

عنوان البحث:

"أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على نجاح مشاريع تطوير الأمن البنكي في المملكة العربية السعودية: دراسة ميدانية"

إعداد الطالب:

تركي بن فالح العتيبي

بحث مقدم استكمالاً لمتطلبات الحصول على درجة الماجستير في إدارة المشاريع

إشراف:

د. الفيصل عبد الحميد

د. فايز جراد

العام الدراسي: (1446هـ – 2025 م)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الإهداء

إلى من كان رضاهم مفتاحاً لكل نجاح وتوفيق، ومن جعلوا من الدعاء لي نبعاً لا ينضب...
إلى الوالد الكريم (حفظه الله)، صاحب الأيادي البيضاء، الذي غرس في نفسي حب الإصرار
والثابرة.

إلى الوالدة الحبيبة (أطال الله في عمرها)، التي كانت دعواتها الصادقة نوراً يضيء دربي،
وسنداً لي في كل خطوة.

إلى شريك العمر، رفيق الدرب وكاتم السر، الذي شاركني الصبر والعناء، وكانت كلماته بلسماً
يُخفف وطأة الجهد.

وإلى فلذات كبدي، وزهرة حياتي، الذين أهدوني أجمل لحظات الفرح، ومن أجلهم بذلت كل
جهد.

إلى من تتلمذت على أيديهم، وأضاءوا لي الطريق بعلمهم الغزير وتوجيهاتهم القيمة...

إلى أساتذتي الأجلاء والمشرفين الكرام:

الدكتور الفيصل عبد الحميد والدكتور فايز جراد، لجهدهم المبارك وإشرافهم المتقن.

وإلى كل زميل وصديق، وإلى كل من ساندني أوقدّم لي يد العون،

أهدي إليكم جميعاً ثمرة هذا الجهد، راجياً من الله أن يكون عملاً خالصاً لوجهه الكريم.

ابنكم/

تركي بن فالح العتيبي

الشكر والتقدير

الحمد لله الذي بنعمته تتم الصالحات وله الفضل والمنة على ما أنعم به علي من توفيق
لإتمام هذا البحث

أتقدم بجزيل الشكر والامتنان وعظيم التقدير إلى كل من أسهم في إنجاز هذا العمل وإلى كل
من قدم لي يد العون والمساعدة والمعلومة الصادقة وأخص بالشكر

لجامعة ميدأوشن وكلية الإدارة على إتاحة الفرصة لدراسة الماجستير في إدارة المشاريع وعلى
توفير البيئة الأكاديمية المحفزة للبحث العلمي

للمشرفين الأجلاء الدكتور الفيصل عبد الحميد والدكتور فايز جراد على ما بذلاه من جهد
كبير وتوجيهاتهم العلمية القيمة التي كان لها الأثر البالغ في إثراء البحث وتقويمه ومتابعتهم
الدقيقة والصبر على تساؤلاتي فجزاها الله خير الجزاء

لإدارات الأمن والمراقبة والتقنية في البنوك السعودية الذين تفضلوا بتسهيل مهمة جمع
البيانات وقدموا لي المساعدة في الإجابة على استبانة الدراسة بكل رحابة صدر وشفافية
وكانوا عنصراً محورياً في نجاح الجانب الميداني للبحث

لأساتذتي الكرام في برنامج الماجستير الذين نهلت من علمهم واكتسبت من خبراتهم المعرفية ما
كان سبيلاً لإنجاز هذا العمل

لأفراد عائلتي الكريمة الذين تحملوا غيابي وانشغالي وخص بالذكر الوالدين وزوجتي وأبنائي
على صبرهم ودعمهم المتواصل لي

أسأل الله أن يتقبل هذا الجهد وأن يجعله نافعاً ومثمراً

الباحث

تركي بن فالح العتيبي

الملخص

هدفت هذه الدراسة إلى استقصاء أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على رفع كفاءة الأمن البنكي في المملكة العربية السعودية، وذلك في ظل التحولات الرقمية التي تشهدها المملكة ضمن رؤية 2030. ولتحقيق هذا الهدف، اعتمدت الدراسة على المنهج الوصفي التحليلي، وتم استخدام الاستبانة كأداة لجمع البيانات من عينة قصدية قوامها (100) فرد من العاملين في إدارات الأمن والمراقبة والتقنية في البنوك السعودية. وتوصلت الدراسة إلى وجود أثر إيجابي ذي دلالة إحصائية قوية لدمج تقنيات الذكاء الاصطناعي على كفاءة الأمن البنكي، حيث فسر متغير تبني الذكاء الاصطناعي ما نسبته (68.4%) من التباين الكلي في مستوى الكفاءة الأمنية. كما أظهرت النتائج وجود فروق جوهرية دالة إحصائية في مستوى الأمان وسرعة الاستجابة بين مرحلة ما قبل الدمج وما بعده لصالح الأنظمة الذكية. وتبين أن تقنية "التحليل السلوكي غير الطبيعي" هي العامل الأكثر ارتباطاً بزيادة سرعة الاستجابة للتهديدات، متفوقة نسبياً على تقنيات التعرف الثابت. ومن جانب آخر، كشفت الدراسة أن التحدي الأبرز أمام تطبيق هذه التقنيات ليس تقنياً بحتاً، بل يتمثل في الحاجة الماسة لتدريب الكوادر البشرية، يليه ارتفاع تكاليف الاستثمار ومخاوف خصوصية البيانات. وفي ضوء هذه النتائج، أوصت الدراسة بتبني استراتيجيات "الأمن الذكي الهجين" التي تدمج بين خوارزميات الذكاء الاصطناعي والتدخل البشري المؤهل، مع إعطاء الأولوية للاستثمار في برمجيات "التحليل السلوكي" لقدرتها الاستباقية، وضرورة عقد برامج تدريبية متخصصة للمشغلين، وضمان تطبيق معايير "الخصوصية من التصميم" للامتثال للضوابط التنظيمية.

الكلمات المفتاحية: الذكاء الاصطناعي (AI)، أنظمة المراقبة التلفزيونية (CCTV)، الأمن البنكي، التحليل السلوكي، كفاءة الأمن، المملكة العربية السعودية.

Abstract

This study aimed to investigate the impact of integrating Artificial Intelligence (AI) technologies into Closed-Circuit Television (CCTV) systems on enhancing banking security efficiency in the Kingdom of Saudi Arabia (KSA), considering the digital transformation the Kingdom is undergoing as part of Vision 2030. To achieve this objective, the study adopted a descriptive analytical approach, utilizing a questionnaire to collect data from a purposive sample of (100) individuals working in security, monitoring, and technology departments in Saudi banks. The study concluded that there is a strong statistically significant positive impact of integrating AI technologies on banking security efficiency, with the AI adoption variable explaining (68.4%) of the total variance in the level of security efficiency. Results also showed statistically significant fundamental differences in the level of security and response speed between the pre-integration and post-integration phases, favoring smart systems. The "Abnormal Behavioral Analysis" technology was found to be the factor most strongly associated with increased speed of threat response, relatively outperforming static recognition technologies. Conversely, the study revealed that the main challenge to adopting these technologies is not purely technical, but rather the urgent need for training human cadres, followed by high investment costs and data privacy concerns. In light of these findings, the study recommended adopting "Hybrid Smart Security" strategies that integrate AI algorithms with qualified human intervention, prioritizing investment in "Behavioral Analysis" software due to its proactive capability, and emphasizing the necessity of specialized training programs for operators, ensuring the application of "Privacy by Design" standards to comply with regulatory controls.

Keywords: Artificial Intelligence (AI), Closed-Circuit Television (CCTV), Banking Security, Behavioral Analysis, Security Efficiency, Kingdom of Saudi Arabia (KSA).

فهرس المحتويات

الصفحة	الموضوع
ج	الإهداء
د	الشكر والتقدير
هـ	الملخص (باللغة العربية)
و	الملخص (باللغة الانجليزية)
ز	فهرس المحتويات
ي	فهرس الجداول
1	الفصل الأول: الإطار العام للدراسة
2	1.1 مقدمة
3	1.2 مشكلة الدراسة
4	1.3 أهداف الدراسة
4	1.4 أهمية الدراسة
5	1.4.1 الأهمية العلمية
5	1.4.2 الأهمية العملية
5	1.5 فرضيات الدراسة
6	1.6 النظريات العلمية المتبعة لإعداد الدراسة
9	الفصل الثاني: الإطار النظري والدراسات السابقة
10	تمهيد
10	2.1 مفاهيم أساسية في أنظمة المراقبة الأمنية البنكية
11	2.1.1 تطور أنظمة المراقبة التلفزيونية في القطاع المصرفي
13	2.1.2 المكونات التشغيلية لأنظمة المراقبة التقليدية
14	2.1.3 تحديات كفاءة الأنظمة التقليدية في البيئة البنكية
15	2.2 مفاهيم الذكاء الاصطناعي في تطبيقات المراقبة الأمنية البنكية
16	2.3 الإطار النظري لدمج الذكاء الاصطناعي في أنظمة المراقبة البنكية
18	2.4 دور الذكاء الاصطناعي في تعزيز كفاءة أنظمة المراقبة البنكية
18	2.4.1 تطبيقات الذكاء الاصطناعي في المراقبة البنكية

19	2.4.2 كفاءة الاكتشاف المبكر والاستجابة التلقائية
20	2.4.3 نماذج تعلم الآلة والتحليل التنبؤي في القطاع المصرفي
21	2.4.4 الاعتبارات الأخلاقية والخصوصية في استخدام الذكاء الاصطناعي في المراقبة البنكية
22	2.5 نموذج مقترح لدمج الذكاء الاصطناعي في التشغيل الأمني البنكي
22	2.5.1 مكونات النموذج المقترح
23	2.5.2 آلية عمل النموذج في البيئة البنكية
23	2.5.3 اعتبارات التوظيف العملي في البنوك السعودية
24	2.6 المبحث الثاني: الدراسات السابقة
24	2.6.1 الدراسات العربية
26	2.6.2 الدراسات الأجنبية
27	2.6.3 التعقيب على الدراسات السابقة
29	خلاصة الفصل
30	الفصل الثالث: منهجية الدراسة وإجراءاتها
31	3.1 منهج الدراسة
31	3.2 مجتمع الدراسة
31	3.3 عينة الدراسة
32	3.3 أداة الدراسة
32	3.4 إجراءات الدراسة
33	3.5 تحليل مؤشرات الصديق والثبات لأداة الدراسة (الاستبانة)
33	3.5.1 الصديق الظاهري وصديق المحتوى
33	3.5.2 الصديق البنائي والاتساق الداخلي
34	3.5.3 ثبات الأداة
35	3.5.4 ملخص مؤشرات الصديق والثبات للأداة
35	3.7 الأساليب الإحصائية
36	3.8 أخلاقيات الدراسة
36	الخلاصة
37	الفصل الرابع: تحليل ومناقشة نتائج الدراسة
38	تمهيد

38	4.1 تحليل الخصائص الديموغرافية لأفراد عينة الدراسة
40	4.2 التحليل الوصفي لمتغيرات الدراسة
40	4.2.1 تحليل التكرارات والنسب المئوية لفقرات الاستبانة
44	4.2.2 المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة على محاور الاستبيان
48	4.3 اختبار فرضيات الدراسة
48	4.3.1 اختبار الفرضية الرئيسة: أثر الذكاء الاصطناعي على كفاءة الأمن
49	4.3.2 اختبار الفرضية الفرعية الرابعة: المقارنة القبلية والبعدية
50	4.3.3 اختبار الفرضيات الفرعية الأخرى (العلاقة الارتباطية)
51	4.4 ملخص نتائج اختبار الفرضيات
52	4.5 مناقشة النتائج في ضوء الدراسات السابقة
52	4.5.1 الأثر التحولي للذكاء الاصطناعي (من التفاعلية إلى الاستباقية)
52	4.5.2 فاعلية المكونات التخصصية (تحليل السلوكيات كعنصر حاسم)
53	4.5.3 التحديات المتمحورة حول العنصر البشري
53	الخلاصة
54	الفصل الخامس: النتائج والتوصيات
55	تمهيد
55	5.1 ملخص نتائج الدراسة
56	5.2 الاستنتاجات
57	5.4 التوصيات
57	5.4 مقترحات لدراسات مستقبلية
58	الخاتمة
59	المراجع والمصادر
60	الملاحق

فهرس الجداول

الجدول	عنوان الجدول	الصفحة
(1-3)	توزيع فقرات الاستبانة حسب المحاور لقياس الصدق الظاهري والمحتوى	33
(2-3)	معاملات ارتباط بيرسون بين فقرات المحاور والدرجة الكلية لكل محور	34
(3-3)	معاملات ثبات كرونباخ ألفا للمحاور والاستبانة ككل	34
(3-4)	ملخص مؤشرات الصدق والثبات للأداة	35
(1-4)	التوزيع التكراري والنسب المئوية لخصائص أفراد عينة الدراسة (ن = 100)	39
(2-4)	التوزيع التكراري والنسب المئوية لاستجابات أفراد العينة على فقرات الاستبانة (ن=100)	40
(3-4)	المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة على محاور الاستبانة	44
(4-4)	نتائج تحليل الانحدار الخطي البسيط لاختبار الفرضية الرئيسة	49
(5-4)	نتائج اختبار (T) للفروق في تقييم الكفاءة الأمنية قبل وبعد دمج الذكاء الاصطناعي	49
(6-4)	نتائج تحليل الارتباط (بيرسون) لاختبار الفرضيات الفرعية	50
(7-4)	ملخص نتائج اختبار فرضيات الدراسة	51

الفصل الأول

الإطار العام للدراسة

1.1 مقدمة

شهد العالم خلال العقد الأخير تطوراً كبيراً في تقنيات الذكاء الاصطناعي (Artificial Intelligence)، ما أدى إلى تأثيرات ملموسة في مختلف القطاعات الحيوية، حيث أصبح الذكاء الاصطناعي عنصراً محورياً في دعم الأنظمة التشغيلية واتخاذ القرارات في البيئات المعقدة. ولم يعد الذكاء الاصطناعي مفهوماً نظرياً أو تكنولوجياً مستقبلية، بل تحول إلى أداة عملية تقدم حلولاً مبتكرة لمجموعة من التحديات المتزايدة، خاصة في المجالات الأمنية التي تواجه تهديدات متصاعدة على مستوى الأفراد والمؤسسات (IBM, 2025).

يُعد القطاع المصرفي من أكثر القطاعات تأثراً بهذه التحديات، نظراً لما يتعامل معه من بيانات مالية حساسة وأصول اقتصادية عالية القيمة. وترافق التوسع في الخدمات المصرفية الرقمية وزيادة حجم المعاملات الإلكترونية مع ارتفاع ملحوظ في مستوى التهديدات الأمنية، بما في ذلك الاحتيال المالي والهجمات السيبرانية. هذا الوضع يفرض ضغوطاً متزايدة على الأنظمة الأمنية التقليدية، التي لم تعد كافية لمواجهة حجم وتعقيد هذه التهديدات (Iskandarani, 2024).

تُعد أنظمة المراقبة التلفزيونية (CCTV) إحدى الوسائل التقليدية المعتمدة في تعزيز الأمن المصرفي، إلا أن اعتمادها على المتابعة البشرية والمراقبة السلبية يحد من قدرتها على الكشف المبكر عن الأنشطة المشبوهة أو الاستجابة الفورية للحوادث. كما أن التزايد المستمر في حجم البيانات المرئية الناتجة عن كاميرات المراقبة يجعل من الصعب على المشغلين البشريين تحليلها بفعالية في الوقت الحقيقي (Adepoju, Omole, & Chianumba, 2024).

في هذا السياق، يُمثل دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة خطوة استراتيجية نحو تطوير حلول أمنية ذكية. تتيح هذه التقنيات قدرات تحليل متقدمة، تشمل التعرف على الوجوه، ورصد السلوكيات غير الطبيعية، والتنبؤ بالأنشطة الإجرامية المحتملة. وتمتاز أنظمة المراقبة الذكية المدعومة بالذكاء الاصطناعي بقدرتها على تحليل كميات كبيرة من بيانات الفيديو بكفاءة وسرعة تفوق الإمكانيات البشرية، مما يساهم في تعزيز دقة وسرعة الاستجابة للتهديدات (Agbala, 2024). تنبع أهمية هذه الدراسة من السياق السعودي، حيث تشهد المملكة تحولات رقمية واقتصادية شاملة في إطار رؤية السعودية 2030، والتي تهدف إلى تطوير البنية التحتية الرقمية وتعزيز الابتكار في مختلف القطاعات، بما في ذلك القطاع المصرفي. ومع توسع هذا القطاع وازدياد تعقيد عملياته، تصبح الحاجة إلى تعزيز أنظمة الأمن أكثر إلحاحاً. وعلى الرغم من

الاعتراف المتزايد بأهمية الذكاء الاصطناعي في المجال المصرفي، إلا أن الدراسات التي تناولت تأثير دمج هذه التقنيات في أنظمة المراقبة البنكية بالمملكة لا تزال محدودة (العتيبي، 2024).

بناءً على ما سبق، تهدف هذه الدراسة إلى سد هذه الفجوة المعرفية من خلال تقديم تحليل ميداني شامل حول أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة المصرفية على كفاءة الأمن البنكي في السعودية. وتسعى الدراسة إلى المساهمة في إثراء الأدبيات العلمية المتعلقة بالأمن المالي الذكي، إلى جانب تقديم توصيات عملية للمؤسسات المصرفية وصناع القرار لدعم جهودهم في بناء بيئة مصرفية أكثر أماناً واستدامة في ظل التحديات الرقمية المتزايدة.

1.2 مشكلة الدراسة:

تتمثل الإشكالية البحثية الأساسية في محدودية قدرة أنظمة المراقبة التلفزيونية التقليدية على مواكبة التحديات الأمنية المتزايدة في القطاع المصرفي السعودي. حيث تكشف الدراسات الحديثة عن وجود فجوة أمنية واضحة في مواجهة التهديدات المعاصرة، خاصة مع التوسع الكبير في الخدمات المصرفية الرقمية وتزايد تعقيد الجرائم المالية (العتيبي، 2024). وتنبع هذه المحدودية من عدة عوامل رئيسية، أهمها الاعتماد المفرط على المراقبة البشرية التي تعجز عن متابعة تدفقات الفيديو المتعددة بشكل متزامن، أو تحليل الأنماط السلوكية المعقدة، أو الكشف الفوري عن الأنشطة المشبوهة (Adepoju et al., 2024). في هذا السياق، تبرز الحاجة الملحة لبحث إمكانية دمج تقنيات الذكاء الاصطناعي لتعزيز كفاءة هذه الأنظمة، مما يطرح التساؤل الرئيسي التالي: ما أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على رفع كفاءة الأمن البنكي في المملكة العربية السعودية؟

وتتفرع عن هذه الإشكالية الرئيسية عدة تساؤلات فرعية تتناول جوانب مختلفة للمشكلة:

- (1) ما مدى فعالية تقنيات الذكاء الاصطناعي (مثل التعرف على الوجوه، تحليل السلوكيات، والتنبيه بالتهديدات) في تحسين دقة وكفاءة أنظمة المراقبة الأمنية في البنوك السعودية؟
- (2) ما أهم التحديات التقنية والتنظيمية التي تواجه تطبيق تقنيات الذكاء الاصطناعي في أنظمة المراقبة الأمنية بالقطاع المصرفي السعودي؟
- (3) كيف يمكن قياس العائد الأمني والاستثماري لدمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة البنكية؟

4) ما الفروق الجوهرية في الأداء الأمني لأنظمة المراقبة قبل وبعد تطبيق تقنيات الذكاء الاصطناعي في البيئة البنكية السعودية؟

5) ما متطلبات نجاح تطبيق هذه التقنيات في تعزيز الأمن البنكي في ضوء رؤية المملكة العربية السعودية 2030؟

1.3 أهداف الدراسة:

تهدف هذه الدراسة إلى الإجابة على التساؤل الرئيسي المتمثل في تحليل الأثر الناتج عن تطبيق تقنيات الذكاء الاصطناعي في تعزيز كفاءة الأمن البنكي بالمملكة العربية السعودية، وذلك في إطار تحقيق مستهدفات رؤية المملكة 2030 في مجال التحول الرقمي الآمن. ولتحقيق هذا الهدف الرئيسي، تسعى الدراسة إلى تحقيق الأهداف الفرعية التالية:

1) رصد وتصنيف أبرز تقنيات الذكاء الاصطناعي المستخدمة في تعزيز أنظمة المراقبة الأمنية بالقطاع المصرفي السعودي، مع التركيز على تطبيقات التعرف على الوجوه، تحليل السلوكيات، والتنبؤ بالتهديدات الأمنية.

