

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص ماجستير إدارة المخاطر



إدارة مخاطر الذكاء الاصطناعي وكفاءة الطاقة

إعداد الطالب / احمد سعود البيشي

إشراف /

د. الفيصّل عبد الحميد

د. فايز جراد

العام الدراسي:

2026

مقدمة:

يشهد قطاع الطاقة في الآونة الأخيرة تحولاً نتيجة دمج تقنيات الذكاء الاصطناعي في إدارة الشبكات الكهربائية و تحسين كفاءة إستهلاك الطاقة بالإضافة الى إدارة مصادر الطاقة المتجددة و على الرغم من الفوائد التشغيلية و الاقتصادية الا أن هذا الدمج يخلق مخاطر تقنية و نظامية و إستراتيجية لذا تتطرق هذه الدراسة الى تحليل تلك المخاطر وفق منهجية إدارة مخاطر معتمدة على مصفوف (Likelihood x Impact) بما يتوافق من المعايير الدولية لـ ISO 31000 .

ويأتي هذا التحول في سياق عالمي يتسم بارتفاع الطلب على الطاقة، وتسارع التحول الرقمي، وتزايد الاعتماد على الأنظمة الذكية في إدارة البنى التحتية الحيوية. فالذكاء الاصطناعي لم يعد مجرد أداة تحليل بيانات، بل أصبح عنصراً فاعلاً في اتخاذ القرار التشغيلي اللحظي داخل الشبكات الكهربائية، وفي تحسين كفاءة تشغيل المحطات، وفي موازنة الأحمال بين مصادر الطاقة التقليدية والمتجددة. هذا الدور المتنامي يرفع من مستوى الاعتماد المؤسسي على الخوارزميات، ويحولها إلى مكوّن أساسي في منظومة اتخاذ القرار.

وفي السياق السعودي، تتضاعف أهمية هذا التحول نظراً للمكانة المحورية لقطاع الطاقة في الاقتصاد الوطني. فالمملكة العربية السعودية ليست فقط من أكبر منتجي الطاقة عالمياً، بل تمر بمرحلة تحول اقتصادي شامل يستهدف تنويع مصادر الدخل ورفع كفاءة الإنفاق وتعزيز الاستدامة. وتُعد مبادرات التحول الرقمي وتبني تقنيات الذكاء الاصطناعي جزءاً أصيلاً من مستهدفات رؤية السعودية 2030، التي تسعى إلى بناء اقتصاد معرفي قائم على الابتكار والتقنية .

علاوة على ذلك، فإن التوسع في البنية الرقمية الداعمة للذكاء الاصطناعي بما يشمل من مراكز بيانات وأنظمة تحليل ومعالجة يفرض تحديات مرتبطة باستهلاك الطاقة ذاته، ما يثير تساؤلات حول الأثر الصافي للتحول الرقمي على أهداف كفاءة الطاقة والاستدامة البيئية. ومن ثم، فإن تقييم المخاطر لا ينبغي أن يقتصر على المخاطر التشغيلية المباشرة، بل يجب أن يشمل المخاطر الاستراتيجية طويلة المدى، بما في ذلك مخاطر الاعتماد التقني، ومخاطر سلاسل التوريد، والمخاطر السيبرانية ذات البعد الأمني .

إن إدماج الذكاء الاصطناعي في منظومات الطاقة ضمن إطار التحول الوطني يتطلب تبني منهج إدارة مخاطر مؤسسية متكاملة (Enterprise Risk Management) ، تضمن تحقيق التوازن بين تعظيم المنافع وتقليل التعرض للمخاطر.

مشكلة الدراسة:

أدى تسارع التوسع في تطبيق تقنيات الذكاء الاصطناعي داخل قطاع الطاقة إلى تغيير جوهري في أساليب إدارة الشبكات الكهربائية وتحسين كفاءة استهلاك الطاقة، وهو تحول تدعمه العديد من الدراسات التي تشير إلى أن الأنظمة الذكية أصبحت تؤدي أدوارًا تشغيلية معقدة داخل منظومات الطاقة الحديثة (Worthmann & Malik, 2025).

ورغم أن هذا التحول أسهم في تعزيز موثوقية الأنظمة ورفع الكفاءة، إلا أنه أدى أيضًا إلى بروز مجموعة من المخاطر التشغيلية والنظامية والاستراتيجية التي تتطلب إدارة دقيقة وفق منهجيات متقدمة لإدارة المخاطر.

وتعد المخاطر التشغيلية أولى الإشكالات التي يثيرها الذكاء الاصطناعي، إذ تعتمد الشبكات الكهربائية على نماذج تعلم آلي في التنبؤ بالأحمال وضبط التوليد، وهي نماذج قد تتأثر بجودة البيانات أو انحرافات الخوارزميات، مما قد يؤدي إلى قرارات تشغيلية غير دقيقة أو غير متوقعة (Pandey et al., 2023). كما أن انتشار الأنظمة الذكية داخل الشبكات يجعلها عرضة للأخطاء المرتبطة بسوء تمثيل الظروف التشغيلية النادرة أو غير المتوقعة، وهو ما تؤكد تقارير قطاع الطاقة المتقدم (U.S. DOE, 2024).

أما الإشكالية الثانية فتربط بالآثار البيئية الناتجة عن التوسع في استخدام الذكاء الاصطناعي، إذ تشير دراسات حديثة إلى أن البنية الرقمية المصاحبة للذكاء الاصطناعي بما في ذلك مراكز البيانات وعمليات التدريب تستهلك كميات كبيرة من الطاقة وتزيد من الانبعاثات الكربونية، مما يخلق فجوة بين هدف التحول الرقمي وهدف الاستدامة البيئية (Oliveira et al., 2026). كما بينت دراسات أخرى أن استهلاك الطاقة في مرحلة الاستدلال inference قد يساوي أو يتجاوز مرحلة التدريب في بعض التطبيقات الضخمة، مما يفاقم هذا التحدي (Oliveira et al., 2026).

وتبرز الإشكالية الثالثة في البعد الاستراتيجي طويل المدى، حيث يشير عدد من الباحثين إلى أن تبني الذكاء الاصطناعي يرافقه اعتماد متزايد على موردي التقنيات وسلاسل الإمداد الرقمية، إضافة إلى التحديات المرتبطة بسرعة تقادم البرمجيات والحاجة المستمرة إلى تحديثات خوارزمية لضمان سلامة الأنظمة (Van Soest et al., 2024). وهذا النوع من الاعتماد قد يخلق مخاطر نظامية تؤثر على مرونة القطاع وقدرته على التكيف مع الأزمات أو التغيرات المفاجئة.

