

دور الذكاء الاصطناعي في تعزيز الأمن السيبراني في البنوك الإسلامية

-دراسة حالة بنك الشريعة الإندونيسية (BSI)-

**The Role of Artificial Intelligence in Enhancing Cybersecurity in Islamic Banks
-A Case Study of Bank Syariah Indonesia (BSI)-**هامل دليلا¹ / Hamel Dalila¹¹ مخبر تقييم سوق رؤوس الاموال الجزائرية في ظل العولمة -جامعة سطيف 1 - ، h.ecoalg@gmail.com

تاريخ النشر: 2025/06/ 30

تاريخ القبول: 2025/06/ 24

تاريخ الاستلام: 2025/02/27

ملخص:

تهدف هذه الدراسة إلى إبراز دور الذكاء الاصطناعي في تعزيز الأمن السيبراني في البنوك الإسلامية، من خلال دراسة حالة بنك الشريعة الإندونيسية (BSI)، وقد أظهر البحث فاعلية تقنيات الذكاء الاصطناعي، على غرار التعلم الآلي وتحليل البيانات الضخمة، في رصد التهديدات السيبرانية والتصدي لها، مما أدى إلى تحسين استجابة البنك للهجمات وتعزيز ثقة العملاء، كما أكدت النتائج على أهمية الاستثمار المستمر في الحلول التقنية المتقدمة وتطوير سياسات الحوكمة الرقمية بما يتماشى مع الضوابط الشرعية، لضمان استدامة الأمان الرقمي في البنوك الإسلامية.

كلمات مفتاحية: الذكاء الاصطناعي، الأمن السيبراني، البنوك الإسلامية، بنك الشريعة الإندونيسية (BSI).

تصنيف JEL : G21, G32, O33.

Abstract: This study aims to highlight the role of artificial intelligence (AI) in enhancing cybersecurity within Islamic banks, through a case study of Bank Syariah Indonesia (BSI). The research demonstrates the effectiveness of AI technologies, such as machine learning and big data analytics, in detecting and mitigating cyber threats, leading to improved incident response and strengthened customer trust. The findings underscore the importance of continuous investment in advanced technological solutions and the development of digital governance policies aligned with Shariah principles to ensure the sustainability of cybersecurity in Islamic financial institutions.

Keywords: Artificial Intelligence; Cybersecurity; Islamic Banks; Bank Syariah Indonesia (BSI).

Jel Classification Codes: G21, O32, G33

Résumé : Cette étude vise à mettre en lumière le rôle de l'intelligence artificielle (IA) dans le renforcement de la cybersécurité au sein des banques islamiques, à travers une étude de cas de la Bank Syariah Indonesia (BSI). La recherche démontre l'efficacité des technologies d'IA, telles que l'apprentissage automatique et l'analyse des mégadonnées, dans la détection et l'atténuation des menaces cybernétiques, contribuant ainsi à une meilleure réactivité face aux incidents et à une consolidation de la confiance des clients. Les résultats soulignent l'importance d'un investissement continu dans des solutions technologiques avancées et de l'élaboration de politiques de gouvernance numérique conformes aux principes de la Charia, afin de garantir la durabilité de la cybersécurité dans les institutions financières islamiques.

Mots-clés : Intelligence artificielle ; Cybersécurité ; Banques islamiques ; Bank Syariah Indonesia (BSI).

Codes de classification JEL : G21, O32, G33

1. مقدمة:

في ظل التحول الرقمي المتسارع والتطور المستمر في التقنيات المالية، أصبح الأمن السيبراني ضرورة حتمية للحفاظ على استقرار المؤسسات المصرفية وحماية البيانات الحساسة للعملاء، وتزداد هذه الأهمية في البنوك الإسلامية التي تلتزم بمبادئ الشريعة الإسلامية، مما يُضيف بعدًا إضافيًا للتحديات الأمنية التي تواجهها. يُعد الذكاء الاصطناعي أحد الأدوات الحديثة التي تسهم بشكل فعال في تعزيز أنظمة الحماية السيبرانية من خلال التنبؤ بالتهديدات، واكتشاف الهجمات المتقدمة، وتحليل البيانات الضخمة في الوقت الحقيقي. إشكالية البحث:

كيف يُسهم الذكاء الاصطناعي في تعزيز الأمن السيبراني في بنك الشريعة الإندونيسي في إطار الالتزام بمتطلبات الشريعة الإسلامية؟

- أهمية البحث

تظهر أهمية البحث من خلال إبراز دور الذكاء الاصطناعي في حماية البنوك الإسلامية والتي تواجه تحديات مزدوجة تتعلق بالأمن السيبراني والالتزام بالضوابط الشرعية. من الناحية العملية، كما يُمكن للنتائج المقترحة أن تسهم في تعزيز قدرة البنوك الإسلامية على مواجهة الهجمات الإلكترونية، وحماية بيانات العملاء، وضمان استمرارية العمليات المالية، ما يدعم استدامة الثقة في هذه المؤسسات ويدفع بتطور القطاع المالي الإسلامي نحو التحول الرقمي الآمن.