2) تقييم الأثر التشغيلي لهذه التقنيات على تحسين كفاءة أنظمة المراقبة التلفزيونية، من خلال تحليل مؤشرات الأداء الرئيسية المتعلقة بدقة الكشف، سرعة الاستجابة، وتقليل معدلات الأخطاء البشرية (SAMA, 2023).

3) تحليل العلاقة الارتباطية بين مستوى تبني تقنيات الذكاء الاصطناعي ومستويات الأمن والسلامة في المنشآت المصرفية، مع تحديد العوامل الوسيطة المؤثرة في هذه العلاقة.

4) تحديد التحديات التنظيمية والتقنية التي تواجه عملية دمج هذه التقنيات في البيئة البنكية السعودية، وتقديم حلول عملية قابلة للتطبيق.

5) وضع إطار استراتيجي لقياس العائد الأمني والاستثماري لتطبيق هذه التقنيات، بما يتوافق مع متطلبات التحول الرقمي في القطاع المصرفي السعودي.

1.4 أهمية الدراسة:

تتجلى أهمية هذه الدراسة في كونها تستجيب لحاجة ملحة وواقعية تتعلق بتطوير مستوى الأمن البنكي في المملكة العربية السعودية، في ظل التحديات المتزايدة التي يفرضها التحول الرقمي وانتشار الخدمات المصرفية الإلكترونية. فمع تزايد حجم

المعاملات المالية الرقمية وتعقيد الأنشطة البنكية، بات من الضروري البحث عن حلول تقنية متقدمة تعزز فعالية أنظمة الحماية، وتقلل من الاعتماد على الأساليب التقليدية في المراقبة الأمنية.

1.4.1 الأهمية العلمية:

وتكمن الأهمية العلمية للدراسة في مساهمتها في سد فجوة معرفية قائمة في الأدبيات العربية والسعودية تحديداً، حيث تندر الدراسات التي تتناول العلاقة بين تقنيات الذكاء الاصطناعي وكفاءة أنظمة المراقبة الأمنية في القطاع المصرفي من منظور ميداني تطبيقي. كما تضيف الدراسة بعداً بحثياً جديداً من خلال تقديم إطار منهجي لتحليل الأثر الفعلي لهذه التقنيات، كالتعرف على الوجوه، وتحليل السلوكيات، والتنبيه بالتهديدات، على جودة وكفاءة الأداء الأمني في البنوك.

1.4.2 الأهمية العملية:

أما من الناحية التطبيقية، فتوفر هذه الدراسة معطيات وتوصيات قابلة للتنفيذ من شأنها أن تدعم صُناع القرار في المؤسسات المصرفية السعودية في تبني حلول ذكاء اصطناعي فعالة، وتوجيه الاستثمارات التقنية نحو تحقيق أعلى عائد أمني وتشغيلي. كما أنها تُسهم في دعم توجهات رؤية السعودية 2030، خاصة فيما يتعلق بتطوير البنية التحتية الرقمية وتعزيز الابتكار في القطاعات الحيوية، بما فيها القطاع المالي. وعليه، تُعد هذه الدراسة ذات قيمة استراتيجية وعملية في ضوء التحديات الرقمية الراهنة والمتغيرات الأمنية المتسارعة.

1.5 فرضيات الدراسة:

بناءً على مشكلة الدراسة وتساؤلاتها البحثية، ووفقاً للإطار النظري والتحليل المبدئي، تفترض هذه الدراسة وجود علاقة ذات دلالة إحصائية بين دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية وكفاءة الأمن البنكي في المملكة العربية السعودية. ويمكن صياغة الفرضية الرئيسية والفرعية على النحو التالي:

الفرضية الرئيسة (H_1): لا يوجد أثر ذو دلالة إحصائية لدمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على كفاءة الأمن البنكي في المملكة العربية السعودية.

ويتفرع عن هذه الفرضية الرئيسة عدد من الفرضيات الفرعية، كما يلي:

H1-1: توجد علاقة ذات دلالة إحصائية بين استخدام تقنيات التعرف على الوجوه وتحسين دقة أنظمة المراقبة الأمنية في البنوك السعودية.

H1-2: توجد علاقة ذات دلالة إحصائية بين تحليل السلوكيات بواسطة الذكاء الاصطناعي وزيادة سرعة الاستجابة للتهديدات الأمنية.

H1-3: توجد علاقة ذات دلالة إحصائية بين التنبؤ بالأنشطة المشبوهة باستخدام تقنيات الذكاء الاصطناعي وتقليل معدلات الجرائم المالية.

H1-4: توجد فروق ذات دلالة إحصائية في كفاءة الأنظمة الأمنية قبل وبعد دمج تقنيات الذكاء الاصطناعي في البيئة المصرفية.

H1-5: توجد علاقة ذات دلالة إحصائية بين مستوى تبني الذكاء الاصطناعي والعائد الاستثماري والأمني لدى المؤسسات المصرفية في السعودية.

1.6 النظريات العلمية المتبعة لإعداد الدراسة:

استندت هذه الدراسة إلى مجموعة من النظريات العلمية التي شكّلت الإطار المفاهيمي والمنهجي لتحليل العلاقة بين دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية وكفاءة الأمن البنكي في المملكة العربية السعودية. وتساعد هذه النظريات على تفسير التأثيرات المتوقعة للتكنولوجيا على الأداء الأمني، وتوضيح سلوك الأفراد والمؤسسات تجاه تبني التقنيات الحديثة، وتقديم مداخل تحليلية متكاملة لفهم الظاهرة المدروسة من أبعادها التقنية والسلوكية والتنظيمية. وفيما يلي عرض لأبرز النظريات التي تم توظيفها في إعداد الدراسة:

أولاً: نظرية الأنظمة (Systems Theory):

ترتكز هذه النظرية، التي طوّرها (Bertalanffy 1968)، على اعتبار المؤسسة كنظام متكامل يتكوّن من مكونات فرعية مترابطة تتفاعل فيما بينها لتحقيق الأهداف العامة. وفي سياق الدراسة، يُمثّل النظام الأمني في البنك منظومة مترابطة تشمل

الأفراد، الأجهزة، الإجراءات، والتقنيات. ومن ثم، فإن دمج تقنيات الذكاء الاصطناعي في نظام المراقبة يُعدّ مدخلاً لتحسين كفاءة النظام الأمني ككل، من خلال رفع مستوى التكامل بين المكونات التقنية والبشرية.

ثانياً: نموذج قبول التكنولوجيا (Technology Acceptance Model – TAM):

طوّره Davis (1989) لتفسير العوامل المؤثرة في قبول الأفراد للتقنيات الجديدة، ويستند إلى متغيرين رئيسيين: المنفعة المتوقعة وسهولة الاستخدام المتوقعة. ويُسهّم هذا النموذج في تحليل مدى تقبّل العاملين في المؤسسات المصرفية السعودية لتقنيات الذكاء الاصطناعي في المراقبة، وتأثير هذا القبول على فعالية التطبيق العملي لتلك التقنيات في البيئة الأمنية البنكية.

ثالثاً: نظرية الحتمية التكنولوجية (Technological Determinism Theory):

تُشير هذه النظرية إلى أن التكنولوجيا تُعدّ قوة دافعة تؤثر على شكل التنظيمات والمجتمعات، وتُعيد تشكيل طرق العمل وأساليب اتخاذ القرار. وفي إطار الدراسة، تُستخدم هذه النظرية لتوضيح كيف يُمكن للذكاء الاصطناعي أن يُحدث تحوّلاً جوهرياً في مفاهيم العمل الأمني، من الرصد التقليدي إلى المراقبة الاستباقية الذكية.

رابعاً: نظرية إدارة المخاطر الأمنية (Security Risk Management Theory):

تعتمد على مبادئ ISO 31000:2018، وتُركّز على منهجية تقييم المخاطر الأمنية وتحديد آليات التحكم فيها. وتُعد هذه النظرية إطاراً تحليلياً لفهم كيف يمكن لتقنيات الذكاء الاصطناعي أن تُسهّم في خفض مستويات المخاطر الأمنية داخل المؤسسات المصرفية من خلال الكشف المبكر، والتحليل الفوري، والاستجابة التلقائية للتهديدات.

خامساً: نظرية الأداء المؤسسي (Organizational Performance Theory):

تهدف هذه النظرية إلى قياس العلاقة بين مدخلات المؤسسة ونتائجها، وتعتمد على مؤشرات أداء كمية ونوعية لتقييم الكفاءة التشغيلية. وتُوظّف في هذه الدراسة لقياس تأثير دمج الذكاء الاصطناعي على كفاءة أنظمة الأمن البنكي، من حيث دقة الرصد، سرعة الاستجابة، وتقليل الهدر البشري في عمليات المراقبة.

سادساً: نظرية انتشار الابتكار (Innovation Diffusion Theory – IDT):

طرحها (2003) Rogers لشرح كيفية تبني وانتشار الابتكارات داخل المجتمعات والمؤسسات. وتُستخدم في الدراسة لتحليل تفاوت تبني تقنيات الذكاء الاصطناعي بين البنوك السعودية، والعوامل التي تؤثر في سرعة وكفاءة هذا التبني، مثل قابلية التجريب، والوضوح، والتوافق مع الأهداف المؤسسية.

سابعاً: نظرية الكفاءة التقنية الاقتصادية (Techno-Economic Efficiency Theory):

تُبنى هذه النظرية، كما ورد في أعمال (Farrell 1957) و (Coelli et al. 2005)، بتحديد العلاقة بين الاستخدام التقني ومدى تحقيق الكفاءة الاقتصادية. وفي ضوء الدراسة، تُستخدم هذه النظرية لقياس العائد الأمني والاستثماري الناتج عن تطبيق تقنيات الذكاء الاصطناعي، بما يعكس تحقيق قيمة مضافة للمؤسسات البنكية من حيث خفض الخسائر ورفع الكفاءة التشغيلية.

إن تكامل هذه النظريات يُوفّر أساساً علمياً راسخاً لفهم طبيعة العلاقة بين التكنولوجيا الأمنية الحديثة ومستوى كفاءة الأداء في المؤسسات المصرفية. كما يُعزز من دقة التحليل ويساعد على تفسير النتائج ضمن أطر علمية واضحة تدعم مصداقية التوصيات التي ستتوصل إليها الدراسة.

الفصل الثاني

الإطار النظري والدراسات
السابقة

تمهيد

في ظل التغيرات المتسارعة التي يشهدها القطاع المصرفي، تزايدت الحاجة إلى تبني تقنيات متقدمة في مجال الأمن، وعلى رأسها أنظمة المراقبة الذكية المدعومة بالذكاء الاصطناعي. وتُعد البنوك من أكثر المؤسسات تعرضاً للمخاطر الأمنية، نظراً لطبيعة نشاطها القائم على التعاملات المالية الحساسة، مما يستوجب امتلاك بنية أمنية قادرة على الرصد المبكر والتدخل الاستباقي. وعليه، يهدف هذا الفصل إلى تقديم خلفية نظرية متكاملة حول المفاهيم الأساسية المرتبطة بأنظمة المراقبة الأمنية التقليدية والمعاصرة في البيئة البنكية، مع استعراض لأهم التحولات التقنية التي شهدها هذا المجال، وبحث دور الذكاء الاصطناعي في تعزيز كفاءة هذه الأنظمة، بالإضافة إلى استعراض الأطر النظرية والنماذج التطبيقية ذات الصلة. كما يتطرق الفصل إلى التحديات المرتبطة باستخدام الذكاء الاصطناعي، لا سيما من حيث الأخلاقيات والخصوصية والامتثال التنظيمي، مما يُسهم في بناء قاعدة معرفية تمهّد للتحليل الميداني في الفصول اللاحقة.

2.1 مفاهيم أساسية في أنظمة المراقبة الأمنية البنكية

تُعد أنظمة المراقبة الأمنية من الدعائم الأساسية لحماية المنشآت البنكية، حيث تهدف إلى توفير بيئة آمنة من خلال المراقبة المستمرة وتسجيل الأحداث الأمنية بشكل دقيق، مما يُساعد في الوقاية من المخاطر الأمنية مثل السطو، الاحتيال، والتلاعب المالي (Chen, Zhang, & Lin, 2021). وتشمل هذه الأنظمة استخدام كاميرات المراقبة التلفزيونية (CCTV)، وأجهزة استشعار الحركة، وأنظمة التنبيه، بالإضافة إلى البرمجيات المتقدمة التي تدعم تحليل البيانات في الوقت الحقيقي. في ظل التحديات الأمنية المتزايدة التي تواجه القطاع المصرفي، مثل الجرائم المالية والاختراقات السيبرانية، أصبحت الحاجة ملحة لتطوير أنظمة مراقبة ذكية تعتمد على الذكاء الاصطناعي والتعلم الآلي لزيادة دقة وكفاءة المراقبة وتحليل السلوك (Wang et al., 2023). يعتمد هذا التوجه على دمج تقنيات التعرف على الوجه، وتحليل الفيديو، والكشف المبكر عن السلوكيات غير الطبيعية داخل الفروع البنكية.

تشمل المفاهيم الأساسية في هذه الأنظمة الانتقال من المراقبة السلبية التي تعتمد على التسجيل فقط، إلى المراقبة النشطة التي توفر إنذارات فورية وتحليلات ذكية تسمح بالتدخل السريع والفعال (Khan et al., 2022). ويُعتبر هذا التطور ضرورياً لمواكبة متطلبات الحوكمة الأمنية والرقمية في القطاع المصرفي.

2.1.1 تطور أنظمة المراقبة التلفزيونية في القطاع المصرفي:

المرحلة الأولى – النشأة (الأنظمة التماثلية):

■ في بدايات استخدامها خلال خمسينيات القرن العشرين، كانت أنظمة المراقبة تتكون من كاميرات تماثلية (Analog Cameras) تنقل إشارات الفيديو مباشرة إلى شاشات العرض دون وجود أنظمة لتسجيل المحتوى. وقد اقتصر مهام هذه الأنظمة على المراقبة اللحظية فقط، حيث كان العامل الأمني يراقب الشاشات بشكل مباشر دون إمكانية للرجوع إلى الأحداث السابقة.

■ غياب أنظمة التسجيل والتحليل جعل هذه الأنظمة ذات فاعلية محدودة في التعامل مع التحقيقات أو مراجعة الوقائع بعد حدوثها (Zhou & Chen, 2021).

المرحلة الثانية – التحول الرقمي (1990s-2000s):

■ بدأت البنوك في اعتماد أنظمة تسجيل رقمية (DVR)، مما أتاح تخزين مقاطع الفيديو لمدة زمنية أطول وإمكانية الرجوع إلى الأحداث المؤرخة.

■ ظهرت الكاميرات الرقمية، خاصة تلك التي تعمل بروتوكول الإنترنت (IP Cameras)، والتي وفرت إمكانيات أكبر في نقل البيانات وتكامل المراقبة مع الشبكات الحاسوبية.

■ أصبح بالإمكان الربط بين الفروع المختلفة ومراكز المراقبة المركزية، مما أدى إلى تحسين مستويات الرقابة والتحكم عن بعد.

■ إتاحة أدوات مثل التحكم في زوايا الكاميرا عن بعد، وضبط الجودة تلقائياً، واسترجاع اللقطات استناداً إلى الوقت أو الموقع.

المرحلة الثالثة – تكامل التكنولوجيا مع الأمن المالي:

■ مع ازدياد الهجمات على البنوك، مثل محاولات السطو على الفروع والتلاعب بأجهزة الصراف الآلي لجأت المصارف إلى استخدام أنظمة مراقبة أكثر تطوراً.

■ بدأ إدخال التحليلات الذكية بالفيديو (Video Analytics) القادرة على: الكشف عن التحركات غير الاعتيادية، تتبع الأفراد، إرسال تنبيهات تلقائية عند الاشتباه بسلوكيات معينة.

أدى ذلك إلى تحسّن في قدرات التدخل المبكر ومنع الحوادث قبل وقوعها (Singh et al., 2023).

المرحلة الرابعة – الذكاء الاصطناعي والتحليل الاستباقي:

شهدت هذه المرحلة دمج تقنيات الذكاء الاصطناعي والتعلم الآلي في أنظمة المراقبة، لتصبح هذه الأنظمة قادرة على التنبؤ بالسلوكيات والتمييز بين الأنشطة الطبيعية والمشبوهة.

أبرز الوظائف الذكية:

- التعرف الآلي على الوجوه ومقارنتها بقاعدة بيانات.
- تحليل نمط حركة الزوار داخل الفرع المصرفي.
- إصدار تنبيهات عند تجاوز شخص لنطاق معين أو التجمهر في نقطة معينة.
- التحول: من "رصد سلبي" إلى "تحليل استباقي"، مما يرفع كفاءة الأداء الأمني ويقلل من الاعتماد على المتابعة البشرية

فقط (Hossain et al., 2022).

التحول في المملكة العربية السعودية – في ظل رؤية 2030:

في إطار التوجه نحو التحول الرقمي والأمن المؤسسي المتكامل، تبنت البنوك السعودية أنظمة مراقبة ذكية تعتمد على الذكاء الاصطناعي كجزء من الحوكمة الإلكترونية.

من أهم ملامح التحول:

- تحديث البنية التحتية لكاميرات المراقبة لتكون متصلة شبكياً وقابلة للتحليل اللحظي.
 - ربط أنظمة المراقبة بالأنظمة الأمنية الداخلية (كأنظمة الدخول البيومتري والتنبيه التلقائي).
 - استخدام تقنيات مثل التعرف على الوجه للتحقق من هوية العملاء وموظفي البنوك.
- هذا التطور يتماشى مع أهداف رؤية 2030 لتعزيز الشفافية، ومكافحة الجرائم المالية، ورفع كفاءة الأنظمة الأمنية

(Almulhim & Alotaibi, 2022).

2.1.2 المكونات التشغيلية لأنظمة المراقبة التقليدية:

أولاً: الكاميرات التماثلية (Analog Cameras):

- تُعد المكون الأساسي في الأنظمة التقليدية، حيث تقوم بالتقاط الصور وإرسالها عبر كابلات متصلة مباشرة بجهاز العرض أو جهاز التسجيل.
- تتميز ببساطة التصميم وانخفاض التكلفة، لكنها محدودة من حيث جودة الصورة والدقة ومجال الرؤية.
- لا تحتوي على تقنيات ذكية كالكشف عن الحركة أو التمييز بين الأشخاص والعناصر، ما يجعلها أقل فعالية في البيئات المصرفية المعقدة (Zhou & Chen, 2021).

ثانياً: أجهزة تسجيل الفيديو الرقمية (DVRs):

- تقوم هذه الأجهزة باستقبال الفيديو من الكاميرات وتخزينه محلياً على أقراص صلبة.
- تُعد عنصراً حاسماً في توثيق الأحداث، ولكنها تتطلب مراقبة يدوية للوصول إلى تسجيل معين.
- تُخزن البيانات غالباً لفترات محدودة بسبب سعة التخزين المحدودة، ما يحد من قدرة الرجوع الزمني الطويل (Singh et al., 2023).

ثالثاً: شاشات المراقبة (Monitoring Displays):

- تُستخدم لعرض بث مباشر من الكاميرات في غرفة التحكم، وغالباً ما تتطلب وجود مراقب بشري دائم.
- بالرغم من أهميتها، تعتمد فعالية الشاشة على كفاءة المراقب وقدرته على الانتباه الدائم.
- عدم وجود مؤشرات تحليلية أو تنبيهات آلية يجعل عملية الاكتشاف تعتمد بالكامل على العنصر البشري.

رابعاً: البنية التحتية الكبلية (Cabling Infrastructure):

- تعتمد الأنظمة التقليدية على كابلات متصلة مباشرة (مثل Coaxial Cable) بين الكاميرات وأجهزة التسجيل.
- تُعد هذه البنية حساسة للأعطال والصيانة، كما أن تركيبها يُعد مكلفاً ويُعيق التوسع المرن أو التعديلات السريعة.
- لا تتيح قابلية الربط الشبكي أو الإدارة عن بعد، ما يحد من مرونة النظام الأمني.

خامساً: غياب الذكاء الاصطناعي والتحليل التنبؤي:

- لا تتضمن الأنظمة التقليدية أدوات تحليل فيديو أو تقنيات التعرف على الأنماط.
- تُركز على تسجيل ما يحدث فقط دون تحليل السلوكيات أو إصدار تنبيهات مبكرة.
- هذه المحدودية تُضعف من فعالية النظام في مواجهة التهديدات المتقدمة، كعمليات الاحتيال المنظمة أو السلوكيات المشبوهة داخل الفروع البنكية.

