

دراسة مخاطر الذكاء الاصطناعي على أمن البيانات في قطاع الخدمات المالية والبنوك،

دراسة حالة البنوك العامة في الرياض

إعداد الباحث:

معتز سعد السبيعي

(233000952)

إشراف:

د. الفیصل عبد الحمید

د. فايز جراد

1445هـ – 2024 م

الشكر

أتقدم بجزيل الشكر والامتنان لجامعة ميدلوزن على توفيرها البيئة الأكاديمية المثالية لإتمام هذا

البحث. كما أخص بالشكر الدكتور الفیصل عبد الحمید، والدكتور فايز جراه، المشرفين على هذا

العمل، لما قدمه من توجيه وإرشاد قيم ساهم بشكل كبير في إثراء هذا البحث. إن دعمكم

وتوجيهاتكم كانت حجر الأساس في نجاح هذا المشروع العلمي.

معتز سعد السبيعي

الإهداء

أهدي هذا العمل إلى أهلي والأعزاء الذين كانوا سندي ومصدر إلهامي طوال رحلتي العلمية.

كما أهديه إلى أصدقائي الأوفياء الذين وقفوا بجاني ودعموني في كل خطوة.

إن عمكم وتشجيعكم كان الدافع وراء إنجاز هذا البحث،

وأنا ممتن لكم جميعاً.

معتز سعد السبيعي

فهرس المحتويات

1	الفصل الأول: الإطار العام للدراسة.....	1
1.1	المقدمة.....	1
1.2	مشكلة الدراسة.....	2
1.3	أهمية الدراسة.....	3
1.4	أهداف الدراسة.....	4
1.5	تساؤلات الدراسة.....	4
1.6	فروض الدراسة.....	5
1.7	مفاهيم الدراسة.....	5
1.8	المنطلقات النظرية للدراسة.....	6
2	الفصل الثاني: الإطار النظري والدراسات السابقة.....	8
2.1	الدراسات السابقة.....	8
2.1.1	التعليق على الدراسات السابقة.....	16
2.2	الإطار النظري.....	20
2.3	المبحث الأول: الذكاء الاصطناعي.....	20
	المبحث الثاني: أمن المعلومات في القطاع المصرفي:.....	26
3	الفصل الثالث: الإطار المنهجي للدراسة.....	39
3.1	الإطار المنهجي للدراسة.....	39
3.1.1	منهج الدراسة:.....	39

39.....	مجتمع الدراسة:	3.1.2
39.....	عينة الدراسة:	3.1.3
43.....	أدوات جمع البيانات ومقاييس الدراسة.....	3.2
45.....	مجالات الدراسة.....	3.3
45.....	المقاييس والاختبارات الإحصائية المقترح استخدامها.....	3.4
46.....	الفصل الرابع: تحليل البيانات والنتائج.....	4
54.....	اختبار فرضيات الدراسة:	4.1
57.....	مناقشة النتائج والتوصيات.....	4.2
65.....	الملاحق.....	5

فهرس الجداول

جدول 1: الخصائص الديموغرافية للعينة.....	40
جدول 2: معاملات الاتساق الداخلي بين العبارة والمحور الذي تنتهي إليه.....	44
جدول 3: معاملات الثبات ألفا كرونباخ.....	45
جدول 4: مستوى الادراك بالتهديدات الحالية والناشئة.....	46
جدول 5: فهم كيفية استغلال الذكاء الاصطناعي الهجمات السيبرانية.....	47
جدول 6: مدى استخدام تقنية الذكاء الاصطناعي في حماية البيانات.....	49
جدول 7: فعالية الحلول القائمة على الذكاء الاصطناعي في كشف التهديدات.....	50
جدول 8: فعالية السياسات والإجراءات الحالية لأمن البيانات.....	52
جدول 8: فعالية السياسات والإجراءات الحالية لأمن البيانات.....	53
جدول 10: اختبارات لإسهام الذكاء الاصطناعي في تعزيز قدرات الهجمات السيبرانية.....	54
جدول 11: اختبارات لاستخدام الذكاء الاصطناعي في تعزيز أمن البيانات.....	55
جدول 12: اختبارات لاستراتيجيات البنوك السعودية في حماية البيانات.....	56

فهرس الأشكال

- شكل 1: توزع العينة وفق الجنس.....42
- شكل 2: توزع العينة وفق العمر42
- شكل 3: توزع العينة وفق المستوى التعليمي42
- شكل 4: توزع العينة وفق سنوات الخبرة42
- شكل 5: توزع أفراد العينة وفق الوظيفة.....43
- شكل 6: توزع أفراد العينة وفق البنك.....43

الملخص

تهدف هذه الدراسة إلى دراسة مخاطر الذكاء الاصطناعي على أمن البيانات في قطاع الخدمات المالية والبنوك، دراسة حالة البنوك العامة في الرياض. كما تهدف الدراسة إلى تقديم فهم شامل لمخاطر الذكاء الاصطناعي على أمن البيانات في البنوك السعودية، وتسعى إلى تحديد التهديدات السيبرانية الحالية والمستقبلية، وتقديم شرح كيف يمكن للذكاء الاصطناعي أن يسهم في تعزيز قدرات الهجمات السيبرانية على البنوك؛ وتحليل دور الذكاء الاصطناعي في الحماية من التهديدات؛ وتقييم فعالية الاستراتيجيات الحالية التي تتبعها البنوك السعودية في حماية البيانات من التهديدات السيبرانية. اعتمدت الدراسة على المنهج الوصفي التحليلي واعتمدت الاستبيان كأداة لجمع البيانات. جرى جمع البيانات من مجموعة من موظفي البنوك العامة في منطقة الرياض وجرى توصيفها وتحليلها باستخدام البرنامج الإحصائي SPSS25. أشارت النتائج إلى أن مستوى الوعي بالتهديدات السيبرانية الحالية والمستقبلية في البنوك السعودية مرتفع جداً. كما أن هناك وعياً عالياً بفهم كيفية استغلال الذكاء الاصطناعي في الهجمات السيبرانية. كما أظهرت النتائج أن البنوك السعودية تستخدم تقنيات الذكاء الاصطناعي بشكل كبير في حماية البيانات. تشمل هذه التقنيات أنظمة كشف التسلل القائمة على الذكاء الاصطناعي، وتحليل النشاط غير المعتاد، وتحليل البيانات في الوقت الحقيقي. أخيراً أظهرت النتائج أن السياسات والإجراءات الحالية لأمن البيانات في البنوك السعودية فعالة إلى حد كبير. أوصت الدراسة بأهمية مراجعة وتحديث السياسات والإجراءات الأمنية بشكل مستمر لمواكبة التطورات التقنية والتهديدات السيبرانية الجديدة. كما أوصت بضرورة زيادة الاستثمارات في تقنيات الذكاء الاصطناعي والأمن السيبراني لضمان فعالية الكشف عن التهديدات والاستجابة لها بسرعة.

Abstract

This study aims to investigate the risks of artificial intelligence (AI) on data security in the financial services and banking sector, with a case study focusing on public banks in Riyadh. The research seeks to provide a comprehensive understanding of AI-related data security risks in Saudi banks, identify current and future cyber threats, and explain how AI can enhance the capabilities of cyberattacks on banks. Additionally, it analyzes AI's role in threat protection and evaluates the effectiveness of current strategies employed by Saudi banks to protect data from cyber threats. The study adopts a descriptive analytical approach, utilizing a questionnaire as the primary data collection tool. Data was collected from a group of public bank employees in the Riyadh region and analyzed using SPSS25 statistical software. Results indicate a very high level of awareness regarding current and future cyber threats in Saudi banks, as well as a strong understanding of how AI can be exploited in cyberattacks. The findings also reveal that Saudi banks extensively use AI technologies for data protection, including AI-based intrusion detection systems, anomaly detection, and real-time data analysis. Furthermore, the study shows that current data security policies and procedures in Saudi banks are largely effective. The research recommends the importance of continuously reviewing and updating security policies and procedures to keep pace with technological developments and new cyber threats. It also emphasizes the need for increased investments in AI technologies and cybersecurity to ensure effective threat detection and rapid response.

1 الفصل الأول: الإطار العام للدراسة

1.1 المقدمة

يعد أمن البيانات أحد أهم التحديات التي تواجه المؤسسات والشركات في العصر الرقمي، خاصة في ظل التحول السريع نحو الرقمنة وتخزين كميات هائلة من البيانات الحساسة إلكترونياً. ويكتسب هذا الموضوع أهمية خاصة في قطاع الخدمات المالية والبنوك، حيث تتعامل هذه المؤسسات مع معلومات مالية وشخصية بالغة الحساسية للعملاء والشركات.

تناولت العديد من الدراسات الحديثة موضوع أمن البيانات وتحدياته المختلفة في القطاع المالي. فقد أشارت دراسة أجراها عمر النور (2023) إلى أن التهديدات السيبرانية تشكل خطراً متزايداً على استقرار النظام المالي العالمي، مع تزايد تعقيد وتواتر الهجمات الإلكترونية على المؤسسات المالية. كما سلطت دراسة أخرى قام بها Voas و Kshetri (2018) الضوء على التكلفة المرتفعة لخروقات البيانات في القطاع المصرفي، والتي تتجاوز في كثير من الأحيان الخسائر المالية المباشرة لتشمل تدهور السمعة وفقدان ثقة العملاء.

يلعب الذكاء الاصطناعي دوراً متزايد الأهمية في مجال أمن البيانات في القطاع المالي والمصرفي. فمن ناحية، تساهم تقنيات الذكاء الاصطناعي في تعزيز قدرات الكشف عن التهديدات والاستجابة لها بشكل استباقي. وقد أظهرت دراسة أجراها Fadlullah وآخرون (2017) أن استخدام خوارزميات التعلم العميق في أنظمة كشف التسلل يمكن أن يحسن بشكل كبير من دقة وسرعة اكتشاف الهجمات الإلكترونية. ومن ناحية أخرى، يمكن استغلال الذكاء الاصطناعي من قبل المهاجمين لتطوير هجمات أكثر تعقيداً وصعوبة في الكشف عنها، مما يشكل تحدياً جديداً لأمن البيانات. وقد حذرت دراسة لـ Brundage وآخرين (2018) من إمكانية استخدام الذكاء الاصطناعي لتعزيز قدرات الهجمات السيبرانية، مما يتطلب تطوير استراتيجيات دفاعية متقدمة

أما فيما يتعلق بواقع أمن المعلومات في البنوك السعودية، فقد أولت المملكة اهتماماً كبيراً بهذا الجانب في إطار رؤية 2030 وخطط التحول الرقمي. وقد أشارت دراسة أجراها Al-Baity (2023) إلى أن المؤسسات المالية السعودية تظهر طلباً كبيراً على توسيع استخدامها لحلول الذكاء الاصطناعي، خاصة في مجالات الامتثال وكشف الاحتيال. كما أكدت الدراسة على أهمية تطوير الكفاءات المحلية في مجال الذكاء الاصطناعي لمواجهة التحديات المتزايدة في أمن البيانات.

في ضوء هذه التطورات، تبرز الحاجة إلى دراسة معمقة لمخاطر الذكاء الاصطناعي على أمن البيانات في قطاع الخدمات المالية والبنوك في المملكة العربية السعودية، مع التركيز بشكل خاص على البنوك العامة. وتهدف هذه الدراسة إلى تحليل التحديات الحالية والمستقبلية، وتقييم فعالية الاستراتيجيات المتبعة لحماية البيانات، واقتراح إطار عمل متكامل لتعزيز أمن المعلومات في ظل التحول الرقمي المتسارع.