- أهداف البحث:

تبرز أهداف البحث فيما يلي:

- إبراز مفهوم الأمن السيبراني ومتطلباته في البنوك الإسلامية؛
- معرفة آليات الذكاء الاصطناعي المستخدمة في تحسين الحماية السيبرانية؛
- استكشاف تطبيقات الذكاء الاصطناعي لتعزيز الأمن السيبراني في بنك الشريعة الإندونيسي؛
- اقتراح استراتيجيات فعالة لتعزيز الأمن السيبراني باستخدام تقنيات الذكاء الاصطناعي في البنوك الإسلامية.

- منهج البحث:

تم الاعتماد على المنهج الوصفي التحليلي لدراسة العلاقة بين الذكاء الاصطناعي والأمن السيبراني في البنوك الإسلامية، كما تم استخدام دراسة الحالة من خلال عرض تجربة بنك الشريعة الإندونيسي وإبراز دور تقنيات الذكاء الاصطناعي المستخدمة في تعزيز الأمن السيبراني للبنك.

الدراسات السابقة:

تناولت العديد من الدراسات العلاقة بين الذكاء الاصطناعي والأمن السيبراني، من أبرزها:

- دراسة Ali et al (2023) حيث طوّرت إطارًا نظريًا لاستخدام الذكاء الاصطناعي في كشف التهديدات السيبرانية في المصارف الإسلامية، دون التطرق لتكاملها مع الحوكمة الشرعية.

- بحث Smith (2021) ركّز على إمكانات الذكاء الاصطناعي في أتمتة الاستجابة للهجمات، مع تطبيقات عامة غير مخصصة للقطاع المالي الإسلامي.
- أما (Al-Rahimi et al, 2023) حيث اقترح نموذجًا أوليًا لدمج الحوكمة الشرعية في أنظمة الأمن الذكية، لكنه بقي في الإطار النظري دون تطبيقات ميدانية.

الفجوة البحثية:

ما يميز هذه الدراسة هو:

- الدمج العملي بين الذكاء الاصطناعي والأمن السيبراني ضمن إطار شرعي تطبيقي في بنك الشريعة الإندونيسي.
- تقديم بيانات ميدانية وتحليل تطبيقي لفعالية الذكاء الاصطناعي في خفض الهجمات وتحسين الامتثال.

2. مفهوم الأمن السيبراني وأهميته في البنوك الإسلامية

1.2 تعريف الأمن السيبراني في البنوك الإسلامية:

يشمل الأمن السيبراني في البنوك الإسلامية عدة مفاهيم أساسية تهدف إلى حماية البيانات المالية والشخصية للعملاء وضمان سلامة العمليات المصرفية، وقد وردت عدة تعريفات نذكر منها ما يلي:

- تعريف 1: الأمن السيبراني في البنوك الإسلامية هو "مجموعة من العمليات والتدابير التي تهدف إلى حماية الأنظمة المصرفية والبيانات المالية للعملاء من التهديدات الإلكترونية، مع الالتزام بالضوابط الشرعية التي تحكم العمليات البنكية الإسلامية، ويشمل ذلك استخدام برامج الحماية، مراقبة الشبكات، وتعزيز الوعي الأمني لدى العاملين والعملاء" (العبادي، 2023).

ومن هذا التعريف تبرز أهمية الأمن السيبراني كدرع وقائي شامل للبنوك الإسلامية.

- تعريف 2: يُعرّف الأمن السيبراني في البنوك الإسلامية على أنه عملية إدارة مستمرة للمخاطر الرقمية التي تهدد البيانات والمعاملات المالية، مع مراعاة الضوابط الشرعية. يشمل ذلك تصميم أنظمة مرنة للتصدي للهجمات السيبرانية، والتأكد من سلامة واستمرارية الخدمات المصرفية (بيئة الاتصالات وتقنية المعلومات، 2021).

ومن خلال هذا التعريف تظهر أهمية الأمن السيبراني كآلية لإدارة للمخاطر الرقمية.

- تعريف 3: الأمن السيبراني هو التزام البنك الإسلامي بتطبيق معايير الحوكمة الرقمية والأمنية، لضمان حماية سرية البيانات المالية وخصوصية العملاء، وفقًا للتشريعات المحلية والدولية، مع الحفاظ على توافق العمليات مع مبادئ الشريعة الإسلامية (مؤسسة النقد العربي السعودي، 2022).

ومن التعريف تتوضح أهمية الأمن السيبراني كالتزام بالامتثال والحوكمة.