كما تشكل المخاطر السيبرانية أحد أبرز التحديات التي ربطتها الأدبيات باستخدام الذكاء الاصطناعي، حيث تؤكد تقارير متخصصة أن دمج الأنظمة الذكية داخل البنية التحتية قد يزيد من الهجمات المعقدة التي تستهدف الخوارزميات أو أنظمة التحكم في الشبكات (Majkut & Abrahams, 2025). وتطوّرت دراسات أخرى إلى أن الذكاء الاصطناعي قد يسهّل للهجمات السيبرانية استغلال الأنماط الخوارزمية أو التلاعب بمصادر البيانات

(U.S. DOE, 2024).

وفي السياق السعودي، يبرز هذا التحدي بصورة أكبر في ظل الدور الحيوي لقطاع الطاقة داخل الاقتصاد الوطني، وتوجهات رؤية السعودية 2030 التي تعتمد على التحول الرقمي وتبني الذكاء الاصطناعي في تعزيز كفاءة التشغيل وتنويع مصادر الطاقة. إلا أن الدراسات تؤكد غياب إطار شامل قادر على قياس المخاطر الناشئة عن الذكاء الاصطناعي وربطها بمؤشرات كفاءة الطاقة ضمن منهجية مؤسسية واضحة. (Rajaperumal & Columbus, 2025)

وبناءً على ما سبق، تتمثل مشكلة الدراسة في غياب إطار منهجي متكامل لتحديد وتقييم وإدارة المخاطر الناتجة عن دمج الذكاء الاصطناعي داخل قطاع الطاقة، وذلك بالاعتماد على منهجية (Likelihood × Impact) المتوافقة مع معايير ISO 31000، بما يضمن تحقيق التوازن بين الاستفادة القصوى من التقنيات الحديثة وتقليل التعرض للمخاطر التشغيلية والاستراتيجية والسيبرانية وتأثيراتها على كفاءة الطاقة.

أهمية الدراسة:

1- المساهمة في المعرفة الأكاديمية:

تعزز الدراسة الفهم العلمي المتعلق بتطبيقات الذكاء الاصطناعي في قطاع الطاقة، من خلال تحليل دوره في إدارة المخاطر التشغيلية والاستراتيجية، ورصد تأثيراته على كفاءة الطاقة واستدامتها. وتمثل الدراسة إضافة نوعية إلى الأدبيات العلمية التي تتناول التقنيات الذكية في القطاعات الحيوية.

2- التحليل العلمي للتحديات والفرص:

تقدم الدراسة تحليلاً معمقاً للتحديات التقنية والاقتصادية التي يواجهها قطاع الطاقة نتيجة التوسع في استخدام الذكاء الاصطناعي، كما تستعرض الفرص الممكنة لتحسين كفاءة الطاقة من خلال تطبيقات الذكاء الاصطناعي ودمجها ضمن إطار مؤسسي لإدارة المخاطر.

3- الإسهام في تطوير الأطر النظرية:

تساهم الدراسة في بناء أساس نظري متقدم لإدارة مخاطر الذكاء الاصطناعي، من خلال مواءمة منهجيات تقييم المخاطر مثل مصفوفة (Likelihood × Impact) مع معايير ISO 31000، بما يدعم صياغة نماذج أكثر ملاءمة للقطاعات الرقمية والذكية.

4- تحسين أداء الجهات المشغلة وصنّاع القرار:

تساعد الدراسة في توجيه الجهات المعنية نحو فهم أفضل لأنواع المخاطر التي تنشأ عن دمج الذكاء الاصطناعي في منظومة الطاقة، مما يعزز قدرتها على اتخاذ قرارات أكثر دقة وفعالية، ورفع مستوى الموثوقية التشغيلية والجاهزية التقنية للشبكات الكهربائية.

5- تعزيز الكفاءة التشغيلية للمؤسسات العاملة في قطاع الطاقة:

من خلال ربط استخدام الذكاء الاصطناعي باستهلاك الطاقة، تسهم الدراسة في تطوير أساليب تشغيلية تدعم تقليل الهدر ورفع مستويات الكفاءة، خصوصاً مع التوسع في مشاريع التحول الرقمي وزيادة الاعتماد على مصادر الطاقة المتجددة.

6- دعم السياسات الوطنية والتشريعات المستقبلية:

توفر الدراسة رؤى يمكن الاستفادة منها في صياغة سياسات وتشريعات تتوافق مع متطلبات التحول الرقمي في قطاع الطاقة، وتساعد صناع السياسات على بناء منظومة أكثر توافقاً مع أهداف الاستدامة وكفاءة الطاقة، بما يعزز تحقيق مستهدفات رؤية السعودية 2030.

أهداف الدراسة:

يهدف هذا البحث إلى التعرف على الهدف الرئيسي المتمثل في تحليل مخاطر دمج تقنيات الذكاء الاصطناعي في قطاع الطاقة، وقياس تأثير هذه المخاطر على كفاءة الطاقة واستدامتها، وذلك ضمن إطار منهجي يعتمد على مصفوفة (Likelihood × Impact) وبما يتوافق مع معايير ISO 31000 وانطلاقاً من هذا الهدف الرئيس، تتفرع الأهداف الفرعية التالية:

1. تحليل الوضع الحالي:

فهم آليات دمج الذكاء الاصطناعي في شبكات الطاقة والتطبيقات المرتبطة بإدارة الأحمال، والتعرف على أبرز التحديات التشغيلية والتقنية المرتبطة بالأتمتة الخوارزمية في هذا القطاع.

2. تحديد وتصنيف المخاطر:

دراسة أنواع المخاطر التي تنشأ عن استخدام الذكاء الاصطناعي في منظومة الطاقة، بما يشمل المخاطر التشغيلية، والبيئية المرتبطة باستهلاك الطاقة، والمخاطر الاستراتيجية، والمخاطر السيبرانية.

3. تقييم تأثير المخاطر على كفاءة الطاقة:

تحليل مدى تأثير تطبيقات الذكاء الاصطناعي على استهلاك الطاقة داخل البنى الرقمية ومراكز البيانات، وقياس الأثر الصافي لهذه التقنيات على أهداف الكفاءة والاستدامة.

