

"أثر دمج تقنيات الذكاء الاصطناعي في أنظمة المراقبة التلفزيونية على رفع كفاءة الأمن البنكي في السعودية: دراسة ميدانية"

إعداد الطالب:

تركي بن فالح العتيبي

إشراف:

د. الفيصل عبد الحميد

د. فايز جراد

العام الدراسي: (1446هـ – 2025 م)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

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.

بالطبع، إليك صياغة أكاديمية محكمة لعنوان القسم 1.6.1 تحت عنوان:

"1.6.1 النظريات العلمية المتبعة لإعداد الدراسة"

بما يتوافق مع المحتوى والمنهج العلمي للبحث:

1.6 النظريات العلمية المتبعة لإعداد الدراسة:

استندت هذه الدراسة إلى مجموعة من النظريات العلمية التي شكلت 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. وتُعدّ 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. وتُوظَّف 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 Rogers (2003) 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 للأنشطة 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 مريبة 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 الفعالية، 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 غسل

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 الاحتيالية. 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 إطاراً 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، مبيّنةً 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

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، وُجمعت 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.
 - المحور الثاني: كفاءة الأمن البنكي قبل وبعد دمج الذكاء الاصطناعي.
 - المحور الثالث: التحديات والفرص المرتبطة باستخدام الذكاء الاصطناعي في المراقبة البنكية.
- وقد اشتملت الاستبانة على (٣٠) فقرة، تم تصميمها باستخدام مقياس ليكرت الخماسي.

3.4 إجراءات الدراسة:

تم تنفيذ الإجراءات الآتية لتحقيق أهداف الدراسة:

- مراجعة الأدبيات والدراسات السابقة ذات العلاقة.
- تصميم الاستبانة الأولية بناءً على الإطار النظري.
- عرض الاستبانة على مجموعة من المحكمين المتخصصين للتأكد من صدقها.
- تعديل الاستبانة بناءً على ملاحظات المحكمين.
- تطبيق الاستبانة على العينة التجريبية (لغايات التحقق من الثبات).
- توزيع الاستبانة النهائية إلكترونياً على العينة الأساسية.
- جمع البيانات وتحليلها باستخدام الحزم الإحصائية المناسبة.

3.5 صدق الأداة وثباتها:

تم التحقق من صدق الأداة من خلال عرضها على لجنة من المحكمين في تخصصات الإدارة وتقنية المعلومات والأمن السيبراني، وقد أبدوا ملاحظاتهم وتم الأخذ بها في التعديل. أما بالنسبة للثبات، فقد تم قياسه باستخدام معامل كرونباخ ألفا (Cronbach's Alpha)، وبلغت قيمته الإجمالية (0)، وهي قيمة تُعد مقبولة إحصائياً وتعكس ثباتاً عالياً.

3.6 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.

ملخص الفصل: عرض هذا الفصل المنهجية العلمية المعتمدة في تنفيذ الدراسة، بدءاً من تحديد المنهج والمجتمع والعينة، ووصولاً إلى تصميم الأداة وإجراءات تطبيقها، والتحقق من صدقها وثباتها، ثم عرض الأساليب الإحصائية المستخدمة في تحليل البيانات. ويمثل هذا الفصل البنية الإجرائية التي ستبنى عليها نتائج الدراسة وتحليلها في الفصل الرابع.

المراجع والمصادر

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.، تيوار، م.، والإنغوفان، م. (2025). تعزيز أمن الخدمات

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

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

الذكاء وتطبيقاتها* (ص. 118-132). سبرينغر. 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 للائتمان 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., & Wildegiorgis, 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/oL59hBs91DuJljSx3>
- 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>