1.2 مشكلة الدراسة

في ظل التحول الرقمي السريع الذي يشهده قطاع الخدمات المالية والمصرفية، تزداد أهمية أمن البيانات بشكل كبير. تتعامل البنوك مع كميات هائلة من البيانات الحساسة التي تشمل معلومات مالية وشخصية للعملاء، مما يجعلها هدفاً رئيسياً للهجمات السيبرانية. على الرغم من الجهود الكبيرة المبذولة لتعزيز أمن البيانات، لا تزال التهديدات تتطور بشكل مستمر، مما يفرض تحديات جديدة على المؤسسات المالية. تكمن مشكلة البحث في الحاجة الملحة لفهم وتقييم المخاطر المرتبطة باستخدام الذكاء الاصطناعي في مجال أمن البيانات في البنوك العامة السعودية. هذا يتضمن دراسة التهديدات المحتملة، وتحليل الاستراتيجيات الحالية لحماية البيانات، وتقييم مدى جاهزية البنوك السعودية للتعامل مع هذه التحديات. كما تشمل المشكلة البحثية الحاجة إلى تطوير إطار عمل متكامل يمكن البنوك من الاستفادة من إمكانيات الذكاء الاصطناعي في تعزيز أمن البيانات، مع التخفيف من المخاطر المحتملة.

1.3 أهمية الدراسة

يهدف هذا البحث إلى تقديم فهم شامل لمخاطر الذكاء الاصطناعي على أمن البيانات في البنوك السعودية، وتقديم توصيات عملية لتعزيز الحماية ضد التهديدات السيبرانية. من خلال تحليل التهديدات الحالية والمستقبلية، وتقييم فعالية الاستراتيجيات الحالية، واقتراح إطار عمل متكامل، يسعى البحث إلى دعم البنوك السعودية في تحقيق أعلى مستويات الأمان في ظل التحول الرقمي المتسارع.

الأهمية العلمية للدراسة:

1. إثراء المعرفة الأكاديمية حول مخاطر الذكاء الاصطناعي على أمن البيانات في القطاع المصرفي.
2. تطوير إطار نظري لفهم العلاقة بين تقنيات الذكاء الاصطناعي وأمن المعلومات في البنوك.
3. المساهمة في سد الفجوة البحثية في مجال أمن البيانات المصرفية في سياق المملكة العربية السعودية.
4. توفير أساس علمي لدراسات مستقبلية حول استخدام الذكاء الاصطناعي في مجال الأمن السيبراني.
5. تحليل وتوثيق التحديات الأمنية الناشئة عن التطور السريع في تقنيات الذكاء الاصطناعي.

الأهمية التطبيقية للدراسة:

1. تقديم توصيات عملية للبنوك السعودية لتعزيز أمن بياناتها باستخدام تقنيات الذكاء الاصطناعي.
2. المساعدة في تطوير استراتيجيات فعالة لمواجهة التهديدات السيبرانية المتقدمة في القطاع المصرفي.
3. تحسين قدرة البنوك على حماية معلومات العملاء وتعزيز الثقة في الخدمات المصرفية الرقمية.
4. دعم صناع القرار في البنوك السعودية في اتخاذ قرارات مستنيرة حول استثمارات الأمن السيبراني.
5. المساهمة في تطوير إطار تنظيمي وقانوني لاستخدام الذكاء الاصطناعي في أمن البيانات المصرفية.
6. تعزيز قدرة القطاع المصرفي السعودي على الاستجابة للتهديدات الأمنية الناشئة وتقليل مخاطر الاختراقات.

7. دعم جهود التحول الرقمي في القطاع المالي السعودي من خلال تعزيز الأمن السيبراني.

1.4 أهداف الدراسة

تهدف هذه الدراسة إلى تقديم فهم شامل لمخاطر الذكاء الاصطناعي على أمن البيانات في البنوك السعودية،
وتسعى الدراسة لتحقيق الأهداف التالية:

- ✓ تحديد التهديدات السيبرانية الحالية والمستقبلية: كيف يمكن للذكاء الاصطناعي أن يسهم في تعزيز قدرات الهجمات السيبرانية على البنوك؟
- ✓ تحليل دور الذكاء الاصطناعي في الحماية من التهديدات: كيف يمكن استخدام تقنيات الذكاء الاصطناعي لتعزيز أمن البيانات وكشف التهديدات بشكل استباقي؟
- ✓ تقييم فعالية الاستراتيجيات الحالية: ما مدى فعالية الاستراتيجيات الحالية التي تتبعها البنوك السعودية في حماية البيانات من التهديدات السيبرانية؟

1.5 تساؤلات الدراسة

السؤال الرئيس للدراسة: ما مخاطر الذكاء الاصطناعي على أمن المعلومات في قطاع البنوك العامة في المملكة العربية السعودية في منطقة الرياض.

يتفرع عنه الأسئلة التالية:

- ✓ ما هي التهديدات السيبرانية الحالية والمستقبلية التي تواجه البنوك السعودية في مجال أمن البيانات؟
- ✓ كيف يمكن للذكاء الاصطناعي أن يسهم في تعزيز قدرات الهجمات السيبرانية على البنوك السعودية؟
- ✓ ما هي تقنيات الذكاء الاصطناعي التي يمكن استخدامها لتعزيز أمن البيانات في البنوك السعودية؟
- ✓ كيف يمكن توظيف الذكاء الاصطناعي للكشف عن التهديدات السيبرانية بشكل استباقي في القطاع المصرفي السعودي؟

✓ ما هي الاستراتيجيات الحالية التي تتبعها البنوك السعودية لحماية البيانات من التهديدات السيبرانية؟

✓ ما مدى فعالية الاستراتيجيات الحالية في مواجهة التهديدات السيبرانية المتطورة في البنوك السعودية؟

1.6 فروض الدراسة

بناءً على أهداف الدراسة المذكورة وأسئلة البحث المرتبطة بها، يمكن صياغة فروض الدراسة على النحو التالي:

1. الفرض الأول: يسهم الذكاء الاصطناعي في تعزيز قدرات الهجمات السيبرانية على البنوك العامة السعودية من خلال تطوير أساليب اختراق أكثر تعقيداً وصعوبة في الكشف عنها.
2. الفرض الثاني: يمكن استخدام تقنيات الذكاء الاصطناعي بفعالية لتعزيز أمن البيانات وكشف التهديدات بشكل استباقي في البنوك السعودية.
3. الفرض الثالث: الاستراتيجيات الحالية التي تتبعها البنوك السعودية في حماية البيانات من التهديدات السيبرانية غير كافية لمواجهة التحديات الناشئة عن تطور تقنيات الذكاء الاصطناعي.

1.7 مفاهيم الدراسة

الذكاء الاصطناعي: هو فرع من علوم الحاسوب يهتم بتطوير أنظمة قادرة على أداء مهام تتطلب عادةً ذكاءً بشرياً، مثل الإدراك البصري، التعرف على الكلام، صنع القرار، والترجمة بين اللغات.

أمن البيانات: مجموعة من الممارسات والتقنيات المستخدمة لحماية المعلومات الرقمية من الوصول غير المصرح به، والتسرب، والتخريب، أو السرقة طوال دورة حياة البيانات.

الخدمات المالية: مجموعة الخدمات التي تقدمها المؤسسات المالية، بما في ذلك البنوك وشركات التأمين وشركات الاستثمار، والتي تشمل إدارة الأموال والمعاملات المالية.

التحديات السيبرانية: أي محاولة ضارة لإلحاق الضرر أو تعطيل أنظمة الكمبيوتر والشبكات أو سرقة البيانات الحساسة باستخدام التقنيات الرقمية.

البنوك العامة: المؤسسات المالية المملوكة كلياً أو جزئياً للدولة والتي تقدم خدمات مصرفية للجمهور.

التعلم الآلي: فرع من الذكاء الاصطناعي يركز على تطوير خوارزميات وأنظمة قادرة على التعلم والتحسين من التجربة دون برمجة صريحة.

الهجمات السيبرانية: محاولات متعمدة لاختراق أنظمة المعلومات بهدف سرقة البيانات أو تعطيل العمليات أو إلحاق الضرر بالبنية التحتية الرقمية.

استراتيجيات الأمن السيبراني: الخطط والإجراءات المتبعة لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية.

1.8 المنطلقات النظرية للدراسة

بناءً على المعلومات المتوفرة في نتائج الدراسات السابقة والسياق العام للدراسة حول مخاطر الذكاء الاصطناعي على أمن البيانات في البنوك السعودية، يمكن تحديد المنطلقات النظرية التالية للدراسة:

1. نظرية الأمن السيبراني: تشكل هذه النظرية أساساً لفهم التهديدات الإلكترونية وآليات الحماية في البيئة الرقمية. وهي ضرورية لتحليل المخاطر التي تواجه البنوك في مجال أمن البيانات.

2. نظرية الذكاء الاصطناعي: تقدم إطاراً لفهم قدرات وتطبيقات الذكاء الاصطناعي، سواء في تعزيز الأمن أو في تطوير هجمات أكثر تعقيداً.

3. نظرية إدارة المخاطر: تساعد في تقييم وإدارة المخاطر المرتبطة باستخدام التكنولوجيا الحديثة في القطاع

المصرفي.

4. نظرية النظم: تسمح بدراسة البنوك كنظم معقدة تتفاعل مع بيئتها التكنولوجية والتنظيمية.
5. نظرية الاختراق والاختبار: تقدم أساساً لفهم أهمية إجراء تقييمات الاختراق المنتظمة للحد من التهديدات السيبرانية، كما ورد في المصدر.
6. نظرية التعلم الآلي: تساعد في فهم كيفية تطور أنظمة الذكاء الاصطناعي وقدرتها على التكيف مع التهديدات الجديدة.
7. نظرية أمن المعلومات: توفر إطاراً لفهم مبادئ حماية البيانات والمعلومات في البيئات الرقمية.
8. نظرية التحول الرقمي: تساعد في فهم التحديات والفرص التي تواجه البنوك في عملية التحول نحو الخدمات الرقمية.

2 الفصل الثاني: الإطار النظري والدراسات السابقة

2.1 الدراسات السابقة

دراسة معاندي وشابي (2021) بعنوان "دور تقنيات التكنولوجيا المالية في تعميم الخدمات المالية وتعزيز

الشمول المالي، الذكاء الاصطناعي نموذجًا"

هدفت الدراسة إلى استكشاف كيف يمكن لتقنيات التكنولوجيا المالية الحديثة، وخاصة الذكاء الاصطناعي، أن تسهم في تعزيز الشمول المالي وتوسيع نطاق الخدمات المالية للفئات الأقل دخلاً والمهمشة. اعتمدت الدراسة على منهجية تحليلية لتقييم تأثير الذكاء الاصطناعي على الشمول المالي، وشملت العينة مجموعة من المؤسسات المالية وغير المالية والحكومات على مستوى العالم. استُخدمت أدوات مثل استبيانات ومقابلات لجمع البيانات وتحليلها. لخصت الدراسة إلى أن الذكاء الاصطناعي له تأثير إيجابي كبير على الشمول المالي، حيث يساعد في اكتشاف المخاطر وقياسها وإدارتها، ويعالج مشكلة عدم تناسق المعلومات، ويدعم العملاء من خلال روبوتات المحادثة، ويكتشف الاحتيال ويعزز الأمن السيبراني. وتوصي الدراسة بأن تقوم المؤسسات المالية وغير المالية والحكومات بتبني وتوسيع نطاق استخدام الذكاء الاصطناعي لتحقيق الشمول المالي. ومن التحديات التي ذكرتها الدراسة، الحاجة إلى تطوير البنية التحتية التكنولوجية وتعزيز القدرات البشرية للتعامل مع هذه التقنيات، وضمان حماية البيانات والخصوصية في ظل استخدام الذكاء الاصطناعي. وتؤكد الدراسة على أهمية هذه التوصيات لضمان أن الفئات الضعيفة تستفيد من الخدمات المالية بشكل كامل وفعال.