4. تطبيق منهجية ISO 31000 في تقييم المخاطر:
بناء إطار لتقييم مخاطر الذكاء الاصطناعي باستخدام مصفوفة (Likelihood × Impact) ، ووضع معايير واضحة لتقدير مستوى الخطورة وآليات الحد منها بما يتوافق مع أفضل الممارسات الدولية.
5. استكشاف الفرص المستقبلية لتحسين كفاءة الطاقة:
تحليل الفرص التي يمكن أن يوفرها الذكاء الاصطناعي لرفع كفاءة الطاقة وتعزيز موثوقية الشبكات، مع دراسة السيناريوهات المستقبلية لتطوير القطاع.
6. اقتراح توصيات عملية للجهات المعنية:
تطوير مجموعة من التوصيات التي يمكن لصناع القرار والجهات المشغلة الاستفادة منها لوضع سياسات واستراتيجيات توازن بين تبني الذكاء الاصطناعي وتقليل المخاطر المترتبة عليه.

تساؤلات الدراسة:

ما هي مخاطر دمج تقنيات الذكاء الاصطناعي في قطاع الطاقة، وكيف يؤثر ذلك على كفاءة الطاقة واستدامتها؟
ويتفرع من هذا التساؤل الرئيسي الأسئلة البحثية التالية:

1. كيف ينعكس الاعتماد المتزايد على نماذج الذكاء الاصطناعي في الشبكات الكهربائية على مستوى المخاطر التشغيلية، وما هي التحديات المرتبطة باتخاذ القرار الآلي داخل منظومة الطاقة؟
2. ما أثر البنية الرقمية الداعمة للذكاء الاصطناعي وخاصة مراكز البيانات وعمليات التدريب الخوارزمي على استهلاك الطاقة، وكيف يمكن قياس هذا الأثر وتحديد حجم التحديات البيئية المرتبطة به؟
3. إلى أي مدى تسهم تقنيات الذكاء الاصطناعي في خلق مخاطر استراتيجية طويلة المدى، مثل الاعتماد التقني، ومخاطر سلاسل الإمداد، والمخاطر السيبرانية المرتبطة بالبنى التحتية الحيوية؟
4. كيف يمكن تطبيق منهجية مصفوفة (Likelihood × Impact) المستندة إلى معايير ISO 31000 في تقييم مخاطر الذكاء الاصطناعي داخل قطاع الطاقة، وما مدى ملاءمتها للسياق التشغيلي المحلي؟
5. ما الفرص المستقبلية التي يمكن أن يوفرها الذكاء الاصطناعي لتحسين كفاءة الطاقة، وكيف يمكن للجهات التشغيلية والاستراتيجية تحقيق توازن بين تعظيم الفائدة وتقليل المخاطر المصاحبة؟
6. كيف ينسجم دمج تقنيات الذكاء الاصطناعي في قطاع الطاقة مع مستهدفات رؤية السعودية 2030، وبخاصة تلك المتعلقة بالاستدامة، وكفاءة الطاقة، والتحول الرقمي، وما التحديات التي قد تعوق تحقيق هذا الانسجام؟

فروض الدراسة:

الفرضية الأولى

يوجد تأثير ذو دلالة إحصائية لاعتماد أنظمة الذكاء الاصطناعي في تشغيل الشبكات الكهربائية على مستوى المخاطر التشغيلية؛ بحيث يزداد احتمال حدوث قرارات آلية غير دقيقة مع ارتفاع الاعتماد على الخوارزميات في التنبؤ بالأحمال وإدارة التوليد.

الفرضية الثانية

يوجد تأثير ذو دلالة إحصائية للبنية الرقمية المصاحبة للذكاء الاصطناعي (مراكز البيانات، تدريب النماذج، منصات التحليل) على استهلاك الطاقة؛ بحيث ينعكس التوسع في قدرات الحوسبة على ارتفاع الاستهلاك الكلي للطاقة ما لم تُتبع ضوابط منهجية للفاعلية الطاقية.

الفرضية الثالثة

يوجد تأثير ذو دلالة إحصائية لتطبيق منهجية تقييم المخاطر ($Likelihood \times Impact$) المتوافقة مع ISO 31000 على تقليل مستوى المخاطر الصافية الناتجة عن دمج الذكاء الاصطناعي في قطاع الطاقة؛ وذلك عبر تحسين إجراءات التعرف والتقييم والمعالجة والمراقبة.

الفرضية الرابعة

يوجد تأثير ذو دلالة إحصائية لممارسات الأمن السيبراني وحوكمة النماذج (Model Governance) على خفض احتمالية وشدة الحوادث السيبرانية المرتبطة بأنظمة الذكاء الاصطناعي في منظومات الطاقة.

الفرضية الخامسة

يوجد تأثير ذو دلالة إحصائية لاعتماد تقنيات الذكاء الاصطناعي الموقر للطاقة (مثل ضغط النماذج، والتحسين الخوارزمي، والأجهزة عالية الكفاءة) على تحسين كفاءة الطاقة في البنية الرقمية لقطاع الطاقة مع الحفاظ على مستويات الأداء التشغيلي.

الفرضية السادسة

يوجد تأثير ذو دلالة إحصائية لملاءمة تطبيقات الذكاء الاصطناعي مع مستهدفات رؤية السعودية 2030 على تعظيم المنافع الاستراتيجية (الاستدامة، كفاءة الطاقة، التحول الرقمي) وتقليل التحديات التنظيمية والتشغيلية.

النظرية العلمية المبنية لإعداد البحث

في إعداد هذا البحث حول أثر دمج الذكاء الاصطناعي على كفاءة الطاقة ضمن إطار إدارة المخاطر، تم الاستناد إلى مجموعة من الأطر والنظريات العلمية الداعمة لصياغة الفروض وتفسير النتائج:

- 1- نظرية إدارة المخاطر (Risk Management Theory) إطار ISO 31000
ترتكز الدراسة إلى مبادئ إدارة المخاطر المؤسسية التي تنظم عمليات التعرف والتقييم والمعالجة والمراقبة. يُعتمد هذا الإطار لتوحيد تقدير الاحتمال/الأثر وتطوير مصفوفة المخاطر وربطها بمؤشرات كفاءة الطاقة.
- 2- نظرية الأمن السيبراني (Cybersecurity Theory)
تُبرز العلاقة بين مستوى الضوابط الأمنية وحوكمة البيانات/النماذج وبين انخفاض احتمالات الاختراق وآثاره على استمرارية الخدمة وموثوقية الشبكات. تدعم تفسير الفرضيات المرتبطة بالمخاطر السيبرانية للأنظمة الذكية.
- 3- نظرية الكلفة/المنفعة (Cost-Benefit Theory)
تعتمد هذه النظرية لقياس المنفعة التشغيلية والطاقة المتحققة من تطبيقات الذكاء الاصطناعي مقابل تكاليف الحوسبة والبنية الرقمية والمخاطر، بما يدعم اتخاذ قرارات تبني التقنية أو الحد منها وفق العائد الصافي.
- 4- نظرية المرونة التنظيمية (Organizational Flexibility/Resilience Theory)
تركز على قدرة الجهات المشغلة على التكيف والاستيعاب مع التحول الرقمي ومتطلبات الأمان والجودة، وتأثير ذلك على امتصاص الصدمات وتقليل حدة المخاطر التشغيلية والنظامية.
- 5- نظرية التكنولوجيا الرقمية/الاستدامة الرقمية (Digital Technology & Green AI Theory)
تفسر العلاقة بين تصميم النماذج والبرمجيات والأجهزة وبين الأثر الطاقي والبيئي، وكيف تُسهم ممارسات "الذكاء الاصطناعي الأخضر" في خفض الاستهلاك مع الحفاظ على الأداء.
- 6- النموذج الاجتماعي/التقني (Socio-Technical Systems Model)
يفسر تفاعل العوامل البشرية والتنظيمية مع العوامل التقنية عند دمج الذكاء الاصطناعي، وتأثير هذا التفاعل على المخاطر والامتثال والموثوقية.

كيفية تطبيق هذه النظريات في البحث

1. تحليل بيانات المخاطر:

يتم توظيف إطار ISO 31000 مع منهجية (Likelihood × Impact) لبناء مصفوفة مخاطر خاصة بتطبيقات الذكاء الاصطناعي في قطاع الطاقة، تتضمن تعريف مصادر الخطر، ومؤشرات الاحتمال، وقياسات الأثر، ومستويات القبول.

2. التقييم الكُلّي/المنفعي:

تُطبّق نظرية الكلفة/المنفعة لمقارنة سيناريوهات تبني الذكاء الاصطناعي (الأجهزة، التدريب، الاستدلال) مقابل مكاسب كفاءة الطاقة والموثوقية، مع احتساب كُلف الضوابط الأمنية والحوكمة.

3. فحص المرونة التنظيمية:

يُستخدم إطار المرونة التنظيمية لتقييم مدى استعداد الجهات المشغلة لتبني الحلول الذكية (سياسات، قدرات، مهارات)، وتأثير ذلك على خفض المخاطر التشغيلية والسيبرانية وتحسين الاستجابة للحوادث.

4. تحليل الأثر السيبراني:

تُستثمر نظرية الأمن السيبراني في تصميم مجموعة ضوابط (حوكمة البيانات، إدارة الهويات، مراقبة النماذج، اختبار الاختراق) وربطها بمؤشرات انخفاض الاحتمال/الأثر في مصفوفة المخاطر.

5. قياس الكفاءة الطاقية الرقمية:

يُفعّل إطار الاستدامة الرقمية Green AI لقياس مؤشرات استهلاك الطاقة في مراحل التدريب والاستدلال ومراكز البيانات، واختبار أثر تقنيات تقليل البصمة الكربونية على النتائج.

6. مواءمة رؤية 2030:

تُستخدم مداخل النظام الاجتماعي/التقني والمرونة التنظيمية لربط النتائج بمستهدفات رؤية السعودية 2030 (الاستدامة، الكفاءة، التحول الرقمي)، وتقييم المعوقات التنظيمية ومكامن التحسين.

الدراسات السابقة:

مقدمة

تُعَدّ الدراسات السابقة أساسًا لفهم الجوانب العلمية لموضوع مخاطر الذكاء الاصطناعي وكفاءة الطاقة، حيث تساعد في تحديد الاتجاهات العامة والتحديات المرتبطة بتطبيقاته في قطاع الطاقة. ويستعرض هذا القسم أبرز ما تناولته الأبحاث السابقة حول تأثير الذكاء الاصطناعي على كفاءة الطاقة، والمخاطر التقنية والبيئية والسيبرانية المرتبطة به، بما يريّ خلفية علمية تدعم دراسة هذا البحث.

* CESER (2024)

العنوان:

المخاطر والفوائد المحتملة للذكاء الاصطناعي في البنى التحتية الحيوية للطاقة.

المحتوى:

استعرضت هذه الدراسة الدور المتزايد للذكاء الاصطناعي في تعزيز كفاءة وتشغيل البنى التحتية للطاقة، بما في ذلك الشبكات الكهربائية وأنظمة التحكم الذكية. تناول التقرير المخاطر التقنية المصاحبة لاستخدام الذكاء الاصطناعي في الأنظمة الحرجة مثل:

- مخاطر سوء فهم النموذج للأنماط التشغيلية.
 - هجمات الخصومة التي تستهدف الخوارزميات.
 - زيادة الاعتماد على الأنظمة الذكية مما يرفع مستوى المخاطر النظامية.
- كما ناقشت الدراسة التأثيرات التشغيلية والبيئية المرتبطة بتوسع الحوسبة وتوفير بيانات دقيقة لتقييم الاستهلاك.

النتائج:

أكدت الدراسة وجود فجوة بين تطبيق الذكاء الاصطناعي في قطاع الطاقة وبين جاهزية الأنظمة لمواجهة المخاطر الناشئة، وأوصت بضرورة تبني نهج إدارة مخاطر مبني على ISO 31000 لمعالجة مخاطر الخصوصية والأمن السيبراني والتشغيل.

* Advai (2023)

العنوان:

تطبيق إطار تنظيم الذكاء الاصطناعي المعتمد على إدارة المخاطر (ISO 31000).

المحتوى:

ركزت الدراسة على كيفية توظيف الذكاء الاصطناعي داخل القطاعات الحيوية بما فيها الطاقة والمرافق، وربطت ذلك بإدارة المخاطر المؤسسية. استعرضت الدراسة مراحل:

- التعرف على المخاطر الخوارزمية.
 - تقييم احتمالية الفشل وتأثيره.
 - الإجابة على أخطاء البيانات والتحيزات.
- كما بينت أهمية ربط نتائج التقييم بمصفوفة "الاحتمال × الأثر" لتقدير مستوى الخطورة.

النتائج:

خلصت الدراسة إلى أن دمج الذكاء الاصطناعي دون إطار إدارة مخاطر واضح يزيد احتمال وقوع أخطاء تشغيلية خطيرة، وأوصت باستخدام ISO 31000 لوضع سياسات تقلل من المخاطر السيبرانية ومخاطر التحيز .