2.2 أهمية الأمن السيبراني في البنوك الإسلامية :

تتمثل أهمية الأمن السيبراني في البنوك الإسلامية فيما يلي:

- حماية البيانات الحساسة: تشمل حماية معلومات العملاء والمعاملات المالية من الاختراق أو التسريب (Ali, 2023).
- إدارة الهوية والتحكم بالوصول: بحيث تضمن أن الأفراد المصرح لهم فقط يمكنهم الوصول إلى الأنظمة الحساسة، مع استخدام تقنيات مثل المصادقة الثنائية والتشفير المتقدم (Khan, 2022).
- رصد التهديدات والاستجابة للحوادث: وهذا بالاعتماد على تقنيات الذكاء الاصطناعي لمراقبة الشبكات بشكل مستمر واكتشاف الأنشطة المشبوهة (Smith, 2022).

- التوافق مع المعايير الشرعية: من خلال تصميم حلول أمنية تتوافق مع مبادئ الشريعة الإسلامية، مثل الحفاظ على السرية وعدم الإضرار بالأطراف المعنية (Ali, 2023).
- التثقيف والتوعية الأمنية: وهذا بتدريب الموظفين والعملاء على أفضل ممارسات الأمن السيبراني وتقوية الوعي بالتهديدات المحتملة (Khan, 2022).
- الاستجابة للطوارئ والتعافي من الكوار: بوضع خطط استجابة فعالة للهجمات السيبرانية لضمان استمرارية العمليات المصرفية مع الحد الأدنى من التأثير على الخدمات. (Smith, AI and the Future of Financial Security, 2021)

3. الذكاء الاصطناعي و الأمن السيبراني في البنوك الإسلامية

1.3 تطبيقات الذكاء الاصطناعي لتعزيز الأمن السيبراني في البنوك الإسلامية:

- تؤدي تطبيقات الذكاء الاصطناعي دورًا حيويًا في تعزيز الأمن السيبراني، حيث تُمكن البنوك الإسلامية من التنبؤ بالتهديدات ومعالجتها بكفاءة، وهذا في إطار الالتزام بالمعايير الشرعية. وهذا من خلال:
- الكشف التلقائي عن التهديدات: وهذا بتحليل سلوكيات الشبكة لاكتشاف الأنشطة غير الطبيعية باستخدام تقنيات التعلم العميق (Brown, 2023).
 - أنظمة الاستجابة للحوادث: من خلال أتمتة عمليات الاستجابة للهجمات السيبرانية، مما يقلل من وقت التفاعل مع التهديدات (Smith, Automated Incident Response with Artificial Intelligence, 2022).
 - تحليل البيانات الضخمة: باستخدام الذكاء الاصطناعي لتحليل كميات هائلة من البيانات لتحديد الأنماط التي تشير إلى محاولات اختراق (Ali M. &, 2021).
 - التنبؤ بالهجمات المستقبلية: من خلال بناء نماذج توقعية تعتمد على التعلم الآلي لتوقع نقاط الضعف المحتملة قبل استغلالها (Williams, 2023).
 - التعرف على الاحتيال في الوقت الفعلي: وهذا برصد المعاملات المالية وكشف الأنشطة المشبوهة فورًا، مع ضمان الامتثال للمعايير الشرعية (Khan R. &, 2022).
 - تحسين التشفير والحماية: من خلال تطوير خوارزميات تشفير ديناميكية تتكيف مع تطور التهديدات السيبرانية (Zhang, 2021) هنا محتوى العنوان الفرعي الأول، أدخل هنا محتوى العنوان الفرعي الأول، أدخل هنا محتوى العنوان الفرعي الأول، أدخل هنا محتوى العنوان الفرعي الأول، أدخل هنا محتوى العنوان الفرعي الأول، أدخل هنا محتوى العنوان الفرعي الأول.
- #### 2.3 الذكاء الاصطناعي والأمن السيبراني في الحوكمة الشرعية للبنوك الإسلامية:
- تؤدي الحوكمة الشرعية دورًا محوريًا في ضمان التزام البنوك الإسلامية بأحكام الشريعة، ومع تسارع التحول الرقمي، ظهرت فرص وتحديات جديدة تتطلب توازنًا بين الابتكار والتقييد بالضوابط الشرعية. تتمثل فيما يلي:
- الالتزام بالضوابط الشرعية في الحلول الرقمية: يجب تصميم الأنظمة الرقمية لتتوافق مع الفتاوى الشرعية والقرارات الصادرة عن هيئات الرقابة (Ahmed, 2022).
 - تفعيل لجان الرقابة الشرعية الرقمية: من خلال استخدام تقنيات الذكاء الاصطناعي لدعم لجان الرقابة الشرعية في متابعة المعاملات والتحقق من الامتثال في الوقت الحقيقي (Al-Rahimi, 2023).
 - الأمن السيبراني المتوافق مع الشريعة: من خلال تطوير أنظمة أمنية تحمي البيانات وتضمن الخصوصية، مع مراعاة القيم الإسلامية مثل الأمانة وحفظ الحقوق (Ibrahim, 2021).
 - العقود الذكية والتمويل الإسلامي: وهذا بتوظيف العقود الذكية في تنفيذ صيغ التمويل الإسلامي، مثل المراجعة والإجارة، مع تضمين آليات تحقق شرعي تلقائية (Yusuf, 2023).

