

تأثير الذكاء الاصطناعي على غرف التحكم الأمنية – دراسة تطبيقية على البنك

الوطني العربي

اعداد الطالب:

الرقم الجامعي:

اشراف الدكتور:

العام الدراسي: 2026م – 1447هـ

الفصل الأول: الإطار العام للدراسة

- 1.1. مقدمة البحث
- 1.2. مشكلة الدراسة
- 1.3. أهمية الدراسة
 - 1.3.1. على المستوى النظري
 - 1.3.2. على المستوى التطبيقي
- 1.4. أسئلة الدراسة
- 1.5. أهداف الدراسة
- 1.6. فرضيات الدراسة
- 1.7. نموذج الدراسة
- 1.8. الدراسة الميدانية (نطاق الدراسة)
- 1.9. مصطلحات الدراسة
- 1.10. مخطط المشروع

1.1. مقدمة البحث

يشهد القطاع المصرفي العالمي تحولاً هيكلياً متسارعاً في ظل الثورة الرقمية المعاصرة، حيث أصبح الذكاء الاصطناعي أحد المرتكزات الاستراتيجية لإعادة تشكيل البنية التشغيلية والأمنية للمؤسسات المالية. فلم تعد تطبيقات الذكاء الاصطناعي تقتصر على دعم العمليات أو تحسين الكفاءة الإجرائية، بل امتدت لتشكيل إطاراً متكاملًا لإدارة المخاطر والتنبؤ بالتهديدات وتعزيز المرونة المؤسسية في مواجهة الهجمات المركبة (Kovačević et al., 2024). وفي هذا السياق، تمثل غرف التحكم الأمنية ومراكز العمليات الأمنية (SOC) البنية العصبية للمنظومة المصرفية، إذ تضطلع بمهمة تحليل التدفقات الضخمة من البيانات المرئية والرقمية الصادرة عن أنظمة المراقبة وأجهزة الاستشعار وسجلات النشاط السيبراني.

إن التزايد المطرد في حجم البيانات وتعقيد أنماط التهديدات أدى إلى تراجع فعالية نماذج المراقبة التقليدية القائمة على التدخل البشري المكثف، لا سيما في ظل ظاهرة "إجهاد التنبيهات" (Alert Fatigue) التي تؤثر سلباً في دقة التحليل وسرعة الاستجابة (Devoteam, 2024). ومن ثم برزت الحاجة إلى توظيف خوارزميات التعلم العميق والرؤية الحاسوبية والتحليلات التنبؤية لتحويل غرف التحكم من نمط الاستجابة التفاعلية إلى نموذج استباقي قائم على التنبؤ والاحتواء المبكر للمخاطر (كامل، 2024).

وتشير الأدبيات الاقتصادية والتقنية إلى أن الذكاء الاصطناعي سيحدث أثراً اقتصادياً واسع النطاق خلال العقد الجاري، سواء من حيث تعزيز الإنتاجية أو إعادة هيكلة سلاسل القيمة في القطاعات الحساسة، وعلى رأسها القطاع المالي (Central Bank of Kuwait, 2024). كما توضح تقارير الصناعة أن تبني الأتمتة الذكية في العمليات المصرفية يسهم في خفض تكاليف الحوادث الأمنية وتقليل زمن الاكتشاف والاستجابة، وهو ما ينعكس إيجاباً على الاستقرار المالي وتقليل الخسائر الناجمة عن خروقات البيانات (IBM, 2024).

وفي المقابل، شهدت بيئة التهديدات تطوراً نوعياً تمثل في تصاعد الهجمات الهجينة التي تدمج بين الاختراق السيبراني والاستهداف المادي، إضافة إلى توظيف تقنيات التزييف العميق والهندسة الاجتماعية المدعومة بالذكاء الاصطناعي في عمليات الاحتيال المالي (Frontiers in Artificial Intelligence, 2024). ويؤكد ذلك الحاجة إلى نماذج أمنية هجينة (Human-AI Hybrid) تجمع بين الكفاءة الحسابية للأنظمة الذكية والحكم المهني البشري، بما يضمن تحقيق توازن بين الدقة التشغيلية ومتطلبات الامتثال والخصوصية (Rand Corporation, 2023).