* IEA (2025)

العنوان:

الذكاء الاصطناعي والطاقة – تحليل التأثيرات المتبادلة على استهلاك الطاقة وأمن الشبكات.

المحتوى:

تناولت هذه الدراسة العلاقة المعقدة بين الذكاء الاصطناعي واستهلاك الطاقة، موضحة أن البنية الرقمية الداعمة للذكاء الاصطناعي (مراكز البيانات، التدريب والاستدلال) تستهلك قدرًا متزايدًا من الكهرباء. كما درست كيف يسهم الذكاء الاصطناعي ذاته في رفع كفاءة الأنظمة الكهربائية مثل موازنة الأحمال والتحكم الذكي بالشبكات.

النتائج:

أكدت الدراسة أن الذكاء الاصطناعي يشكل "معضلة طاقة" لأنه في الوقت الذي يساهم فيه في رفع الكفاءة التشغيلية للشبكات، فإنه يرفع أيضًا استهلاك مراكز البيانات للطاقة. وأوصت بضرورة تقييم المخاطر البيئية المرتبطة باستخدام الذكاء الاصطناعي على المدى الطويل.

* WEF (2025)

العنوان:

معضلة الطاقة في الذكاء الاصطناعي: التحديات والفرص والمسارات المستقبلية.

المحتوى:

ناقشت الدراسة النمو المتسارع في استهلاك الطاقة لأنظمة الذكاء الاصطناعي، وبيّنت أن استهلاك مراكز البيانات قد يرتفع من 1% من الطلب العالمي في 2022 إلى أكثر من 3% بحلول 2030. واستعرضت الدراسة أهم التحديات، ومنها:

- ارتفاع انبعاثات الطاقة بسبب نماذج الذكاء الاصطناعي الضخمة.
 - الضغط المتزايد على مصادر الطاقة المحلية.
 - الحاجة لتنظيم استهلاك الطاقة في الأنظمة الذكية.
- كما تناولت الفرص مثل مساهمة الذكاء الاصطناعي في تحسين البطاريات والطاقة المتجددة.

النتائج:

أوضحت الدراسة أن نجاح تطبيق الذكاء الاصطناعي في قطاع الطاقة يعتمد على بناء منظومة متوازنة تنظم الاستهلاك، وتعالج المخاطر التشغيلية والبيئية، وتعزز الابتكار المسؤول.

* Nour Tobar (2025)

العنوان:

التكامل بين الذكاء الاصطناعي وإدارة المخاطر وفق ISO 31000

المحتوى:

ناقشت الدراسة أثر الذكاء الاصطناعي على تطوير منظومات إدارة المخاطر، مع التركيز على كيفية انتقال المؤسسات من نهج "رد الفعل" إلى نهج "التقييم الاستباقي للمخاطر". كما تناولت الدراسة:

- تحليل مخاطر البيانات.
- تقييم خلل النماذج الخوارزمية.
- استخدام الذكاء الاصطناعي في مراقبة المخاطر في الوقت الفعلي.

النتائج:

أكدت الدراسة أن تطبيق ISO 31000 مع الأدوات الذكية يمكن أن يزيد من كفاءة المؤسسات في التنبؤ بالمخاطر السيبرانية والتشغيلية، ويعزز قدرة الأنظمة على التعامل مع الأحداث الطارئة.

المنطلقات النظرية للدراسة:

التطور التقني للذكاء الاصطناعي في قطاع الطاقة

يُعرّف الذكاء الاصطناعي في قطاع الطاقة بأنه توظيف الخوارزميات (التعلم الآلي، التعلم العميق، النظم الخبيرة) لمعالجة بيانات التشغيل الضخمة للشبكات الكهربائية وأنظمة المباني الذكية ومراكز البيانات، بهدف رفع الكفاءة، وتحسين الموثوقية، وترشيد الاستهلاك، وتقليل الانبعاثات. ومع اتساع الاعتماد على البيانات الحية وأجهزة الاستشعار وإنترنت الأشياء الصناعي، أصبحت مخرجات الذكاء الاصطناعي عنصراً أساسياً في اتخاذ القرار التشغيلي اللحظي. ويصحب هذا التقدم طيفٌ من المخاطر التقنية والبيئية والسيبرانية والتنظيمية، ما يستلزم إطاراً لإدارة المخاطر يوازن بين المنافع والتكاليف.

مراحل تطوّر الذكاء الاصطناعي في قطاع الطاقة

يقترح هذا البحث تقسيم تطوّر الذكاء الاصطناعي في الصناعة الطاقية إلى ست مراحل مترابطة:

1. مرحلة الرقمنة الأولية: (Digitalization)
تركيزها على رقمنة السجلات والعمليات الأساسية (قراءات العدّادات، أوامر التشغيل، صيانة الأصول)، وإتاحة البيانات بصورة معيارية تُمدّد لاستخدام التحليلات المتقدمة.
2. مرحلة الأتمتة القائمة على القواعد: (Rule-based Automation)
تطبيق قواعد محددة مسبقاً للتحكّم في الأحمال وموازنة التوليد/الطلب، مع قدر محدود من التكيف والتعلّم الذاتي.
3. مرحلة التنبؤ الإحصائي والتعلّم الآلي التقليدي:
نماذج تنبؤ الأحمال، كشف الشذوذ، تقدير الأعطال، تحسين الجداول، اعتماداً على بيانات تاريخية واسعة، مع بداية ربط النتائج بمؤشرات كفاءة الطاقة.
4. مرحلة التعلّم العميق والقرارات اللحظية:
إدخال الشبكات العميقة والرؤية الحاسوبية ومعماريات السلاسل الزمنية المتقدمة للتحكّم الآلي، بما يرفع الحساسية تجاه جودة البيانات ويزيد التعقيد الخوارزمي.
5. مرحلة التكامل مع المصادر الموزعة والتخزين: (DER + Storage)
دمج التنبؤات مع مصادر الطاقة المتجددة والتخزين، وإدارة الطلب المرن، والتحكّم الدقيق على مستوى الميكروغريد، مع تعاظم مخاطر الهجمات السيبرانية والاعتماد التقني على الموردّين.
6. مرحلة الذكاء الاصطناعي الأخضر (Green AI) والحوكمة الشاملة:
التركيز على خفض البصمة الكربونية للذكاء الاصطناعي ذاته (تحسين العتاد/الخوارزميات/مراكز البيانات)، وتطبيق حوكمة نماذج صارمة متوافقة مع المعايير ISO 31000، ضوابط الأمن، الخصوصية، الشفافية.