سادساً: ضعف الربط مع أنظمة الأمن الأخرى:

- لا تتكامل الأنظمة التقليدية بسهولة مع أنظمة الإنذار، التحكم بالدخول، أو قواعد بيانات الهوية.
- هذا الانفصال يخلق فجوة أمنية ويمنع تحقيق رؤية أمنية شاملة ومتراصة.
- في بيئة مصرفية حديثة، يُعد التكامل ضرورة لتعزيز الاستجابة السريعة واتخاذ القرار الفوري (Hossain et al., 2022).

2.1.3 تحديات كفاءة الأنظمة التقليدية في البيئة البنكية:

تواجه أنظمة المراقبة التقليدية في القطاع المصرفي العديد من التحديات التي تؤثر على فعاليتها:

- الاعتماد الكبير على العنصر البشري: يُعد الاعتماد على المراقبة اليدوية نقطة ضعف جوهريّة، حيث يُظهر المشغلون البشريون قابلية للتشتت والإرهاق، مما يقلل الدقة في كشف التهديدات بنسبة تصل إلى 68% في البيئات المصرفية (Chatterjee et al., 2022). وقد أكدت دراسات حديثة أن الخطأ البشري يظل العامل المساهم الرئيسي في 74% من حالات الفشل الأمني (Almeida et al., 2023).
- محدودية التحليل الزمني واللحظي: تعاني الأنظمة التقليدية من تأخر زمني متوسط (>4 دقائق) في 82% من الحالات، مما يعيق الكشف الفوري للتهديدات (Zhou & Chen, 2021). هذا التأخر يحول دون التدخل الوقائي، خاصة في هجمات السطو السريع التي تتطلب استجابة خلال >60 ثانية (Singh et al., 2023).
- صعوبة التكامل مع الأنظمة الأمنية: يؤدي غياب التكامل بين أنظمة CCTV والأنظمة الأمنية الأخرى (مثل التحكم في الدخول) إلى انخفاض كفاءة الاستجابة بنسبة 40% (Hossain et al., 2022). وقد لاحظ الباحثون أن 67% من الثغرات الأمنية في البنوك ناتجة عن انفصال الأنظمة (NIST, 2023).

- قصور في الاستجابة الذكية: تفشل الأنظمة التقليدية في التعامل مع 73% من هجمات الهندسة الاجتماعية بسبب عدم قدرتها على تحليل السياق السلوكي (Singh et al., 2023). كما تفتقر إلى آليات الاستجابة التلقائية مثل إغلاق الأبواب أو عزل المناطق المهددة (NIST, 2023).
- تحديات تخزين البيانات: تواجه 65% من البنوك السعودية صعوبات في استرجاع التسجيلات الأقدم من 30 يوماً بسبب سياسات الحذف التلقائي (Al-Ghamdi & Al-Harbi, 2022). وهذا يتعارض مع متطلبات الهيئات التنظيمية التي توجب الاحتفاظ بالتسجيلات 90 يوماً على الأقل (SAMA, 2023).
- عدم قدرة تحليل السلوك: تتجاهل الأنظمة التقليدية 62% من السلوكيات المشبوهة المعقدة (Wang et al., 2023)، خاصة تلك التي تتضمن أنماطاً غير نمطية كالتجوال المتكرر في مناطق حساسة أو التفاعل غير المعتاد مع أجهزة الصراف الآلي (Chatterjee et al., 2022).

2.2 مفاهيم الذكاء الاصطناعي في تطبيقات المراقبة الأمنية البنكية

- التحول من المراقبة التقليدية إلى الذكاء الاصطناعي:
 - تعتمد أنظمة المراقبة الذكية على تقنيات الذكاء الاصطناعي مثل شبكات الأعصاب الاصطناعية العميقة (Deep Neural Networks) ونماذج الكشف المباشر (Object Detection Models) مثل YOLO و SSD، مما يتيح الكشف اللحظي عن الأسلحة أو السلوكيات المشبوهة داخل الفروع البنكية (Zahrawi & Shaalan, 2023).
 - تحل هذه الأنظمة مشكلة الإرهاق البشري والمراقبة المستمرة غير الفعالة، بتوفير تنبيهات فورية مبكرة لمعالجة التهديد قبل وقوع الحادث.
- قدرات الكشف والتنبؤ المتقدمة:
 - تستخدم تقنيات التعلم الآلي (مثل SVM، LOF، RNN) في تصنيف وتحليل الأنماط السلوكية، مما يُمكن من تمييز السلوك غير المعتاد، مثل التجمهر المفاجئ أو التحركات العدوانية داخل تلك الفروع (Kovacevic et al., 2024).
 - تدعم أنظمة المراقبة التنبؤية الذكاء الاصطناعي قدرة النظام على التنبؤ بالحوادث محتملة قبل وقوعها استناداً إلى أنماط سابقة وتحليل استمراري للبيانات المرئية.

■ الحفاظ على الخصوصية والشفافية من خلال XAI وFederated Learning:

- تُقدّم تقنيات Explainable AI (XAI) تفسيرًا لمخرجات الذكاء الاصطناعي، مما يدعم التفسير المؤسسي ويُعزز الثقة في أنظمة الأمان البنكي.
- تتيح تقنيات التعلم الفيدرالي (Federated Learning) تدريب نماذج مشتركة عبر بنوك متعددة دون مشاركة بيانات العملاء مباشرة، ما يحافظ على الخصوصية الأمنية (Awosika et al., 2023).

■ دعم متكامل لإدارة المخاطر البنكية:

- تُستخدم نماذج التعلم الآلي أيضًا في مجالات مثل إدارة السيولة، تقييم المخاطر الائتمانية، والاكتشاف المبكر للأزمات المرتبطة بالجريمة أو الاحتيال (Gerard et al., 2025).
- يُظهر هذا الاستخدام كيف يمكن للذكاء الاصطناعي تقديم مساهمات شاملة تتعدى المراقبة، لتشمل تحسين الاستراتيجيات التشغيلية والأمنية للبنوك.

■ الامتثال التنظيمي والتحذير من المخاطر الناجمة عن AI:

- منظمات الإشراف المالي (مثل لجنة بازل) تحت البنوك على وضع ضوابط وسياسات لإدارة المخاطر الناجمة عن استخدام الذكاء الاصطناعي، بما في ذلك ضبط الإنذارات الخاطئة والانحياز في النماذج (Reuters, 2024).
- يُعد ضمان الشفافية والمساءلة أحد المفاتيح لانتشار أنظمة الذكاء الاصطناعي بفعالية داخل القطاع المالي.
- إن دمج الذكاء الاصطناعي في أنظمة المراقبة البنكية يمثل نقلة نوعية نحو بيئة أمنية أكثر فاعلية واستباقية. من خلال قدرات الكشف الذكي، توفير تنبيهات لحظية، وتحقيق التكامل مع استراتيجيات إدارة المخاطر، تُمكن هذه الأنظمة من رفع جودة الأداء الأمني وتقليل الاعتماد على المتابعة البشرية.

2.3 الإطار النظري لدمج الذكاء الاصطناعي في أنظمة المراقبة البنكية

■ نظرية التفاعل بين الإنسان والآلة في مراقبة أمنية:

- تقوم هذه النظرية على أن تكامل الذكاء الاصطناعي مع العنصر البشري يُعزز درجة اليقظة والدقة خلال عمليات المراقبة، مما يقلص الخطأ الناتج عن الإرهاق البشري.

○ تظهر الأبحاث أن أنظمة التعرف الآلي (مثل SSD، YOLO) تقود إلى تحسينات ملموسة في سرعة وكفاءة الاستجابة مقارنة بالمراقبة البشرية فقط (Zahrawi & Shaalan, 2023).

■ نظرية الكشف المبكر والتحليل الاستباقي:

○ تعمل تقنيات التعلم العميق على تحليل سلوك الأشخاص داخل الفيديو باستخدام شبكة CNN، مما يدعم اكتشاف السلوكيات المشبوهة مثل حمل الأسلحة أو الاقتحام قبل وقوع الحدث (Zahrawi & Shaalan, 2023).

○ تركز هذه النظرية على استخدام خوارزميات رؤية الحاسوب لتعزيز فاعلية التدخل المبكر والحد من الأضرار.

■ نظرية التعلم الفيدرالي والخصوصية التعاونية:

○ يسمح التعلم الفيدرالي بتدريب نماذج مُحسَّنة على بيانات موزعة عبر بنوك مختلفة دون مشاركة البيانات الفعلية، مما يحافظ على الخصوصية ويعزز التعاون الجماعي (Francki, 2025; Lucinity, 2024).

○ تؤكد هذه النظرية على أهمية تعزيز الأمان التنظيمي دون التضحية بسرية معلومات العملاء.

■ نظرية الحماية الأمنية ضد هجمات تعلم الآلة:

○ تشمل هذه النظرية تناول التهديدات الممكنة على نماذج التعلم الفيدرالي، مثل استخراج البيانات الحساسة عبر تحديثات النماذج (Model Updates)، واقتراح أساليب حماية مثل التشفير التبادلي (NIST, Input Privacy) (2023).

○ تحقق هذه الحماية التوازن بين الاستفادة من نماذج فعّالة والحفاظ على سلامة بيانات البنوك والعملاء.

■ نظرية تعزيز الأداء الأمني عبر الذكاء الاصطناعي:

تستند هذه النظرية إلى نتائج دراسات متعددة تُظهر أن أنظمة المراقبة المدعومة بالذكاء الاصطناعي تحسّن مؤشرات الأداء الأمني مثل:

1. دقة اكتشاف التهديد (مثلاً كشف الأسلحة).

2. سرعة الاستجابة.

3. تقليل الإنذارات الخاطئة (Zahrawi & Shaalan, 2023).

وتبرز فائدتها في البيئة البنكية حيث الأمان وقت النمو والخصوصية.

يجمع هذا الإطار بين مناهج النظرية البشرية-الآلية، والرؤية الاستباقية، والخصوصية التعاونية، مع آليات الحماية المتقدمة. يشكل هذا الإطار قاعدة صلبة لفهم كيف يُمكن دمج الذكاء الاصطناعي في أنظمة المراقبة البنكية بفاعلية مع الحفاظ على الأمان التنظيمي والخصوصية.

2.4 دور الذكاء الاصطناعي في تعزيز كفاءة أنظمة المراقبة البنكية

2.4.1 تطبيقات الذكاء الاصطناعي في المراقبة البنكية:

- تحليل الفيديو في الزمن الحقيقي (Real-Time Video Analytics): تعتمد أنظمة الذكاء الاصطناعي في مراقبة المؤسسات البنكية على تحليل مباشر لتدفقات الفيديو باستخدام تقنيات الرؤية الحاسوبية (Computer Vision)، بهدف الكشف المبكر عن السلوكيات غير الاعتيادية مثل الوقوف المطول عند أجهزة الصراف الآلي أو الدخول غير المصرح به لمناطق حساسة. يساهم هذا النوع من التحليل في تقليل الاعتماد على المراقبة البشرية، وتسريع الاستجابة للحوادث الأمنية، مما يزيد من كفاءة الأنظمة الأمنية (Zahrawi & Shaalan, 2023).
- التعرف على الوجوه والتحقق من الهوية: تُوظف تقنيات التعرف على الوجه لتحديد الأشخاص غير المصرح لهم بدخول الفروع البنكية أو المشتبه في تورطهم في عمليات احتيالية. يتم مقارنة صور الأشخاص في الزمن الفعلي مع قواعد بيانات مركزية، ويتم إصدار إنذارات فورية عند اكتشاف تطابقات مرعبة أو غير متوقعة، مما يعزز أمان الفروع ويقلل من المخاطر (Kovacevic, Radenkovic, & Nikolic, 2024).
- تحليل سلوك العملاء داخل الفروع البنكية: تستخدم خوارزميات الذكاء الاصطناعي لمراقبة أنماط حركة العملاء داخل الفروع، مثل تتبع تحركاتهم، أنماط استخدام أجهزة الخدمة الذاتية، والتفاعل مع الموظفين. يُمكن من خلال هذه التحليلات اكتشاف السلوكيات الشاذة التي قد تشير إلى تهديد أمني أو محاولة احتيال، كما تساهم في تحسين تجربة العملاء من خلال التعرف على احتياجاتهم وسلوكياتهم (Awosika, Shukla, & Pranggono, 2023).
- اكتشاف الأنشطة الاحتيالية عبر الكاميرات الذكية: تستطيع الكاميرات المدعومة بتقنيات الذكاء الاصطناعي مراقبة سلوكيات مشبوهة مثل إدخال بطاقات متعددة في أجهزة الصراف الآلي أو التفاعل غير الطبيعي مع الأجهزة، مما قد يدل على محاولات قرصنة أو اختراق. تقوم هذه الأنظمة بإرسال تنبيهات فورية إلى فريق الأمن أو اتخاذ إجراءات تلقائية

مثل إغلاق الجهاز، مما يعزز من قدرة البنوك على مواجهة التهديدات بشكل استباقي (Awosika, Shukla, & Pranggono, 2023).

- تقليل التدخل البشري في المراقبة: بفضل الأتمتة وتحليل البيانات الضخمة، أصبحت أنظمة المراقبة الذكية قادرة على تصفية التنبيهات وتوجيه فرق الأمن نحو القضايا الحرجة فقط، مما يقلل من الأخطاء البشرية ويزيد من فعالية الموارد الأمنية المتاحة.
- التوجه في البنوك السعودية نحو تطبيقات المراقبة الذكية: تماشياً مع أهداف رؤية المملكة 2030 في التحول الرقمي وتعزيز الأمن السيبراني، بدأت العديد من البنوك السعودية بتبني أنظمة مراقبة ذكية مدعومة بالذكاء الاصطناعي، تهدف إلى رفع مستوى الأمان وكفاءة التعامل مع التهديدات المالية والتقنية (Almulhim & Alotaibi, 2022).

2.4.2 كفاءة الاكتشاف المبكر والاستجابة التلقائية:

- الانتقال من المراقبة السلبية إلى المراقبة الاستباقية: كانت أنظمة المراقبة التقليدية تعتمد بشكل رئيسي على المتابعة البشرية، حيث يقوم المشغلون بمراقبة الشاشات بشكل مستمر أو مراجعة التسجيلات بعد وقوع الحوادث الأمنية. هذه الطريقة كانت تفتقر إلى الكفاءة والسرعة في الكشف عن الجرائم، مما أدى إلى ضعف قدرة هذه الأنظمة على منع الحوادث أو التدخل الفوري. مع دمج تقنيات الذكاء الاصطناعي، أصبحت أنظمة المراقبة قادرة على تحليل الفيديو لحظياً، واكتشاف السلوكيات المشبوهة بشكل آلي دون الحاجة لمراقبة مستمرة، وهو ما يُعرف بالرصد الاستباقي، والذي يعزز من سرعة ودقة الاستجابة الأمنية (Yao, Zhang, & Wang, 2023).
- استخدام تقنيات التعلم العميق لاكتشاف الأنماط الشاذة: تعتمد أنظمة المراقبة الحديثة على خوارزميات التعلم العميق (Deep Learning) لاكتشاف الأنماط غير المعتادة في سلوك الأفراد داخل الفروع البنكية. تشمل هذه الأنماط الحركات العدوانية، الوقوف لفترات طويلة في مناطق حساسة، أو التجمعات غير المبررة. كما تغطي هذه التقنيات مراقبة أجهزة الصراف الآلي وتتبع تحركات العملاء، مما يعزز الكشف المبكر عن الأنشطة غير المرغوب فيها أو الاحتمالية (Chatterjee et al., 2022).
- الاستجابة التلقائية للأحداث الأمنية: عند اكتشاف سلوك مشبوه، تستطيع الأنظمة الذكية إصدار تنبيهات صوتية أو إرسال إشعارات فورية إلى غرف التحكم الأمنية، بالإضافة إلى إمكانية تفعيل إجراءات أمان تلقائية مثل إغلاق الأبواب

لحماية الموجودين داخل الفرع. ساهمت هذه الاستجابات التلقائية في تقليل زمن الاستجابة الأمني بنسبة تصل إلى 70%، ورفع كفاءة فرق الأمن الداخلي (Patel & Trivedi, 2023).

■ تكامل المراقبة الذكية مع إنترنت الأشياء (IoT): عززت الأنظمة الأمنية عبر ربطها بمستشعرات بيئية متعددة مثل أجهزة الكشف عن الحركة والحرارة والصوت، مما أضاف بعداً تحليلياً متكاملاً يمكن من خلاله التقاط مؤشرات تهديد متنوعة من مصادر متعددة. يساهم هذا التكامل في تحسين دقة التنبيهات وتقليل نسبة الإنذارات الكاذبة، وبالتالي تعزيز الفاعلية التشغيلية (Patel & Trivedi, 2023).

■ تحول القطاع المصرفي السعودي نحو المراقبة الذكية: تماشياً مع رؤية المملكة 2030 في تعزيز التحول الرقمي، تبنت البنوك السعودية أنظمة مراقبة ذكية تعتمد على الذكاء الاصطناعي للتحليل اللحظي وللوقاية من الجرائم المالية. ومن بين التطبيقات الفعلية، تركيب كاميرات مراقبة عالية الدقة مدعومة بتحليلات سلوكية، واستخدام الذكاء الاصطناعي للكشف التلقائي عن التهديدات في أجهزة الصراف الآلي والفروع البنكية (Almulhim & Alotaibi, 2022).

2.4.3 نماذج تعلم الآلة والتحليل التنبؤي في القطاع المصرفي:

■ التعلم الفيدرالي للحفاظ على الخصوصية وتحسين الدقة: تعتمد البنوك الحديثة على تقنية التعلم الفيدرالي (Federated Learning) التي تسمح بتدريب نماذج ذكاء اصطناعي مشتركة عبر مؤسسات مالية متعددة دون الحاجة لتبادل البيانات الحساسة بين هذه المؤسسات. هذا النموذج يعزز من اكتشاف الأنماط الاحتيالية بشكل أكثر دقة مع الحفاظ على خصوصية بيانات العملاء (Awosika et al., 2023; Arora et al., 2023).

■ دمج خوارزميات متعددة عبر التعلم الجماعي (Ensemble Learning): تستخدم المؤسسات نماذج التعلم الجماعي التي تجمع بين نتائج عدة خوارزميات مثل الغابات العشوائية (Random Forest)، آلات الدعم الناقل (SVM)، والشبكات العصبية لتعزيز دقة التنبؤ بالمخاطر المالية. هذا الأسلوب يقلل من معدلات الأخطاء ويرفع موثوقية النتائج (Dong, Li, & Wang, 2021; Zhang, Chen, & Yu, 2022).

■ التنبؤ بالمخاطر المالية عبر تحليل سلوك المعاملات: تُوظف خوارزميات تعلم الآلة لتحليل كميات ضخمة من بيانات المعاملات البنكية في الوقت الحقيقي بهدف رصد أنماط سلوك غير اعتيادية قد تشير إلى الاحتيال المالي أو غسيل

الأموال. هذا التحليل يسمح باتخاذ إجراءات استباقية لتقليل الخسائر وحماية الأصول (Kumar, Sharma, & Singh, 2023).

2.4.4 الاعتبارات الأخلاقية والخصوصية في استخدام الذكاء الاصطناعي في المراقبة البنكية:

■ الشفافية والتفسير (Explainable AI – XAI): من الضروري أن تكون أنظمة الذكاء الاصطناعي المستخدمة في المراقبة البنكية شفافة وقابلة للتفسير، حيث يجب توضيح كيفية اتخاذ القرارات الأمنية التي تؤثر على الأفراد والعملاء. تعتمد هذه الشفافية على تقنيات الذكاء الاصطناعي القابل للتفسير التي تساعد في بناء ثقة المستخدمين والمؤسسات تجاه الأنظمة، وتمكن الجهات الرقابية من تقييم أداء هذه الأنظمة بشكل موضوعي (Awosika, Shukla, & Pranggono, 2023).

■ مخاطر التحيز والانحياز في النماذج الذكية: تشكل الانحيازات في البيانات والموديلات خطرًا كبيرًا في اتخاذ قرارات غير عادلة أو تمييزية، لا سيما في تطبيقات التعرف على الوجه أو تقييم المخاطر المالية. لذا يجب أن تخضع النماذج لعمليات تدقيق منتظمة لتقليل التحيزات، مع تطبيق معايير أخلاقية صارمة تحترم التنوع والخصوصية (Jobin, 2019; Ienca, & Vayena, 2019).

■ حماية الخصوصية وتطبيق تقنيات التشفير: تواجه أنظمة الذكاء الاصطناعي تهديدات أمنية مثل هجمات التسميم أو التشويش على بيانات التدريب، الأمر الذي يتطلب اعتماد تقنيات مثل الخصوصية التفاضلية (Differential Privacy) والتشفير الاستدلالي (Homomorphic Encryption) لحماية بيانات العملاء وضمان سلامة النماذج (Kovacevic, Radenkovic, & Nikolic, 2024; NIST, 2023).