- تطوير منصات الفتوى الرقمية: ببناء منصات تعتمد على الذكاء الاصطناعي لتقديم الفتاوى الفورية حول المنتجات المالية الرقمية (Ibrahim, Cybersecurity and Islamic Ethics in Financial Institutions, 2021)
- تعزيز الشفافية والمساءلة الرقمية: بتطبيق أدوات التحليل الرقمي لتعزيز الشفافية في المعاملات وتقوية آليات المساءلة وفقاً للمعايير الشرعية (Rahman et al., 2021).

3.3 الأسس النظرية لتكامل الذكاء الاصطناعي والأمن السيبراني في البنوك الإسلامية

يتطلب فهم العلاقة بين الذكاء الاصطناعي والأمن السيبراني في السياق الإسلامي الرجوع إلى مجموعة من الأسس النظرية التي تُظهر كيف يمكن للتقنيات الذكية أن تُعزز أمان المعلومات ضمن منظومات متوافقة مع الشريعة:

1.3.3 نظرية النظام (System Theory):

تُبرز هذه النظرية أن البنك يعمل كنظام متكامل، حيث تتفاعل المكونات التكنولوجية والتنظيمية والشرعية، ويؤدي إدخال الذكاء الاصطناعي إلى تعديل ديناميكية هذا النظام، من خلال أتمتة القرارات الأمنية وتقليص التدخل البشري في الرصد والتحقق، بشرط الحفاظ على الرقابة الشرعية كجزء لا يتجزأ من هذا النظام (Bertalanffy, 1968)

2.3.3 نظرية إدارة المخاطر الرقمية (Digital Risk Management)

تُستخدم هذه النظرية لتصنيف وتقييم التهديدات الإلكترونية، وتقديم أدوات كمية ونوعية للتعامل معها، فالذكاء الاصطناعي يُعد وسيلة متقدمة لتحليل البيانات السلوكية والأنماط التهديدية، ما يسمح بتحديد المخاطر قبل وقوعها، وفق إطار استباقي بالبنوك الإسلامية يُضاف بعدد خاص يتعلق بـ "مخاطر الامتثال الشرعي"، والتي يجب أن تُرصد إلى جانب المخاطر التقني (Hashim, 2023)

3.3.3 نموذج TOE (التكنولوجيا-المنظمة-البيئة)

يوضح هذا النموذج أن تبني أي تكنولوجيا جديدة - مثل الذكاء الاصطناعي - يتأثر بثلاثة أبعاد:

- البُعد التكنولوجي: ويتعلق بجاهزية البنية الرقمية للبنك؛
- البُعد التنظيمي: ويتعلق بثقافة البنك وكفاءة العاملين فيه؛
- البُعد البيئي: ويشمل القوانين والتشريعات، ويظهر الامتثال الشرعي كعامل رئيسي في البنوك الإسلامية (Omar, 2023)

4.3.3 نظرية الحوكمة الشرعية (Shariah Governance Theory)

تنص هذه النظرية على ضرورة وجود آليات رقابة داخلية وخارجية لضمان توافق الأنظمة المصرفية مع أحكام الشريعة الإسلامية، حيث يُدمج الذكاء الاصطناعي في البنوك الإسلامية، يصبح من الضروري برمجة أنظمة الأمن السيبراني بآليات تحقق تلقائي للامتثال الشرعي (Al-Rahimi, 2023)

وهو ما يُمكن تحقيقه من خلال العقود الذكية وفلترة البيانات حسب الأحكام الشرعية.

4. نظرية الثقة الرقمية (Digital Trust Theory)

تعدّ الثقة الرقمية من المفاهيم المركزية في نجاح تبني التكنولوجيا داخل المؤسسات المالية، وخاصة في البنوك الإسلامية التي ترتبط بعلاقات تعاقدية وأخلاقية مبنية على مبادئ الشفافية والعدالة والمساءلة، حيث تركز نظرية الثقة الرقمية على أنّ ثقة المستخدمين في النظم الذكية لا تنبع فقط من الكفاءة التقنية، وإنما من مدى التزام تلك النظم بالقيم الأخلاقية والتنظيمية (Söllner, 2016)

وفي الإطار الإسلامي، يكتسب هذا المفهوم بعداً إضافياً من خلال ارتباطه بالامتثال الشرعي وخصوصية البيانات، حيث ينظر العملاء المسلمون إلى أمن المعلومات باعتباره جزءاً من الأمانة والضوابط الشرعية وليس مجرد مسألة فنية (Zarrouk, 2023)

ووفقاً للنظرية فإنّ الذكاء الاصطناعي رغم قدراته العالية في التنبؤ والكشف، قد يؤدي إلى فقدان الثقة إذا لم يكن مدعوماً بآليات رقابة شرعية رقمية ومبادئ شفافية واضحة في معالجة البيانات. ولذلك، فإن دمج الذكاء الاصطناعي ضمن بيئة مصرفية إسلامية يستوجب تضمين مكوّنات الثقة الرقمية التالية:

- الشفافية في كيفية اتخاذ قرارات أمنية آلية؛
- المسؤولية الأخلاقية: وذلك من خلال البرمجة الخوارزمية وفقاً للقيم الإسلامية؛
- الامتثال الشرعي الفوري: بالنسبة لنتائج الذكاء الاصطناعي عبر وحدات تحقق ذكية؛
- حماية خصوصية العميل: وهذا بما لا يتعارض مع الضوابط الإسلامية الخاصة بالمعلومات الشخصية.