دراسة Hinge (2022) بعنوان "Impact of Artificial Intelligence in Banking Sector"

هدفت الدراسة إلى استكشاف الذكاء الاصطناعي وأهميته في قطاع البنوك، مع التركيز على الأسباب التي تجعل الذكاء الاصطناعي ضروريًا للتنافسية في السوق العالمية. تناولت الدراسة الأثر العميق للثورة الصناعية 4.0 على القطاع المصرفي، مشيرة إلى أن التكنولوجيا لم تعد مقتصرة على استخدام الحواسيب في المعاملات المصرفية فحسب، بل تعدت ذلك إلى استخدام العملاء للخدمات المصرفية عبر الإنترنت والهواتف المحمولة لإجراء المعاملات اليومية. تطرقت الدراسة إلى خطوة أبعد من ذلك، وهي استخدام تقنيات متقدمة مثل الذكاء الاصطناعي، والروبوتات، ونظام البلوك تشين في البنوك، والتي تمثل ذروة التكنولوجيا. يُعرف الذكاء الاصطناعي بأنه الذكاء الذي تظهره الآلات، وهو ضروري للبنوك للبقاء في صدارة المنافسة العالمية. تشير الدراسة إلى أن العملاء المتمرسين تقنيًا يتوقعون تقنيات متقدمة في معاملاتهم اليومية مع البنوك لتوفير تجارب سلسة. ولتلبية هذه التوقعات والبقاء في مقدمة السوق المتغيرة باستمرار، يجب على البنوك أن تتوسع وتتكيف في أنشطتها للحفاظ على العملاء الحاليين وجذب عملاء جدد، خاصة الشباب. أظهرت الدراسة أن الذكاء الاصطناعي هو التكنولوجيا الأخيرة التي تتطور بسرعة في جميع أنحاء العالم. وتتضمن الأهداف الرئيسية للدراسة فهم معنى الذكاء الاصطناعي وأسبابه، وتقييم تأثيره على صناعة البنوك، وتحليل تأثيره على الموارد البشرية العاملة في القطاع المصرفي على مستوى العالم وفي الهند. اعتمدت الدراسة على منهجية تحليلية لفحص البيانات المتاحة وشملت عينة من البنوك التي تطبق تقنيات الذكاء الاصطناعي في عملياتها. تم تحليل تأثير هذه التقنيات على الخدمات المصرفية ورضا العملاء وكفاءة العمليات البنكية. أظهرت النتائج أن الذكاء الاصطناعي يعزز الكفاءة ويحسن تجربة العملاء، ولكنه يتطلب أيضًا تدريبًا مكثفًا للموظفين للتعامل مع التقنيات الجديدة. ومن التوصيات التي خرجت بها الدراسة، ضرورة تطوير البنية التحتية التكنولوجية للبنوك وتعزيز مهارات العاملين لمواكبة التطورات التكنولوجية. ومن المقترحات التي قدمتها الدراسة، إجراء مزيد من الأبحاث لتقييم تأثير الذكاء الاصطناعي على الأمن السيبراني في القطاع المصرفي وتحديد الفرص والتحديات التي قد تنشأ نتيجة لذلك. كما أوصت بضرورة الاستثمار في التدريب والتطوير المستمر للموظفين لضمان استعدادهم للتغيرات المستقبلية.

دراسة غوانمة وآخرون (2023) بعنوان "أثر نظم الذكاء الاصطناعي على تحسين جودة الخدمات المصرفية في

المصارف الإسلامية الأردنية"

هدفت الدراسة إلى استكشاف إمكانية استخدام نظم الذكاء الاصطناعي في تحسين جودة الخدمات المصرفية بالمصارف الإسلامية الأردنية، متضمنة ثلاثة بنوك رئيسية. اعتمدت الدراسة على المنهج الوصفي والتحليلي، وتم جمع البيانات عبر استبانة شملت ثلاثة أبعاد لنظم الذكاء الاصطناعي، ووُزعت على عينة من (150) فردًا من العاملين في البنوك المذكورة. أظهرت نتائج الدراسة أن نظم الذكاء الاصطناعي لها تأثير إيجابي وملاموس في تحسين جودة الخدمات المصرفية، وتوصلت إلى أن الأبعاد الثلاثة للذكاء الاصطناعي - النظم الخبيرة، تمثيل المعارف والاستدلال، والتعلم التلقائي - لها دور فعال في تعزيز الاعتمادية، الاستجابة، التعاطف، الأمان، والملموسية في الخدمات المصرفية. وأوصت الدراسة بضرورة تطوير المصارف الإسلامية لتواكب التقدم في مجال الأتمتة والرقمنة، وتحديثها بأحدث تقنيات الذكاء الاصطناعي لضمان الاستمرارية والتنافسية في السوق المصرفي. تُعد هذه الدراسة إضافة قيمة للمعرفة في مجال تطبيق الذكاء الاصطناعي بالمصارف الإسلامية، وتسليط الضوء على الفرص والتحديات المرتبطة بتبني هذه التقنيات في تحسين الخدمات المصرفية.

دراسة عمر النور (2023) بعنوان "دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر أمن

المعلومات المحاسبية"

تناولت الدراسة الأهمية المتزايدة للمراجعة الداخلية في ظل التحديات الراهنة التي تواجه أمن المعلومات المحاسبية، خاصةً في القطاع المصرفي الذي يشهد تطورًا مستمرًا ومخاطر متزايدة نتيجة للتقدم التكنولوجي. ركزت الدراسة على بنك الخرطوم كحالة دراسية لتحليل كيف يمكن للمراجعة الداخلية أن تساهم في تقليل هذه المخاطر وتعزيز الشفافية والدقة في التقارير المالية. استخدم الباحث منهجًا متعدد الأبعاد يجمع بين التاريخي، الاستنباطي الاستقرائي، والوصفي التحليلي، مما سمح بتحليل شامل للبيانات المجمعة من خلال

استبيانات تم توزيعها على عينة عشوائية من العاملين في البنك. تم تحليل البيانات باستخدام برنامج SPSS للكشف عن العلاقات الإحصائية بين المتغيرات المختلفة. أكدت النتائج على أهمية الاتجاهات الحديثة للمراجعة الداخلية في تحقيق الحوكمة الفعالة والشفافية المالية. وجدت الدراسة أن هناك علاقة إيجابية بين الالتزام بمعايير المحاسبة وحوكمة الشركات وبين جودة المعلومات المالية المقدمة، مما يساهم في تقليل مخاطر أمن المعلومات المحاسبية. من التحديات التي أبرزتها الدراسة، الحاجة إلى تعزيز الإجراءات الرقابية والمراجعة الداخلية لمواجهة التهديدات السيبرانية والحفاظ على سلامة البيانات المحاسبية. وأوصت الدراسة بضرورة تطبيق أفضل الممارسات في المراجعة الداخلية وتحديث الأنظمة المحاسبية لتتوافق مع التطورات التكنولوجية الحديثة. تُعد هذه الدراسة مساهمة مهمة في فهم كيف يمكن للمراجعة الداخلية أن تلعب دورًا حيويًا في تعزيز أمن المعلومات المحاسبية وتحقيق الشفافية المالية، وهو ما يعتبر أساسيًا للثقة في القطاع المصرفي.

دراسة غريد ونصري (2023) بعنوان "دور تحليل البيانات الضخمة المدعم بالذكاء الاصطناعي في تحسين عملية

التدقيق المالي، دراسة حالة شركة Presight لحلول الذكاء الاصطناعي"

سلطت الدراسة الضوء على أهمية تحليلات البيانات الضخمة المدعمة بالذكاء الاصطناعي في تعزيز كفاءة التدقيق المالي. تُظهر الدراسة كيف أن الانتشار الواسع للبيانات وتنوع مصادرها يستدعي استخدام أدوات متطورة تمكن من معالجة وتحليل هذه البيانات بفعالية، مما يساهم في تحسين الأداء المؤسسي عبر مختلف الوظائف. من خلال دراسة حالة شركة Presight في الإمارات، التي تعد رائدة في مجال تحليلات البيانات الضخمة المدعمة بالذكاء الاصطناعي، توصلت الدراسة إلى أن استخدام هذه التقنيات يوفر أساسًا متينًا لاتخاذ قرارات مالية مستنيرة. تستخدم الشركة منصة تدمج بين تحليلات البيانات الضخمة والذكاء الاصطناعي لتحليل وأتمتة كميات كبيرة من البيانات، مما يسهل عملية تحديد الانحرافات المالية، تصنيف المخاطر، والكشف عن الاحتيال بشكل أكثر سرعة ودقة مقارنةً بالأساليب التقليدية. أشارت الدراسة إلى أن هذا النهج يمكن المدققين من التركيز

بشكل أكبر على التحليل النوعي والتنبؤ بالتوجهات المستقبلية للمؤسسة، بدلاً من الغرق في البيانات الكمية. كما اقترحت الدراسة ضرورة تعزيز القدرات البشرية في التعامل مع التكنولوجيات الحديثة وعلوم البيانات لتحقيق الاستفادة القصوى من هذه الأدوات المتقدمة.

دراسة جمعة (2023) بعنوان "آليات التحول الرقمي وأثره على سلامة البيانات المالية (دراسة حالة مصرف الراجحي)"

تناولت الدراسة المنجزة حول مصرف الراجحي آليات التحول الرقمي وتأثيرها على سلامة البيانات المالية، مستندةً إلى التقرير السنوي للمصرف لعام 2022. الأهداف الرئيسية للدراسة تضمنت بيان واقع التحول الرقمي وأهميته، فوائده، والمعوقات التي تحول دون تطبيقه، بالإضافة إلى تحديد العلاقة بين التحول الرقمي وسلامة البيانات المالية. اعتمدت الدراسة على منهجية تحليلية لتقييم تأثير التحول الرقمي في مصرف الراجحي، وشملت العينة البيانات المستقاة من التقرير السنوي للمصرف. النتائج أظهرت أن مصرف الراجحي يستخدم التحول الرقمي لتعزيز حماية البيانات المالية وتحسين الشفافية والثقة في التعاملات، مما يساهم في تحسين جودة الخدمات المالية المقدمة. كما أن المصرف يولي اهتماماً بالخدمات المصرفية المفتوحة والمجهزة ببنية تحتية وخبرات عالية الكفاءة. التوصيات التي خرجت بها الدراسة تشدد على ضرورة تطبيق آليات التحول الرقمي لضمان حماية البيانات المالية وبناء الثقة بين مقدمي الخدمات المالية والمستفيدين. كما توصي بتنبيه قطاع المصارف إلى أهمية التحول الرقمي ودوره في تحسين العمليات المصرفية. الدراسة تبرز أهمية التحول الرقمي في العصر الحالي وتأثيره الإيجابي على القطاع المصرفي.