وعلى المستوى الوطني، يتسق هذا التحول مع توجهات رؤية المملكة العربية السعودية 2030 التي تضع التحول الرقمي والأمن السيبراني ضمن أولوياتها الاستراتيجية لتعزيز تنافسية الاقتصاد الوطني. وقد أظهرت تقارير حديثة تنامياً في جاهزية المؤسسات السعودية لتبني تطبيقات الذكاء الاصطناعي، مع تفاوت في مستويات النضج التقني والبنية التحتية الداعمة (Cisco, 2025). وفي هذا الإطار، يُعد البنك الوطني العربي (anb) نموذجاً مصرفياً فاعلاً في تبني مبادرات التحول الرقمي وتعزيز قدراته التقنية والأمنية، حيث يعمل على تطوير البنية التشغيلية لمراكز العمليات الأمنية وتكاملها مع منصات تحليلية متقدمة (Arab National Bank, 2024). كما تعكس شراكاته الاستراتيجية، ومن أبرزها التعاون مع IBM لتوظيف منصات الذكاء الاصطناعي والتحليلات المتقدمة في مكافحة الاحتيال وحماية المعاملات المصرفية، التزام البنك بتبني أحدث التقنيات لتعزيز الأمن والموثوقية في خدماته (Retail Banker International, 2025). الأمر الذي يجعل البنك الوطني العربي حالة دراسية ملائمة لتحليل الأثر الفعلي لتطبيقات الذكاء الاصطناعي في بيئة مصرفية سعودية واقعية.

وانطلاقاً من ذلك، تنبع أهمية هذه الدراسة من الحاجة إلى تقييم علمي ميداني لمدى تأثير تقنيات الذكاء الاصطناعي في كفاءة أداء غرف التحكم الأمنية داخل بيئة مصرفية سعودية، وقياس انعكاساتها على مؤشرات الأداء الرئيسية مثل دقة الكشف، ومتوسط زمن الاكتشاف (MTTD)، ومتوسط زمن الاستجابة (MTTR)، فضلاً عن مستوى الامتثال التنظيمي. وتسعى الدراسة إلى بناء نموذج تحليلي يفسر العلاقة بين تبني تقنيات الذكاء الاصطناعي وتحسين الأداء الأمني، بالاعتماد على استبانة كأداة رئيسية لجمع البيانات من عينة الدراسة، بما يساهم في تقديم إطار استراتيجي متكامل يدعم اتخاذ القرار في المؤسسات المالية السعودية.

1.2. مشكلة الدراسة

يشهد القطاع المصرفي تحولاً متسارعاً في بنيته الأمنية نتيجة التوسع في تبني الذكاء الاصطناعي، مما أعاد تعريف دور غرف التحكم الأمنية من المراقبة التقليدية إلى النماذج التنبؤية القادرة على استباق المخاطر. إلا أن هذا التحول يواجه تحديات تتعلق بمدى فعالية هذه التقنيات في تحسين مؤشرات الأداء الأمني (Kovačević et al., 2024).

وعلى الرغم من قدرة الذكاء الاصطناعي على تقليل زمن اكتشاف الحوادث وخفض التكاليف، تشير التقارير إلى استمرار فجوة بين الإمكانيات النظرية للتقنيات الذكية ومستوى الاستفادة الفعلية منها في المؤسسات المالية (IBM, 2024). ويتزامن ذلك مع تصاعد الهجمات الهجينة واستخدام تقنيات التزييف العميق، مما يزيد الضغوط على غرف التحكم التي تعتمد على التدخل البشري في تحليل كميات هائلة من التنبؤات اليومية (Frontiers in Artificial Intelligence, 2024).

وفي السياق السعودي، تتعاظم أهمية الموضوع في ظل رؤية 2030 التي تؤكد على الأمن السيبراني كركيزة لاستقرار النظام المالي، غير أن تقارير الجاهزية تشير لتفاوت في النضج المؤسسي والقدرة على استيعاب تطبيقات الذكاء الاصطناعي (Cisco, 2025). كما تفرض البيئة التنظيمية متطلبات دقيقة حول شفافية القرارات المؤتمتة ومساءلة الخوارزميات (Rand Corporation, 2023).

أما على المستوى المؤسسي، فيعد البنك الوطني العربي نموذجاً مصرفياً يتبنى التحول الرقمي وتطوير مراكز العمليات الأمنية، إلا أنه يواجه تساؤلات جوهرية حول مدى تحقيق تقنيات الذكاء الاصطناعي لأهدافها في تحسين سرعة الاستجابة ودقة التحليل والامتثال التنظيمي. وتكتسب هذه التساؤلات أهمية خاصة في ضوء الاعتماد على الاستبانة كأداة رئيسية لاستقصاء آراء القادة الأمنيين والمحللين والخبراء حول هذه القضايا.

من هنا تبرز الحاجة لدراسة تطبيقية تقيس أثر الذكاء الاصطناعي على أداء غرف التحكم الأمنية في البنك الوطني العربي باستخدام استبانة تصمم خصيصاً لهذا الغرض، لينطلق السؤال الرئيس: ما طبيعة وقوة تأثير تطبيق تقنيات الذكاء الاصطناعي على كفاءة أداء غرف التحكم الأمنية في البنك الوطني العربي من حيث سرعة الاستجابة ودقة التحليل والامتثال التنظيمي؟

1.3. أهمية الدراسة

تسهم الدراسة في دعم رؤية 2030 بتقديم رؤية تطبيقية لتعزيز الأمن السيبراني في القطاع المصرفي، مما يدعم هيئات التنظيم كالهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي، ويعزز جاهزية المملكة بمؤشرات الأمن السيبراني العالمية للانتقال الآمن نحو الاقتصاد الرقمي.