وفي هذا الإطار ، تؤدي نظرية الثقة الرقمية دوراً تكاملياً في فهم العلاقة بين الذكاء الاصطناعي والأمن السيبراني في البنوك الإسلامية، حيث تُعد الثقة بمثابة المتغير المحوري الذي يربط بين الأداء التقني والشرعية الأخلاقية.

5. دور الذكاء الاصطناعي في تعزيز الأمن السيبراني في بنك الشريعة الإندونيسي

1.5 تعريف بنك الشريعة الإندونيسي (Bank Syariah Indonesia)

يعتبر بنك الشريعة الإندونيسي (BSI) أكبر بنك إسلامي في إندونيسيا، تأسس في عام 2021 نتيجة اندماج ثلاثة بنوك إسلامية مملوكة للدولة (بنك BRI Syariah، بنك Mandiri Syariah، وبنك BNI Syariah)، ويهدف البنك إلى تقديم خدمات مالية متوافقة مع الشريعة الإسلامية، مع التركيز على الابتكار الرقمي لتعزيز الشمول المالي ودعم الاقتصاد الحلال في إندونيسيا، كما يتميز البنك بتقديم مجموعة متنوعة من المنتجات المصرفية، بدءاً من التمويل الشخصي والتجاري إلى الحلول الرقمية، مع التركيز على تعزيز الأمن السيبراني من خلال تقنيات الذكاء الاصطناعي لحماية البيانات وتحسين تجربة العملاء. (Bank Syariah Indonesia. 2021)

2.5 تطبيقات الذكاء الاصطناعي في بنك الشريعة الإندونيسي (BSI)

يُعد بنك الشريعة الإندونيسي (Bank Syariah Indonesia) من البنوك الإسلامية الرائدة التي تبنت تقنيات الذكاء الاصطناعي لتعزيز خدماتها المصرفية وأمنها السيبراني، وفيما يلي أبرز تطبيقات الذكاء الاصطناعي المستخدمة في بنك الشريعة الإندونيسي (BSI):

- روبوتات الدردشة (Chatbots): حيث قام بنك الشريعة الإندونيسي (BSI) بتطوير روبوتات دردشة مدعومة بالذكاء الاصطناعي لتقديم خدمة عملاء فورية وفعّالة، كما تُساعد هذه الروبوتات في التعامل مع استفسارات العملاء المتكررة، مما يقلل من الضغط على موظفي خدمة العملاء ويحسن من تجربة العميل (Hamadou, Modern Finance)
- الخدمات المصرفية عبر الهاتف المحمول المدعومة بالذكاء الاصطناعي: حيث يقدم البنك تطبيقات مصرفية ذكية تستخدم تقنيات الذكاء الاصطناعي لتحليل سلوك العملاء وتقديم توصيات مخصصة. وهذا ما يُسهم في تعزيز رضا العملاء وزيادة ولائهم من خلال تقديم خدمات تتناسب واحتياجاتهم الفردية (Hamadou, Modern Finance)
- الكشف المبكر عن التهديدات الأمنية: حيث يستخدم بنك الشريعة الإندونيسي (BSI) أنظمة ذكاء اصطناعي متقدمة لرصد الأنشطة غير الطبيعية والكشف المبكر عن التهديدات السيبرانية المحتملة. تُساعد هذه الأنظمة في حماية بيانات العملاء والحفاظ على سلامة العمليات المصرفية (Hamadou, Modern Finance).
- الاستجابة التلقائية للحوادث السيبرانية: حيث طوّر البنك أنظمة تعتمد على الذكاء الاصطناعي قادرة على التعامل الفوري مع الحوادث الأمنية، وتقوم هذه الأنظمة بتحليل التهديدات واتخاذ الإجراءات المناسبة بشكل تلقائي، مما يقلل من تأثير هذه الحوادث على العمليات المصرفية (Hamadou, Modern Finance)
- التنبؤ بالاحتياجات المالية للعملاء: وهذا من خلال تحليل البيانات التاريخية وسلوكيات الإنفاق، يستخدم بنك الشريعة الإندونيسي (BSI) تقنيات الذكاء الاصطناعي لتوقع احتياجات العملاء المستقبلية. يُمكن ذلك البنك من تقديم عروض وخدمات مخصصة تلي توقعات العملاء وتزيد من رضاهم (Hamadou, Modern Finance)
- أتمتة العمليات الداخلية: حيث اعتمد البنك على الذكاء الاصطناعي لأتمتة العديد من العمليات الداخلية، مثل معالجة الطلبات والموافقات الائتمانية. وهذا لزيادة الكفاءة التشغيلية وتقليل الأخطاء البشرية (Hamadou et al., 2024).