دراسة كاظم وعلائي (2023) بعنوان "تقنيات الذكاء الاصطناعي ودورها في الحد من الاحتيال المحاسبي"

تركز الدراسة على دور تقنيات الذكاء الاصطناعي، وبالأخص الانحدار اللوجستي، في الحد من الاحتيال المحاسبي، وهي قضية متنامية في العراق. تُظهر الدراسة أن الاحتيال المحاسبي يشكل تهديدًا كبيرًا يستلزم مواجهة فعالة. تُفند الدراسة الفرضية القائلة بأن تقنيات الذكاء الاصطناعي لا تملك القدرة على التقليل من الاحتيال المحاسبي في الوحدات الاقتصادية العراقية. من خلال التحليل، توصل الباحثون إلى استنتاجات مهمة تؤكد أن تطبيق تقنيات الذكاء الاصطناعي في المحاسبة سيؤدي إلى تطورات كبيرة في اكتشاف ومنع الاحتيال. تُعزز تقنية الانحدار اللوجستي من قدرة الأنظمة المحاسبية على الكشف عن الاحتيال بكفاءة وسرعة، مما يحسن من دقة المخرجات وأمان النظام. تُوصي الدراسة بضرورة استخدام وتطوير تقنيات الذكاء الاصطناعي، وخصوصًا الانحدار اللوجستي، لتعزيز الدفاع السيبراني وحماية الأنظمة الحاسوبية، والتصدي لمحاولات الاختراق والاحتيال، والحفاظ على سلامة أنظمة المعلومات المحاسبية. هذه الدراسة تُسلط الضوء على أهمية التكنولوجيا في تحسين العمليات المحاسبية وتأمين البيانات المالية.

دراسة El-Adawy (2023) بعنوان "Artificial Superintelligence and Arab National Security."

استكشفت الدراسة التحديات الأمنية المرتبطة بتقنيات الذكاء الاصطناعي الفائق في المنطقة العربية، مشيرةً إلى أن هذه التقنيات تفوق الذكاء البشري وتثير مخاوف متعلقة بالسيطرة والتحكم. تُبرز الورقة أهمية الاستعداد للتطورات التكنولوجية كجزء حاسم من الأمن الوطني العربي، مع التأكيد على أن الأنظمة الحالية لا تزال تعتمد على مراقبة البشر، مما يجعلها عرضة للتجاوز بسبب التطور المتسارع للخوارزميات. أشارت الدراسة إلى أن منظومة الأمن العربية لم تدرك بعد خطورة هذا التهديد، وتدعو إلى تبني سياسات استباقية لاحتواء المخاطر والتهديدات. تُحدد الورقة عقبات مثل ضعف البنية التحتية التكنولوجية وقيود الخصوصية على البيانات كعوائق أمام تقدم الدول العربية في مجال الذكاء الاصطناعي الفائق، مما قد يؤدي إلى تبعية تكنولوجية. كما

ناقشت الدراسة أيضًا مخاطر إساءة استخدام البيانات، اضطرابات سوق العمل، والاستعمار التكنولوجي، وتأثير القيم الغربية على تكنولوجيا الذكاء الاصطناعي. تُحذر من مخاطر الأسلحة المستقلة وجنود الذكاء الاصطناعي والتحديات الأخلاقية المرتبطة بها. لمواجهة هذه التحديات، أوصت الورقة بضرورة استثمار الدول العربية في البنية التحتية الرقمية، تطوير الكفاءات الوطنية في مجال الذكاء الاصطناعي، وضع الأطر التنظيمية، ضمان التمثيل العادل في التعامل مع البيانات، بناء آليات التحكم لموائمة القيم، وتعزيز التعاون الدولي لضمان استخدام آمن ومسؤول لتقنيات الذكاء الاصطناعي الفائق.

دراسة قشي (2023) بعنوان "الذكاء الاصطناعي في الصناعة 4.0، الفرص والتحديات المستقبلية"

سلطت الدراسة الضوء على الدور الثوري للذكاء الاصطناعي في قطاع التكنولوجيا والمعلومات، مؤكدةً على أنه يشكل نقطة تحول كبيرة في الصناعة العالمية. تُظهر الدراسة أن الذكاء الاصطناعي يدمج بشكل متزايد مع التطبيقات الصناعية المبتكرة، مما يُمكن المؤسسات الصناعية من تحسين أدائها التشغيلي والتجاري وزيادة المرونة والابتكار. هدفت الدراسة إلى تحديد الفرص والتحديات المستقبلية للذكاء الاصطناعي، وتقييم التكامل المتزايد للذكاء الاصطناعي مع التطبيقات الصناعية. اعتمدت الدراسة على تحليل الاتجاهات الحالية والمستقبلية للذكاء الاصطناعي في الصناعة، وعلى استعراض الدراسات والتقارير الصناعية العالمية. توصلت الدراسة إلى أن الذكاء الاصطناعي يُحسن الأداء التشغيلي والتجاري للمؤسسات الصناعية. كما أنه يُساهم في تنامي سوق الذكاء الاصطناعي الصناعي عالميًا. أوصت الدراسة باتباع نهج شامل ومتكامل لنشر الذكاء الاصطناعي الصناعي، وإجراء تغييرات تنظيمية وفنية وتكنولوجية لتنفيذ ناجح.

دراسة بدروني وكورائش (2024) بعنوان "دور الذكاء الاصطناعي في تحسين وتطوير الخدمات المالية على مستوى

البنوك - عرض تجارب بنكية دولية"

هدفت الدراسة إلى إبراز كيفية مساهمة تقنيات الذكاء الاصطناعي في تحسين وتطوير الخدمات المالية البنكية. استخدمت الدراسة منهجية تحليلية لتقييم آثار استخدام تقنيات الذكاء الاصطناعي على جودة وتطور الخدمات المالية، مع الإشارة إلى تجارب بنكية دولية كنماذج تطبيقية. خلصت الدراسة إلى أن الذكاء الاصطناعي يعزز نوعية الخدمات المالية المقدمة من البنوك، مما يسمح بتقديم خدمات مالية ومصرفية أسرع وأكثر كفاءة. كما أكدت على أن الذكاء الاصطناعي يوفر مستوى عالٍ من الأمان والأداء، ويسهل الوصول إلى المعلومات، ويضمن تكاليف معقولة للخدمات مقارنة بالطرق التقليدية. أضافت الورقة البحثية معلومات قيمة حول الإمكانيات الهائلة للذكاء الاصطناعي في إحداث ثورة في القطاع المالي والبنكي، مما يدعو إلى ضرورة تبني هذه التقنيات لتعزيز الكفاءة والابتكار في الخدمات المالية. تطرقت الورقة البحثية إلى مخاطر وتحديات استخدام الذكاء الاصطناعي في القطاع المالي والبنكي. أشارت إلى أنه بالرغم من الفوائد الكبيرة للذكاء الاصطناعي، هناك تحديات تتعلق بالأمان السيبراني وحماية البيانات. كما نوقشت الحاجة إلى تطوير أنظمة قادرة على مواجهة التهديدات الأمنية المتزايدة وضمان خصوصية المستخدمين. بالإضافة إلى ذلك، تم التأكيد على أهمية وضع إطار تنظيمي واضح يتعامل مع القضايا الأخلاقية المتعلقة بالذكاء الاصطناعي لضمان استخدامه بما يخدم مصلحة العملاء والمجتمع بشكل عام.

دراسة Al-Nasani (2024) بعنوان " The Impact of Using Artificial Intelligence Applications on

" Mitigating Risks in Banking Operations: A Field Study Applied to Al Rajhi and Al Ahli Banks

هدفت الدراسة لتقييم أثر استخدام تطبيقات الذكاء الاصطناعي في تخفيف المخاطر في العمليات المصرفية، مع التركيز على بنك الراجحي والبنك الأهلي. هدفت الدراسة إلى تحليل كيفية مساهمة تطبيقات الذكاء

الاصطناعي في الحد من المخاطر المصرفية وإعادة هندسة الأعمال المصرفية لحماية المصارف من التعثر المالي. اعتمدت الدراسة على منهجية تحليلية وصفية، حيث تم توزيع استبيانات إلكترونيًا على عينة من العاملين في فروع مختارة من البنوك المذكورة لجمع البيانات. توصلت الدراسة إلى أن تطبيقات الذكاء الاصطناعي لها دور مهم في تقليل مخاطر الأعمال المصرفية، ولكن استخدامها الفعلي ما زال محدودًا بسبب معوقات تقنية ومعلوماتية، بالإضافة إلى نقص المتخصصين في هذا المجال. وأبرزت الدراسة التحديات المتمثلة في عمليات الغش والتلاعب التي تؤثر على الاستقرار المالي للمصارف، مؤكدة على أهمية تطوير القدرات التقنية والمعلوماتية لتحقيق الاستفادة القصوى من الذكاء الاصطناعي في القطاع المصرفي. وأوصت الدراسة بضرورة تطوير القدرات التقنية والمعلوماتية للمصارف وتدريب المتخصصين لتحقيق الاستثمار الأمثل لتطبيقات الذكاء الاصطناعي في تخفيف المخاطر المصرفية.

2.1.1 التعليق على الدراسات السابقة

قمنا باستعراض الدراسات الحديثة في مجال تأثير الذكاء الاصطناعي على القطاع المصرفي حيث يشهد القطاع المصرفي ثورةً تقنيةً هائلةً بفضل الذكاء الاصطناعي، مما يُساهم في تحسين الخدمات المالية وتقديم تجارب مُبتكرة للعملاء. تُقدم هذه الدراسة تحليلًا موجزًا لبعض الدراسات الحديثة التي تتناول تأثير الذكاء الاصطناعي على مختلف جوانب القطاع المصرفي.

تناولت الدراسات السابقة مجموعة من الأهداف يمكن تلخيصها كما يلي:

1. تحسين وتطوير الخدمات المالية: دراسة بدروني وكورايش (2024): تُشير الدراسة إلى أن الذكاء الاصطناعي يُعزز جودة الخدمات المالية المقدمة من البنوك، من خلال تسريع وتيرة المعاملات، وتحسين الكفاءة، وتعزيز الأمان، وتسهيل الوصول إلى المعلومات، وتخفيض التكاليف.

2. تعزيز جودة الخدمات المصرفية الإسلامية: دراسة غوانمة وآخرون (2023): تُظهر الدراسة أن أنظمة الذكاء الاصطناعي تُساهم بشكل إيجابي في تحسين جودة الخدمات المصرفية في المصارف الإسلامية الأردنية، من خلال تعزيز الاعتمادية، والاستجابة، والتعاطف، والأمان، والملموسية.
 3. الحد من مخاطر أمن المعلومات المحاسبية: دراسة عمر النور (2023): تُركز الدراسة على دور المراجعة الداخلية في الحد من مخاطر أمن المعلومات المحاسبية في القطاع المصرفي، باستخدام اتجاهات حديثة مثل تحليل البيانات الضخمة والذكاء الاصطناعي.
 4. تحسين عملية التدقيق المالي: دراسة غريد ونصري (2023): تُوضح الدراسة كيف يُمكن لتحليلات البيانات الضخمة المدعومة بالذكاء الاصطناعي تعزيز كفاءة التدقيق المالي، من خلال تحليل كميات كبيرة من البيانات وتحديد الانحرافات المالية وتصنيف المخاطر والكشف عن الاحتيال بدقة وسرعة.
 5. تخفيف المخاطر في العمليات المصرفية: دراسة: Al-Nasani (2024) تُقيّم الدراسة تأثير تطبيقات الذكاء الاصطناعي في تخفيف المخاطر في العمليات المصرفية، وتُشير إلى دورها في الحد من مخاطر الأعمال المصرفية وإعادة هندسة العمليات لحماية المصارف من التعثر المالي.
 6. تعميم الخدمات المالية: دراسة معاندي وشابي (2021): تُناقش الدراسة دور تقنيات التكنولوجيا المالية، بما في ذلك الذكاء الاصطناعي، في تعميم الخدمات المالية وتقديمها لمناطق جغرافية جديدة وزيادة الشمول المالي.
- كما نلاحظ تُظهر الدراسات الحديثة أن الذكاء الاصطناعي يُحدث ثورةً في القطاع المصرفي من خلال تحسين الخدمات المالية، وتعزيز جودة الخدمات المصرفية الإسلامية، والحد من مخاطر أمن المعلومات المحاسبية، وتحسين عملية التدقيق المالي، وتخفيف المخاطر في العمليات المصرفية، وتعميم الخدمات المالية.