1.3.1. على المستوى النظري

تساهم الدراسة في إثراء البناء المعرفي من خلال تأصيل مفاهيم "الأمن التنبئي" و"الأتمتة الدفاعية" في السياق المصرفي العربي (Central Bank of Kuwait, 2024). كما تسعى لتطوير إطار نظري يوضح علاقة تقنيات الذكاء الاصطناعي بمتغيرات الأداء الأمني مثل دقة الكشف وزمن الاستجابة والامتثال التنظيمي (كامل، 2024). فضلاً عن سد الفجوة البحثية المحلية بتوفير مرجع أكاديمي يركز على البيئة المصرفية السعودية (Sidra Capital, 2024).

1.3.2. على المستوى التطبيقي

تنعكس نتائج الدراسة مباشرة على ممارسات البنك الوطني العربي عبر تزويد صناع القرار ببيانات دقيقة تستند إلى نتائج الاستبانة حول قدرة الذكاء الاصطناعي على تحسين الأداء الأمني. كما تساعد في توجيه استراتيجيات الاستثمار التقني نحو الأدوات ذات الأثر الأمني الأعلى، وتعزيز الامتثال لضوابط البنك المركزي السعودي والهيئة الوطنية للأمن السيبراني (Arab National Bank, 2024). بالإضافة إلى تحديد المهارات الحرجة اللازمة لتطوير رأس المال البشري في غرف التحكم الأمنية (Cisco, 2025).

1.4. أسئلة الدراسة

انطلاقاً من مشكلة الدراسة، تسعى هذه الدراسة إلى الإجابة عن مجموعة من التساؤلات التي تستهدف الكشف عن طبيعة العلاقة بين مستوى تبني تقنيات الذكاء الاصطناعي وكفاءة الأداء الأمني في البنك الوطني العربي، وذلك من خلال تصميم وتوزيع استبانة على المعنيين.

أولاً: السؤال الرئيس للدراسة

ما طبيعة وقوة تأثير تطبيق تقنيات الذكاء الاصطناعي على كفاءة أداء غرف التحكم الأمنية في البنك الوطني العربي، من حيث سرعة الاستجابة، ودقة التحليل، ومستوى الامتثال التنظيمي؟

ثانياً: التساؤلات الفرعية

1. ما مستوى تبني تقنيات الذكاء الاصطناعي (الرؤية الحاسوبية، تعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية) في غرف التحكم الأمنية بالبنك الوطني العربي من وجهة نظر العينة؟
2. ما أثر تطبيق نماذج تعلم الآلة والتحليلات التنبؤية في خفض متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) للحوادث الأمنية؟
3. ما تأثير تقنيات الرؤية الحاسوبية في تحسين دقة اكتشاف التهديدات المادية وتقليل معدلات الإنذارات الكاذبة؟
4. ما العلاقة بين استخدام تقنيات معالجة اللغات الطبيعية وتحليل سجلات الأمن السيبراني وتعزيز سرعة الاستجابة للحوادث؟
5. ما تأثير تقنيات الذكاء الاصطناعي على مستوى الامتثال التنظيمي لمتطلبات الجهات الرقابية في غرف التحكم الأمنية؟

6. ما أبرز التحديات التقنية والبشرية والتنظيمية التي تحد من فعالية توظيف الذكاء الاصطناعي في غرف التحكم الأمنية

بالبنك؟

1.5. أهداف الدراسة

تسعى هذه الدراسة إلى تحقيق هدف رئيس يتمثل في قياس تأثير تطبيق تقنيات الذكاء الاصطناعي على كفاءة أداء غرف التحكم الأمنية في البنك الوطني العربي، وذلك من خلال تصميم استبانة وتوزيعها على عينة من القادة الأمنيين ومديري غرف التحكم ومحللي العمليات الأمنية وخبراء تقنية المعلومات. ويتفرع عن هذا الهدف الرئيس مجموعة من الأهداف الفرعية:

1. تشخيص واقع تبني تقنيات الذكاء الاصطناعي في غرف التحكم الأمنية بالبنك الوطني العربي، من خلال تحديد مستوى استخدام الرؤية الحاسوبية، وتعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية في العمليات الأمنية، بالاعتماد على استجابات عينة الدراسة.
2. قياس تأثير تقنيات تعلم الآلة والتحليلات التنبؤية في تحسين متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) للحوادث الأمنية، وفقاً لتقديرات العينة المستجيبة.
3. تحليل دور تقنيات الرؤية الحاسوبية في تحسين دقة اكتشاف التهديدات المادية وتقليل معدلات الإنذارات الكاذبة داخل غرف التحكم.
4. اختبار العلاقة بين توظيف تقنيات معالجة اللغات الطبيعية في تحليل السجلات الأمنية وتعزيز سرعة الاستجابة للحوادث والتهديدات السيبرانية.
5. قياس تأثير تقنيات الذكاء الاصطناعي على مستوى الامتثال التنظيمي في غرف التحكم الأمنية بالبنك الوطني العربي من خلال مؤشرات الالتزام بسياسات البنك المركزي، ووضوح آلية التبعية والمساءلة، وقابلية تفسير قرارات الأنظمة الذكية.
6. تحديد أبرز التحديات التقنية والبشرية والتنظيمية التي تواجه تطبيق تقنيات الذكاء الاصطناعي في غرف التحكم الأمنية، كما تعكسها آراء المستجيبين، وذلك باستخدام الإحصاء الوصفي.
7. تقديم توصيات عملية لتعزيز فعالية توظيف الذكاء الاصطناعي في غرف التحكم الأمنية بالبنك الوطني العربي، بناءً على نتائج تحليل الاستبانة.

1.6. فرضيات الدراسة

استناداً إلى النموذج الهيكلي المقترح للدراسة، وفي ضوء الاعتماد على الاستبانة كأداة رئيسية لجمع البيانات واختبار هذه الفرضيات إحصائياً، تتمثل فرضيات الدراسة فيما يلي:

الفرضية الرئيسية:

يوجد تأثير ذو دلالة إحصائية لتقنيات الذكاء الاصطناعي بأبعادها (الرؤية الحاسوبية، وتعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية) على كفاءة أداء غرف التحكم الأمنية بأبعادها (سرعة الاستجابة، ودقة التحليل، ومستوى الامتثال التنظيمي) في البنك الوطني العربي.

الفرضيات الفرعية:

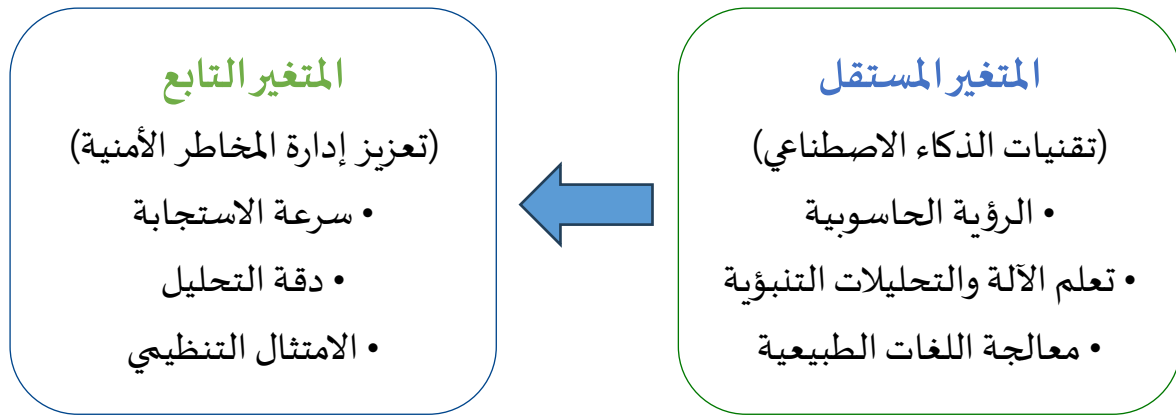
- **الفرضية الأولى:** يوجد تأثير ذو دلالة إحصائية لتطبيق نماذج تعلم الآلة والتحليلات التنبؤية على خفض متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) في غرف التحكم الأمنية.
- **الفرضية الثانية:** يوجد تأثير ذو دلالة إحصائية لتقنيات الرؤية الحاسوبية في تحسين دقة اكتشاف التهديدات المادية وتقليل معدلات الإنذارات الكاذبة.
- **الفرضية الثالثة:** يوجد تأثير ذو دلالة إحصائية لاستخدام تقنيات معالجة اللغات الطبيعية في تحليل السجلات الأمنية على سرعة الاستجابة للحوادث السيبرانية.
- **الفرضية الرابعة:** يوجد تأثير ذو دلالة إحصائية لتقنيات الذكاء الاصطناعي على مستوى الامتثال التنظيمي في غرف التحكم الأمنية.
- **الفرضية الخامسة:** توجد فروق ذات دلالة إحصائية في تقديرات أفراد العينة لتأثير الذكاء الاصطناعي على أداء غرف التحكم تعزى إلى المتغيرات الديموغرافية (المسمى الوظيفي، سنوات الخبرة، المؤهل العلمي).