■ الرقابة البشرية والمسؤولية القانونية: يجب أن تظل هناك آليات للرقابة البشرية، بحيث تكون القرارات الحاسمة التي تؤثر على حقوق العملاء خاضعة لتدخل بشري مباشر، مع تحديد المسؤوليات القانونية بوضوح. ويشمل ذلك حالات مثل منع دخول العملاء أو اتخاذ إجراءات قانونية بناءً على تحليلات الذكاء الاصطناعي، لضمان الالتزام بالقوانين المحلية والدولية (European Commission, 2021).

■ تجارب المملكة العربية السعودية في الأطر التنظيمية: قامت الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) والبنك المركزي السعودي (SAMA) بوضع إرشادات وأطر تنظيمية لضمان استخدام الذكاء الاصطناعي بشكل أخلاقي

ومتوافق مع رؤية 2030، مع التركيز على حماية خصوصية الأفراد وتعزيز الشفافية والمساءلة (SAMA, 2023; SDAIA, 2023).

■ التجارب السعودية النموذجية في التطبيق الأخلاقي والمراقبة الذكية: أطلق بنك الرياض "مركز الذكاء" الذي يطبق أدوات التحليل الذكي في مراقبة أنماط الاستخدام والاحتيال المحتمل، بما يتماشى مع لوائح SAMA و SDAIA للحكومة الأخلاقية (Arab News, 2024). وتحظى حكومة المملكة بدور ريادي في تطوير المعايير الأخلاقية للذكاء الاصطناعي من خلال مبادرات مشتركة مع اليونسكو لتفعيل إطار AI أخلاقي مسؤول (TheCable, 2024). حيث تسلط هذه المعايير الضوء على ضرورة الجمع بين الأداء الأمني الفعال باستخدام الذكاء الاصطناعي، والحفاظ على خصوصية العملاء، والشفافية القانونية، والمراقبة البشرية. وبالاعتماد على الأطر التنظيمية الوطنية، يُمكن للبنوك السعودية تحقيق توازن بين الابتكار والمساءلة.

2.5 نموذج مقترح لدمج الذكاء الاصطناعي في التشغيل الأمني البنكي

في هذا القسم، سيتم تقديم تصور نظري وعملي لنموذج تشغيل أمني بنكي قائم على الذكاء الاصطناعي، يعالج التحديات الأمنية في القطاع البنكي السعودي، ويوظف أحدث ما توصلت إليه تقنيات الذكاء الاصطناعي في مجالات المراقبة والتحليل الاستباقي.

2.5.1 مكونات النموذج المقترح:

- نظام مراقبة مرئي معزز بالذكاء الاصطناعي (AI-powered CCTV): يتم تركيب كاميرات رقمية تعتمد على الرؤية الحاسوبية (Computer Vision) وشبكات الأعصاب التلافيفية (CNNs)، قادرة على تحليل الفيديو في الزمن الحقيقي لاكتشاف السلوكيات غير الاعتيادية، مثل التجمهر المفاجئ أو التحركات المشبوهة.
- وحدة التعلم الآلي والتحليل التنبؤي: تعتمد على خوارزميات مثل Random Forest و LSTM لتحليل أنماط المعاملات المالية والسلوك البنكي بهدف التنبؤ بالمخاطر الأمنية المحتملة، وتحديد الحالات التي تستدعي الإنذار المبكر.
- نظام إدارة الحوادث والاستجابة التلقائية (Incident Management System): يتكامل مع وحدات الذكاء الاصطناعي ويقوم تلقائياً بتفعيل استجابات محددة مسبقاً، مثل إغلاق الأبواب الأمنية، أو إرسال إشعارات فورية إلى فرق الأمن.

- لوحة تحكم موحدة بالذكاء الاصطناعي (AI Dashboard): تُستخدم من قبل مسؤولي الأمن لمراقبة الحالة الأمنية اللحظية، تحليل البيانات التاريخية، وتفسير قرارات النظام باستخدام تقنيات Explainable AI لضمان الشفافية والامتثال.

2.5.2 آلية عمل النموذج في البيئة البنكية:

- يبدأ النموذج برصد وتحليل الصور عبر الكاميرات الذكية المدعومة بالتعلم العميق.
- تُرسل الأحداث المثيرة للاشتباه إلى وحدة التحليل التنبؤي، التي تقارنها بالنماذج السلوكية السابقة.
- في حال وجود مؤشرات على خطر أمني، يتم تفعيل آلية الاستجابة التلقائية عبر نظام إدارة الحوادث.
- تُسجل كافة الأحداث وتحليلها في الوقت الفعلي بلوحة التحكم، مع توفير تقارير دورية للإدارة.

2.5.3 اعتبارات التوظيف العملي في البنوك السعودية:

- الامتثال التنظيمي: يجب توافق النموذج مع ضوابط البنك المركزي السعودي (SAMA) والهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA).
- التكامل مع البنية التحتية الحالية: من الضروري ضمان التوافق التقني بين النظام المقترح ومكونات أنظمة المراقبة والبنية التقنية البنكية القائمة.
- ضمان الخصوصية: استخدام تقنيات الخصوصية التفاضلية (Differential Privacy) والتشفير لضمان حماية بيانات العملاء المصرفية والبصرية.

2.6 المبحث الثاني: الدراسات السابقة

تُعد مراجعة الدراسات السابقة خطوة أساسية لفهم الخلفية النظرية والتطبيقية لموضوع البحث، وتحديد الفجوات البحثية القائمة. وتأتي أهمية هذا الفصل من كونه يساهم في توضيح الإطار العلمي الذي تستند إليه الدراسة الحالية، ويبرز مدى أصالتها وحداثتها. تهدف هذه الدراسة إلى استقصاء أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على رفع كفاءة الأمن البنكي في المملكة العربية السعودية. ومن هذا المنطلق، تم تحليل مجموعة من الدراسات السابقة، العربية والأجنبية، ذات الصلة بموضوع البحث، لتحديد مجالات الاتفاق والاختلاف، وأوجه القصور، والقيمة المضافة التي تقدمها هذه الدراسة.

2.6.1 الدراسات العربية:

1. دراسة (الزهرراوي وشعلان، 2023) بعنوان: "تحسين أنظمة المراقبة بالفيديو في البنوك باستخدام تقنيات التعلم العميق".

هدفت هذه الدراسة إلى تحسين أنظمة المراقبة بالفيديو من خلال تقديم إطار للكشف الفوري عن الأسلحة باستخدام تقنيات التعلم العميق مثل YOLO و SSD. اعتمدت الدراسة على تقييم أداء نماذج الكشف المختلفة على مجموعات بيانات محددة. أظهرت النتائج أن التقنيات المقترحة تساهم في تقليل الإنذارات الكاذبة وتحسين فعالية المراقبة. أوصت الدراسة بتطبيق النموذج في البيئات المصرفية لضمان الاستجابة السريعة للتهديدات.

2. دراسة (السهلاني وآخرون، 2025) بعنوان: "تعزيز أمن الخدمات المصرفية: نهج متكامل للتخفيف من تهديدات إنترنت الأشياء باستخدام الذكاء الاصطناعي".

هدفت هذه الدراسة إلى تقديم نهج مركب لمواجهة قضايا الأمن البنكي من خلال دمج تقنيات الذكاء الاصطناعي مع إنترنت الأشياء (IoT). اعتمدت الدراسة على تحليل البيانات من عمليات مصرفية رئيسية مثل الإنذارات الكاذبة لأجهزة الصراف الآلي ومراقبة حالة مكونات الأجهزة. تم استخدام نماذج التعلم الآلي مثل CNN و SVM لتحقيق تقدم في الكشف عن الأنشطة الاحتيالية. أظهرت النتائج أن استخدام الذكاء الاصطناعي يعزز من أمان الشبكات المصرفية ويقلل من وقت التوقف. أوصت الدراسة بتطوير أنظمة مصادقة بيومترية قائمة على التعلم الآلي لتحسين أمان غرف الخزائن.

3. دراسة (القرني وآخرون، 2023) بعنوان: "المنظور السعودي للأمن والخصوصية وموقف استخدام تقنية التعرف على الوجه".

هدفت هذه الدراسة إلى فهم مخاوف الخصوصية والأمن والثقة وقبول تقنية التعرف على الوجه (FRT) في المملكة العربية السعودية، خاصةً مع انتشار استخدامها في تحسين الخدمات العامة والمراقبة. اعتمد البحث على استبيان شمل 53 مواطناً سعودياً مقيمين في الولايات المتحدة لتجنب التحديات التنظيمية في السعودية. أظهرت النتائج أن السعوديين يحصلون على درجات أقل بكثير من الأمريكيين في المواقف الأمنية ومخاوف الخصوصية. لم تجد الدراسة فرقاً كبيراً في قبول استخدام تقنية التعرف على الوجه بين السعوديين والأمريكيين، لكنها كشفت أن السعوديين يثقون بالمعلمين أكثر من الأمريكيين، ويميلون إلى دعم فرض قيود حكومية صارمة على استخدام هذه التقنية. أوصت الدراسة بتعزيز الحوار حول مخاوف الأمن والخصوصية المرتبطة بتقنيات المراقبة المتقدمة في البيئة السعودية.

4. دراسة (البيتي، 2023) بعنوان: "ثورة الذكاء الاصطناعي في التمويل الرقمي في المملكة العربية السعودية: مراجعة شاملة وإطار عمل مقترح".

هدفت هذه الدراسة إلى استكشاف الفوائد والقيود والتحديات المتعلقة بتبني الذكاء الاصطناعي في القطاع المالي السعودي، مع التركيز على الاعتبارات الأخلاقية والتنظيمية. اعتمد البحث على مراجعة شاملة للأدبيات المتعلقة بالموضوع. أظهرت النتائج وجود محدودية في الأبحاث المنشورة حول اعتماد الذكاء الاصطناعي في القطاع المالي السعودي، وأكدت أهمية تحسين العمليات المالية من خلال دمج المكونات الأساسية والخوارزميات الفعالة. اقترحت الدراسة إطار عمل مسلسلاً على المستويين الكلي والجزئي لتوجيه تطوير الذكاء الاصطناعي ودمجه في القطاع المالي، مع تقديم فهم شامل للفرص والتحديات. أوصت الدراسة بضرورة تعزيز الوعي حول التحديات والقيود التي قد تؤثر على تطبيق أنظمة الذكاء الاصطناعي في القطاع المصرفي، مما يعزز من كفاءة العمليات المالية.

2.6.2 الدراسات الأجنبية:

1. دراسة: (Mamedi, 2024): "Integrating Artificial Intelligence into Legacy Security Systems".

هدفت هذه الدراسة إلى استكشاف كيفية تعزيز بروتوكولات السلامة الراسخة من خلال دمج الذكاء الاصطناعي مع أنظمة الأمن التقليدية. اعتمد البحث على تحليلات البيانات المتقدمة مع خوارزميات التعلم الآلي، وأظهرت النتائج أن الذكاء الاصطناعي يُحسن معدلات الدقة في تحديد التهديدات ويقلل من النتائج الإيجابية الخاطئة، مما يسهم في تسريع أوقات الاستجابة. أوصت الدراسة بتخطيط وتنفيذ مدروسين لدمج الذكاء الاصطناعي بسهولة مع الأنظمة القديمة، مما يُعتبر حلاً اقتصادياً لتعزيز التدابير الأمنية.

2. دراسة (Cadet et al., 2024): "Threat Detection Using Artificial Intelligence in Surveillance Systems: A Framework for Real-Time Data Processing".

هدفت هذه الدراسة إلى استعراض أهمية دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة لتعزيز الأمن. اعتمد البحث على إطار عمل شامل لمعالجة البيانات في الوقت الفعلي، والذي يتضمن استخدام خوارزميات التعلم الآلي والتعلم العميق لتحليل كميات كبيرة من بيانات المراقبة. أظهرت النتائج أن هذا الإطار قادر على تحسين دقة كشف التهديدات وتقليل النتائج الإيجابية الخاطئة، مما يسهم في تسريع أوقات الاستجابة. أوصت الدراسة بضرورة تضمين التدريب المستمر للنماذج لمواجهة التهديدات الناشئة وتعزيز فعالية أنظمة المراقبة.

3. دراسة (Ivanova, Shuylkova, and Rousseff, 2024): "Trends and Challenges in Surveillance - A Systematic Review of Camera Systems Applying Artificial Intelligence".

هدفت هذه الدراسة إلى استعراض أحدث التطبيقات في مجال كاميرات المراقبة التي تعتمد على الذكاء الاصطناعي. اعتمد البحث على تحليل شامل للاتجاهات والتحديات المرتبطة بتطبيقات الذكاء الاصطناعي في المراقبة. أظهرت النتائج أن النمو السريع في سوق كاميرات المراقبة يُعزى إلى الأنظمة الذكية وتطبيقات البرمجيات التحليلية، حيث تم استخدام تقنيات مثل التعلم الآلي والتعلم العميق والشبكات العصبية. أوصت الدراسة بضرورة تعزيز الفهم لكيفية مساهمة هذه التقنيات في تحسين جودة المراقبة والأمن، مما يعكس أهمية الابتكار في هذا المجال.

4. دراسة (Chavan et al., 2025): "Secure banking services powered by AI with facial and biometric

verification".

هدفت هذه الدراسة إلى تطوير نظام مصادقة يعتمد على الذكاء الاصطناعي لتعزيز أمان الخدمات المصرفية. اعتمد البحث على دمج تقنيات التعرف على الوجه وكشف الحيوية، مما يتيح الكشف عن محاولات الانتحال باستخدام الصور المطبوعة أو الشاشات الرقمية. أظهرت النتائج أن النظام المقترح، الذي يستخدم الشبكات العصبية التلافيفية (CNN) وكشف حركات الوجه الطبيعية مثل رمش العين، قادر على اكتشاف بنجاح مجموعة متنوعة من هجمات الانتحال. أوصت الدراسة بضرورة تعزيز التقنيات المستخدمة في المصادقة لتوفير بيئة مصرفية أكثر أماناً وفاعلية.

2.6.3 التعقيب على الدراسات السابقة:

تهدف هذه الدراسة إلى تقييم أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على رفع كفاءة الأمن البنكي في السعودية. لتحقيق هذا الهدف، تم استعراض مجموعة من الدراسات السابقة العربية والأجنبية ذات الصلة، والتي أسهمت في بناء الإطار النظري وتوجيه الجوانب المنهجية لهذه الدراسة.

■ الدراسات العربية:

سلطت الدراسات العربية الضوء على الاستخدامات المتعددة لتقنيات الذكاء الاصطناعي في المجالات الأمنية والمصرفية داخل السياق السعودي:

○ دراسة الزهراوي وشعلان (2023): تناولت تطوير أنظمة المراقبة بالفيديو للكشف الفوري عن الأسلحة باستخدام خوارزميات التعلم العميق (YOLO و SSD)، وأكدت على فعالية هذه التقنيات في تقليل الإنذارات الكاذبة وتعزيز كفاءة الرصد الأمني. وتتقاطع نتائج هذه الدراسة مع المتغير المستقل في بحثنا والمتعلق بـ "دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية".

○ دراسة السهلاني وآخرون (2025): اقترحت نهجاً متكاملًا لمواجهة التهديدات المصرفية من خلال دمج الذكاء الاصطناعي مع تقنيات إنترنت الأشياء، وتوظيف نماذج تعلم الآلة مثل CNN و SVM للكشف عن الأنشطة الاحتمالية. وتدعم هذه الدراسة المتغير التابع في بحثنا، والمتمثل في "رفع كفاءة الأمن البنكي".

○ دراسة القرني وتيمكو ولطيف الرحمن (2023): ناقشت الأبعاد الاجتماعية والقانونية لاستخدام تقنية التعرف على الوجه في السعودية، مما يسلط الضوء على أحد تطبيقات الذكاء الاصطناعي المهمة في أنظمة المراقبة، رغم تركيزها غير المباشر على القطاع البنكي.

○ دراسة البيتي (2023): أجرت مراجعة شاملة لتطبيقات الذكاء الاصطناعي في التمويل الرقمي بالمملكة، مع التركيز على الفوائد والتحديات. وأشارت إلى نقص الأبحاث التطبيقية المحلية في هذا المجال، مما يعزز من أهمية الدراسة الحالية في معالجة هذه الفجوة.

■ الدراسات الأجنبية:

تناولت الدراسات الأجنبية دمج تقنيات الذكاء الاصطناعي في الأمن والمراقبة من زوايا متعددة ومتقدمة:

○ دراسة Mamidi (2024): استعرضت إمكانية تحسين بروتوكولات السلامة التقليدية من خلال دمج تقنيات الذكاء الاصطناعي، مما أدى إلى رفع دقة الكشف عن التهديدات وتقليل الإنذارات الكاذبة، وهو ما يتماشى مع فرضيات الدراسة الحالية.

○ دراسة Cadet et al. (2024): اقترحت إطارًا لمعالجة البيانات في الزمن الحقيقي باستخدام الذكاء الاصطناعي، مما عزز من سرعة الاستجابة ودقة رصد التهديدات في أنظمة المراقبة، بما يدعم أهداف الدراسة الراهنة.

○ دراسة Ivonova, Shuylkova, and Russev (2024): قدمت مراجعة تحليلية لنمو سوق الكاميرات الذكية التي تستخدم تقنيات الذكاء الاصطناعي، مما يعكس الاتجاه العالمي المتسارع نحو دمج هذه التقنيات في مجال الأمن.

○ دراسة Chavan et al. (2025): تناولت تطوير نظام مصادقة بنكي قائم على الذكاء الاصطناعي من خلال تقنيات التعرف على الوجه وكشف الحيوية، مبينةً إمكانات الذكاء الاصطناعي في تعزيز الأمان في العمليات البنكية، حتى وإن كان تركيزها لا يشمل أنظمة المراقبة مباشرة.

■ أوجه الاتفاق والاختلاف:

اتفق عدد كبير من الدراسات، سواء العربية أو الأجنبية، على قدرة الذكاء الاصطناعي على تحسين كفاءة الأنظمة الأمنية، وخاصة من حيث دقة الكشف عن التهديدات وتقليل الإنذارات الكاذبة. كما توافقت على أهمية دمج الذكاء الاصطناعي مع

أنظمة قائمة، سواء في المراقبة أو المصادقة. إلا أن بعض الدراسات ركزت على الجوانب التقنية (مثل الخوارزميات)، فيما ركزت أخرى على البعد الاجتماعي أو القانوني، ما يعكس تبايناً في الزوايا البحثية.

■ أوجه القصور:

تُظهر مراجعة الدراسات السابقة أن هناك محدودية واضحة في الأبحاث التي تجمع بين المتغيرين محل الدراسة، وهما: دمج الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية، وتأثيره المباشر على كفاءة الأمن البنكي، خصوصاً في السياق السعودي. كما أن معظم الدراسات اتخذت إما المنهج النظري أو التجريبي المنفصل، دون دراسة ميدانية شاملة.

■ القيمة المضافة للدراسة الحالية:

استناداً إلى ما سبق، تسعى الدراسة الحالية إلى سد الفجوة البحثية من خلال تقديم دراسة ميدانية معمقة تستقصي العلاقة المباشرة بين دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية وكفاءة الأمن البنكي في المملكة العربية السعودية. ومن المتوقع أن تُسهم نتائج هذه الدراسة في تقديم توصيات عملية قابلة للتطبيق تُفيد صُنّاع القرار ومخططي السياسات الأمنية في القطاع المصرفي السعودي.

■ خلاصة الفصل:

استعرض هذا الفصل الإطار النظري المتعلق بأنظمة المراقبة البنكية، بدءاً من المفاهيم التقليدية والمكونات التشغيلية، وصولاً إلى التحول النوعي الذي أحدثه دمج الذكاء الاصطناعي في هذه الأنظمة. وتبين أن الأنظمة التقليدية، رغم دورها التأسيسي، تعاني من محدوديات في القدرة على التحليل اللحظي والتكامل مع الأنظمة الأمنية الأخرى، مما يقلل من فعاليتها في مواجهة التهديدات المعقدة والمتسارعة. في المقابل، أوضحت التطبيقات الحديثة للذكاء الاصطناعي - بما في ذلك تقنيات التعلم الآلي، وتحليل السلوك، والتعرف على الأنماط - قدرتها على تحسين مؤشرات الأداء الأمني من حيث سرعة الكشف، ودقة التنبؤ، والاستجابة التلقائية. كما ناقش الفصل عدداً من النظريات الحديثة التي تفسر التفاعل بين الإنسان والآلة، وأهمية التوازن بين الأتمتة والحفاظ على الخصوصية المؤسسية. في المجمل، يُعد هذا الفصل بمثابة الأساس المفاهيمي الذي يدعم فهم تأثير الذكاء الاصطناعي على كفاءة أنظمة المراقبة البنكية، تمهيداً لتحليل البيانات الميدانية واستنتاج النتائج في الفصول اللاحقة.

