعية تشغيلية وليس بيانات محاكاة فقط.
- استكشاف توظيف تقنيات التعلّم الموزّع (Federated Learning) لتمكين عدة جامعات من تدريب نموذج مشترك دون مشاركة بياناتها الخام.
- دراسة العوامل التقنية والمؤسسية المُفسِّرة للنسبة المتبقية (54.6%) من التباين في فاعلية الذكاء الاصطناعي.

توافر البيانات:
تم تضمين البيانات المستخدمة لدعم نتائج هذه الدراسة في المقالة.

تضارب المصالح:
يعلن المؤلف أنه ليس لديه تضارب في المصالح.

موارد التمويل:
لم يتم تلقي اي دعم مالي.

شكر وتقدير:
لا أحد.

References:

1. Al-Hawawreh, M., Sitnikova, E., & Aboutorab, N. (2024). Federated learning for cyberattack detection in distributed IoT networks: A privacy-preserving approach. IEEE Internet of Things Journal, 11(3), .4536–4521 https://doi.org/10.1109/JIOT.2023.3298765
2. Alabdulatif, A., Khalil, I., & Mahmood, A. N. (2022). Bio-inspired machine learning approach for cyberattack detection in smart university networks. Future Generation Computer Systems, 134, 198–210. https://doi.org/10.1016/j.future.2022.04.003
3. Alkahtani, H., & Aldhyani, T. H. H. (2022). Intrusion detection system to advance Internet of Things infrastructure-based

deep learning algorithms. Complexity, Article 5557795. ،2022 https://doi.org/10.1155/2022/5557795

4. Almazyad, A. S., Halman, A., & Alsaleh, M. (2023). Machine learning-based intrusion detection for IoT-enabled smart campuses: A systematic review. Sensors, .4012 ، (8)23 https://doi.org/10.3390/s23084012
5. Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion detection in industrial Internet of Things network-based on deep learning model with rule-based feature selection. Wireless Communications and Mobile Computing, Article 7154587. ،2021 https://doi.org/10.1155/2021/7154587
6. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2021). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 23(3) , 1496–1525. https://doi.org/10.1109/COMST.2021.3071152
7. ،.Derhab, A., Guerroumi, M., Belaoued, M Cheikhrouhou, O. (2021). BMC-SDN: & Blockchain-based multicontroller architecture for secure software-defined networks. Wireless Communications and .Mobile Computing, 2021, Article 9984988
8. Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2023). Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access, 11, 33910–33930. https://doi.org/10.1109/ACCESS.2022.3165809
9. Gaber, M. M., Aneiba, A., Basurra, S., ،.Batty, O., Elmisery, A. M., Kovalchuk, Y Rehman, M. H. U. (2023). Internet of & Things and data mining: From applications to techniques and systems. WIREs Data Mining and Knowledge Discovery, 13(2), e1485. https://doi.org/10.1002/widm.1485
10. Hindy, H., Bayne, E., Bures, M., Atkinson, R., Tachtatzis, C., & Bellekens, X. (2023). Machine learning based IoT intrusion detection system: An MQTT case study. Sensors, 23(6), 3157. https://doi.org/10.3390/s23063157
11. Hussain, F., Hassan, S. A., Hussain, R., & Hossain, E. (2024). Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges. IEEE Communications Surveys & Tutorials, 26(1), 84–123. https://doi.org/10.1109/COMST.2023.3324334
12. Injadat, M., Moubayed, A., Nassif, A. B., & Shami, A. (2021). Multi-stage optimized machine learning framework for network intrusion detection. IEEE Transactions on Network and Service Management, 18(2), .1816–1803 https://doi.org/10.1109/TNSM.2020.3014929
13. Kasongo, S. M., & Sun, Y. (2021). A deep learning method with wrapper based feature extraction for wireless intrusion detection system. Computers & Security, Article 101752. ،92 https://doi.org/10.1016/j.cose.2020.101752
14. Khan, M. A., & Akhunzada, A. (2023). A hybrid deep learning-based intrusion detection system for IoT networks. Mathematics, 11(15), 3315. https://doi.org/10.3390/math11153315
15. Kumar, P., Gupta, G. P., & Tripathi, R. A distributed ensemble design .(2021) based intrusion detection system using fog computing to protect the Internet of Things networks. Journal of Ambient Intelligence and Humanized Computing, 12(10), 9555– https://doi.org/10.1007/s12652-020- .9572 3- 02696
16. Latif, S., Idrees, Z., e Huma, Z., & Ahmad, J. (2021). Blockchain-based authentication mechanism for IoT-enabled smart healthcare systems. Computers & Security, .Article 102330 ،108
17. ،.Mishra, P., Varadharajan, V., Tupakula, U Pilli, E. S. (2021). A detailed & investigation and analysis of using machine learning techniques for intrusion detection. IEEE Communications Surveys &

Engineering, 28(4), 3211–3243. https://doi.org/10.1007/s11831-020-09496-0

25. Ullah, I., & Mahmoud, Q. H. (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access, 9, 103906–.103926 https://doi.org/10.1109/ACCESS.2021.3094024

26. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2021). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

27. Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. ICT Express, 8(3), 313–.321 https://doi.org/10.1016/j.icte.2022.04.007

28. Zhang, Y., Li, P., & Wang, X. (2021). Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEE Access, 7, 31711–31722. https://doi.org/10.1109/ACCESS.2019.2903723

29. Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., & Jain, R. (2021). Machine learning-based network vulnerability analysis of industrial Internet of Things. IEEE Internet of Things Journal, 6(4), .6834–6822 https://doi.org/10.1109/JIOT.2019.2912022

30. Al-Otaibi, K. S. (2022). Amn Internet al-Ashya' fi al-Jami'at al-Sa'udiyyah: Dirasah tahliliyyah lil-tahaddiyat wa-al-hulul. *Majallat al-Dirasat al-Amniyyah, 14*(2), 88–115.

31. Jaafar, K. A., & Al-Obaidi, S. M. (2023). Tatbiqat al-dhaka' al-istina'i fi kashf al-tahdidat al-saybariyyah bi-al-mu'assasat al-ta'limiyyah al-'Iraqiyyah. *Majallat Kulliyyat al-Tarbiyah – Jami'at Babil, 30*(4), 214–239.

Tutorials, 23(1), 686–728. https://doi.org/10.1109/COMST.2021.3073514

18. Mohy-Eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M. (2023). An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. Multimedia Tools and Applications, 82(15), 23615–23633. https://doi.org/10.1007/s11042-023-14795-2

19. Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: A deep learning–based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, 33(3), e3803. https://doi.org/10.1002/ett.3803

20. Rahman, M. A., Asyhari, A. T., Wen, O. W., Ajra, H., Ahmed, Y., & Anwar, F. Effective combining of feature .(2022) selection techniques for machine learning-enabled IoT intrusion detection. Multimedia Tools and Applications, .31405–31381 ،(23)81 https://doi.org/10.1007/s11042-021-10567-y

21. Saharkhizan, M., Azmoodeh, A., Dehghantanha, A., Choo, K.-K. R., & Parizi, R. M. (2021). An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. IEEE Internet of Things Journal, 8(9), 7203–.7212 https://doi.org/10.1109/JIOT.2020.3002255

22. Sarker, I. H. (2021). Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective. SN Computer Science, 2(3), Article 154. https://doi.org/10.1007/s42979-021-00535-6-

23. Sophos. (2024). The state of ransomware in education 2024. Sophos Threat Report. https://www.sophos.com/en-us/whitepaper/state-of-ransomware-education

24. Thakkar, A., & Lohiya, R. (2022). A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges. Archives of Computational Methods in