3.5 دور تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني لبنك الشريعة الإندونيسي (BSI)

- يعتمد بنك الشريعة الإندونيسي على تقنيات الذكاء الاصطناعي لتعزيز أمنه السيبراني وحماية بيانات عملائه ومصالحهم بكفاءة عالية من خلال :
- الكشف المبكر عن التهديدات السيبرانية: حيث يستخدم بنك الشريعة الإندونيسي أنظمة ذكاء اصطناعي متقدمة لتحليل كميات هائلة من البيانات بسرعة، مما يتيح التعرف على التهديدات السيبرانية الجديدة والتصدي لها بفعالية. تُسهم هذه القدرة في تعزيز حماية الشبكة والبيانات الحساسة من الهجمات المحتملة؛
 - التحليل السلوكي لرصد الأنشطة المشبوهة: حيث تعتمد أنظمة الذكاء الاصطناعي في بنك الشريعة الإندونيسي على تحليل سلوك المستخدمين لتحديد الأنماط غير الطبيعية التي قد تشير إلى محاولات اختراق أو احتيال، ومن خلال هذا التحليل يمكن للبنك اتخاذ إجراءات استباقية لمنع التهديدات قبل تفاقمها؛
 - الاستجابة التلقائية للحوادث الأمنية: حيث تمكّن تقنيات الذكاء الاصطناعي البنك من تنفيذ استجابات تلقائية وسريعة عند اكتشاف تهديدات سيبرانية، مما يقلل من الوقت المستغرق لتخفيف الأضرار المحتملة ويضمن استمرارية العمليات المصرفية دون انقطاع؛
 - التنبؤ بالهجمات المستقبلية: وهذا من خلال تحليل البيانات التاريخية والاتجاهات الحالية، كما تساعد تقنيات الذكاء الاصطناعي في توقع الهجمات السيبرانية المحتملة، مما يتيح للبنك تعزيز دفاعاته واتخاذ تدابير وقائية مناسبة؛
 - تعزيز أنظمة المصادقة: حيث يستخدم بنك الشريعة الإندونيسي (BSI) تقنيات الذكاء الاصطناعي لتطوير أنظمة مصادقة متعددة العوامل تعتمد على التعرف على الأنماط السلوكية والبيومترية، مما يزيد من صعوبة اختراق الحسابات المصرفية ويحمي بيانات العملاء.

تؤكد البيانات الصادرة عن بنك الشريعة الإندونيسي (BSI) في تقريره السنوي لسنة 2023 أن إدراج تقنيات الذكاء الاصطناعي ساهم بشكل كبير في تحسين مستوى الحماية السيبرانية ورفع كفاءة الأداء الأمني، حيث تم تسجيل انخفاض في عدد محاولات الاختراق الشهري من حوالي 2500 محاولة سنة 2021 إلى ما يقارب 1600 محاولة فقط سنة 2023. كما ارتفعت نسبة كشف محاولات الاحتيال الإلكتروني من 68% إلى 91%. ما يعكس فعالية الأنظمة الذكية في رصد التهديدات السيبرانية في الوقت الحقيقي (Indonesia, 2023)

أما على مستوى زمن الاستجابة للحوادث السيبرانية، فقد تراجع من 120 دقيقة كمتوسط سنة 2021 إلى أقل من 40 دقيقة سنة 2023، نتيجة اعتماد آليات الاستجابة التلقائية المبنية على الذكاء الاصطناعي (Hamadou, Modern Finance)

وفيما يتعلق بالامتثال الشرعي الرقمي، فقد ساعدت أدوات التحليل الذكي على معالجة 85% من المعاملات المالية بشكل تلقائي من قبل لجان الرقابة، مع مراجعة فورية لمدى توافقها مع الأحكام الشرعية. وضمن السياق العام، تحتل إندونيسيا المرتبة 24 عالمياً في مؤشر الجاهزية السيبرانية الصادر عن الاتحاد الدولي للاتصالات (ITU)، بنسبة استجابة قدرها 78.4%، مما يوفر بيئة رقمية مناسبة لاعتماد أدوات الذكاء الاصطناعي في البنوك الإسلامية (ITU, 2023).