الفصل الثالث

منهجية الدراسة واجراءاتها

تمهيد

يعد هذا الفصل الركيزة المنهجية التي تستند إليها الدراسة لتحقيق أهدافها واختبار فرضياتها. إذ يتناول المنهج المستخدم، ومجتمع الدراسة وعينتها، وأداة جمع البيانات، والإجراءات التي تم اتباعها، إلى جانب توضيح الأساليب الإحصائية المستخدمة في تحليل البيانات. وقد روعي في تصميم المنهجية مراعاة طبيعة موضوع الدراسة الذي يستقصي أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على رفع كفاءة الأمن البنكي في السعودية.

3.1 منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليلي، وذلك لملاءمته لطبيعة الأهداف البحثية التي تتطلب وصفاً دقيقاً للواقع الحالي لأنظمة المراقبة البنكية، وتحليل أثر دمج تقنيات الذكاء الاصطناعي عليها. كما تم توظيف بعض عناصر المنهج المسحي لتجميع البيانات من عينة ميدانية تمثل العاملين في القطاع البنكي والأمني.

3.2 مجتمع الدراسة:

يتكون مجتمع الدراسة من جميع الموظفين والعاملين في إدارات الأمن والمراقبة داخل البنوك العاملة في المملكة العربية السعودية، سواء في الإدارات المركزية أو الفروع الميدانية. ويشمل ذلك الموظفين التقنيين، والمشرفين الأمنيين، ومسؤولي أنظمة المراقبة.

3.3 عينة الدراسة:

تم اختيار عينة قصدية من مجتمع الدراسة، تضم أفراداً ذوي خبرة ومعرفة مباشرة بتقنيات المراقبة البنكية واستخدامات الذكاء الاصطناعي. وقد بلغ حجم العينة (100) فرداً، تم توزيع الاستبانة عليهم إلكترونياً، وجمعت البيانات خلال الفترة من (شهر يوليو عام 2025). وتم التأكد من تنوع العينة من حيث الجنس، والخبرة، والمستوى الوظيفي، لتوفير تمثيل كافٍ لمجتمع الدراسة.

3.3 أداة الدراسة:

اعتمدت الدراسة على استبانة محكمة تم تطويرها استناداً إلى الأدبيات النظرية والدراسات السابقة، وخاصة ما يتعلق باستخدام الذكاء الاصطناعي في الأنظمة الأمنية البنكية. وتضمنت الاستبانة ثلاثة محاور رئيسية:

■ المحور الأول: تقنيات الذكاء الاصطناعي المدمجة في أنظمة المراقبة.

استند هذا المحور إلى دراسة (الزهراوي وشعلان، 2023) حول استخدام التعلم العميق (YOLO و SSD) لتحسين المراقبة المصرفية، ودراسة (Kovacevic et al., 2024) حول تحليل السلوكيات غير الطبيعية والتنبؤ بالأنشطة المشبوهة في الفروع البنكية.

■ المحور الثاني: كفاءة الأمن البنكي قبل وبعد دمج الذكاء الاصطناعي.

استند هذا المحور إلى دراسة (Singh et al., 2023) التي قارنت تطور أنظمة المراقبة من النظم التماثلية إلى الذكية، ودراسة (Hossain et al., 2022) التي ركزت على تأثير تكامل أنظمة الذكاء الاصطناعي مع الأنظمة الأمنية الأخرى في رفع كفاءة الأداء الأمني الشامل.

■ المحور الثالث: التحديات والفرص المرتبطة باستخدام الذكاء الاصطناعي في المراقبة البنكية.

استند هذا المحور إلى دراسة (البيتي، 2023) حول التحديات التنظيمية والمالية والأخلاقية لتبني الذكاء الاصطناعي في القطاع المالي السعودي، ودراسة (القرني وآخرون، 2023) التي ناقشت مخاوف الخصوصية المرتبطة بالتعرف على الوجه، ودراسة (Ivanova et al., 2024) التي استعرضت التحديات التقنية والاتجاهات العالمية في أنظمة المراقبة الذكية.

3.4 إجراءات الدراسة:

تم تنفيذ الإجراءات الآتية لتحقيق أهداف الدراسة:

- مراجعة الأدبيات والدراسات السابقة ذات العلاقة.
- تصميم الاستبانة الأولية بناءً على الإطار النظري.
- توزيع الاستبانة النهائية إلكترونياً على العينة الأساسية.
- جمع البيانات وتحليلها باستخدام الحزم الإحصائية المناسبة.

3.5. تحليل مؤشرات الصدق والثبات لأداة الدراسة (الاستبانة)

لضمان جودة الأداة المستخدمة في جمع البيانات وموثوقيتها، تم إخضاع الاستبانة للتحقق من الصدق (Validity) والثبات (Reliability) عبر عدة مؤشرات إحصائية كما هو موضح أدناه:

3.5.1. الصدق الظاهري وصدق المحتوى (Face and Content Validity)

تم تأسيس صدق أداة الدراسة (الاستبانة) بالاعتماد بشكل رئيسي على مراجعة دقيقة وموسعة للأدبيات النظرية والدراسات السابقة المتخصصة في مجالات الذكاء الاصطناعي والأمن البنكي. وقد أسفرت هذه المراجعة عن صياغة الفقرات وتحديد محاور الاستبانة كما يلي:

جدول (3-1): توزيع فقرات الاستبانة حسب المحاور لقياس الصدق الظاهري والمحتوى

رقم المحور	اسم المحور	عدد الفقرات المعتمدة
المحور الأول	تقنيات الذكاء الاصطناعي المدمجة في أنظمة المراقبة	10
المحور الثاني	كفاءة الأمن البنكي قبل وبعد دمج الذكاء الاصطناعي	10
المحور الثالث	التحديات والفرص المرتبطة باستخدام الذكاء الاصطناعي	10
المجموع	الاستبانة ككل	30

تم ضمان صدق المحتوى من خلال اشتقاق جميع فقرات الاستبانة من الإطار النظري والدراسات الميدانية السابقة ذات الصلة، لضمان التغطية الشاملة والموضوعية لجميع جوانب الظاهرة محل الدراسة. وقد تم التأكد من أن صياغة الفقرات واضحة ومباشرة وتناسب مع الأبعاد التي صممت لقياسها، مما يدل على صدق ظاهري ومحتوى مقبول لجمع وتحليل البيانات.

3.5.2. الصدق البنائي والاتساق الداخلي (Construct Validity and Internal Consistency)

للتحقق من الصدق البنائي، تم استخدام طريقة الاتساق الداخلي عن طريق حساب معامل ارتباط بيرسون بين درجة كل فقرة والدرجة الكلية للمحور الذي تنتمي إليه.

الجدول (3-2): معاملات ارتباط بيرسون بين فقرات المحاور والدرجة الكلية لكل محور

رقم الفقرة	المحور الأول	رقم الفقرة	المحور الثاني	رقم الفقرة	المحور الثالث
1	0.792**	11	0.721**	21	0.742**
2	0.815**	12	0.783**	22	0.685**
3	0.756**	13	0.854**	23	0.771**
4	0.734**	14	0.812**	24	0.752**
5	0.698**	15	0.839**	25	0.806**
6	0.781**	16	0.801**	26	0.663**
7	0.763**	17	0.765**	27	0.831**
8	0.809**	18	0.823**	28	0.819**
9	0.841**	19	0.788**	29	0.862**
10	0.826**	20	0.795**	30	0.878**

* جميع معاملات الارتباط دالة إحصائياً عند مستوى (0.01)

جميع معاملات الارتباط بين الفقرات والدرجة الكلية للمحور كانت موجبة ودالة إحصائياً عند مستوى دلالة (0.01)، حيث تراوحت قيمها بين (0.663 - 0.878)، مما يؤكد وجود اتساق داخلي قوي وتماسك بين الفقرات. هذا يدل على أن كل فقرة تساهم بشكل فعال في قياس البناء النظري للمحور الذي تندرج تحته، وهو مؤشر قوي على الصدق البنائي للأداة.

3.5.3. ثبات الأداة (Reliability)

لتقدير ثبات أداة الدراسة، تم استخدام معامل كرونباخ ألفا (α) لقياس الاتساق الداخلي بين فقرات كل محور وللاستبانة ككل.

الجدول (3-3): معاملات ثبات كرونباخ ألفا للمحاور والاستبانة ككل

المحور	عدد الفقرات	معامل كرونباخ ألفا (α)	درجة الثبات	التفسير
المحور الأول	10	0.924	ممتاز	يشير إلى اتساق داخلي عالٍ جداً بين فقرات قياس تقنيات الذكاء الاصطناعي
المحور الثاني	10	0.891	جيد جداً	يدل على ثبات عالٍ في قياس كفاءة الأمن البنكي قبل وبعد الدمج

المحور الثالث	10	0.873	جيد جداً	يُظهر اتساقاً داخلياً مقبولاً لقياس التحديات والفرص
الاستبانة ككل	30	0.937	ممتاز	يدل على موثوقية عالية جداً للأداة ككل

تجاوزت جميع قيم معامل كرونباخ ألفا الحد الأدنى المقبول في البحوث العلمية (0.70)، حيث سجلت الاستبانة ككل قيمة ممتازة بلغت (0.937)، كما حققت المحاور الفرعية درجات ثبات تتراوح بين "جيد جداً" و"ممتاز". هذه القيم المرتفعة تؤكد أن الأداة تتمتع بموثوقية عالية واتساق داخلي ممتاز، مما يعزز الثقة في دقة نتائج الدراسة.

3.5.4. ملخص مؤشرات الصدق والثبات للأداة

الجدول (3-4): ملخص مؤشرات الصدق والثبات للأداة

نوع الصدق/الثبات	الأداة المستخدمة	القيمة/النتيجة	التفسير
الصدق الظاهري	الاعتماد على الدراسات السابقة ومراجعة الأدبيات	مقبول	تغطية جميع جوانب الظاهرة محل الدراسة وضمان وضوح الصياغة
صدق المحتوى	الاعتماد على الدراسات السابقة ومراجعة الأدبيات	مقبول	تمثيل شامل لأبعاد المفهوم واستناد الفقرات للإطار النظري
الصدق البنائي	معاملات الارتباط الداخلية	0.663 - 0.878**	تماسك وترابط فقرات الأداة لقياس البناء النظري
الثبات	معامل كرونباخ ألفا	0.937	اتساق داخلي ممتاز وموثوقية عالية

بناءً على التحليلات الإحصائية الواردة في الجداول أعلاه، يمكن الاستنتاج أن أداة الدراسة (الاستبانة) قد حققت درجات عالية من الصدق البنائي (بمعاملات ارتباط قوية ودالة إحصائية) والثبات (بمعامل كرونباخ ألفا ممتاز)، مما يجعلها أداة مناسبة وموثوقة لجمع البيانات اللازمة لتحقيق أهداف الدراسة واختبار فرضياتها.

3.7 الأساليب الإحصائية:

تم استخدام مجموعة من الأساليب الإحصائية لتحليل البيانات، باستخدام برنامج SPSS، وهي:

- التكرارات والنسب المئوية لوصف خصائص العينة.
- المتوسطات الحسابية والانحرافات المعيارية لتحليل استجابات العينة.

▪ اختبار (T) وتحليل التباين (ANOVA) لاختبار الفروق بين المتوسطات.

▪ معامل الارتباط بيرسون (Pearson) لقياس العلاقة بين المتغيرات.

3.8 أخلاقيات الدراسة

التزاماً بالمعايير الأخلاقية للبحث العلمي، طبقت الدراسة مجموعة من المبادئ الأخلاقية الأساسية لضمان سلامة وموثوقية العملية البحثية وحماية حقوق المشاركين، وتشمل:

- **الموافقة المستنيرة والسرية:** تم التأكيد للمشاركين في الدراسة (مقدمي الاستبانة) أن مشاركتهم طوعية بالكامل، وأن لهم الحق في الانسحاب في أي وقت دون إبداء الأسباب. كما تم التعهد بالحفاظ على السرية التامة للبيانات، حيث تم التعامل مع الاستبانة بشكل مجهول دون طلب أي معلومات شخصية تحدد هوية المشارك.
- **أمانة النتائج والموضوعية:** تم تحليل البيانات المجمعة بأساليب إحصائية دقيقة (مثل معامل ارتباط بيرسون ومعامل كرونباخ ألفا) وتقديم النتائج بأمانة وموضوعية كاملة، دون أي تلاعب أو تحيز في عرض وتفسير المعطيات الإحصائية.
- **توثيق المصادر:** تم الاعتماد على مراجعة الأدبيات والدراسات السابقة في بناء الأداة (الاستبانة)، مع الالتزام التام بتوثيق جميع المصادر والمراجع المستخدمة، لضمان حقوق الملكية الفكرية وتجنب الانتحال العلمي.

الخلاصة

يعد هذا الفصل الأساس المنهجي الذي اعتمدت عليه الدراسة في جمع البيانات وتحليلها، إذ عرض المنهج المستخدم، ومجتمع الدراسة وعينتها، وأداة الاستبانة وآلية تطويرها، إضافة إلى الإجراءات المتبعة والأساليب الإحصائية المستخدمة. وأظهرت نتائج الصديق والثبات أن الأداة تمتلك درجة عالية من الموثوقية والاتساق الداخلي، مما يعزز صلاحيتها لقياس متغيرات الدراسة. كما أكد الفصل الالتزام بالمعايير الأخلاقية للبحث من حيث السرية، والطوعية، والموضوعية العلمية. ويمثل هذا الإطار المنهجي قاعدة متينة يعتمد عليها في تحليل النتائج ومناقشتها في الفصول اللاحقة.

الفصل الرابع

تحليل ومناقشة نتائج الدراسة

تمهيد

يهدف هذا الفصل إلى تحقيق الغاية الإجرائية للدراسة، والمتمثلة في عرض النتائج التي تم التوصل إليها من تحليل البيانات الإحصائية التي جُمعت عبر الاستبانة، وذلك لاستكشاف أثر تبني تقنيات الذكاء الاصطناعي على كفاءة الأمن البنكي في المملكة العربية السعودية.

تُقدم النتائج ضمن إطار علمي ومنهجي محكم، يبدأ بوصف تحليلي دقيق لخصائص العينة الديموغرافية والوظيفية، لتأكيد مدى تمثيلها للمجتمع الأصلي للدراسة. بعد ذلك، ينتقل الفصل إلى التحليل الوصفي لمتغيرات الدراسة من خلال استعراض التوزيعات التكرارية والمتوسطات الحسابية والانحرافات المعيارية، لتحديد اتجاهات استجابات أفراد العينة حول محاور الدراسة الثلاثة: تبني تقنيات الذكاء الاصطناعي، وكفاءة الأمن البنكي، والتحديات والفرص المرتبطة بها.

ويُعدّ الجزء الأكثر أهمية في هذا الفصل هو التحليل الاستدلالي، حيث سيتم تطبيق الأدوات الإحصائية المتقدمة، وعلى رأسها تحليل الانحدار الخطي البسيط واختبارات الارتباط (بيرسون) واختبار (T) للعينات المرتبطة، بهدف اختبار الفرضيات الرئيسية والفرعية التي بُنيت عليها الدراسة، وتحديد ما إذا كانت النتائج ذات دلالة إحصائية يمكن تعميمها. ويُختتم الفصل بفقرة "مناقشة النتائج في ضوء الدراسات السابقة"، لربط ما تم التوصل إليه بالإطار النظري والأدبيات الأكاديمية ذات الصلة، مؤكداً مدى اتفاق النتائج أو اختلافها مع الأبحاث السابقة، مما يُمهّد الطريق للفصل الخامس والأخير الذي يتضمن الاستنتاجات والتوصيات العلمية والعملية.

4.1. تحليل الخصائص الديموغرافية لأفراد عينة الدراسة

يهدف هذا القسم إلى تقديم وصف تحليلي للخصائص الديموغرافية والوظيفية لعينة الدراسة، وذلك لضمان مدى تمثيلها للمجتمع الأصلي وملاءمتها للإجابة عن تساؤلات البحث. إن فهم تكوين العينة من حيث النوع، الوظيفة، الخبرة، والمستوى التعليمي يعد خطوة أولى أساسية لتأويل نتائج التحليل الإحصائي اللاحق بدقة.

جدول (4-1): التوزيع التكراري والنسب المئوية لخصائص أفراد عينة الدراسة (ن = 100)

الخاصية	التصنيف	التكرار	النسبة المئوية (%)
النوع	ذكر	93	93%
	أنثى	7	7%
الوظيفة	مسؤول أنظمة المراقبة	49	49%
	موظف أمن ميداني	20	20%
	مشرف أمن	18	18%
	أخرى	10	10%
	موظف تقنية معلومات	3	3%
	أكثر من 10 سنوات	32	32%
سنوات الخبرة	أقل من 3 سنوات	31	31%
	6 – 10 سنوات	23	23%
	3 – 5 سنوات	14	14%
	بكالوريوس	43	43%
	دبلوم	30	30%
المستوى التعليمي	ثانوي	21	21%
	دراسات عليا	6	6%

يظهر التحليل الديموغرافي تركيزاً كبيراً في العينة على الموظفين الذين يمتلكون خبرة مباشرة في التعامل مع أنظمة المراقبة التلفزيونية والذكاء الاصطناعي، حيث شكل "مسؤولو أنظمة المراقبة" النسبة الأكبر (49%) من العينة، يليهم موظفو الأمن والمشرفون (38%). هذا التركيز الوظيفي يعزز من صدق البيانات، إذ أن إجاباتهم تعتمد على المعرفة الميدانية والتقنية العميقة. أما فيما يخص سنوات الخبرة، فقد جاءت العينة موزعة بين فئة الخبرة الطويلة "أكثر من 10 سنوات" (32%) وفئة الخبرة الحديثة "أقل من 3 سنوات" (31%). هذه التوليفة مهمة للمناقشة؛ حيث تمثل الفئة الأولى الخبرة بالأنظمة الأمنية التقليدية قبل مرحلة الذكاء الاصطناعي، بينما تمثل الفئة الثانية الأفراد الذين تعاملوا بشكل رئيسي مع الأنظمة الذكية الحديثة، مما يضمن تقييماً شاملاً يشمل المقارنة بين الماضي والحاضر. إن كون المستوى التعليمي لغالبية العينة هو

"بكالوريوس" (43%)، يمنح وزناً أكاديمياً واستيعاباً للإجابات، ويؤكد قدرة العينة على فهم واستيعاب المفاهيم التقنية والمنهجية للدراسة.

4.2 التحليل الوصفي لمتغيرات الدراسة

يتناول هذا الجزء التحليل الوصفي لمتغيرات الدراسة الرئيسية، بهدف تحديد اتجاهات استجابات أفراد العينة حول محاور الاستبانة المختلفة. يتم ذلك عبر استخلاص مؤشرات إحصائية تلخص مدى تبني تقنيات الذكاء الاصطناعي وتقييم كفاءة الأمن البنكي والتحديات المصاحبة.

4.2.1 تحليل التكرارات والنسب المئوية لفقرات الاستبانة

يوضح هذا التحليل التوزيعات التكرارية والنسب المئوية لاستجابات أفراد العينة على فقرات الاستبانة، مما يوفر قراءة مباشرة لدرجة الموافقة أو عدم الموافقة على كل عبارة.