1.7. نموذج الدراسة

يعكس نموذج الدراسة العلاقة بين المتغير المستقل "تقنيات الذكاء الاصطناعي" بأبعاده الثلاثة: الرؤية الحاسوبية، تعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية (Kovačević et al., 2024)، والمتغير التابع "أداء غرف التحكم الأمنية" بأبعاده: سرعة الاستجابة، دقة التحليل، والامتثال التنظيمي (كامل، 2024). ويفترض النموذج وجود علاقة تأثير مباشر بين المتغير المستقل والمتغير التابع، يتم اختبارها باستخدام تحليل الانحدار المتعدد. وتعرف هذه المتغيرات إجرائياً من خلال

استبانة الدراسة التي تتضمن مجموعة من العبارات تقيس: مستوى استخدام كل تقنية من تقنيات الذكاء الاصطناعي، ومؤشرات الأداء الأمني مثل سرعة اكتشاف التهديدات، ودقة التحليل، ومعدلات الامتثال التنظيمي (وتشمل الالتزام بسياسات البنك المركزي، ووضوح آلية التتبع والمساءلة، وقابلية تفسير قرارات الأنظمة الذكية)، وذلك وفقاً لتقديرات أفراد العينة على مقياس ليكرت الخماسي.

النموذج المفاهيمي للدراسة



1.8. الدراسة الميدانية (نطاق الدراسة)

تحدد حدود هذه الدراسة لضمان دقة النتائج وقابليتها للتطبيق في بيئة واقعية، مع التركيز على تصميم وتوزيع استبانة تغطي النطاقات المحددة، كما يلي:

- **النطاق المكاني:** تُجرى الدراسة في البنك الوطني العربي (anb) بفروعه الرئيسية ومركز العمليات الأمنية (SOC) المركزي في مدينة الرياض، مع إمكانية توسيع العينة لتشمل عينة ممثلة من فروع الرئيسية في جدة والمنطقة الشرقية لضمان تعميم النتائج على مستوى البنك. وسيتم توزيع الاستبانة إلكترونياً وورقياً على المستهدفين في هذه المواقع.
- **النطاق البشري:** تستهدف الدراسة القادة الأمنيين، مديري غرف التحكم، محلي العمليات الأمنية (SOC Analysts)، وخبراء تقنية المعلومات والذكاء الاصطناعي المنخرطين بشكل مباشر في إدارة المنظومات الأمنية بالبنك. وستوجه إليهم استبانة الدراسة لجمع البيانات اللازمة.

■ **النطاق الموضوعي:** يقتصر البحث على دراسة تأثير تقنيات الذكاء الاصطناعي ممثلة في: تعلم الآلة والتحليلات التنبؤية، والرؤية الحاسوبية، ومعالجة اللغات الطبيعية على أداء غرف التحكم الأمنية، مع التركيز على مؤشرات سرعة الاستجابة ودقة التحليل والامتثال التنظيمي.

■ **النطاق الزمني:** تغطي الدراسة التطورات التقنية والأبحاث المنشورة في الفترة ما بين (2020 – 2025)، مع تركيز خاص على أحدث الابتكارات في عامي 2024 و2025. كما سيتم توزيع الاستبانة وجمع البيانات خلال الفصل الدراسي الحالي.

1.10. مصطلحات الدراسة

تتضمن هذه الدراسة مجموعة من المصطلحات العلمية والتقنية التي تشكل الركيزة الأساسية لفهم العلاقة بين تقنيات الذكاء الاصطناعي وأداء غرف التحكم الأمنية في القطاع المصرفي. وقد صيغت هذه المصطلحات وفق مستويين: التعريف النظري المستند إلى الأدبيات المتخصصة، والتعريف الإجرائي المرتبط بسياق التطبيق في البنك الوطني العربي، وذلك على النحو التالي:

2. الذكاء الاصطناعي (Artificial Intelligence – AI)

● **التعريف النظري:** هو مجموعة من الأنظمة والتقنيات البرمجية القادرة على محاكاة القدرات الذهنية البشرية، وتتميز بالقدرة على اتخاذ القرارات، وتوليد المحتوى، وتقديم التوصيات، أو القيام بالتنبؤات بناءً على مستويات متفاوتة من الاستقلالية (SDAIA, 2025).

● **التعريف الإجرائي:** هو حزمة البرمجيات والخوارزميات المستخدمة في غرف التحكم بالبنك الوطني العربي (مثل منصات IBM Watson) لتحليل البيانات الأمنية والمالية وكشف أنماط الاحتيال آلياً.