المفاهيم الأساسية ذات الصلة بموضوع الدراسة

1- إدارة المخاطر وفق (ISO 31000)

- إطارٌ مبني على مبادئ التكامل والسياق والتخصيص، يتضمن: التواصل والمشاورة، تحديد السياق، التعرّف على المخاطر، التقييم ($Likelihood \times Impact$)، المعالجة، المراقبة والتحسين المستمر.
- يُستخدم لتحديد معايير القبول وحدود المخاطر، وبناء مصفوفة المخاطر الخاصة بتطبيقات الذكاء الاصطناعي في الطاقة.

2- حوكمة النماذج (Model Governance)

- سياسات وإجراءات تضمن صلاحية النموذج، وتتبع الإصدارات، واعتماد البيانات، وضمانات القابلية للتفسير، واختبارات التحيز، وخطط الاستجابة للأخطاء.
- تشمل: مراجعات مستقلة للنموذج، بروتوكولات التحديث، سجل قرارات، وضوابط الإيقاف الآمن. (Safe-Fail)

3 - الأمن السيبراني لأنظمة الذكاء الاصطناعي

- يعالج تهديدات البيانات والواجهات والنماذج (هجمات الخصومة، تسميم البيانات، الانتحال)، وضبط الهويات والامتيازات، ومراقبة الشذوذ.
- يتقاطع مع استمرارية الأعمال، حماية الشبكات الصناعية (OT)، وسلامة نظم التحكم الإشرافي. (SCADA)

4- الذكاء الاصطناعي الأخضر (Green AI) وكفاءة الطاقة الرقمية

- محوران: تقليل استهلاك الذكاء الاصطناعي للطاقة ضغط النماذج، كَمْنَنَة الأوزان، العتاد عالي الكفاءة، مراكز بيانات منخفضة الكربون ورفع كفاءة قطاع الطاقة بواسطة الذكاء الاصطناعي تحسين الأحمال، التنبؤ بالمصادر المتجددة، الصيانة التنبؤية.

5- نظرية الكلفة/المنفعة

- موازنة مكاسب الكفاءة والموثوقية مقابل تكاليف الحوسبة والبنية الرقمية والمخاطر، وتقدير العائد الصافي على الاستثمار (ROI) على مستوى النظام.

6 - المرونة المؤسسية والنظام الاجتماعي/ التقني

- اعتبار التفاعل بين العوامل البشرية والتنظيمية والخيارات التقنية محددًا رئيسًا للمخاطر: التدريب، إجراءات العمل، وضوح الأدوار، ثقافة السلامة، وسلاسة التكامل مع الأنظمة القائمة.

مجالات المخاطر المستهدفة بالدراسة

1. مخاطر جودة البيانات والتحيز:

- بيانات ناقصة/منحازة تُنتج قرارات تشغيلية غير دقيقة (تذبذب جهد غير مُبرَّر، جدولة توليد غير مثلى).
- مؤشرات: معدلات أخطاء التنبؤ، حالات تجاوز حدود التشغيل، شكاوى الأداء.

2. مخاطر الأعطال الخوارزمية وعدم القابلية للتفسير:

- سلوك "صندوق أسود" يُصعَّب التحقيق في الحوادث ويؤخر اتخاذ القرار.
- إجراءات علاجية: تبني نماذج قابلة للتفسير، طبقات تحقق بشرية. (Human-in-the-Loop)

3. المخاطر السيبرانية:

- هجمات خصومية على بيانات الحساسات أو النماذج، وصول غير مصرح به لنظم التحكم.
- ضوابط: تقسيم الشبكات، MFA، مراقبة شذوذ، اختبارات اختراق مخصصة للـ AI

4. المخاطر البيئية والطاقة- استهلاك AI للطاقة:

- تصاعد أحمال مراكز البيانات وتبريدها، أثر التدريب/الاستدلال على ميزانيات الطاقة.
- حلول: جداول تدريب ذكية، انتقاء معماريات خفيفة، تبريد فعال، طاقة متجددة للمراكز.

5. المخاطر الاستراتيجية وسلاسل التوريد:

- الاعتماد على موردين محددين، تقادم برمجي سريع، قيود ترخيص/دعم.
- حلول: تنوع الموردين، عقود مستويات خدمة صارمة، خطط استمرارية.

مصفوفة "الاحتمال × الأثر" المخصصة للبحث

- أبعاد الاحتمال: جودة البيانات، التعقيد الخوارزمي، التعرض السيبراني، كثافة التشغيل.
- أبعاد الأثر: السلامة والموثوقية، الكفاءة الطاقية، الاستدامة البيئية، الامتثال التنظيمي، السمعة.
- مستويات القبول:
 - مخاطر مرتفعة: تتطلب معالجة فورية وخطط احتواء (Run-Book) واختبارات فاعلية.
 - مخاطر متوسطة: تُدار بتقليل الاحتمال/الأثر ورفع المراقبة.
 - مخاطر منخفضة: تُقبل مع متابعة دورية.
- ملاحظة تطبيقية: يُربط كل خطر بضوابط محدّدة (Preventive/Detective/Corrective) ومؤشرات أداء للمخاطر (KRIs)، وجدول مراجعة دوري.

الأنظر والنظريات الداعمة لتفسير النتائج

1. إطار ISO 31000 لإدارة المخاطر: لفهم دورة المخاطر وتحديد معايير القبول وبناء المصفوفة.
2. نظرية الأمن السيبراني: لربط نضج الضوابط بانخفاض الاحتمال/الأثر للأحداث السيبرانية.
3. نظرية الكلفة-المنفعة: لحساب العائد الصافي من تبني الذكاء الاصطناعي الموقر للطاقة.
4. نظرية المرونة المؤسسية: لتفسير قدرة الجهة المشغلة على امتصاص الصدمات.

5. الذكاء الاصطناعي الأخضر (Green AI): لتبرير تدخلات خفض استهلاك الطاقة الرقمي.

6. النظام الاجتماعي-التقني: لتفسير أثر الثقافة والمهارات وسير العمل على الفاعلية والمخاطر.

مزاياء دمج الذكاء الاصطناعي في كفاءة الطاقة (محور موجز)

- تحسين التنبؤ بالأحمال وتقليل الفاقد الفني والتجاري.
- إدارة الطلب المرن وتفعيل التسعير الزمني، ما يخفض ذروة الاستهلاك.
- الصيانة التنبؤية لمعدات الشبكة والمباني، وتقليل التوقفات المكلفة.
- تحسين مزيج التوليد بدمج المتجددة والتخزين بكفاءة أعلى.
- رفع الشفافية التشغيلية عبر لوحات مراقبة آنية مدفوعة بالبيانات.