أوجه الاتفاق مع الدراسات السابقة

تتفق الدراسات الحديثة التي تم استعراضها في التأكيد على أن الذكاء الاصطناعي يُحدث تأثيرًا عميقًا على مختلف جوانب القطاع المصرفي، وتشمل النواحي التالية:

- تحسين الخدمات المالية: توفر تطبيقات الذكاء الاصطناعي مثل الروبوتات المحادثة والذكاء الاصطناعي التنبؤي والتعلم الآلي للعملاء تجربةً شخصيةً مُحسَّنة، وتُساهم في تسريع المعاملات، وتُعزز كفاءة العمليات، وتُقدم خدماتٍ ماليةً مُبتكرةً.
 - تعزيز الامتثال والتحكم في المخاطر: يُمكن للذكاء الاصطناعي تحليل كميات هائلة من البيانات للكشف عن الاحتيال وغسل الأموال، وتقييم المخاطر الائتمانية، والامتثال للوائح المالية، مما يُقلل من المخاطر ويُعزز السلامة المالية.
 - تطوير منتجات وخدمات جديدة: يُمكن للذكاء الاصطناعي تمكين البنوك من تطوير منتجات وخدمات جديدة مُخصصة لاحتياجات العملاء، وتقديم عروضٍ مُخصصة، وتحديد فرص جديدة لزيادة الإيرادات.
 - تحسين كفاءة العمليات: يُمكن للذكاء الاصطناعي أتمتة المهام المُتكررة، وتقليل الأخطاء البشرية، وتحسين سير العمليات الداخلية، مما يؤدي إلى خفض التكاليف وتحسين الربحية.
 - تعزيز الشمول المالي: يُمكن لتطبيقات الذكاء الاصطناعي مثل الخدمات المصرفية عبر الهاتف المحمول وتقنيات التعرف على الوجه توسيع نطاق الوصول إلى الخدمات المالية، وتقديمها لمناطق جغرافية بعيدة، ودمج الفئات السكانية غير المُدرجة في النظام المالي.
- منهجية البحث: تستخدم الدراسات المذكورة منهجيات بحثية متنوعة، تشمل:
- الدراسات المسحية: جمع البيانات من خلال استطلاعات الرأي للمهنيين في القطاع المصرفي والعملاء لتقييم استخدام تطبيقات الذكاء الاصطناعي وآثارها.
- الدراسات الحالة: تحليل تطبيقات الذكاء الاصطناعي في بنوك محددة لفهم كيفية تأثيرها على العمليات والخدمات.

التحليلات التجريبية: اختبار تأثير تطبيقات الذكاء الاصطناعي على جوانب محددة من العمليات المصرفية، مثل خدمة العملاء أو الاكتشاف الاحتيالي.

التحليلات النظرية: استكشاف المفاهيم النظرية لتأثير الذكاء الاصطناعي على نماذج الأعمال المصرفية وسلوكيات العملاء.

نقاط القوة وحدود الدراسات: تُقدم الدراسات المُستعرضة نظرةً ثاقبةً لفهم تأثير الذكاء الاصطناعي على القطاع المصرفي، وتُسلط الضوء على فوائده وإمكانياته.

ومع ذلك، من المهم ملاحظة بعض نقاط القوة والحدود في هذه الدراسات:

- التركيز على جوانب محددة: تُركز بعض الدراسات على جوانب محددة من تأثير الذكاء الاصطناعي، مثل خدمة العملاء أو الاكتشاف الاحتيالي، مما قد لا يُقدم صورةً شاملةً للتأثير الكامل.
- الاختلافات في السياقات: قد تختلف نتائج الدراسات اعتمادًا على السياق المحدد للبنك أو المنطقة الجغرافية، مما قد يُعيق تعميم النتائج.
- التطورات المستمرة: يتطور مجال الذكاء الاصطناعي بوتيرةٍ سريعة، ونشر الدراسات قد لا يُواكب أحدث التطورات والتطبيقات.

2.2 الإطار النظري

2.3 المبحث الأول: الذكاء الاصطناعي

أولاً: الذكاء الاصطناعي وأمن البيانات في قطاع الخدمات المالية والبنوك :

يلعب الذكاء الاصطناعي دورًا متزايد الأهمية في قطاع الخدمات المالية والبنوك، حيث يستخدم في مجموعة واسعة من التطبيقات مثل التحليلات المالية المتقدمة، التداول الآلي، إدارة المحافظ الاستثمارية، والخدمات المصرفية الرقمية. ومع ذلك، فإن هذا الاعتماد المتزايد على الذكاء الاصطناعي ينطوي على مخاطر أمنية محتملة كاختراق البيانات الحساسة والتلاعب بالنتائج التحليلية. لذلك، يتزايد الاهتمام بوضع إطار تنظيمي قوي لحماية بيانات العملاء وتطوير آليات حوكمة وضوابط أمنية لاستخدام الذكاء الاصطناعي في هذا القطاع الحيوي. وتتضمن الحلول الأمنية تطبيق تقنيات التشفير المتقدمة، إجراءات الهوية والتحقق المتعددة، والتخطيط لاستمرارية الأعمال في حالات الطوارئ. (زهران، 2020)

مفهوم الذكاء الاصطناعي وتطبيقاته في القطاع المصرفي

الذكاء الاصطناعي (Artificial Intelligence - AI) هو مجال من علوم الحاسب يهدف إلى تطوير أنظمة وتقنيات قادرة على محاكاة الذكاء البشري وتقليد قدراته المعرفية في مختلف المجالات. ويشمل الذكاء الاصطناعي مجموعة متنوعة من التقنيات والأساليب، بما في ذلك التعلم الآلي (Machine Learning)، الشبكات العصبية (Neural Networks)، معالجة اللغة الطبيعية (Natural Language Processing)، الرؤية الحاسوبية (Computer Vision)، والتخطيط والاستدلال الآلي. (صاديق، ناصر، 2008)

في القطاع المصرفي والمالي، يتم توظيف الذكاء الاصطناعي في العديد من التطبيقات الحيوية، مثل التحليلات المالية المتقدمة لاكتشاف الاتجاهات والنماذج في البيانات، وتطوير نماذج التداول الآلي وإدارة المحافظ الاستثمارية، وتطبيقات الخدمات المصرفية الرقمية كالاعرف على الكلام والصور وتحليل السلوك المصرفي للعملاء. كما يساعد الذكاء الاصطناعي في مكافحة الغش والاحتيال المالي من خلال نماذج الاكتشاف المبكر

والتحليلات المتقدمة. وتعتبر هذه التطبيقات مهمة لتعزيز الكفاءة والخدمة المصرفية وتحسين تجربة العميل.

(البار، 2018)

يشهد قطاع الخدمات المالية والبنكية ثورة تقنية هائلة بفضل الذكاء الاصطناعي، حيث تُستخدم تقنياته المتطورة لتقديم منتجات وخدمات مبتكرة تُعزّز الكفاءة، وتُحسّن تجربة العملاء، وتُقلّل من المخاطر.

وهذه بعض المجالات الرئيسية لتطبيقات الذكاء الاصطناعي في هذا القطاع

1. خدمة العملاء:

✓ الدردشة الآلية (Chatbots): تُقدم خدمة عملاء على مدار الساعة وطوال أيام الأسبوع، وتُجيب

على الأسئلة، وتُحلّ المشاكل، وتُقدّم الدعم للعملاء بطريقة تفاعلية.

✓ التعرف على الصوت واللغة: يُمكن العملاء من التفاعل مع البنوك عبر الأوامر الصوتية، مثل:

الاستعلام عن الرصيد، وتحويل الأموال، ودفع الفواتير.

✓ تحليل المشاعر: يُقيّم مشاعر العملاء من خلال تحليل تعليقاتهم على وسائل التواصل الاجتماعي،

واستطلاعات الرأي، ومحادثات خدمة العملاء، مما يُساعد البنوك على فهم احتياجات العملاء

بشكل أفضل وتحسين تجربتهم. (عقيلي، ، 2013)

2. مكافحة الاحتيال:

✓ الكشف عن الاحتيال: يُحلّل كميات هائلة من البيانات للكشف عن الأنماط المشبوهة التي قد تُشير

إلى عمليات احتيال، مثل: معاملات البطاقات غير المعتادة، وطلبات القروض الاحتيالية.

✓ التحقق من هوية العملاء: يُستخدم تقنيات التعرف على الوجه وبصمات الأصابع للتحقق من هوية

العملاء بشكل آمن ودقيق، مما يُقلّل من مخاطر الاحتيال وانتحال الهوية.

مكافحة غسل الأموال: يُراقب المعاملات المالية للكشف عن الأنشطة المشبوهة التي قد تُشير إلى غسل الأموال، ويُساعد في الامتثال للقوانين واللوائح المتعلقة بمكافحة غسل الأموال.

3. إدارة المخاطر:

✓ تقييم المخاطر الائتمانية: يُحلّل البيانات المالية والمعلومات الشخصية للمقترضين لتقييم قدرتهم

على سداد القروض، مما يُساعد البنوك على اتخاذ قرارات إقراضية أكثر ذكاءً.

✓ إدارة المخاطر الاستثمارية: يُحلّل البيانات السوقية وعوامل الاقتصاد الكلي لتقييم المخاطر

المرتبطة بالاستثمارات، ويُساعد في بناء محافظ استثمارية أكثر كفاءة. (النعيمي، التميمي، 2110)

✓ التنبؤ بالمخاطر: يُستخدم نماذج التعلم الآلي للتنبؤ بالمخاطر المستقبلية، مثل: مخاطر الائتمان،

ومخاطر السوق، ومخاطر التشغيل، مما يُساعد البنوك على اتخاذ خطوات استباقية للتخفيف

من هذه المخاطر. (لفتالوي، 2020)

4. تقديم المشورة المالية:

✓ مستشارون ماليون افتراضيون: يُقدمون نصائح مالية مخصصة للعملاء بناءً على احتياجاتهم

وأهدافهم المالية، وذلك باستخدام خوارزميات الذكاء الاصطناعي.

✓ إدارة الثروات: تُساعد في إدارة محافظ استثمارات العملاء وتقديم توصيات استثمارية مخصصة

بناءً على ملفاتهم الشخصية واحتياجاتهم من المخاطر.

✓ التخطيط المالي: يُساعد العملاء على وضع خطط مالية طويلة الأجل لتحقيق أهدافهم، مثل:

تقاعدهم، وتعليم أطفالهم، وشراء منزل. (الشواورة، 2013)

5. تحسين العمليات:

✓ الأتمتة: يُمكن أتمتة العديد من المهام المُستهلكة للوقت، مثل: معالجة المعاملات، وإدخال البيانات، وخدمة العملاء، مما يُقلّل من التكاليف ويُحسّن الكفاءة.

✓ التحليل التنبؤي: يُستخدم للتنبؤ بالطلب على المنتجات والخدمات، مما يُساعد البنوك على تحسين إدارة المخزون وتقديم تجربة أفضل للعملاء.

اكتشاف الفرص: يُحلّل البيانات للعثور على فرص جديدة لزيادة الإيرادات وتحسين الربحية.