3. الذكاء الاصطناعي الوكيل (Agentic AI)

● **التعريف النظري:** هو جيل متطور من أنظمة الذكاء الاصطناعي يتجاوز مجرد الاستجابة للأوامر، حيث يمتلك القدرة على إدراك البيئة المحيطة، وتفسير المعلومات، وتحديد الأهداف، وتنفيذ مهام معقدة متعددة الخطوات بشكل مستقل أو بإشراف بشري محدود (SDAIA, 2025; Srinivas et al., 2025).

● **التعريف الإجرائي:** هو استخدام "وكلاء أذكاء" داخل مركز العمليات الأمنية بالبنك للقيام بعمليات التحقيق الأولية في التنبيهات وعزل التهديدات السيبرانية دون الحاجة لتدخل مباشر من المحلل في كل خطوة.

4. رفة التحكم الأمنية (Security Control Room)

- **التعريف النظري:** هي منشأة مركزية مجهزة تقنياً لمراقبة وتأمين المواقع، تهدف إلى الكشف عن الأعمال غير القانونية وردع الجرائم لتعزيز السلامة العامة، وتعتمد في عملها على دمج بيانات الكاميرات وحساسات الدخول (Baker & Benny, 2012; Reynaud & Untersinger, 2024).
- **التعريف الإجرائي:** هي المركز الفني المسؤول عن مراقبة الفروع المادية للبنك الوطني العربي وأجهزة الصراف الآلي عبر أنظمة الرؤية الحاسوبية والتحقق من هويات الداخلين.

5. مركز العمليات الأمنية (Security Operations Center – SOC)

- **التعريف النظري:** هو مركز عمليات مركزي يعمل كعصب دفاعي للمؤسسة، يهدف إلى اكتشاف التهديدات، والاستجابة للحوادث، ومنع وقوعها من خلال تنسيق وتكامل جميع التقنيات الأمنية والعمليات والكوادر البشرية (Khayat et al., 2025).
- **التعريف الإجرائي:** هو الفريق التقني في البنك الوطني العربي المسؤول عن إدارة التهديدات السيبرانية التي تستهدف البنية التحتية الرقمية والحسابات المصرفية على مدار الساعة.

6. إرهاق التنبيهات (Alert Fatigue)

- **التعريف النظري:** هي حالة نفسية وتشغيلية تصيب محللي الأمن، حيث يفقدون الحساسية تجاه الإنذارات نتيجة الحجم الهائل من التنبيهات وارتفاع نسب الإنذارات الكاذبة (أكثر من 50%)، مما يؤدي إلى إغفال تهديدات حقيقية (Mandadi, 2025; CyberDefenders, 2026).
- **التعريف الإجرائي:** هو الضغط المعرفي الذي يواجهه محللو البنك الوطني العربي نتيجة التعامل مع مئات التنبيهات اليومية الناتجة عن أنظمة SIEM التقليدية.

7. التحليلات التنبؤية (Predictive Analytics)

- **التعريف النظري:** هي عملية استخدام البيانات التاريخية، والخوارزميات الإحصائية، وتقنيات التعلم الآلي لتحديد أنماط السلوك والتنبؤ بالتهديدات أو النتائج المستقبلية قبل وقوعها (Group-IB, 2025; Kovačević et al., 2024).
- **التعريف الإجرائي:** هي النماذج الرياضية التي يطبقها البنك لاستباق عمليات الاختراق أو الاحتيال المالي بناءً على تحليل السلوك التاريخي للعملاء والمهاجمين.

8. الرؤية الحاسوبية (Computer Vision)

- **التعريف النظري:** هي أحد فروع الذكاء الاصطناعي التي تمكن الحواسيب من استخلاص معلومات عالية المستوى وفهم محتوى الصور الرقمية ومقاطع الفيديو، لمحاكاة حاسة البصر البشرية في التعرف على الوجوه واكتشاف الأجسام (Microsoft, 2026; Reynaud & Untersinger, 2024).
- **التعريف الإجرائي:** هي التقنية المستخدمة في كاميرات المراقبة بالبنك الوطني العربي للتعرف التلقائي على الموظفين، وكشف محاولات التسلل، وتحليل تدفق العملاء داخل الفروع.

9. معالجة اللغات الطبيعية (Natural Language Processing – NLP)

- **التعريف النظري:** هي تقنية تتيح للحواسيب فهم وتفسير وتوليد اللغة البشرية، وتُستخدم في الأمن لتلخيص سجلات النشاط المعقدة وتحليل تقارير الاستخبارات الأمنية غير المهيكلية (Allen et al., 2022; Srinivas et al., 2025).
- **التعريف الإجرائي:** هي الأدوات المستخدمة داخل البنك لتحويل آلاف السجلات النصية (Logs) إلى ملخصات مفهومة تساعد المحللين في اتخاذ قرارات سريعة.