التحديات والقيود:

- حاجة عالية للبيانات الموثوقة وتكلفة إعدادها وتنظيفها.
- تعقيد نماذج "الصندوق الأسود" وما يرافقه من تحديات تفسير وامثال.
- مخاطر سيبرانية مركبة على الأنظمة الصناعية الحرجة.
- بصمة طاقة لعمليات التدريب والاستدلال ومراكز البيانات.
- اعتماد تقني على الموردّين واحتمالات تقادم سريع.

العوامل المؤثرة في نجاح التطبيق

- حوكمة بيانات قوية - لمصدر، الجودة، النسخ، الحماية.
- كفاءات بشرية متخصصة - علم البيانات، الأمن الصناعي، تشغيل الشبكات.
- تكامل الأنظمة مع البنى القائمة (SCADA/DMS/EMS/BMS).
- تمويل مستدام ونموذج عائد واضح.
- سياسات وتنظيم واضحان للخصوصية والأمن ومعايير الكفاءة الطاقية.
- بنية تحتية رقمية - شبكات، حوسبة طرفية/سحابية، تبريد فعال.

نموذج مفاهيمي للدراسة (وصف نصي مختصر)

المدخلات:

(1) جودة البيانات وحوكمتها، (2) نضج الضوابط السيبرانية، (3) تعقيد النموذج وحوكمتها، (4) كفاءة البنية الرقمية (عتاد/مراكز بيانات)، (5) قدرات المرونة المؤسسية.

العملية:

تطبيق إطار ISO 31000 لبناء مصفوفة (Likelihood × Impact) على مخاطر: التحيز/الجودة، الأعطال الخوارزمية، السيبرانية، البيئية/الطاقية، وسلاسل التوريد.

المخرجات:

أ- مستوى المخاطر الصافية، ب- تحسّن الكفاءة الطاقية المقاسة بمؤشرات انخفاض الذروة، انخفاض الفاقد، تحسّن عامل القدرة، توافرية النظام، ج- خريطة أولويات المعالجة.

الافتراض الرئيس:

كلما ارتفع نضج الحوكمة والضوابط (بيانات/نموذج/أمن/Green-AI)، انخفضت المخاطر الصافية وتحسّنت مؤشرات كفاءة الطاقة.

خلاصة الإطار النظري

يُبيّن الإطار النظري أن الفائدة الصافية من دمج الذكاء الاصطناعي في قطاع الطاقة تتحقق عندما تُدار المخاطر وفق ISO 31000 مع حوكمة نموذجية وأمن سيبراني متقدّم، وبمراعاة الذكاء الاصطناعي الأخضر لضبط كُلف الطاقة الرقمية. كما تؤكد النظريات الداعمة أن العامل البشري والتنظيمي لا يقلّ أهمية عن العامل التقني في تحقيق الاستدامة والكفاءة.

المنهجية وطرق البحث:

مقدمة

تركّز هذه الدراسة على تحليل مخاطر الذكاء الاصطناعي في قطاع الطاقة، وتقييم تأثيرها على كفاءة استهلاك الطاقة باستخدام منهجية علمية مبنية على إطار ISO 31000، مع الاعتماد على البيانات التشغيلية، وآراء الخبراء، والأدوات الإحصائية لتحديد مستويات المخاطر وقياس أثرها.

أولاً: المنهجية

تعتمد الدراسة على المنهج الوصفي التحليلي، والذي يهدف إلى وصف الظواهر التقنية المرتبطة بتطبيقات الذكاء الاصطناعي في قطاع الطاقة، وتحليل المخاطر الناتجة عنها، وتفسير كيف تؤثر هذه المخاطر على كفاءة استهلاك الطاقة. ويركّز هذا المنهج على الربط بين نتائج الذكاء الاصطناعي التشغيلية وبين المعايير المعتمدة لإدارة المخاطر.

1- تحليل المحتوى

يتضمن مراجعة الأدبيات الحديثة، والتقارير الدولية ذات الصلة بالذكاء الاصطناعي في الطاقة، وممارسات إدارة مخاطر الأنظمة الرقمية، بما في ذلك:

- تقرير وزارة الطاقة الأمريكية حول مخاطر الذكاء الاصطناعي في البنى التحتية للطاقة
- تقرير وكالة الطاقة الدولية حول تأثير الذكاء الاصطناعي على استهلاك الطاقة
- تقرير المنتدى الاقتصادي العالمي حول "معضلة الطاقة في الذكاء الاصطناعي"

2- المقارنة المرجعية (Benchmarking)

مقارنة ممارسات إدارة مخاطر الذكاء الاصطناعي في قطاع الطاقة مع:

- دراسات GOV.UK حول أدوات تقييم المخاطر والخطوات العملية لتطبيق ISO 31000 في الأنظمة الذكية
- ممارسات الشركات العالمية والمنشآت التي تُشغل أنظمة تبني على الذكاء الاصطناعي في إدارة الأحمال والطلب.

3- التحليل الكمي

استخدام أدوات الإحصاء الوصفي لقياس العلاقة بين مستوى تطبيق أنظمة الذكاء الاصطناعي ومستوى المخاطر التشغيلية، وتصنيفها ضمن مصفوفة (Likelihood × Impact) المعتمدة في إطار ISO 31000.

4- التحليل النوعي

يتضمن تحليل آراء المتخصصين، والمهندسين، والعاملين في مجال الطاقة، إضافة إلى قراءة المخاطر المتوقعة، ونوعية القرارات التي تنتج عن النماذج الذكية.

ثانيًا: طرق البحث

1- الاستبيانات

تُوجّه استبيانات لمجموعة من العاملين في قطاع الطاقة لجمع بيانات حول:

- مستوى الاعتماد على الذكاء الاصطناعي.
- أبرز المخاطر التشغيلية والبيئية والسيبرانية التي تواجههم.
- أثر الذكاء الاصطناعي على عمليات التشغيل وكفاءة الطاقة.

2- المقابلات شبه المهيكلية

إجراء مقابلات مع خبراء في الطاقة والتحول الرقمي لتحليل:

- طبيعة المخاطر الناشئة عن الذكاء الاصطناعي.

- إجراءات التخفيف الحالية.

- توقعات المتخصصين لآثار التقنية على الشبكات الكهربائية.