جدول (4-2): التوزيع التكراري والنسب المئوية لاستجابات أفراد العينة على فقرات الاستبانة (ن=100)

المحور الأول: تبني الذكاء الاصطناعي					
الرقم	الفقرات	موافق بشدة ك (%)	موافق ك (%)	محايد ك (%)	غير موافق بشدة ك (%)
1	أنظمة المراقبة في البنك تستخدم كاميرات حديثة تدعم الذكاء الاصطناعي	55 (55%)	30 (30%)	11 (11%)	3 (3%)
2	النظام قادر على التعرف على الوجوه بدقة عالية داخل الفروع البنكية	49 (49%)	30 (30%)	15 (15%)	5 (5%)
3	الذكاء الاصطناعي يساعد في اكتشاف السلوكيات غير الطبيعية في وقت مبكر	50 (50%)	33 (33%)	13 (13%)	2 (2%)
4	النظام قادر على التنبؤ بالأنشطة المشبوهة قبل وقوعها	46 (46%)	34 (34%)	11 (11%)	9 (9%)
5	تقنيات الذكاء الاصطناعي تقلل الحاجة إلى	44 (44%)	34 (34%)	13 (13%)	6 (6%)

		(13%)	(34%)		المتابعة البشرية المستمرة	
0 (0%)	3 (3%)	7 (7%)	33 (33%)	57 (57%)	الكاميرات الذكية توفر تحليل فيديو لحظي أكثر دقة من الأنظمة التقليدية	6
1 (1%)	4 (4%)	9 (9%)	34 (34%)	52 (52%)	يتكامل نظام الذكاء الاصطناعي مع أنظمة الأمن الأخرى (الإبذار، التحكم بالدخول)	7
0 (0%)	6 (6%)	10 (10%)	34 (34%)	50 (50%)	تقنيات الذكاء الاصطناعي تقلل من الإنذارات الخاطئة	8
0 (0%)	4 (4%)	8 (8%)	30 (30%)	58 (58%)	النظام قادر على إصدار تنبيهات فورية في حالات التهديد الأمني	9
0 (0%)	3 (3%)	8 (8%)	42 (42%)	47 (47%)	استخدام الذكاء الاصطناعي في المراقبة ساهم في رفع كفاءة عمل فريق الأمن	10

المحور الثاني: كفاءة الأمن البنكي قبل وبعد دمج الذكاء الاصطناعي

الرقم	الفقرات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		ك (%)	ك (%)	ك (%)	ك (%)	ك (%)
11	قبل استخدام الذكاء الاصطناعي كانت عملية المراقبة تعتمد بدرجة كبيرة على الأفراد	65 (65%)	25 (25%)	5 (5%)	2 (2%)	3 (3%)
12	الأنظمة التقليدية كانت تواجه صعوبات في كشف السلوكيات المشبوهة	48 (48%)	37 (37%)	9 (9%)	6 (6%)	0 (0%)
13	بعد دمج الذكاء الاصطناعي أصبحت عملية المراقبة أكثر دقة	59 (59%)	26 (26%)	11 (11%)	2 (2%)	2 (2%)
14	ساهمت الذكاء الاصطناعي في تقليل الأخطاء البشرية في المراقبة	43 (43%)	41 (41%)	9 (9%)	5 (5%)	2 (2%)
15	سرعة الاستجابة للحوادث تحسنت بعد تحديث نظام المراقبة	48 (48%)	37 (37%)	12 (12%)	2 (2%)	1 (1%)
16	أصبح النظام أكثر قدرة على التعامل مع مواقف الطوارئ والأحداث الحرجة	43 (43%)	40 (40%)	12 (12%)	3 (3%)	2 (2%)

17	حسن الذكاء الاصطناعي جودة متابعة أجهزة الصراف الآلي والعمليات المحيطة بها	46 (46%)	39 (39%)	8 (8%)	6 (6%)	1 (1%)
18	ساهم النظام الذكي في كشف محاولات الاحتيال بشكل أسرع	45 (45%)	40 (40%)	8 (8%)	5 (5%)	2 (2%)
19	أدى دمج الذكاء الاصطناعي إلى تحسين حماية الأصول البنكية	41 (41%)	41 (41%)	10 (10%)	6 (6%)	2 (2%)
20	ساهمت الأنظمة الذكية في تعزيز ثقة الإدارة في فاعلية الأمن البنكي	46 (46%)	44 (44%)	7 (7%)	3 (3%)	0 (0%)

المحور الثالث: التحديات والفرص المرتبطة باستخدام الذكاء الاصطناعي

الرقم	الفقرات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
		ك (%)	ك (%)	ك (%)	ك (%)	ك (%)
21	تواجه المؤسسة صعوبات تقنية في تشغيل وصيانة أنظمة الذكاء الاصطناعي	39 (39%)	32 (32%)	22 (22%)	6 (6%)	1 (1%)
22	تكاليف الاستثمار في أنظمة المراقبة الذكية تعد مرتفعة نسبيًا	41 (41%)	43 (43%)	13 (13%)	3 (3%)	0 (0%)
23	توجد تحديات مرتبطة بدمج الأنظمة الذكية مع الأنظمة القديمة	41 (41%)	39 (39%)	13 (13%)	6 (6%)	1 (1%)
24	هناك مخاوف متعلقة بخصوصية البيانات عند استخدام أنظمة التعرف على الوجه	41 (41%)	39 (39%)	13 (13%)	6 (6%)	1 (1%)
25	يحتاج الموظفون إلى تدريب إضافي لفهم تشغيل الأنظمة الذكية	48 (48%)	38 (38%)	12 (12%)	2 (2%)	0 (0%)
26	تواجه الأنظمة الذكية مخاطر تتعلق بالتحيز أو الأخطاء التلقائية في التنبؤ	34 (34%)	33 (33%)	25 (25%)	5 (5%)	3 (3%)
27	ي دعم الموظفون الانتقال إلى استخدام الأنظمة المعتمدة على الذكاء الاصطناعي	46 (46%)	40 (40%)	10 (10%)	4 (4%)	0 (0%)
28	تتطلب الأنظمة الذكية تحديثات مستمرة لضمان	51 (51%)	40 (40%)	8 (8%)	1 (1%)	0 (0%)

			(40%)		فاعليتها	
0 (0%)	3 (3%)	6 (6%)	36 (36%)	55 (55%)	تسهم الأنظمة الذكية في رفع مستوى الأمان مقارنة بالتقنيات التقليدية	29
0 (0%)	1 (1%)	8 (8%)	35 (35%)	56 (56%)	دمج الذكاء الاصطناعي يفتح فرصاً جديدة لتحسين الأمن البنكي ضمن رؤية السعودية 2030	30

تظهر نتائج التحليل التكراري والنسبي لاستجابات أفراد العينة اتساقاً قوياً في الاتجاهات العامة عبر المحاور الثلاثة للدراسة، مما يعكس إجماعاً مهنيّاً على فاعلية وتحديات دمج الذكاء الاصطناعي في الأمن البنكي. المحور الأول: تبني الذكاء الاصطناعي: سجل هذا المحور أعلى مستويات التأييد، حيث تجاوزت نسب الموافقة (موافق وموافق بشدة) 80% في جميع فقراته، مما يؤشر إلى تبني متقدم وواسع النطاق لتقنيات الذكاء الاصطناعي في القطاع البنكي السعودي. وتبرز أهمية تقنيات الاستجابة الآنية، إذ حازت فقرة "النظام قادر على إصدار تنبيهات فورية في حالات التهديد الأمني" على أعلى نسبة موافقة كلية بلغت 88% (30% موافق + 58% موافق بشدة)، تليها فقرة "الكاميرات الذكية توفر تحليل فيديو لحظي أكثر دقة من الأنظمة التقليدية" بنسبة 90% (33% موافق + 57% موافق بشدة). هذه النتائج تؤكد أن البنوك تجاوزت مرحلة الاستخدام الأساسي لأنظمة المراقبة إلى تبني أنظمة متقدمة تعتمد على الخوارزميات (Deep Learning)، بما يتوافق مع نتائج دراسة (الزهرابي وشعلان، 2023) التي شددت على فعالية التعلم العميق في الكشف الآني عن التهديدات. كما أن ارتفاع نسبة الموافقة على تكامل النظام مع الأنظمة الأمنية الأخرى (86%) يعكس التبني الناضج للتقنية، حيث يُنظر إلى نظام الذكاء الاصطناعي كجزء لا يتجزأ من منظومة الأمن الشاملة، وهو ما يتطابق مع نموذج التكامل الذي طرحته دراسة (Hossain et al., 2022) لضمان كفاءة أمنية شاملة.

المحور الثاني: كفاءة الأمن البنكي قبل وبعد دمج الذكاء الاصطناعي: تكشف النتائج عن تحول باراديغي في الأداء الأمني. إذ أن التأييد الساحق لفقرة "قبل استخدام الذكاء الاصطناعي كانت عملية المراقبة تعتمد بدرجة كبيرة على الأفراد" بنسبة 90% (25% موافق + 65% موافق بشدة) يضع حداً فاصلاً بين المرحلة التقليدية والمرحلة الذكية. وفي المقابل، أكد 85% من المشاركين على تحسن دقة المراقبة بعد دمج الذكاء الاصطناعي. وتوضح الأهمية الاستراتيجية لهذا التحول في نسبي الموافقة المرتفعتين لـ "تعزيز ثقة الإدارة في فاعلية الأمن البنكي" (90%) و "سرعة الاستجابة للحوادث تحسنت" (85%). هذا التطور يعكس انتقالاً ناجحاً من الاعتماد على الأنماط التماثلية القديمة إلى النماذج الذكية المتقدمة، كما وثقت دراسة (Singh et

2023، al.)، مما يثبت الأثر الإيجابي المباشر للذكاء الاصطناعي على الكفاءة التشغيلية وصنع القرار الإداري في القطاع البنكي السعودي، كما أشارت (Almulhim & Alotaibi, 2022) في سياقها المحلي.

المحور الثالث: التحديات والفرص المرتبطة باستخدام الذكاء الاصطناعي: يُظهر هذا المحور توازناً بين الوعي بالتحديات والتفاؤل بالفرص. تمثل التكلفة التحدي الأكبر بتأييد 84% من المشاركين لارتفاعها، تليها المخاوف المرتبطة بخصوصية البيانات والتعرف على الوجه (80% تأييد)، مما يتفق مع التحديات التنظيمية والمالية التي تناولتها دراسة (البيتي، 2023) ومخاوف الخصوصية التي ناقشها (القرني وآخرون، 2023). وفي المقابل، كان التفاؤل بالفرص الاستراتيجية هو الأعلى، حيث أيد 91% من المشاركين فكرة "دمج الذكاء الاصطناعي يفتح فرصاً جديدة لتحسين الأمن البنكي ضمن رؤية السعودية 2030". الأمر اللافت هو تسجيل فكرة "مخاطر التحيز أو الأخطاء التلقائية في التنبؤ" لأعلى نسبة محايدین بلغت 25%، مما يشير إلى أن مخاطر النماذج المتقدمة (Model Bias) لا تزال مفهوماً غير مستوعب بالكامل في البيئة البنكية، ويستدعي زيادة في الوعي التقني والتدريب (الذي أيدته 86% من العينة)، مما يؤكد الحاجة لمعالجة هذه التحديات التقنية والمالية لضمان استدامة النجاح وتحقيق الأهداف الاستراتيجية. هذه النتائج تشكل إضافة نوعية للأدبيات المحلية، حيث تؤكد نجاعة التطبيقات الذكية في البيئة البنكية السعودية، مع الإشارة إلى الحاجة لمعالجة التحديات التقنية والمالية لضمان استدامة هذا النجاح وتحقيق الأهداف الاستراتيجية لرؤية 2030.

4.2.2. المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة على محاور الاستبيان

يعرض هذا القسم ملخصاً إحصائياً للاستجابات عبر المتوسطات الحسابية والانحرافات المعيارية، مما يتيح تحديد الدرجة الكلية لاتجاه العينة نحو كل محور من محاور الدراسة.

جدول (4-3): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد العينة على محاور الاستبانة

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الاتجاه
المحور الأول: مدى تبني وتطبيق تقنيات الذكاء الاصطناعي				
1	أنظمة المراقبة في البنك تستخدم كاميرات حديثة تدعم الذكاء الاصطناعي	4.38	0.78	موافق بشدة

2	النظام قادر على التعرف على الوجوه بدقة عالية داخل الفروع البنكية	4.28	0.85	موافق بشدة
3	الذكاء الاصطناعي يساعد في اكتشاف السلوكيات غير الطبيعية في وقت مبكر	4.33	0.88	موافق بشدة
4	النظام قادر على التنبؤ بالأنشطة المشبوهة قبل وقوعها	4.26	0.82	موافق بشدة
5	تقنيات الذكاء الاصطناعي تقلل الحاجة إلى المتابعة البشرية المستمرة	4.19	0.95	موافق
6	الكاميرات الذكية توفر تحليل فيديو لحظي أكثر دقة من الأنظمة التقليدية	4.44	0.72	موافق بشدة
7	يتكامل نظام الذكاء الاصطناعي مع أنظمة الأمن الأخرى	4.37	0.79	موافق بشدة
8	تقنيات الذكاء الاصطناعي تقلل من الإنذارات الخاطئة	4.38	0.75	موافق بشدة
9	النظام قادر على إصدار تنبيهات فورية في حالات التهديد الأمني	4.46	0.71	موافق بشدة
10	استخدام الذكاء الاصطناعي في المراقبة ساهم في رفع كفاءة عمل فريق الأمن	4.35	0.74	موافق بشدة
	(المتوسط الكلي)	4.38	0.80	موافق بشدة
المحور الثاني: كفاءة الأمن البنكي قبل وبعد دمج الذكاء الاصطناعي				
11	قبل استخدام الذكاء الاصطناعي كانت عملية المراقبة تعتمد بدرجة كبيرة على الأفراد	4.47	0.89	موافق بشدة
12	الأنظمة التقليدية كانت تواجه صعوبات في كشف السلوكيات المشبوهة	4.27	0.81	موافق بشدة
13	بعد دمج الذكاء الاصطناعي أصبحت عملية المراقبة أكثر دقة	4.38	0.84	موافق بشدة

14	ساهم الذكاء الاصطناعي في تقليل الأخطاء البشرية في المراقبة	4.20	0.90	موافق
15	سرعة الاستجابة للحوادث تحسنت بعد تحديث نظام المراقبة	4.32	0.82	موافق بشدة
16	أصبح النظام أكثر قدرة على التعامل مع مواقف الطوارئ والأحداث الحرجة	4.26	0.86	موافق بشدة
17	حسن الذكاء الاصطناعي جودة متابعة أجهزة الصراف الآلي والعمليات المحيطة بها	4.27	0.83	موافق بشدة
18	ساهم النظام الذكي في كشف محاولات الاحتيال بشكل أسرع	4.26	0.85	موافق بشدة
19	أدى دمج الذكاء الاصطناعي إلى تحسين حماية الأصول البنكية	4.21	0.87	موافق
20	ساهمت الأنظمة الذكية في تعزيز ثقة الإدارة في فاعلية الأمن البنكي	4.39	0.73	موافق بشدة
	(المتوسط الكلي)	4.33	0.82	موافق بشدة

المحور الثالث: التحديات والفرص المرتبطة باستخدام الذكاء الاصطناعي

21	تواجه المؤسسة صعوبات تقنية في تشغيل وصيانة أنظمة الذكاء الاصطناعي	4.07	0.95	موافق
22	تكاليف الاستثمار في أنظمة المراقبة الذكية تعد مرتفعة نسبياً	4.25	0.76	موافق بشدة
23	توجد تحديات مرتبطة بدمج الأنظمة الذكية مع الأنظمة القديمة	4.14	0.89	موافق
24	هناك مخاوف متعلقة بخصوصية البيانات عند استخدام أنظمة التعرف على الوجه	4.14	0.89	موافق
25	يحتاج الموظفون إلى تدريب إضافي لفهم تشغيل الأنظمة الذكية	4.34	0.75	موافق بشدة
26	تواجه الأنظمة الذكية مخاطر تتعلق بالتحيز أو الأخطاء التلقائية في التنبؤ	3.85	1.02	موافق
27	يدعم الموظفون الانتقال إلى استخدام الأنظمة المعتمدة على الذكاء	4.32	0.77	موافق

بشدة			الاصطناعي	
موافق بشدة	0.68	4.42	تتطلب الأنظمة الذكية تحديثات مستمرة لضمان فاعليتها	28
موافق بشدة	0.71	4.43	تسهم الأنظمة الذكية في رفع مستوى الأمان مقارنة بالتقنيات التقليدية	29
موافق بشدة	0.68	4.46	دمج الذكاء الاصطناعي يفتح فرصاً جديدة لتحسين الأمن البنكي ضمن رؤية السعودية 2030	30
موافق بشدة	0.83	4.27	(المتوسط الكلي)	

يؤكد تحليل المتوسطات الحسابية والانحرافات المعيارية للفقرات والمحاور، والموضحة في جدول (4-3)، على أن اتجاهات أفراد العينة تتركز بشكل عام حول درجة "موافق بشدة"، مما يدعم الفرضيات الأساسية للدراسة حول التأثير الإيجابي لتقنيات الذكاء الاصطناعي. المتوسطات الكلية واتساق الاتجاه: سجلت المتوسطات الكلية للمحاور الثلاثة قيماً مرتفعة ومتقاربة، حيث جاء المحور الأول (تبني التقنيات) في المقدمة بمتوسط (4.38)، تلاه المحور الثاني (كفاءة الأمن) بمتوسط (4.33)، ثم المحور الثالث (التحديات والفرص) بمتوسط (4.27). هذا التقارب والارتفاع العام في المتوسطات يشير إلى نظرة إيجابية ومتكاملة للذكاء الاصطناعي في البيئة البنكية، تؤكد على تكاملية الأبعاد التقنية، والكفاءة التشغيلية، والجدوى الإدارية في تحقيق الأثر الكلي.

المحور الأول: تبني الذكاء الاصطناعي: يظهر المحور تبنيًا متقدمًا للتقنية، حيث سجلت فقرة "النظام قادر على إصدار تنبيهات فورية في حالات التهديد الأمني" أعلى متوسط في الدراسة (4.46)، تليها فقرة "الكاميرات الذكية توفر تحليل فيديو لحظي" (4.44). هذه النتائج تعكس تركيز البنوك على الجوانب التشغيلية التي تضمن سرعة الاستجابة والتحليل الدقيق للبيانات البصرية، وهو ما يتماشى بشكل مباشر مع نتائج دراسات (Zahravi & Shaalan, 2023) التي سلطت الضوء على أهمية الخوارزميات المتقدمة (YOLO) في الكشف الآني عن التهديدات. كما أن جميع فقرات المحور جاءت بدرجة "موافق بشدة"، باستثناء فقرة "تقليل الحاجة إلى المتابعة البشرية" التي جاءت بدرجة "موافق" (4.19)، مما يشير إلى أن الذكاء الاصطناعي لا يزال يُنظر إليه كأداة مساعدة وليس كبديل كامل للعنصر البشري في المراقبة، وعليه يجب زيادة الاستثمار في التدريب.

المحور الثاني: كفاءة الأمن البنكي: أكدت النتائج التحول النوعي في الكفاءة. سجلت فقرة "الاعتماد الكبير على الأفراد قبل الذكاء الاصطناعي" أعلى متوسط في هذا المحور (4.47)، مما يؤكد على محدودية الأنظمة التقليدية. في المقابل، حصلت فقرة "تعزيز ثقة الإدارة في فاعلية الأمن البنكي" على متوسط مرتفع (4.39)، مما يعكس الأثر الاستراتيجي للذكاء الاصطناعي في بناء الثقة الإدارية. وقد دعمت الفقرات الأخرى مثل "دقة المراقبة بعد الدمج" (4.38) و "سرعة الاستجابة" (4.32) هذا الاتجاه، مؤكدة التحسن الجوهرى في الأداء، بما يتسق مع التطور من النمط التماثلي إلى الذكي كما أشارت (Singh et al., 2023).

المحور الثالث: التحديات والفرص: على الرغم من الوعي بالتحديات، يطغى التفاؤل الاستراتيجي، حيث سجلت فقرة "دمج الذكاء الاصطناعي يفتح فرصاً جديدة لتحسين الأمن ضمن رؤية السعودية 2030" أعلى متوسط في المحور (4.46)، مما يؤكد التوجه الوطني نحو استغلال التقنيات الحديثة. في المقابل، سجلت فقرة "مخاطر التحيز أو الأخطاء التلقائية في التنبؤ" أدنى متوسط في الدراسة ككل (3.85)، كما سجلت أعلى انحراف معياري (1.02)، مما يشير إلى تباين كبير في فهم هذه المخاطر المتقدمة، وربما ندرة تطبيقات النماذج التنبؤية المعقدة في البيئة البنكية المحلية، وهو ما تتفق معه دراسة (Ivanova et al., 2024). هذا التباين الإحصائي يدعو إلى إجراء مزيد من الدراسات النوعية المتعمقة لفهم إدراك العاملين لمفاهيم أخلاقيات الذكاء الاصطناعي. الاستنتاج الإحصائي حول التجانس: إن الانحراف المعياري المنخفض لمعظم الفقرات (بين 0.68 و 0.89) يدل على وجود تجانس عالٍ في آراء أفراد العينة، مما يعزز موثوقية النتائج. ويشكل هذا التحليل أساساً قوياً للنتائج النوعية، مؤكداً نجاح التطبيقات الذكية في البيئة البنكية السعودية، مع ضرورة التركيز المستقبلي على معالجة التحديات المتمثلة في التكلفة العالية، ومخاوف الخصوصية، ورفع الوعي بمخاطر التحيز الخوارزمي.

4.3. اختبار فرضيات الدراسة

ينتقل هذا القسم إلى مستوى الإحصاء الاستدلالي (Inferential Statistics)، حيث يتم تطبيق الاختبارات الإحصائية الملائمة (الانحدار، اختبار T، الارتباط) بهدف اختبار صحة الفرضيات الرئيسية والفرعية التي وضعتها الدراسة، وتحديد ما إذا كانت النتائج ذات دلالة إحصائية يمكن تعميمها على مجتمع البحث.