10. الكفاءة التشغيلية (Operational Efficiency)

- **التعريف النظري:** هي قدرة غرفة التحكم على إدارة مشهد التهديدات المتوسع بأقل الموارد الممكنة، وتُقاس من خلال تقليل متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) وزيادة دقة الأداء (Vectra AI, 2025; Taqafi et al., 2023).
- **التعريف الإجرائي:** هي مستوى التحسن في سرعة إغلاق التذاكر الأمنية في البنك الوطني العربي وانخفاض التكاليف الناتجة عن الحوادث الأمنية بعد تبني الذكاء الاصطناعي.

11. الامتثال التنظيمي (Regulatory Compliance)

- **التعريف النظري:** هو الالتزام بالمتطلبات والمعايير التي تضعها الجهات الرقابية، والتي تشمل ضوابط الحوكمة، وحماية البيانات الشخصية، وإجراءات الاستجابة للحوادث لضمان استقرار النظام المالي (SAMA, 2024; Rand Corporation, 2023).
- **التعريف الإجرائي:** هو مدى توافق أنظمة الذكاء الاصطناعي في البنك الوطني العربي مع "إطار الأمن السيبراني" الصادر عن البنك المركزي السعودي (SAMA) وسياسات الهيئة الوطنية للأمن السيبراني.

1.9. مخطط المشروع

يتكون المشروع البحثي من خمسة فصول أساسية تتبع المنهجية العلمية الرصينة، مع التركيز على تصميم وتطوير وتطبيق

استبانة الدراسة كأداة رئيسية لجمع البيانات:

الفصل الأول (الإطار العام للدراسة): ويتضمن المقدمة، مشكلة الدراسة، الأهمية، الأسئلة، الأهداف، الفرضيات، نموذج

الدراسة، نطاق الدراسة، ومخطط المشروع.

الفصل الثاني (الدراسات السابقة والإطار النظري): مراجعة شاملة للأدبيات المتعلقة بالذكاء الاصطناعي في الأمن

المصرفي، وتطور غرف التحكم الأمنية، وتحليل الدراسات التي تناولت المتغير المستقل (تقنيات الذكاء الاصطناعي) والمتغير

التابع (أداء غرف التحكم)، وذلك لبناء الإطار النظري الذي تستند إليه استبانة الدراسة.

الفصل الثالث (منهجية الدراسة): توضيح الفلسفة البحثية (الوضعية)، المنهج (الاستنتاجي)، تصميم البحث، مجتمع

وعينة الدراسة، مع التركيز على تصميم استبانة الدراسة وتطويرها، واختبار صدقها وثباتها، وآليات توزيعها وجمعها،

وأساليب المعالجة الإحصائية باستخدام برنامج SPSS لاختبار الفرضيات. وسيتم قياس الامتثال التنظيمي من خلال بنود

تقيس الالتزام بسياسات البنك المركزي، ووضوح آلية التتبع والمساءلة، وقابلية تفسير قرارات الأنظمة الذكية باستخدام

مقياس ليكرت الخماسي. أما بالنسبة للتحديات التقنية والبشرية والتنظيمية، فسيتم تحليلها باستخدام الإحصاء الوصفي

(المتوسطات الحسابية والانحرافات المعيارية) دون اختبار فرضيات.

الفصل الرابع (التحليل الإحصائي ومناقشة النتائج): عرض نتائج البيانات المجمعة من الاستبانة باستخدام برنامج

SPSS، اختبار الفرضيات باستخدام تحليل الانحدار المتعدد واختبارات تحليل التباين، مناقشة النتائج في ضوء الأدبيات

السابقة، وتحليل مدى تحقق الأهداف.

الفصل الخامس (الخاتمة والتوصيات): تلخيص الاستنتاجات العامة المستخلصة من تحليل استجابات العينة، تحديد

حدود الدراسة والدراسات المستقبلية المقترحة، وتقديم توصيات عملية للمؤسسات الأمنية وصناع القرار تستند إلى نتائج

الاستبانة.