3- تحليل البيانات الكمية

استخدام أدوات الإحصاء لتحليل بيانات الاستبيانات والمقابلات، وتصنيف المخاطر وفق مستويات:

- (مرتفع – متوسط – منخفض)

وفق معايير ISO 31000 ومصفوفة (Likelihood × Impact)

4- تحليل مضمون الوثائق الفنية

تحليل تقارير الأداء والتشغيل في أنظمة الطاقة الذكية (مثل أنظمة إدارة الأحمال، التنبؤ بالأحمال، ونظم مراقبة الشبكات).

ثالثاً: مجتمع البحث

يتكوّن مجتمع الدراسة من:-

- العاملين في شركات الكهرباء.

- مهندسي الشبكات والطاقة.

- العاملين في أقسام التحول الرقمي والطاقة المتجددة.

- مسؤولي الأمن السيبراني في مراكز البيانات ومنشآت الطاقة.

رابعاً: عينة البحث

نوع العينة:

عينة قصدية من المتخصصين الذين لهم علاقة مباشرة بتشغيل الأنظمة الذكية.

حجم العينة:

يتراوح بين 200-100 مشارك لضمان كفاية البيانات الإحصائية، مع مراعاة تنوع المشاركين بين الفنيين، المهندسين، والعاملين في الأمن السيبراني.

معايير اختيار العينة:

- خبرة لا تقل عن سنتين في تشغيل أو إدارة أنظمة الطاقة.
- تعامل مباشر مع أنظمة الذكاء الاصطناعي أو البيانات التشغيلية.
- معرفة سابقة بإدارة المخاطر أو تشغيل الشبكات.

أدوات الدراسة :

الاستبيانات: لقياس تصوّر العاملين لمخاطر الذكاء الاصطناعي وأثره على كفاءة الطاقة .
المقابلات: للحصول على رؤى معمّقة حول طبيعة المخاطر والإجراءات المتبعة .
تحليل البيانات التشغيلية: لدراسة أداء أنظمة الذكاء الاصطناعي في الواقع العملي .
مصفوفة تقييم المخاطر المبنية على معيار ISO 31000.

حدود الدراسة :

1- الحدود الموضوعية

تركّز الدراسة على:

- مخاطر الذكاء الاصطناعي في قطاع الطاقة.
 - العلاقة بين هذه المخاطر وكفاءة استهلاك الطاقة.
- ولا تتناول المجالات الأخرى غير ذات العلاقة مثل التمويل أو الأنظمة التجارية.

2- الحدود الزمنية

تشمل الفترة 2023–2026 وهي فترة تزايد دمج الذكاء الاصطناعي في الطاقة عالميًا بحسب تقارير CESER و IEA و WEF.

3- الحدود الجغرافية

تركّز على تطبيقات الذكاء الاصطناعي في قطاع الطاقة في المملكة العربية السعودية، مع مقارنة دولية مرجعية عند الحاجة.

المراجع العربية :

- وحدة أبحاث الطاقة – موقع الطاقة 2023
عمار، أحمد. (2023). كيف يدعم الذكاء الاصطناعي زيادة كفاءة الطاقة وتحقيق الاستدامة؟
وحدة أبحاث الطاقة – موقع الطاقة.
- المركز المصري للفكر والدراسات الاستراتيجية 2024
سلطان، أحمد. (2024). الذكاء الاصطناعي والطاقة: شراكة استراتيجية نحو مستقبل مستدام.
المركز المصري للفكر والدراسات الاستراتيجية – قسم الدراسات الاقتصادية.
- سكاى نيوز عربية – تقرير مشترك بين أدنوك ومصدر ومايكروسوفت 2024
تؤكد قدرة الذكاء الاصطناعي على خفض انبعاثات قطاع الطاقة.
أبوظبي.
- مصدر للطاقة النظيفة – تقرير رسمي 2024
أدنوك – مصدر – مايكروسوفت. (2024). تعزيز الإمكانيات: الذكاء الاصطناعي والطاقة من أجل مستقبل مستدام.
Masdar Clean Energy Reports.
- مركز تريندز للبحوث والاستشارات 2024
المدفع، نجلاء. (2024). الذكاء الاصطناعي في تحول الطاقة: تعزيز الكفاءة والاستدامة في قطاع الطاقة الحديث.
مركز تريندز للبحوث والاستشارات.
- موقع 24 الإخباري – الإمارات 2024
موقع 24. (2024). الإمارات.. تقرير مشترك حول قدرات الذكاء الاصطناعي في الطاقة.
أبوظبي.

المراجع الأحدث:

- Worthmann, C. & Malik, K. (2025). Comprehensive and comparative analysis of AI in the energy sector. AI and Ethics (Springer).
- Pandey, U., Pathak, A., Kumar, A., & Mondal, S. (2023). Applications of artificial intelligence in power system operation, control and planning: a review. Clean Energy
- U.S. Department of Energy (DOE) – CESER. (2024). Potential Benefits and Risks of Artificial Intelligence for Critical Energy Infrastructure.
- IEA – International Energy Agency. (2025). Energy and AI.
- World Economic Forum (2025). AI's energy dilemma: Challenges, opportunities, and a path forward.
- Majkut, J., & Abrahams, L. (2025). AI for the Grid: Opportunities, Risks, and Safeguards. CSIS.
- RAND Europe. (2024). The use of AI for improving energy security: Exploring risks and opportunities
- GOV.UK – Advai Case Study. (2023). Implementing a Risk-Driven AI Regulatory Compliance Framework.
- Nour Tobar. (2025). ISO 31000 Meets Generative AI: Elevating Risk Management to the Next Level.
- European Parliament (2025). AI and the energy sector (EPRS Briefing).
- World Economic Forum & Accenture (2025). From Paradox to Progress: A Net-Positive AI Energy Framework.
- UNECE (2024). Balancing the electricity supply and demand with Artificial Intelligence (Case Study).
- Nature (2025). How much energy will AI really consume?
- IEA (2025). Energy demand from AI.

روابط المراجع:

- [\[link.springer.com\]](#)
- [\[academic.oup.com\]](#)
- [\[energy.gov\]](#)
- [\[mdpi.com\]](#)
- [\[rand.org\]](#)
- [\[csis.org\]](#)
- [\[energy.gov\]](#)
- [\[energy.gov\]](#)
- [\[gov.uk\]](#)
- [\[iea.org\]](#)
- [\[weforum.org\]](#)
- [\[linkedin.com\]](#)
- [\[masdar.ae\]](#)
- [\[24.ae\]](#)
- [\[trendsresearch.org\]](#)
- [\[skynewsarabia.com\]](#)
- [\[ecss.com.eg\]](#)
- [\[attaqa.net\]](#)