مزايا استخدام الذكاء الاصطناعي في الخدمات المالية والبنكية :

✓ تحسين تجربة العملاء:

- تقديم خدمة عملاء أسرع وأكثر كفاءة ودقة.
- تخصيص المنتجات والخدمات لتلبية احتياجات العملاء الفردية.
- توفير إمكانية الوصول إلى الخدمات المالية على مدار الساعة طوال أيام الأسبوع.(ادم، 2010)

✓ زيادة الكفاءة:

- أتمتة المهام المُستهلكة للوقت، مما يُقلّل من التكاليف ويُحسّن الإنتاجية.
- تحسين دقة معالجة المعاملات والتقليل من الأخطاء.
- تسريع عملية اتخاذ القرار.

✓ تخفيض المخاطر:

- الكشف عن الاحتيال ومنع غسل الأموال.

– تقييم مخاطر الائتمان والاستثمار بشكل أفضل.

– تحسين الامتثال للقوانين واللوائح. (صالح، 2012)

✓ خلق فرص جديدة:

– تطوير منتجات وخدمات جديدة مبتكرة.

– استهداف عملاء جدد.

– توسيع نطاق الوصول إلى الخدمات المالية.

ومع ذلك، يجب بعض التحديات المرتبطة باستخدام الذكاء الاصطناعي في الخدمات المالية والبنكية:

مخاوف الخصوصية والأمان: حماية بيانات العملاء الشخصية والمحافظة عليها أمرٌ ضروري.

التحيز الخوارزمي: ضمان أن تكون الخوارزميات المستخدمة عادلة وغير متحيزة. قبول العملاء: التغلب على

مخاوف العملاء بشأن استخدام الذكاء الاصطناعي في إدارة أموالهم. التأثير على الوظائف: قد تؤدي أتمتة المهام

إلى فقدان بعض الوظائف (ماهر، 2002)

تأثير الذكاء الاصطناعي على العمليات المصرفية:

يحدث الذكاء الاصطناعي ثورة هائلة في قطاع الخدمات المصرفية، حيث يُمكنه أتمتة العديد من المهام، وتحسين

كفاءة العمليات، وتقديم منتجات وخدمات جديدة مُبتكرة.

ومن بعض التأثيرات الرئيسية للذكاء الاصطناعي على العمليات المصرفية: (السيد، 1999)

1. أتمتة المهام: يمكن للذكاء الاصطناعي أتمتة العديد من المهام المُستهلكة للوقت، مثل:

— معالجة المعاملات، إدخال البيانات، خدمة العملاء، مما يؤدي إلى: خفض التكاليف، تحسين الإنتاجية، تقليل الأخطاء (ابراهيم، 2012)

2. تحسين كفاءة العمليات: يمكن للذكاء الاصطناعي تحسين كفاءة العمليات المصرفية من خلال:

— تحليل البيانات للكشف عن الأنماط واتخاذ قرارات أفضل

— التنبؤ بالطلب على المنتجات والخدمات وتلبية احتياجات العملاء بشكل أفضل

— إدارة المخاطر بشكل أكثر فعالية (اليازوري، 2008)

3. تقديم منتجات وخدمات جديدة: يُمكن للذكاء الاصطناعي تمكين البنوك من تقديم منتجات وخدمات جديدة مُبتكرة، مثل:

— حسابات مخصصة تناسب احتياجات العملاء الفردية

— أدوات إدارة الثروات المتقدمة (ادريس، المرسى، 2003)

— خدمات الاستشارة المالية المُخصصة

4. تحسين تجربة العملاء: يُمكن للذكاء الاصطناعي تحسين تجربة العملاء من خلال:

— تقديم خدمة عملاء أسرع وأكثر كفاءة ودقة

— تخصيص المنتجات والخدمات لتلبية احتياجات العملاء

— توفير إمكانية الوصول إلى الخدمات المصرفية على مدار الساعة طوال أيام الأسبوع (مرسي واخرون 2007)

أمثلة على تطبيقات الذكاء الاصطناعي في العمليات المصرفية:

- ✓ مكافحة الاحتيال: استخدام خوارزميات التعلم الآلي للكشف عن المعاملات الاحتيالية ومنعها.
- ✓ إدارة المخاطر: تحليل البيانات لتقييم مخاطر الائتمان والاستثمار بشكل أفضل.
- ✓ خدمة العملاء: استخدام روبوتات الدردشة (Chatbots) للإجابة على أسئلة العملاء وحل مشاكلهم.
- ✓ التحقق من هوية العملاء: استخدام تقنيات التعرف على الوجه وبصمات الأصابع للتحقق من هوية العملاء.
- ✓ التخطيط المالي: مساعدة العملاء على وضع خطط مالية لتحقيق أهدافهم. (حريم، 2006)

المبحث الثاني: أمن المعلومات في القطاع المصرفي:

يُعدّ أمن المعلومات في القطاع المصرفي ذا أهمية قصوى، حيثُ تُصبح فيه البيانات والمعاملات المالية عرضةً لخطر السرقة والاحتيال والقرصنة.

لذا، تُطبّق البنوك والمؤسسات المالية مُختلف الإجراءات والتقنيات المتقدمة لحماية هذه المعلومات، وذلك لضمان:

سرية البيانات: منع الوصول غير المصرح به إلى المعلومات الحساسة، مثل: بيانات العملاء، وسجلات المعاملات، والمعلومات المالية.

سلامة البيانات: ضمان دقة البيانات ومُحافظتها على حالتها الأصلية دون أيّ تغيير أو تلف.

توفر البيانات: ضمان إمكانية الوصول إلى البيانات واستخدامها عند الحاجة، دون أيّ انقطاع أو تعطل.

ومن بعض العناصر الرئيسية لأمن المعلومات في القطاع المصرفي: (الزغبى، 2007)

1. تقييم المخاطر:

– تُحدّد البنوك جميع المخاطر المُحتملة التي قد تُهدّد أمن المعلومات، مثل: الهجمات الإلكترونية، والاختراقات، والبرمجيات الضارة، وفقدان البيانات.

– تُقيّم هذه المخاطر من حيث احتمالية حدوثها وشدة تأثيرها. (بني حمدان، ادريس، 2007)

2. الضوابط الوقائية:

– تُطبّق البنوك مجموعة من الضوابط الوقائية لمنع حدوث المخاطر، وتشمل:

– التحكم في الوصول: تحديد من يمكنه الوصول إلى المعلومات والأنظمة، وكيفية الوصول إليها. (الطيبي، 2013)

– التشفير: حماية البيانات من خلال تحويلها إلى شكل غير قابل للقراءة.

– جدران الحماية: منع الوصول غير المُصرح به إلى الشبكات والأنظمة.

– برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة: حماية الأنظمة من البرامج الضارة.

3. المراقبة والكشف عن التهديدات:

– تُراقب البنوك أنظمتها وشبكاتهما بشكلٍ مستمر للكشف عن أيّ نشاط مُريب أو مُخالف.

– تُستخدم تقنيات مُتقدمة، مثل:

– نُظم الكشف عن التطفّلات (IDS)

– نُظم منع التطفّلات (IPS)

— للكشف عن التهديدات والتصدّي لها في الوقت المناسب. (السماع، 1999)

4. الاستجابة للحوادث:

— تُعدّ البنوك خططاً مُسبقة للتعامل مع حوادث أمن المعلومات، مثل:

— خرق البيانات والهجمات الإلكترونية

تهدف هذه الخطط إلى: احتواء الضرر، استعادة البيانات، استئناف العمليات، منع تكرار الحادث(السماع، 2007،

5. التوعية والتدريب:

— تُدرّب البنوك موظفيها على ممارسات أمن المعلومات الجيدة، مثل:

— إنشاء كلمات مرور قوية، عدم مشاركة المعلومات الحساسة، الإبلاغ عن أيّ نشاط مُريب

6. الامتثال للقوانين واللوائح:

— تلتزم البنوك بالقوانين واللوائح المتعلقة بحماية البيانات، مثل:

— قانون حماية البيانات الشخصية، معايير أمن صناعة بطاقات الدفع (PCI DSS)

— يُعدّ أمن المعلومات مسؤولية مشتركة بين البنوك والمؤسسات المالية والعملاء من خلال التعاون والتزام

جميع الأطراف، يمكن ضمان حماية البيانات والمعاملات المالية بشكلٍ فعّال.

أهمية أمن البيانات في البنوك:

يُعدّ أمن البيانات في البنوك ذا أهمية قصوى، حيث تُصبح فيه البيانات والمعاملات المالية عرضةً لخطر السرقة والاحتيال والقرصنة.

وتكمن أهمية أمن البيانات في البنوك في النقاط التالية:

- حماية البيانات الحساسة: تشمل بيانات العملاء، مثل: الأسماء، والعناوين، وأرقام الحسابات، والمعلومات المالية. كما تشمل بيانات البنك، مثل: بيانات العمليات، والأنظمة المالية، والملكية الفكرية (الحري، 2010)
- الحفاظ على الثقة: تُعدّ ثقة العملاء ضرورية لنجاح أيّ بنك. يمكن أن تُؤدّي خروقات البيانات إلى فقدان ثقة العملاء، ممّا قد يُؤدّي إلى خسائر فادحة.
- الامتثال للقوانين: تُوجد العديد من القوانين واللوائح التي تُلزم البنوك بحماية بيانات العملاء. قد تواجه البنوك التي لا تمتثل لهذه القوانين غرامات كبيرة وعقوبات أخرى.
- الحفاظ على استمرارية العمل: يمكن أن تُؤدّي خروقات البيانات إلى تعطلّ العمليات المصرفية، ممّا قد يُؤدّي إلى خسائر كبيرة.
- الحفاظ على سمعة البنك: يمكن أن تُلحق خروقات البيانات ضرراً كبيراً بسمعة البنك، ممّا قد يُؤدّي إلى فقدان العملاء والمستثمرين.
- التحديات الأمنية الرئيسية في القطاع المصرفي: يواجه القطاع المصرفي العديد من التحديات الأمنية،

وتشمل بعض التحديات الرئيسية:

الهجمات الإلكترونية: تُصبح الهجمات الإلكترونية أكثر تعقيداً ودقّة، ممّا يُشكّل تهديداً كبيراً للبنوك.

البرمجيات الضارة: تُستخدم البرمجيات الضارة لسرقة البيانات أو تعطيل الأنظمة.

التصيد الاحتيالي: يُحاول المُحتالون خداع العملاء للحصول على معلوماتهم الشخصية أو المالية.

التحديات الداخلية: يمكن أن تُشكّل الإجراءات الخاطئة أو الضارة من قبل الموظفين تهديدًا لأمن البيانات.

امتثال البيانات: تُصبح قوانين ولوائح حماية البيانات أكثر تعقيدًا، ممّا يُشكل تحديًا للبنوك للامتثال لها.

نقص الوعي: قد لا يكون بعض الموظفين على دراية بممارسات أمن المعلومات الجيدة، ممّا قد يُعرض البيانات للخطر.

الأطر التنظيمية والقانونية لأمن المعلومات في البنوك السعودية:

تُخضع البنوك في المملكة العربية السعودية لعدد من الأطر التنظيمية والقانونية التي تُنظم أمن المعلومات، وتشمل بعض اللوائح الرئيسية (منصوري، 2015)

تُحدّد تعليمات أمن المعلومات الصادرة عن البنك المركزي السعودي متطلبات أمن المعلومات التي يجب على جميع البنوك في المملكة الالتزام بها. وتشمل متطلبات حماية البيانات، والتحكم في الوصول، وإدارة المخاطر، والكشف عن التهديدات، والاستجابة للحوادث.