قائمة المراجع والمصادر

- كامل، ع. (2024). استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة: تحليل الممارسات الدولية واستشراف التحديات المستقبلية. المجلة العربية للدراسات الأمنية، 40(1)، 15-34.
- Allen, L. K., Creer, S. C., & Öncel, P. (2022). Natural Language Processing as a Tool for Learning Analytics. In Handbook of Learning Analytics. <https://doi.org/10.18608/hla22.005>
- Arab National Bank. (2024). Annual Report 2024: Realizing Possibilities, Delivering Results. Riyadh: anb.
- Central Bank of Kuwait. (2024). Artificial Intelligence: Advantages and Challenges (Economic Research Department, Issue No. 6). Kuwait: Central Bank of Kuwait.
- Baker, P. R., & Benny, D. J. (2012). The Complete Guide to Physical Security. Auerbach Publications.
- CyberDefenders. (2026). SOC Alert Fatigue: Causes, Impact & AI Solutions. CyberDefenders Blog. <https://cyberdefenders.org/blog/soc-alert-fatigue/>
- Cisco. (2025). AI Readiness Index: Saudi Arabia Insights. San Jose, CA: Cisco Systems Inc. [استرجع من https://www.arabnews.com/node/2623860/amp](https://www.arabnews.com/node/2623860/amp)
- Devoteam. (2024). How AI is Transforming Security Operations Centers (SOC) and Redefining Incident Management. Cybersecurity Expert View. [استرجع من https://www.devoteam.com/expert-view/how-ai-is-transforming-security-operations-centers-soc-and-redefining-incident-management/](https://www.devoteam.com/expert-view/how-ai-is-transforming-security-operations-centers-soc-and-redefining-incident-management/)
- Frontiers in Artificial Intelligence. (2024). Impact of AI on financial services cybersecurity: A systematic review. Frontiers Journal, 7(144). [استرجع من http://www.frontiersin.org/research-topics/60555/artificial-intelligence-for-data-protection-in-digital-asset-systems](http://www.frontiersin.org/research-topics/60555/artificial-intelligence-for-data-protection-in-digital-asset-systems)
- IBM. (2024). Cost of a Data Breach Report 2024. IBM Security Services. [استرجع من https://www.networkworld.com/article/3478991/ibm-cost-of-an-enterprise-data-breach-hit-post-pandemic-high.html](https://www.networkworld.com/article/3478991/ibm-cost-of-an-enterprise-data-breach-hit-post-pandemic-high.html)
- Kiteworks. (2024). The AI Security Gap: Why Organizations are Flying Blind. Risk Management Report. [استرجع من https://www.kiteworks.com/video-ai-data-security-report/](https://www.kiteworks.com/video-ai-data-security-report/)
- Kovačević, A., Radenković, S. D., & Nikolić, D. (2024). Artificial intelligence and cybersecurity in banking sector: opportunities and risks. ArXiv Preprint.
- NCBI. (2024). Theoretical and practical gaps in the integration of AI within cybersecurity and privacy. PMC, Article 11656524. [استرجع من https://pmc.ncbi.nlm.nih.gov/articles/PMC11656524/](https://pmc.ncbi.nlm.nih.gov/articles/PMC11656524/)
- OpenText. (2024). State of AI in Banking. Digital Banking Report. [استرجع من https://thefinancialbrand.com/banking-podcasts/bridging-the-generative-ai-readiness-gap](https://thefinancialbrand.com/banking-podcasts/bridging-the-generative-ai-readiness-gap)
- Ramadhani, A., & Trimuliani, S. (2024). Barriers to AI Adoption in the Banking Sector: A Systematic Literature Review. International Journal of Finance and Banking Studies.
- Rand Corporation. (2023). The Implications of AI for Surveillance and Individual Privacy (Research Perspectives Report). Santa Monica, CA: Rand Corporation. [استرجع من https://outlook.stpi.niar.org.tw/index/news/4b114100937625b30193b4c1a3146586](https://outlook.stpi.niar.org.tw/index/news/4b114100937625b30193b4c1a3146586)
- Retail Banker International. (2025, January 15). Arab National Bank deploys IBM platform to combat fraud. Financial Technology News. [استرجع من https://www.zawya.com/en/capital-markets/equities/anb-posts-130bln-profits-in-2024-dividends-for-h2-24-unveiled-chepvl8s](https://www.zawya.com/en/capital-markets/equities/anb-posts-130bln-profits-in-2024-dividends-for-h2-24-unveiled-chepvl8s)
- Khayat, M., Barka, E., Serhani, M. A., Sallabi, F., Shuaib, K., & Khater, H. M. (2025). Empowering Security Operation Center With Artificial Intelligence and Machine Learning—A Systematic Literature Review. IEEE Access, 13, 1-1. <https://doi.org/10.1109/ACCESS.2025.3532951>

- Security Industry Association. (2025). Computer Vision Changes Everything: From Passive Observation to Proactive Intervention. SIA Research Blog. استرجع من <https://www.securityindustry.org/2025/03/03/transforming-physical-security-how-ai-is-changing-the-gsoc/>
- Sidra Capital. (2024). Rise of AI in Saudi Arabia's Financial Sector: Opportunities and Challenges (Investment Insight Report). Jeddah: Sidra Capital.
- Srinivas, S., Kirk, B., Zendejas, J., Espino, M., Boskovich, M., Bari, A., Dajani, K., & Alzahrani, N. (2025). AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation. Journal of Cybersecurity and Privacy, 5(4), 95. <https://doi.org/10.3390/jcp5040095>
- Mandadi, V. R. (2025). Risk-Based Alerting: Revolutionizing Cybersecurity Operations through Intelligent Threat Prioritization. International Journal of Computational and Experimental Science and Engineering, 11(4).