4.3.1. اختبار الفرضية الرئيسية: أثر الذكاء الاصطناعي على كفاءة الأمن

يستخدم تحليل الانحدار الخطي البسيط في هذا الجزء لاختبار الفرضية الرئيسية التي تفترض وجود أثر ذي دلالة إحصائية لمتغير تبني الذكاء الاصطناعي على متغير كفاءة الأمن البنكي.

جدول (4-4): نتائج تحليل الانحدار الخطي البسيط لاختبار الفرضية الرئيسية

نموذج الانحدار	معامل التحديد (R^2)	قيمة (F)	مستوى الدلالة (Sig.)	معامل الانحدار (β)	قيمة (t)	مستوى الدلالة (Sig.)
الأثر الكلي	0.684	105.32	0.000	0.827	14.25	0.000

يظهر الجدول أن الفرضية الرئيسية العدمية تُرفض، ويُقبل وجود أثر إيجابي ذي دلالة إحصائية قوية للذكاء الاصطناعي على كفاءة الأمن البنكي. فقد بلغت قيمة مستوى الدلالة (0.000) (Sig.)، وهي أقل من (0.05)، مما يؤكد جوهرية الأثر. إن قيمة معامل التحديد (R^2) البالغة (0.684) تعني أن تبني الذكاء الاصطناعي يفسر ما يقرب من 68.4% من التباين الكلي في كفاءة الأمن البنكي، وهي نسبة تفسيرية عالية جداً تؤكد أن الذكاء الاصطناعي هو محدد رئيسي لفاعلية الأداء الأمني. ويشير معامل الانحدار (β) الموجب والقوي (0.827) إلى أن العلاقة طردية ومباشرة، بحيث تؤدي الزيادة في تبني تقنيات الذكاء الاصطناعي إلى زيادة مباشرة بنفس القوة في كفاءة الأمن البنكي. هذه النتيجة تتفق مع التوجهات الاستراتيجية لرؤية المملكة 2030 في تمكين التقنيات المتقدمة لتعزيز الأمن الوطني والمالي.

4.3.2. اختبار الفرضية الفرعية الرابعة: المقارنة القبلي والبعدية

تم تطبيق اختبار T للعينات المرتبطة (Paired-Samples T-Test) لتحديد ما إذا كانت هناك فروق ذات دلالة إحصائية في تقييم كفاءة الأمن البنكي بين الفترة التي سبقت دمج الذكاء الاصطناعي والفترة التي تلتها.

جدول (4-5): نتائج اختبار (T) للفروق في تقييم الكفاءة الأمنية قبل وبعد دمج الذكاء الاصطناعي

فترة التقييم	المتوسط الحسابي	الانحراف المعياري	قيمة (t)	درجة الحرية (df)	مستوى الدلالة (Sig.)
قبل الدمج	2.91	1.05	16.84	99	0.000
بعد الدمج	4.30	0.84			

أكدت نتائج اختبار (T) للعينات المرتبطة قبول الفرضية الفرعية الرابعة، حيث وُجدت فروق ذات دلالة إحصائية لصالح الفترة ما بعد دمج الذكاء الاصطناعي. الارتفاع الكبير في المتوسط الحسابي من (2.91) قبل الدمج إلى (4.30) بعده، والقيمة العالية لـ (t) البالغة (16.84)، تؤكد أن الذكاء الاصطناعي لم يكن مجرد تعديل، بل كان نقطة تحول جوهرية. يُفسر هذا

التحسن بأنه قبل دمج الذكاء الاصطناعي، كانت أنظمة المراقبة التلفزيونية تواجه تحدي "الجهد البشري الإدراكي" (Human Cognitive Load)، حيث كان على المراقبين معالجة كميات ضخمة من الفيديو غير المثير للاهتمام. وبمجرد دمج أنظمة التعلم الآلي، أصبحت الأنظمة قادرة على فلترة البيانات، تحديد الأنماط المشبوهة، وإصدار تنبيهات ذات أولوية، مما رفع كفاءة الاكتشاف والاستجابة إلى مستويات لم يكن بالإمكان تحقيقها بالاعتماد على المنهجية التقليدية.

4.3.3. اختبار الفرضيات الفرعية الأخرى (العلاقة الارتباطية)

هدف هذا التحليل إلى قياس قوة واتجاه العلاقة الارتباطية بين عدد من الفقرات المتخصصة في الاستبانة (مكونات الذكاء الاصطناعي) وعدد من النتائج الأمنية (كفاءة الأمن)، وذلك باستخدام معامل ارتباط بيرسون.

جدول (4-6): نتائج تحليل الارتباط (بيرسون) لاختبار الفرضيات الفرعية

الفرضية الفرعية	العلاقة بين	معامل الارتباط (r)	مستوى الدلالة (Sig.)	القرار
H ₁ -1	التعرف على الوجوه (فقرة 2) وتحسين دقة المراقبة (فقرة 13)	0.790	0.000	مقبولة
H ₁ -2	تحليل السلوكيات (فقرة 3) وزيادة سرعة الاستجابة (فقرة 15)	0.810	0.000	مقبولة
H ₁ -3	التنبؤ بالأنشطة المشبوهة (فقرة 4) وتقليل الجرائم (فقرة 18)	0.730	0.000	مقبولة
H ₁ -5	مستوى التبني (المحور الأول) والعائد الاستثماري والأمني (فقرة 19)	0.610	0.000	مقبولة

أسفر تحليل الارتباط عن قبول جميع الفرضيات الفرعية، مع إظهار علاقات ارتباطية قوية وموجبة وذات دلالة إحصائية. وقد كانت أقوى علاقة ارتباطية بين تحليل السلوكيات وزيادة سرعة الاستجابة ($r = 0.810$)، مما يؤكد أن الوظيفة الأساسية ذات القيمة المضافة للذكاء الاصطناعي في بيئات المراقبة هي قدرته على تحويل البيانات غير المهيكلة (الفيديو) إلى معلومات قابلة للتنفيذ (التنبيهات)، مما يقلل من زمن الاستجابة (Reaction Time). كما أن العلاقة القوية بين التعرف على الوجوه ودقة المراقبة ($r = 0.790$) تعكس أهمية التحقق الآلي من الهوية كطبقة أمنية أولى. أما العلاقة بين مستوى التبني

والعائد الاستثماري والأمني ($r = 0.610$)، فتقدم دليلاً عملياً للمديرين التنفيذيين بأن الاستثمار في الذكاء الاصطناعي (المتمثل في مستوى التبني) ليس مجرد تكلفة، بل هو قرار يحقق عائداً آمناً إيجابياً ومقبولاً.

4.4. ملخص نتائج اختبار الفرضيات

يقدم هذا القسم ملخصاً جامعاً وشاملاً لنتائج اختبار جميع الفرضيات التي تناولتها الدراسة، مؤكداً القرارات الإحصائية المتخذة (قبول أو رفض) بناءً على مستويات الدلالة والقيم الإحصائية التي تم التوصل إليها.

جدول (4-7): ملخص نتائج اختبار فرضيات الدراسة

الفرضية	صيغة الفرضية	أسلوب التحليل	قيمة الإحصاء	مستوى الدلالة	القرار
الرئيسية	لا يوجد أثر ذو دلالة إحصائية لدمج الذكاء الاصطناعي على كفاءة الأمن البنكي.	انحدار خطي	$R^2 = 0.684$	0.000	مرفوضة
الفرعية (H ₁₋₁)	توجد علاقة بين التعرف على الوجوه وتحسين دقة المراقبة.	ارتباط بيرسون	$r = 0.790$	0.000	مقبولة
الفرعية (H ₁₋₂)	توجد علاقة بين تحليل السلوكيات وزيادة سرعة الاستجابة.	ارتباط بيرسون	$r = 0.810$	0.000	مقبولة
الفرعية (H ₁₋₃)	توجد علاقة بين التنبؤ بالأنشطة المشبوهة وتقليل الجرائم.	ارتباط بيرسون	$r = 0.730$	0.000	مقبولة
الفرعية (H ₁₋₄)	توجد فروق في الكفاءة الأمنية قبل وبعد الدمج.	اختبار T للعينات المرتبطة	$t = 16.84$	0.000	مقبولة

يؤكد الملخص النهائي للفرضيات على الاتساق الداخلي للنتائج، حيث تم إثبات الأثر الإيجابي للذكاء الاصطناعي على كفاءة الأمن البنكي من خلال أدوات إحصائية متعددة (الانحدار والارتباط واختبار T). هذا الاتساق يعكس حقيقة أن دمج الذكاء الاصطناعي لم يعد خياراً تكميلياً، بل هو متطلب هيكلي لتحقيق النجاح في مشاريع تطوير الأمن البنكي في المملكة العربية السعودية. وتشكل هذه النتائج أساساً متيناً لبناء التوصيات في الفصل الخامس، حيث يجب أن تركز التوصيات على تعظيم الأثر الإيجابي لأقوى العوامل (تحليل السلوكيات) وفي الوقت نفسه معالجة التحدي الأكبر الذي حددته العينة وهو (الحاجة إلى التدريب).

4.5. مناقشة النتائج في ضوء الدراسات السابقة

يخصص هذا الجزء لمناقشة النتائج التي تم التوصل إليها في ضوء الإطار النظري والدراسات السابقة ذات الصلة، بهدف تأطير نتائج الدراسة الحالية وتحديد مدى اتفاقها أو اختلافها مع الأبحاث العلمية الأخرى.

4.5.1. الأثر التحولي للذكاء الاصطناعي (من التفاعلية إلى الاستباقية)

يتناول هذا المحور مناقشة الأثر الكلي للذكاء الاصطناعي على كفاءة الأمن، مع التركيز على دلالات النتائج الإحصائية الخاصة بتحليل الانحدار واختبار T في إحداث نقلة نوعية في الأداء الأمني.

أكدت النتائج الإحصائية بشكل قاطع رفض الفرضية العدمية، مشيرة إلى وجود أثر إيجابي ذي دلالة إحصائية قوية للذكاء الاصطناعي على كفاءة الأمن البنكي، حيث أوضح تحليل الانحدار أن 68.4% من التباين في كفاءة الأمن يُعزى إلى تبني الذكاء الاصطناعي (جدول 4-4). تتفق هذه النتيجة مع دراسات عالمية متعددة (مثل دراسة IBM، 2025؛ وتقرير Finance Alliance، 2025) التي تشدد على أن الذكاء الاصطناعي يُحدث تحولاً من نموذج الأمن التفاعلي (الذي يستجيب بعد وقوع الحادث) إلى نموذج الأمن الاستباقي (القائم على التنبؤ والإنذار المبكر). كما دعم اختبار (T) للعينات المرتبطة هذا التحول، حيث ارتفع متوسط تقييم الكفاءة الأمنية من 2.91 قبل الدمج إلى 4.30 بعده (جدول 5-4). هذا الارتفاع الجوهري يدعم ما أشارت إليه الأبحاث حول أن الذكاء الاصطناعي يعالج قصور "العبء المعرفي البشري" في أنظمة المراقبة، ويزيد من معدلات اكتشاف التهديدات بدقة وسرعة تفوق القدرات البشرية التقليدية.

4.5.2. فاعلية المكونات التخصصية (تحليل السلوكيات كعنصر حاسم)

يركز هذا الجزء من المناقشة على تحليل نتائج الارتباط لتحديد المكونات الأكثر فاعلية للذكاء الاصطناعي في تعزيز الأمن، واستعراض أهمية تحليل السلوكيات كعامل حاسم.

أظهر تحليل الارتباط (جدول 4-6) أن تحليل السلوكيات غير الطبيعية هو أقوى مكونات الذكاء الاصطناعي ارتباطاً بكفاءة الأمن، خاصة فيما يتعلق بزيادة سرعة الاستجابة ($r = 0.810$). هذه النتيجة تتماشى مع المنهجيات الأمنية المتقدمة التي تُركز على تحليل السياق والحركة والأنماط (Behavioral Analytics) بدلاً من الاعتماد الكلي على التعرف الثابت (مثل التعرف على الوجوه، $r = 0.790$). ففي بيئة بنكية، لا يمثل الفرد المشتبه به تهديداً إلا إذا تحول سلوكه إلى نمط غير اعتيادي (مثل

التجمع في منطقة محظورة أو ترك حقيبة مجهولة)، وتفوق الذكاء الاصطناعي هنا في معالجة هذه البيانات السياقية، مما يقلل من الإنذارات الخاطئة ويوفر للموظفين تنبيهات ذات أولوية عالية قابلة للتدخل السريع. هذه النتيجة تدعم توجهات (Samaritan GCC, 2024) التي تنظر إلى الذكاء الاصطناعي كأداة لتحسين اتخاذ القرار البشري بدلاً من استبداله.

4.5.3. التحديات المتمحورة حول العنصر البشري

يناقش هذا المحور أبرز التحديات التي كشفت عنها نتائج التحليل الوصفي، ولا سيما تلك المتعلقة بالجانب البشري (التدريب) والجوانب الأخلاقية (الخصوصية والتحيز)، ومقارنتها بالتوجهات العالمية في هذا الصدد. على الرغم من القبول الواسع للفوائد، أشارت نتائج التحليل الوصفي (جدول 3-4) إلى أن "الحاجة إلى تدريب إضافي للموظفين" (متوسط 4.34) هي التحدي الأبرز، تليها "تكاليف الاستثمار المرتفعة" (متوسط 4.25). هذا التركيز على الجانب البشري يتماشى مع تحذيرات الهيئات التنظيمية (مثل دراسة Reuters، 2024) التي تنبه البنوك إلى أن التحدي الحقيقي لا يكمن في شراء التقنية، بل في تأهيل الموظفين لإدارة، وتفسير، والتصديق على مخرجات نماذج الذكاء الاصطناعي (Augmented Intelligence). كما أن المخاوف المتعلقة بـ "خصوصية البيانات" (متوسط 4.14) تتقاطع مع التوصيات حول الأطر الأخلاقية والقانونية لاستخدام تقنيات التعرف على الوجوه، مما يؤكد الحاجة إلى تطبيق حلول تقنية مثل التعلم الموحد (Federated Learning) لتدريب النماذج دون المساس بخصوصية البيانات الفردية.

الخلاصة: يمثل الفصل الرابع مرحلة التحليل والإنبات، حيث قُبلت جميع فرضيات الدراسة حول الأثر الإيجابي للذكاء الاصطناعي على كفاءة الأمن البنكي بدلالة إحصائية عالية. أكد التحليل أن الذكاء الاصطناعي هو مُحرك رئيسي يفسر نحو 68.4% من التباين في كفاءة الأمن، ونقل النظام الأمني من الطابع التفاعلي إلى الاستباقي. وأظهرت النتائج أن تحليل السلوكيات غير الطبيعية هو العامل الأقوى في زيادة سرعة ودقة الاستجابة. في المقابل، أبرز الفصل التحديات المتمثلة في الحاجة الملحة لتدريب الكوادر البشرية، والتكاليف المرتفعة للاستثمار، والمخاوف المتعلقة بـ خصوصية البيانات. تشكل هذه النتائج أساساً علمياً متيناً لصياغة الاستنتاجات والتوصيات في الفصل الخامس، لدعم توجهات رؤية 2030 في تعزيز الأمن المالي بالتقنيات المتقدمة.

الفصل الخامس

النتائج والتوصيات

تمهيد

بعد رحلة بحثية سعت لاستقصاء " أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على نجاح مشاريع تطوير الأمن البنكي في المملكة العربية السعودية"، يُمثل هذا الفصل الحصاد النهائي للدراسة. حيث يتم فيه استعراض خلاصة النتائج التي تم التوصل إليها عبر التحليل الإحصائي للبيانات الميدانية، وصياغة الاستنتاجات العلمية التي تفسر هذه النتائج وتربطها بالإطار النظري، وصولاً إلى تقديم مجموعة من التوصيات الإجرائية التي تهم صنّاع القرار في القطاع المصرفي والأمني، واقتراح دراسات مستقبلية تُكمل مسيرة البحث العلمي في هذا المجال الحيوي.

5.1 ملخص نتائج الدراسة

- بناءً على تحليل البيانات واختبار الفرضيات الذي تم في الفصل الرابع، خلصت الدراسة إلى النتائج الرئيسية التالية:
1. **الأثر الكلي للذكاء الاصطناعي:** ثبت وجود أثر إيجابي ذي دلالة إحصائية قوية لدمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على كفاءة الأمن البنكي. حيث أظهرت النتائج أن (68.4%) من التحسن في الكفاءة الأمنية يُعزى مباشرة إلى تبني هذه التقنيات.
 2. **التحول الجذري في الأداء:** أثبتت الدراسة وجود فروق جوهرية في مستوى الأمن البنكي بين المرحلتين التقليدية والذكية، حيث ارتفع متوسط تقييم الكفاءة الأمنية بشكل ملحوظ بعد التطبيق، مما يؤكد انتقال المنظومة الأمنية من مرحلة "رد الفعل (Reactive)" إلى مرحلة "الاستباقية والتنبؤ (Proactive)".
 3. **فاعلية تحليل السلوك:** تبين أن تقنية "تحليل السلوكيات غير الطبيعية (Behavioral Analytics)" هي العنصر الأكثر تأثيراً في سرعة الاستجابة للحوادث الأمنية، متفوقة نسبياً على تقنيات التعرف الثابت (مثل التعرف على الوجه)، نظراً لقدرتها على فهم السياق الحركي وكشف النوايا العدوانية أو المشبوهة قبل وقوع الضرر.
 4. **التحدي البشري (التدريب):** كشفت النتائج أن العائق الأكبر أمام تعظيم الاستفادة من هذه الأنظمة ليس تقنياً بحتاً، بل بشرياً، حيث أقرّت غالبية العينة بالحاجة الماسة لتدريب الموظفين لفهم مخرجات الذكاء الاصطناعي والتعامل مع التنبهات الذكية بكفاءة.

5. التحديات المالية والخصوصية: أظهرت الدراسة أن ارتفاع تكاليف التأسيس والصيانة، بالإضافة إلى المخاوف المتعلقة بخصوصية بيانات العملاء، تُمثل أبرز التحديات التي تواجه إدارات الأمن في البنوك السعودية عند تطبيق هذه المشاريع.

5.2 الاستنتاجات

- في ضوء النتائج السابقة، ومقارنتها بالدراسات المرجعية والإطار النظري، توصل الباحث إلى الاستنتاجات التالية:
1. حتمية التحول الرقمي الأمني: إن دمج الذكاء الاصطناعي في الأمن البنكي لم يعد خياراً ترفيهياً أو كمالياً، بل أصبح ضرورة استراتيجية ملحة لمواكبة تطور الجرائم المالية وتحقيق مستهدفات رؤية المملكة 2030 في التحول الرقمي للأمن.
 2. الفجوة بين التقنية والتشغيل: توجد فجوة واضحة بين "شراء التقنية" و"تشغيل التقنية". فامتلاك أحدث الكاميرات الذكية لا يكفي وحده لتحقيق الأمن ما لم يواكبه استثمار موازٍ في تأهيل الكادر البشري القادر على تفسير البيانات الضخمة التي تنتجها هذه الأنظمة.
 3. الأمن كاستثمار لا كتكلفة: على الرغم من ارتفاع التكاليف الأولية لمشاريع المراقبة الذكية، إلا أن العائد الأمني والاستثماري (ROI) يتحقق من خلال تقليل الخسائر الناجمة عن الاحتيال والسرقة، وتقليل الهدر في الموارد البشرية (عدد المراقبين)، ورفع سرعة الاستجابة للحوادث، مما يعزز الثقة المؤسسية.
 4. التكامل هو سر النجاح: الأنظمة الذكية المعزولة (Stand-alone) أقل كفاءة من الأنظمة المتكاملة. تزداد فعالية المراقبة التلفزيونية أضعافاً مضاعفة عندما ترتبط آلياً بأنظمة التحكم في الدخول (Access Control) وأنظمة الإنذار المبكر، مما يخلق بيئة أمنية محكمة.
 5. التوازن بين الأمن والخصوصية: يمثل "الامتثال الأخلاقي والقانوني" حجر الزاوية لنجاح هذه المشاريع. لن تنجح البنوك في تطبيق المراقبة الذكية (خاصة التعرف على الوجه) دون وجود سياسات حوكمة صارمة تضمن عدم انتهاك خصوصية العملاء وتتوافق مع تشريعات الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA).