4.5 تحديات تطبيق تقنيات الذكاء الاصطناعي لتعزيز الأمن السيبراني في بنك الشريعة الإندونيسي (BSI)
يواجه بنك الشريعة الإندونيسي عدة تحديات عند تطبيق تقنيات الذكاء الاصطناعي لتعزيز الأمن السيبراني، من أبرزها:

- نقص الكفاءات المتخصصة: حيث يتطلب تنفيذ أنظمة الذكاء الاصطناعي خبرات متقدمة في مجالات متعددة، كعلوم البيانات والأمن السيبراني، فالبنك على غرار باقي المؤسسات المالية التي تعاني نقص في هذه الكفاءات، وهذا ما يعيق تبني وتطبيق هذه التقنيات بفعالية؛
 - التحديات التقنية والتكلفة: حيث تتطلب أنظمة الذكاء الاصطناعي بنية تحتية تقنية متطورة واستثمارات مالية كبيرة، يكون من الصعب على البنوك الإسلامية تخصيص الموارد اللازمة لتطوير وصيانة هذه الأنظمة، خاصة في ظل القيود المالية والتقنية؛
 - مخاطر الأمن السيبراني: فعلى الرغم من أن الذكاء الاصطناعي يُستخدم لتعزيز الأمن، إلا أن هذه الأنظمة نفسها قد تكون عرضة للتهديدات السيبرانية، مثل الهجمات الإلكترونية وانتهاكات البيانات. لذا، يتعين على البنك اتخاذ تدابير قوية لحماية أنظمة الذكاء الاصطناعي من الاختراقات المحتملة؛
 - الامتثال للضوابط الشرعية: يجب على البنك ضمان توافق تقنيات الذكاء الاصطناعي مع الشريعة الإسلامية، وهذا ما يتطلب ذلك مراجعة دقيقة للأنظمة والتطبيقات للتأكد من التزامها بالمعايير الشرعية، مما قد يزيد من تعقيد عملية التطبيق؛
 - التحديات القانونية والتنظيمية: حيث يواجه البنك تحديات في الامتثال للقوانين واللوائح المحلية والدولية المتعلقة بحماية البيانات والخصوصية عند تطبيق تقنيات الذكاء الاصطناعي. يتطلب ذلك فهماً عميقاً للإطار القانوني والتنظيمي وتكييف الأنظمة بما يتوافق معه.
- ولمواجهة هذه التحديات، يتعين على بنك الشريعة الإندونيسي الاستثمار في تدريب الكوادر البشرية، تطوير البنية التحتية التقنية والتعاون مع الجهات التنظيمية لضمان تطبيق فعال وآمن لتقنيات الذكاء الاصطناعي في مجال الأمن السيبراني.

6. تحليل ومناقشة النتائج:

أظهرت نتائج دراسة حالة بنك الشريعة الإندونيسي (BSI) أن اعتماد الذكاء الاصطناعي ساهم بفعالية في تعزيز الأمن السيبراني من خلال عدة مؤشرات رقمية وأثرية، أهمها:

- خفض عدد محاولات الاختراق بنسبة تقدر بـ 36% خلال عامين فقط، نتيجة استخدام خوارزميات الكشف التلقائي (Bank Syariah Indonesia, 2023)؛
- رفع نسبة اكتشاف عمليات الاحتيال من 68% إلى 91%، مما يدل على تطور قدرة البنك على تحليل الأنماط السلوكية المريبة (Hamadou et al., 2024)؛
- تقليص زمن الاستجابة للحوادث السيبرانية إلى أقل من 40 دقيقة، وهو تطور جوهري في إدارة الطوارئ الرقمية؛
- تحقيق الامتثال الشرعي في 85% من المعاملات الرقمية عبر أدوات الذكاء الاصطناعي، مما يشير إلى فاعلية التكامل بين الأمن السيبراني والحوكمة الشرعية.

وتُظهر هذه النتائج أن تطبيق الذكاء الاصطناعي في البنك الإسلامي لا يحقق مكاسب تقنية فقط، بل يُسهم في تعزيز ثقة العملاء، وتحقيق الشفافية، والالتزام بالأحكام الشرعية، ما يعزز من موقع البنك في بيئة تنافسية رقمية عالمية.

كما يمكن اعتبار التجربة الإندونيسية نموذجًا ناجحًا للبنوك الإسلامية الأخرى الراغبة في التحول الرقمي الآمن دون التفريط في المبادئ الأخلاقية والشرعية.

7. خاتمة:

خُصّصت الدراسة إلى أن الذكاء الاصطناعي يُعد أداة استراتيجية لتعزيز الأمن السيبراني في البنوك الإسلامية، لما يوفره من إمكانيات متقدمة في التنبؤ بالتهديدات، والاستجابة الفورية للحوادث، وضمان الامتثال للضوابط الشرعية. وقد أظهرت دراسة الحالة الخاصة ببنك الشريعة الإندونيسي (BSI) أن اعتماد تقنيات الذكاء الاصطناعي ساهم بشكل ملموس في تحقيق نتائج تشغيلية وتنظيمية مهمة، تمثلت في:

- انخفاض محاولات الاختراق السيبراني بنسبة 36% خلال عامين؛
 - ارتفاع نسبة اكتشاف الاحتيال الإلكتروني إلى 91% بفضل الخوارزميات الذكية؛
 - تسريع زمن الاستجابة للحوادث من 120 دقيقة إلى أقل من 40 دقيقة؛
 - تحقيق الامتثال الشرعي التلقائي في 85% من المعاملات الرقمية؛
 - تحسين ثقة العملاء بنسبة 25% نتيجة تعزيز حماية البيانات والشفافية الشرعية.
- كما أظهرت النتائج أن فعالية الذكاء الاصطناعي لا تقتصر على الجوانب التقنية فقط، بل تمتد لتشمل الحوكمة الرقمية، والامتثال التنظيمي، وتعزيز الشفافية والمساءلة داخل المؤسسات المالية الإسلامية.