— قانون حماية البيانات الشخصية: يُنظم هذا القانون كيفية جمع البيانات الشخصية واستخدامها وحمايتها. يُلزم البنوك بالحصول على موافقة العملاء قبل جمع بياناتهم الشخصية، واستخدامها فقط للغرض الذي تمّ جمعها من أجله.

— قانون مكافحة الجرائم الإلكترونية: يُجرّم هذا القانون الجرائم الإلكترونية، مثل: اختراق البيانات، الاحتيال الإلكتروني، سرقة الهوية يُحدّد عقوبات للمُدانين بهذه الجرائم. بالإضافة إلى هذه اللوائح، تُوجد العديد من المعايير الدولية التي يمكن للبنوك السعودية اتباعها لتحسين أمن المعلومات، مثل: معايير أمن صناعة بطاقات الدفع (PCI DSS)

معايير أمن صناعة بطاقات الدفع (PCI DSS) هي مجموعة من المعايير الأمنية التي وضعتها مجلس صناعة بطاقات الدفع (PCI Security Standards Council) للمساعدة في حماية بيانات حاملي بطاقات الدفع. (Johri، 1997)

تهدف هذه المعايير إلى تقليل مخاطر الاحتيال الإلكتروني، حماية بيانات بطاقات الدفع، ضمان الامتثال للقوانين واللوائح تتكون معايير PCI DSS من ستة أقسام رئيسية:

إدارة ثغرات الشبكة والأنظمة، وحماية بيانات حاملي بطاقات الدفع، والتحكم في الوصول إلى البيانات، وقياس ومراقبة الأنظمة، واختبار الشبكة والأنظمة بانتظام، وصيانة سياسة أمن المعلومات.

يجب على جميع المنظمات التي تُعالج أو تُخزّن أو تُنقل بيانات بطاقات الدفع الامتثال لمعايير PCI DSS. يمكن أن تُساعد معايير PCI DSS البنوك السعودية على:

حماية بيانات العملاء، تقليل مخاطر الاحتيال الإلكتروني، تحسين الامتثال للقوانين واللوائح، بناء الثقة مع العملاء، نظام إدارة الأمن والمعلومات (ISMS)، نظام إدارة الأمن والمعلومات (ISMS) هو نهج منهجي لإدارة أمن المعلومات في المنظمة.

يهدف نظام ISMS إلى: (Duarte، 2020)

حماية البيانات والمخزونات، تقييم المخاطر وإدارتها، ضمان الامتثال للقوانين واللوائح، تحسين كفاءة عمليات الأمن المعلوماتي. يتكون نظام ISMS من خطوات رئيسية:

- 1- تحديد نطاق النظام، 2- تقييم المخاطر، 3- تحديد الضوابط الوقائية، 4- تنفيذ الضوابط، 5- المراقبة والقياس
- 6- تحسين النظام

يمكن أن يُساعد نظام ISMS البنوك السعودية على:

1-تحسين أمن المعلومات بشكل عام،-2تقليل مخاطر خروقات البيانات،-3بناء الثقة مع العملاء والمستثمرين،-4تحسين كفاءة عمليات الأمن المعلوماتي.

التهديدات السيبرانية في القطاع المصرفي

يواجه القطاع المصرفي اليوم تهديدات سيبرانية متزايدة الخطورة والتعقيد مما يُشكل تحديات جمة للبنوك في جميع أنحاء العالم.

ومن أنواع التهديدات السيبرانية التي تواجه البنوك وتتنور هذه التهديدات، وتأثير الذكاء الاصطناعي عليها.

أنواع التهديدات السيبرانية التي تواجه البنوك:(Banitaan، 2023)

- الاختراقات الإلكترونية: اختراق أنظمة الكمبيوتر والشبكات للوصول إلى البيانات الحساسة،
مثل: بيانات العملاء المعلومات المالية الملكية الفكرية
 - البرمجيات الضارة: برامج ضارة تُستخدم لسرقة البيانات أو تعطيل الأنظمة، مثل: برامج
الفدية برامج التجسس الفيروسات
 - الهجمات الإلكترونية: هجمات تهدف إلى تعطيل أو تدمير أنظمة الكمبيوتر والشبكات، مثل:
هجمات رفض الخدمة (DoS)، هجمات رفض الخدمة الموزعة (DDoS)
 - التصيد الاحتيالي: محاولات خداع العملاء للحصول على معلوماتهم الشخصية أو المالية،
مثل: رسائل البريد الإلكتروني الاحتيالية مواقع الويب المزيفة مكالمات الهاتف الاحتيالية
 - التهديدات الداخلية: إجراءات ضارة من قبل الموظفين، مثل: السرقة، التجسس، التخريب
- (Almonte، 2023).

- الهندسة الاجتماعية: استغلال المشاعر الإنسانية لخداع الأشخاص للكشف عن معلومات حساسة أو اتخاذ إجراءات ضارة.

تطور التهديدات السيبرانية وتأثير الذكاء الاصطناعي فتزداد التهديدات السيبرانية تعقيدًا ودقةً. يُصبح مهاجمو الإنترنت أكثر ذكاءً واستخدامًا لتقنيات متقدمة مما يُشكل تحديًا أكبر للبنوك في حماية أنظمتها وبياناتها.

يلعب الذكاء الاصطناعي دورًا متزايدًا في التهديدات السيبرانية يُستخدم الذكاء الاصطناعي من قبل المهاجمين لتطوير برامج ضارة أكثر ذكاءً وشن هجمات أكثر استهدافًا ودقة. كما يُستخدم الذكاء الاصطناعي في مكافحة التهديدات السيبرانية،

حيث تُطور البنوك أنظمة ذكية للكشف عن التهديدات والاستجابة لها بشكل أسرع وأكثر كفاءة. (Machine، 2021)

تأثير الذكاء الاصطناعي على مكافحة التهديدات السيبرانية:

- تحليل البيانات: يُمكن للذكاء الاصطناعي تحليل كميات هائلة من البيانات للكشف عن الأنماط والسلوكيات المشبوهة التي قد تُشير إلى وجود تهديد سيبراني.
- الكشف التلقائي عن التهديدات: يُمكن للأنظمة المُستندة إلى الذكاء الاصطناعي الكشف عن التهديدات السيبرانية في وقت مبكر والاستجابة لها بشكل أسرع من تدخل الإنسان.
- التنبؤ بالتهديدات: يُمكن للذكاء الاصطناعي تحليل البيانات والتنبؤ بالتهديدات السيبرانية المحتملة قبل حدوثها، مما يسمح للبنوك باتخاذ إجراءات وقائية. (Huang، 2020).

دراسة حالة البنوك العامة في المملكة العربية السعودية:

تُعدّ البنوك العامة في المملكة العربية السعودية ركيزة أساسية للاقتصاد الوطني وتلعب دورًا محوريًا في دعم التنمية المستدامة وتمكين مختلف القطاعات. يلعب قطاع الخدمات المالية والبنوك في المملكة العربية السعودية دورًا حيويًا في دعم التنمية الاقتصادية وتحقيق الرؤية 2030.

يتمتع هذا القطاع ب:

- شبكة واسعة من المؤسسات المالية: تضم أكثر من 20 بنكًا تجاريًا، و10 بنوك إسلامية، وشركات تأمين، وشركات استثمارية.
- سوق مالي مُتطور: يتميز بوجود سوق الأسهم السعودي (تداول) وسوق الصناديق الاستثمارية.
- تنظيم رقابي فعال: يُشرف عليه البنك المركزي السعودي، هيئة السوق المالية.

تلعب البنوك العامة في المملكة دورًا هامًا في:

- تمويل التنمية الاقتصادية: من خلال تقديم قروض للشركات والأفراد ودعم المشاريع الاستثمارية.
- تعزيز الشمول المالي: من خلال تقديم خدمات مصرفية مُيسرة، للأفراد ذوي الدخل المحدود والمقيمين في المناطق الريفية.
- دعم الابتكار وريادة الأعمال: من خلال تقديم تمويل وخدمات استشارية للشركات الناشئة.
- الحفاظ على الاستقرار المالي: من خلال المشاركة في عمليات السوق المفتوحة وإدارة الاحتياطيات الأجنبية.

تواجه البنوك العامة في المملكة بعض التحديات، منها: (Sharma, 2021) & Mahto (

- المنافسة المتزايدة من قبل البنوك المحلية والأجنبية.
 - التغيرات في المشهد التنظيمي تتطلب التكيف المستمر والامتثال.
 - الحاجة إلى الابتكار لتلبية احتياجات العملاء المتطورة.
 - اكتساب المواهب لجذب كفاءات مهنية عالية.
 - التعامل مع المخاطر السيبرانية: لحماية البيانات والأنظمة.
- على الرغم من هذه التحديات، تتمتع البنوك العامة في المملكة بفرص نمو كبيرة، مدفوعة ب:
- النمو الاقتصادي المتوقع في المملكة.
 - الشمول المالي الذي تسعى المملكة لتحقيقه.
 - التكنولوجيا المالية التي تُقدم فرصًا جديدة للابتكار.
 - التوسع الإقليمي من خلال الاستحواذ على أو الدخول في شراكات مع بنوك في دول أخرى.
 - الاستفادة من خلال تقديم منتجات وخدمات، تُساهم في تحقيق أهداف الاستدامة.

مخاطر الذكاء الاصطناعي في البنوك السعودية: (Henke & Miremad 2018)

يُعدّ استخدام الذكاء الاصطناعي في البنوك السعودية سلاحًا ذا حدين، حيث يُقدم من ناحية فرصًا كبيرة لتحسين الكفاءة والابتكار، ولكنه يُشكل من ناحية أخرى مخاطر قد تُهدد الأمن المالي واستقرار النظام المصرفي.

دعونا نُلقي نظرة على بعض أهم مخاطر الذكاء الاصطناعي التي تواجهها البنوك السعودية:

1. المخاطر التشغيلية:

- الاعتماد على الخوارزميات: قد تؤدي الاعتمادية المفرطة على خوارزميات الذكاء الاصطناعي إلى اتخاذ قرارات خاطئة أو غير عادلة مما قد يلحق الضرر بالعملاء ويُعرض البنك للمخاطر القانونية.
- الثغرات الأمنية: قد تصبح أنظمة الذكاء الاصطناعي عرضة للاختراق أو الهجمات السيبرانية، مما قد يؤدي إلى سرقة البيانات أو تعطيل العمليات.
- الخطأ البشري: قد يؤدي سوء فهم أو إدخال بيانات خاطئة إلى أنظمة الذكاء الاصطناعي إلى نتائج كارثية.

2. المخاطر المالية:

- التمويل غير المنظم: قد تُستخدم تقنيات الذكاء الاصطناعي لتسهيل عمليات التمويل غير المنظم أو غسل الأموال، مما قد يُعرض البنك للمخاطر المالية والقانونية.
- الاحتيال: قد تُستخدم تقنيات الذكاء الاصطناعي لابتكار أساليب احتيال جديدة أكثر تعقيداً، مما قد يُصعب على البنوك اكتشافها ومنعها.
- تقلبات السوق: قد تُستخدم تقنيات الذكاء الاصطناعي للتلاعب بالأسواق المالية أو الاستفادة من تقلباتها، مما قد يؤدي إلى خسائر مالية كبيرة للبنوك.