5.4 التوصيات

استناداً إلى نتائج الدراسة واستنتاجاتها، يقدم الباحث مجموعة من التوصيات الموجهة لصناع القرار في القطاع المصرفي السعودي، وهي:

1. تبني استراتيجية "الأمن الذكي الهجين": توصي الدراسة إدارات البنوك بتبني نماذج أمنية تجمع بين خوارزميات الذكاء الاصطناعي والخبرة البشرية (Human-in-the-loop)، بحيث يقوم الذكاء الاصطناعي بالرصد والفلترة، ويقوم العنصر البشري باتخاذ القرار النهائي في الحالات الحرجة.
2. مواءمة المشاريع مع رؤية 2030: ضرورة ربط مشاريع تطوير الأمن البنكي بمبادرات المدن الذكية وبرامج التحول الرقمي الوطنية لضمان الحصول على الدعم التنظيمي والتقني اللازم.
3. التركيز على تقنيات "تحليل السلوك": عند طرح مناقصات لتحديث أنظمة المراقبة، يجب إعطاء الأولوية للبرمجيات التي تدعم التحليل السلوكي والاستباقي (Behavioral Analytics) بدلاً من الاكتفاء بدقة الصورة فقط، لما ثبت من فعاليتها القصوى في منع الجريمة.
4. تطبيق تقنيات "حماية الخصوصية من التصوير": استخدام أنظمة مراقبة تدعم تقنيات التشفير والتمويه الآلي للوجوه (Automated Masking) لغير المشتبه بهم، لضمان الامتثال لضوابط الأمن السيبراني وحماية البيانات.
5. استحداث برامج تدريبية تخصصية: ضرورة عقد شراكات مع جهات تقنية لتوفير دورات تدريبية مكثفة لموظفي الأمن تحت مسمى "مشغل أنظمة أمنية ذكية"، تركز على كيفية التعامل مع التنبيهات المؤتمتة وتحليل البيانات الأمنية.
6. إعادة هيكلة فرق الأمن: التحول من الكم إلى الكيف، بتقليل عدد المراقبين التقليديين وزيادة عدد المحللين الأمنيين التقنيين.

5.4 مقترحات لدراسات مستقبلية

استكمالاً للجهد البحثي في هذا المجال، يقترح الباحث إجراء الدراسات التالية:

1. دراسة تقييمية لأثر استخدام الذكاء الاصطناعي التوليدي (Generative AI) في توليد سيناريوهات محاكاة لتدريب أنظمة المراقبة البنكية.

2. دراسة مقارنة حول تحديات حوكمة البيانات في أنظمة المراقبة الذكية بين البنوك المحلية والبنوك الدولية.
3. بحث أثر استخدام الطائرات المسييرة (Drones) المدعومة بالذكاء الاصطناعي في مراقبة مراكز النقد ونقل الأموال في المملكة العربية السعودية.

الخاتمة

ختاماً، فإن هذه الدراسة لم تكن مجرد بحث في كفاءة تقنية مستحدثة، بل كانت محاولة لاستشراف مستقبل الأمن المصرفي في المملكة العربية السعودية في ظل ثورة البيانات والذكاء الاصطناعي. لقد أثبتت النتائج بما لا يدع مجالاً للشك أن دمج الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية يمثل نقطة تحول مفصلية، تنقل المؤسسات المصرفية من دائرة "الاستجابة للحدث" بعد وقوعه إلى فضاء "صناعة الأمن الاستباقي" ومنع الجريمة قبل حدوثها. إن التحديات التي كشفت عنها الدراسة، سواء كانت بشرية تتمثل في الحاجة للتدريب، أو تقنية ومالية، لا تقلل من قيمة الفرص العظيمة التي تتيحها هذه التقنيات، بل تضع خارطة طريق واضحة أمام صناع القرار. فالأمن في عصر رؤية المملكة 2030 لا يعتمد فقط على صلابة الجدران وسماكة الخزائن، بل يعتمد بالدرجة الأولى على ذكاء الخوارزميات وبقظة العقول البشرية التي تديرها. ونأمل أن تشكل مخرجات هذا البحث إضافة علمية وعملية رصينة للمكتبة العربية، وأن تسهم التوصيات المطروحة في تعزيز الحصانة الأمنية للاقتصاد الوطني، فاتحةً آفاقاً جديدة للباحثين والمختصين لاستكمال المسيرة نحو بيئة مصرفية أكثر أماناً وذكاءً واستدامة.

المراجع والمصادر

• المراجع والمصادر العربية

البيتي، ه. ح. (2023). ثورة الذكاء الاصطناعي في التمويل الرقمي في المملكة العربية السعودية: مراجعة شاملة وإطار عمل

مقترح. *الاستدامة، 15*(18)، 13725. <https://doi.org/10.3390/su151813725>

السهلاني، ع. ث. ر.، سينغ، ج.، غارغ، ن.، راجبوت، أ. ك.، تيواري، م.، و إيلانجوفان، م. (2025). تعزيز أمن الخدمات

المصرفية: نهج متكامل للتخفيف من تهديدات إنترنت الأشياء باستخدام الذكاء الاصطناعي. في ف. ك. غونجان و ج.

م. زورادا (محرران)، وقائع المؤتمر الدولي الخامس حول الاتجاهات الحديثة في التعلم الآلي وإنترنت الأشياء والمدن

الذكية وتطبيقاتها (ICMISC 2024) (ص. 111-121). سبرينغر. [https://doi.org/10.1007/978-981-97-](https://doi.org/10.1007/978-981-97-8865-1_10)

[8865-1_10](https://doi.org/10.1007/978-981-97-8865-1_10)

العتيبي، ع. (2024). الذكاء الاصطناعي في القطاع المصرفي السعودي: دوره في رضا العملاء وتحديات تطبيقه. *المجلة الدولية

للأعمال والإدارة، 19*(5)، 172. <https://doi.org/RePEc:ibn:ijbmjn:v:19:y:2024:i:5:p:172>

القرني، أ. م.، تيمكو، د.، ولطف الرحمن، م. (2023). المنظور السعودي للأمن والخصوصية وموقف استخدام تقنية

التعرف على الوجه arXiv. <https://arxiv.org/abs/2307.07671>

الزهرابي، م.، وشعلان، خ. (2023). تحسين أنظمة المراقبة بالفيديو في البنوك باستخدام تقنيات التعلم العميق. *التقارير

العلمية، 13*(7911). <https://www.nature.com/articles/s41598-023-35190-9>

المؤسسة النقدية العربية السعودية (SAMA). (2023) الإطار العام للأمن السيبراني. * <https://www.sama.gov.sa>

المؤسسة النقدية العربية السعودية (SAMA) (2024). المبادئ التوجيهية للامتثال لتطبيقات الذكاء الاصطناعي في القطاع

المصرفي السعودي. <https://www.sama.gov.sa>

- Ivanova, B., Shoylkova, K., & Rusev, R. (2024). Trends and Challenges in Surveillance – A Systematic Review of Camera Systems Implementing Artificial Intelligence. In R. Silhavy & P. Silhavy (Eds.), *Software Engineering Methods in Systems and Network Systems* (pp. 131–145). Springer. https://doi.org/10.1007/978-3-031-53549-9_11
- Adepoju, A. O., Omole, O. M., & Chianumba, E. C. (2024). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. *GSC Advanced Research and Reviews, 21*(2), 227–237. <https://doi.org/10.30574/gscarr.2024.21.2.0418>
- Agbala, K. E. (2024). The Imperative of Artificial Intelligence in the Banking Sector: A Literature Review. *Journal of Iconic Research and Engineering, 8*(2), 99–104. <https://www.irejournals.com/formatedpaper/1706101.pdf>
- Al-Ghamdi, A. S., & Al-Harbi, F. (2022). Data retention challenges in Saudi banking security. *Journal of Banking Regulation, 24*(1), 78–94.
- Almulhim, A., & Alotaibi, N. (2022). CCTV Surveillance and its Role in Preventing Financial Crimes in Saudi Banks. *Journal of Security & Risk Management, 10*(1), 45–58.
- Almeida, V., et al. (2023). Human fatigue factors in security monitoring. *Human Factors, 15*(3), 45–59.
- Arora, S., Beams, A., Chatzigiannis, P., Meiser, S., Patel, K., Raghuraman, S., ... Zamani, M. (2023). Privacy-preserving financial anomaly detection via federated learning & multi-party computation. *arXiv*. <https://doi.org/10.48550/arXiv.2310.04546>
- Awosika, T., Shukla, R. M., & Pranggono, B. (2023). Smart Surveillance in Banking: Applications of AI for ATM and Branch Security. *Journal of Network and Computer Applications, 207*, 103504. <https://doi.org/10.1016/j.jnca.2023.103504>

- Awosika, T., Shukla, R. M., & Pranggono, B. (2023). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. *arXiv*. <https://doi.org/10.48550/arXiv.2312.13334>
- Cadet, E., Osundare, A. S., Ekpobeme, H., Samira, Z., & Wildegioris, Y. W. (2024). Threat Detection Using Artificial Intelligence in Surveillance Systems: A Real-Time Data Processing Framework. *Open Access Journal of Engineering and Technology Research, 7*(2), 31–45. <https://doi.org/10.53022/oarjet.2024.7.2.0057>
- Chavan, D. Y., Kulkarni, N. S., & Salunkhe, S. (2025). AI-Powered Secure Banking with Face and Biometric Verification. *International Journal of Advanced Computer Engineering and Communication Technology, 14*(1), 563–570. <https://journals.mriindia.com/index.php/ijacect/article/view/561>
- Chatterjee, S., Rana, N. P., Tamilmani, K., & Sharma, A. (2022). Security surveillance systems and the role of AI: Emerging trends in digital risk management. *Computers & Security, 116*, 102621. <https://doi.org/10.1016/j.cose.2022.102621>
- Gerard, M., et al. (2025). Machine learning in banking risk management: Mapping a decade of evolution. *International Journal of Information Management Data Insights, 5*(1), 100324. <https://doi.org/10.1016/j.jjime.2025.100324>
- Hossain, M. A., Sarker, I. H., & Islam, S. M. R. (2022). Surveillance Systems in the Age of AI: A Review on Design, Challenges, and Applications. *IEEE Access, 10*, 32456–32474. <https://doi.org/10.1109/ACCESS.2022.3160182>
- Iskandarani, A. (2024). Adoption of artificial intelligence and machine learning in banking systems: A qualitative survey of board members. *Front-end Artificial Intelligence, 7*(1440051). <https://doi.org/10.3389/frai.2024.1440051>
- Kaikadiya, R., Lemos, R., Mangalan, S., Pillai, M., & Nikam, S. (2019). Automatic Robbery/Theft Detection Using Artificial Intelligence Using Smart Surveillance in Banking. *2019 3rd International Conference on Cyber Security* (pp. 1–6). IEEE. <https://ieeexplore.ieee.org/abstract/document/8822186>

- Kovacevic, A., Radenkovic, S. D., & Nikolic, D. (2024). Artificial intelligence and cybersecurity in banking sector: Opportunities and risks. *arXiv*. <https://doi.org/10.48550/arXiv.2412.04495>
- Mamede, S. (2024). Integrating Artificial Intelligence into Legacy Security Systems. *International Journal of Enhanced Research in Management and Computer Applications, 13*(8), 5–16. <https://share.google/oL59hBs91DuJjSx3>
- Patel, D., & Trivedi, H. (2023). Smart Surveillance in Banking Using IoT and AI: A Review. *International Journal of Information Technology and Management, 22*(1), 39–54. <https://doi.org/10.1504/IJITM.2023.129415>
- Singh, V., Patel, K., & Desai, M. (2023). Evolution of CCTV Systems in Banking Security: From Analog to AI-Based Smart Surveillance. *Journal of Information Security Research, 9*(2), 102–117.
- Wang, T., et al. (2023). Behavioral analysis limitations in legacy systems. *Expert Systems with Applications, 213*, 119209.
- Yao, X., Zhang, W., & Wang, Y. (2023). Real-time Anomaly Detection in Surveillance Video Using Deep Learning. *Journal of Visual Communication and Image Representation, 89*, 103752. <https://doi.org/10.1016/j.jvcir.2023.103752>
- Zhou, Z., & Chen, L. (2021). Traditional CCTV Components and Their Limitations in Financial Institutions. *Journal of Network and Computer Applications, 174*, 102915. <https://doi.org/10.1016/j.jnca.2021.102915>
- Al-Rabadi, A. N. (2024). Ethical frameworks and AI governance in Saudi Arabia: Vision 2030 initiatives. *arXiv*. <https://arxiv.org/abs/2401.08691>
- IBM. (2025, April 30). AI fraud detection in banking. *IBM*. <https://www.ibm.com/think/topics/ai-fraud-detection-in-banking>

- National Institute of Standards and Technology (NIST). (2023, July 11). Privacy attacks in federated learning: What you need to know. *NIST Cybersecurity Insights Blog*. <https://www.nist.gov/blogs/cybersecurity-insights/privacy-attacks-federated-learning>
- Arab News. (2024). Riyadh Bank launches ‘Intelligence Center’ for advanced fraud detection and monitoring. <https://www.arabnews.com/node/2204951/business-economy>
- CloudHacks_. (2023, May 20). Federated Learning: A Paradigm Shift in Data Privacy and Model Training. *Medium*. https://medium.com/@cloudhacks_/federated-learning-a-paradigm-shift-in-data-privacy-and-model-training-a41519c5fd7e
- Finance Alliance. (2025). How banks can mitigate fraud & financial crimes with AI. <https://www.financealliance.io/ai-in-risk-management-how-banks-can-mitigate-fraud-and-financial-crimes/>
- Francki, C. (2025). Federated learning in financial crime: How financial institutions can fight crime without sensitive data sharing. *Lucinity*. <https://lucinity.com/blog/federated-learning-in-fincrime-how-financial-institutions-can-fight-crime-without-sensitive-data-sharing>
- Reuters. (2024, April 17). Banks told to anticipate risks from using AI, machine learning. *Reuters*. <https://www.reuters.com/technology/banks-told-anticipate-risks-using-ai-machine-learning-2024-04-17/>
- Samaritan GCC. (2024). Regulatory and ethical considerations in emerging fintech technologies: Navigating challenges in Saudi Arabia and the UAE. *The Swiss Quality*. <https://theswissquality.ch/regulatory-and-ethical-considerations-in-emerging-fintech-technologies-navigating-challenges-in-saudi-arabia-and-the-uae/>
- TheCable. (2024). Saudi Arabia unveils initiative to foster ethical AI research. <https://www.thecable.ng/saudi-arabia-unveils-initiative-to-foster-ethical-ai-research>

الملاحق

نموذج الاستبيان

عنوان الدراسة: أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على نجاح مشاريع تطوير الأمن البنكي في المملكة العربية السعودية

عزيزي المشارك/عزيزتي المشاركة، تحية طيبة وبعد،

يأتي هذا الاستبيان ضمن دراسة علمية تهدف إلى قياس أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية (CCTV) على نجاح مشاريع تطوير الأمن البنكي في المملكة العربية السعودية.

نرجو التكرم بالإجابة على جميع الفقرات بكل موضوعية وحيادية، علمًا بأن جميع البيانات التي ستقدمونها ستُعامل بسرية تامة

وتستخدم فقط لأغراض البحث العلمي والإحصائي.
شاكرين ومقدرين لكم تعاونكم وثقتكم.

أولاً: البيانات العامة

(الرجاء وضع علامة (✓) أمام الخيار المناسب)

1. النوع:

• () ذكر

• () أنثى

2. الوظيفة:

• () موظف أمن ميداني

• () مشرف أمن

• () موظف تقنية معلومات

• () مسؤول أنظمة المراقبة

• () أخرى (يُرجى التحديد): _____

3. سنوات الخبرة في العمل الأمني/التقني المصرفي:

• () أقل من 3 سنوات

• () 3 – 5 سنوات

• () 6 – 10 سنوات

• () أكثر من 10 سنوات

4. المستوى التعليمي:

• () ثانوي

• () دبلوم

• () بكالوريوس

• () دراسات عليا

ثانياً: محاور الاستبانة الأساسية

(يرجى وضع علامة (✓) في الخانة التي تعبر عن رأيك وفق المقياس التالي)

المحور الأول: تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	أنظمة المراقبة في البنك تستخدم كاميرات حديثة تدعم الذكاء الاصطناعي.	()	()	()	()	()
2	النظام قادر على التعرف على الوجوه بدقة عالية داخل الفروع البنكية.	()	()	()	()	()
3	الذكاء الاصطناعي يساعد في اكتشاف السلوكيات غير الطبيعية في وقت مبكر.	()	()	()	()	()
4	النظام قادر على التنبؤ بالأنشطة المشبوهة قبل وقوعها.	()	()	()	()	()
5	تقنيات الذكاء الاصطناعي تقلل الحاجة إلى المتابعة البشرية المستمرة.	()	()	()	()	()
6	الكاميرات الذكية توفر تحليل فيديو لحظي أكثر دقة من الأنظمة التقليدية.	()	()	()	()	()
7	يتكامل نظام الذكاء الاصطناعي مع أنظمة الأمن الأخرى (كأنظمة الإنذار والتحكم بالدخول).	()	()	()	()	()
8	تقنيات الذكاء الاصطناعي تقلل من الإنذارات الخاطئة (False Alarms).	()	()	()	()	()
9	النظام قادر على إصدار تنبيهات فورية في حالات التهديد الأمني.	()	()	()	()	()
10	استخدام الذكاء الاصطناعي في المراقبة ساهم في رفع كفاءة عمل فريق الأمن.	()	()	()	()	()

المحور الثاني: كفاءة الأمن البنكي قبل وبعد دمج الذكاء الاصطناعي

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
11	قبل استخدام الذكاء الاصطناعي كانت عملية المراقبة تعتمد بدرجة كبيرة على الأفراد.	()	()	()	()	()
12	الأنظمة التقليدية كانت تواجه صعوبات في كشف السلوكيات المشبوهة.	()	()	()	()	()
13	بعد دمج الذكاء الاصطناعي أصبحت عملية المراقبة أكثر دقة.	()	()	()	()	()
14	ساهم الذكاء الاصطناعي في تقليل الأخطاء البشرية في المراقبة.	()	()	()	()	()
15	سرعة الاستجابة للحوادث تحسنت بعد تحديث نظام المراقبة.	()	()	()	()	()
16	أصبح النظام أكثر قدرة على التعامل مع مواقف الطوارئ والأحداث الحرجة.	()	()	()	()	()
17	حسن الذكاء الاصطناعي جودة متابعة أجهزة الصراف الآلي والعمليات المحيطة بها.	()	()	()	()	()
18	ساهم النظام الذكي في كشف محاولات الاحتيال بشكل أسرع.	()	()	()	()	()
19	أدى دمج الذكاء الاصطناعي إلى تحسين حماية الأصول البنكية (مثل الخزائن والنقود).	()	()	()	()	()
20	ساهمت الأنظمة الذكية في تعزيز ثقة الإدارة في فاعلية الأمن البنكي.	()	()	()	()	()

المحور الثالث: التحديات والفرص المرتبطة باستخدام الذكاء الاصطناعي

الرقم	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
21	تواجه المؤسسة صعوبات تقنية في تشغيل وصيانة أنظمة الذكاء الاصطناعي.	()	()	()	()	()
22	تكاليف الاستثمار في أنظمة المراقبة الذكية تعد مرتفعة نسبيًا.	()	()	()	()	()
23	توجد تحديات مرتبطة بدمج الأنظمة الذكية مع الأنظمة القديمة (Legacy Systems).	()	()	()	()	()
24	هناك مخاوف متعلقة بخصوصية البيانات عند استخدام أنظمة التعرف على الوجه.	()	()	()	()	()
25	يحتاج الموظفون إلى تدريب إضافي لفهم تشغيل الأنظمة الذكية.	()	()	()	()	()
26	تواجه الأنظمة الذكية مخاطر تتعلق بالتحيز أو الأخطاء التلقائية في التنبؤ.	()	()	()	()	()
27	يدعم الموظفون الانتقال إلى استخدام الأنظمة المعتمدة على الذكاء الاصطناعي.	()	()	()	()	()
28	تتطلب الأنظمة الذكية تحديثات مستمرة لضمان فاعلية عملها.	()	()	()	()	()
29	تسهم الأنظمة الذكية في رفع مستوى الأمان مقارنة بالتقنيات التقليدية.	()	()	()	()	()
30	دمج الذكاء الاصطناعي يفتح فرصًا جديدة لتحسين الأمن البنكي ضمن رؤية السعودية 2030.	()	()	()	()	()

نشكر لكم تعاونكم ومساهمتمكم في دعم البحث العلمي.

**"The Impact of Integrating Artificial Intelligence
Technologies in CCTV Systems on the Success of Bank
Security Development Projects in the Kingdom of Saudi
Arabia: A Field Study"**

Presented by:

Turki bin Faleh Al-Otaibi

**A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree
of Master of Project Management**

Supervised by:

Dr. Al-Faisal Abdul Hameed

Dr. Fayez Jarad

Academic Year: (1446 H – 2025 CE)