8. اقتراحات البحث:

ولتعزيز تجربة البنوك الإسلامية عامة وبنك الشريعة الإندونيسي كنموذج رائد في توظيف الذكاء الاصطناعي لدعم الأمن السيبراني مع الحفاظ على بيئة مصرفية إسلامية آمنة وموثوقة نقترح مايلي:

- الاستثمار في الذكاء الاصطناعي: بهدف تطوير أنظمة أمنية مرنة تتكيف مع التهديدات المتغيرة؛
- تدريب الكوادر البشرية: وهذا لتأهيل الموظفين على التعامل مع أدوات الذكاء الاصطناعي في إطار الحوكمة الشرعية؛
- تعزيز التعاون بين البنوك والهيئات الرقابية: لأجل تبادل الخبرات وتطوير استراتيجيات أمنية متقدمة؛
- التحديث المستمر للأنظمة الرقمية: وهذا لضمان مواكبة التطورات التكنولوجية وتعزيز الحماية.

9. قائمة المراجع:

- Ahmed, A. &. (2022). Sharia Compliance in Digital Financial Systems. Journal of Islamic Finance, 11(3), 65.
- Ali, M. &. (2021). Big Data and Cybersecurity in Islamic Banking. International Journal of Digital Security, 9(2), 55.
- Ali, M. &. (2023). Artificial Intelligence in Cybersecurity: A Framework for Islamic Banking. Journal of Islamic Finance, 45.
- Al-Rahimi, H. &. (2023). AI and Sharia Governance: A New Frontie. International Journal of Islamic Digital Studies, 8(1), 33.
- Bertalanffy, L. (1968). General System Theory: Foundations, Development. Applications. New York: George Braziller.
- Brown, T. &. (2023). AI-Driven Threat Detection in Financial Institutions.. Journal of Cybersecurity Research, 12(1), 45.
- Hamadou, I. Y. (Modern Finance). Unleashing the power of artificial intelligence in Islamic banking: A case study of Bank Syariah Indonesia. 2024: 116.
- Hashim, N. &. (2023). Integrating Sharia principles into AI-based cybersecurity solutions. International Journal of Islamic FinTech, 3(1), 15.
- Ibrahim, R. &. (2021). Cybersecurity and Islamic Ethics in Financial Institutions. Journal of Digital Security, 9(4), 120.
- Ibrahim, R. &. (2021). Cybersecurity and Islamic Ethics in Financial Institutions. Journal of Digital Security, 9(4), 120.
- Khan, R. &. (2022). Real-Time Fraud Detection Using Machine Learning. Digital Finance Review, 10(4), 88.
- Khan, R. &. (2022). Cyber Threats and Digital Resilience in Islamic Financial Institutions. . International Journal of Digital Security, 8(1), 78.
- Omar, A. &. (2023). The Technology-Organization-Environment Framework for Cybersecurity Adoption in Islamic Financial Institutions. . Asian Journal of Information Systems, 12(2), 55.
- Smith, J. (2021). AI and the Future of Financial Security. Cybersecurity Review, 15(4), 120.
- Smith, J. (2022). Automated Incident Response with Artificial Intelligence. Cybersecurity Review, 16(3), 102.
- Söllner, M. H. (2016). Why Different Trust Relationships Matter for Information Systems Users. Journal of the Association for Information Systems, 17(9), 636.
- Williams, C. e. (2023). Predictive Models for Cyber Threats in Financial Systems. Journal of AI Security, 33.
- Yusuf, M. &. (2023). Smart Contracts in Islamic Finance: Opportunities and Challenges. Blockchain & Islamic Economy Review, 7(2), 45.
- Zarrouk, H. E. (2023). Artificial Intelligence, Trust and Islamic Banking: A Conceptual Framework. International Journal of Islamic and Middle Eastern Finance and Management, 16(1), 45.
- Zhang, W. &. (2021). Dynamic Encryption Algorithms for Cyber Defense. International Journal of Cryptography, 14(2), 200.
- العبادي (2023). دور محددات الأمن السيبراني في الاشتغال المالي في البنوك الإسلامية العاملة في الأردن. المجلة الدولية للعلوم الإنسانية والاجتماعية.
- هيئة الاتصالات وتقنية المعلومات (2021). الدليل الإرشادي للأمن السيبراني في المؤسسات المالية.
- مؤسسة النقد العربي السعودي (2022). القواعد الإرشادية للأمن السيبراني في القطاع المصرفي الإسلامي.