3. المخاطر الأخلاقية:

- التحيز والتمييز: قد تؤدي خوارزميات الذكاء الاصطناعي إلى التحيز ضد بعض فئات العملاء أو اتخاذ قرارات تمييزية مما قد يلحق الضرر بسمعة البنك ويُعرضه للمساءلة القانونية.
- قلة الشفافية: قد يصعب فهم كيفية عمل خوارزميات الذكاء الاصطناعي واتخاذ قرارات بشأنها مما قد يُثير قلق العملاء ويُؤدي إلى فقدان الثقة. (Netw. 2009)

- استخدام البيانات الشخصية: قد تُستخدم بيانات العملاء الشخصية دون موافقتهم أو علمهم لغرض الإعلانات المُوجهة أو لأغراض أخرى، ممّا قد يُخالف قواعد الخصوصية.

4. المخاطر الاستراتيجية:

- التخلف عن الركب: قد تُواجه البنوك التي لا تُواكب أحدث تطورات الذكاء الاصطناعي خطر فقدان ميزتها التنافسية وربما الخروج من السوق.
- التكاليف العالية: قد تتطلب الاستثمارات في تقنيات الذكاء الاصطناعي وبنى تحتية جديدة تكاليف مالية كبيرة، ممّا قد يُشكل عبئًا على بعض البنوك.
- ندرة المواهب: قد تواجه البنوك صعوبة في جذب الكفاءات المهنية القادرة على تطوير واستخدام تقنيات الذكاء الاصطناعي بفعالية. (Zimmermann، 2012)

استراتيجيات حماية البيانات في البنوك السعودية:

تُدرّك البنوك السعودية أهمية حماية بيانات عملائها وتواجه تحديات كبيرة في ظل التطورات التكنولوجية المتسارعة

والتهديدات السيبرانية المتزايدة. لذا، تُطبق البنوك السعودية استراتيجيات متعددة لحماية البيانات منها:

1. التزامات تنظيمية:

تُلزم الجهات التنظيمية، مثل البنك المركزي السعودي وهيئة حماية البيانات والخصوصية، البنوك باتباع معايير صارمة لحماية البيانات.

تتضمن هذه المعايير:

الحصول على موافقة العملاء على جمع واستخدام بياناتهم. تحديد أهداف واضحة لجمع البيانات واستخدامها. حماية البيانات من الوصول غير المصرح به أو الاستخدام غير المشروع. الإبلاغ عن خروقات البيانات للسلطات المختصة.(Maree، 2021)

2. تقنيات الحماية:

تُستخدم تقنيات حماية البيانات المتقدمة، مثل التشفير وتقنيات التحكم في الوصول، لحماية البيانات من الوصول غير المصرح به. تُطبق البنوك أيضًا أنظمة للكشف عن التهديدات والتعامل معها لمراقبة الشبكات والأنظمة بحثًا عن أي نشاط مشبوه.

3. التوعية والتدريب:

تُقدم البنوك تدريبات مُنظمة لموظفيها لتعريفهم بأفضل ممارسات حماية البيانات ومساعدتهم على اكتشاف الاحتيال والهجمات السيبرانية.

تُنظم البنوك حملات توعية لعملائها لتثقيفهم حول مخاطر مشاركة البيانات الشخصية وكيفية حماية معلوماتهم.

4. إدارة المخاطر:

تُقيم البنوك مخاطر حماية البيانات بشكلٍ دوري وتُضع خططًا للحد من هذه المخاطر.

تُشمل خطط إدارة المخاطر: تحديد الأصول الحساسة للبيانات. تقييم المخاطر التي تواجه هذه الأصول. وضع ضوابط للحد من هذه المخاطر، اختبار فعالية هذه الضوابط بشكلٍ دوري.

5. التعاون مع الجهات الخارجية:

تتعاون البنوك مع شركات متخصصة في مجال حماية البيانات للحصول على الدعم والخبرة. تشارك البنوك أيضًا المعلومات حول التهديدات السيبرانية مع البنوك الأخرى والجهات الحكومية.(Durairaj، 2022)

3 الفصل الثالث: الإطار المنهجي للدراسة

3.1 الإطار المنهجي للدراسة

3.1.1 منهج الدراسة:

ستعتمد هذه الدراسة على المنهج الوصفي التحليلي، وهو منهج بحثي يتيح للباحث جمع معلومات وبيانات دقيقة عن الظاهرة قيد الدراسة، ثم تحليلها للوصول إلى نتائج وتوصيات مفيدة. يتميز هذا المنهج بقدرته على دراسة الظواهر في سياقها الطبيعي وتفسير العلاقات بين متغيراتها.

3.1.2 مجتمع الدراسة:

مجتمع الدراسة يشمل جميع العاملين في القطاع المصرفي السعودي، بما في ذلك البنوك الخاصة والعامة. هذا الاختيار يضمن تغطية شاملة للقطاع المصرفي في المملكة العربية السعودية، مما يتيح فهماً أعمق للموضوع المدروس.

3.1.3 عينة الدراسة:

تم الاعتماد على عينة عشوائية من مجتمع الدراسة بحيث تشمل موظفين في البنوك السعودية على دراية بموضوع امن المعلومات.

تكونت عينة الدراسة من 99 موظفًا في البنوك وفيما يلي توصيفًا لها.

جدول 1: الخصائص الديموغرافية للعينة

العنصر	الفئات	التكرار	النسبة المئوية
العمر	25-34 سنة	22	22.2
	سنة 35-44	29	29.3
	سنة 45-54	48	48.5
الجنس	ذكر	68	68.7
	أنثى	31	31.3
المستوى التعليمي	بكالوريوس	73	73.7
	ماجستير	25	25.3
	دكتوراه	1	1.0
سنوات الخبرة	أقل من سنة	1	1.0
	1-5 سنوات	3	3.0
	6-10 سنوات	22	22.2
	11-15 سنوات	69	69.7
	16-20 سنة	3	3.0
	أكثر من 20 سنة	1	1.0
الوظيفة الحالية	خدمة عملاء	21	21.2
	محلل مالي	17	17.2
	مسؤول تقنية معلومات	31	31.3
	ادارة عليا	16	16.2
	مسؤول حسابات	3	3.0
	مدير ادارة	7	7.1
	مسؤول امن معلومات	1	1.0
	مدير فرع	3	3.0
البنك الذي تعمل به	البنك الاهلي السعودي	20	20
	البنك الأهلي	29	29
	الراجحي	18	18
	البنك السعودي	16	16
	العربي	4	4
	البلاد	1	1

نلاحظ من الجدول توزع العينة كما يلي:

من حيث العمر: بلغ عدد الأفراد الذين تتراوح أعمارهم بين 34 و 25 سنة (22) بنسبة (22.2%) بينما بلغ عدد الذين تتراوح أعمارهم بين 44 و 35 (29) بنسبة (29.3%) أما الذين تتراوح أعمارهم بين 54 و 45 (48) بنسبة (48.5%)

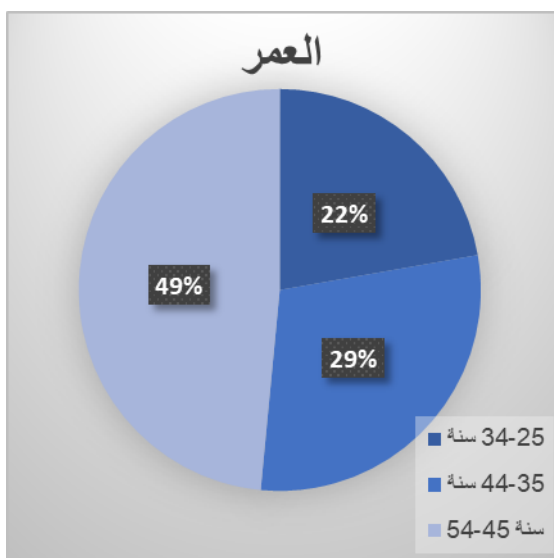
حيث عمر الجنس: بلغ عدد الذكور 68 بنسبة (68.7%) بينما عدد الاناث كان 31 بنسبة (31.3%)
من حيث المستوى التعليمي: بلغ عدد الذين كانوا من فئة البكالوريوس (73) بنسبة (73.7%) وبعدد أقل للذين كانوا من فئة طلاب الماجستير حيث كان عددهم 25 بنسبة (25.3%) وكانت أقل نسبة من فئة الدكتوراه حيث كان موظف واحد فقط.

من حيث سنوات الخبرة: ان الذين تتراوح خبرتهم بين 1-5 سنوات و 20-16 سنة كان عددهم بقيم متساوية 3 ثم الذين خبرتهم بين 10-6 سنوات كان عددهم 22 بنسبة (22.2%) ثم أعلى نسبة للذين خبرتهم بين 11-15 سنوات وكان عددهم 69 بنسبة (69.7%) وكانت أقل نسبة للذين كان خبرتهم أكثر من 20 سنة وأقل من سنة وعددهم واحد فقط.

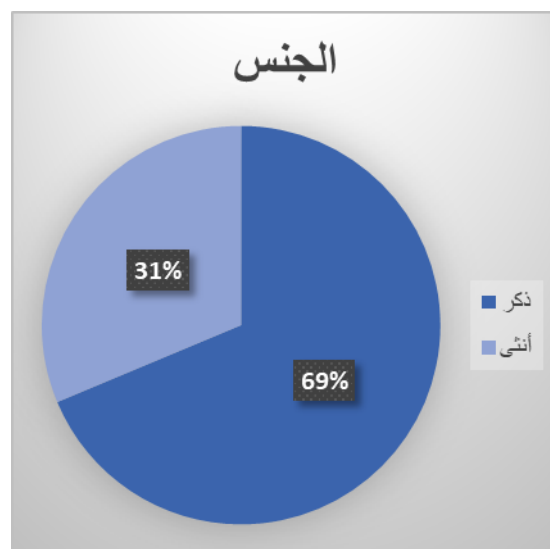
من حيث الوظيفة الحالية: بلغ أعلى عدد للذين يعملون مسؤول تقنية معلومات حيث كان عددهم 31 بنسبة (31.3%) بينما بلغ الذين يعملون 141 خدمة عملاء 21 بنسبة (21.2%) أما المحلل المالي والإدارة العليا كانوا بأعداد متقاربة 17 و 16 بنسب 16.2 و 17.2 ثم يليه الذين يعملون مدير إدارة بعدد 7 ونسبة 7.1 وبقيم متساوية للذين يعملون مسؤول حسابات ومدير فرع بقيم 3 وأقل قيمة كانت لمسؤول أمن المعلومات حيث كان موظف واحد

من حيث البنك الذي تعمل به: بلغ عدد الذين يعملون في البنك الأهلي 29 وفي البنك الراجحي 18 وفي البنك السعودي 16 في البنك العربي 4 وفي بنك البلاد 1

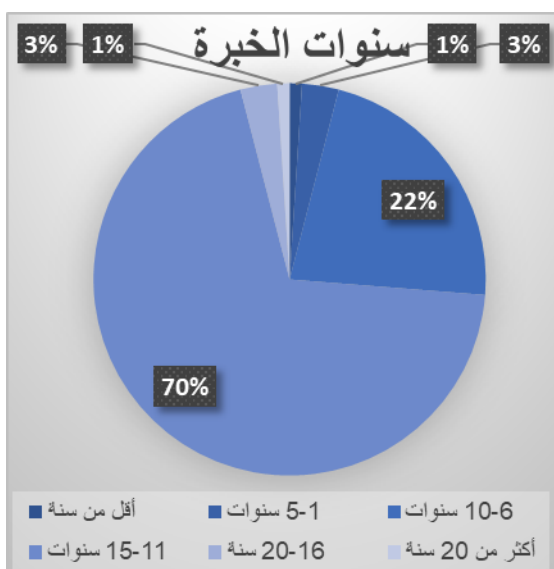
الأشكال البيانية التي تعبر عن الجدول السابق



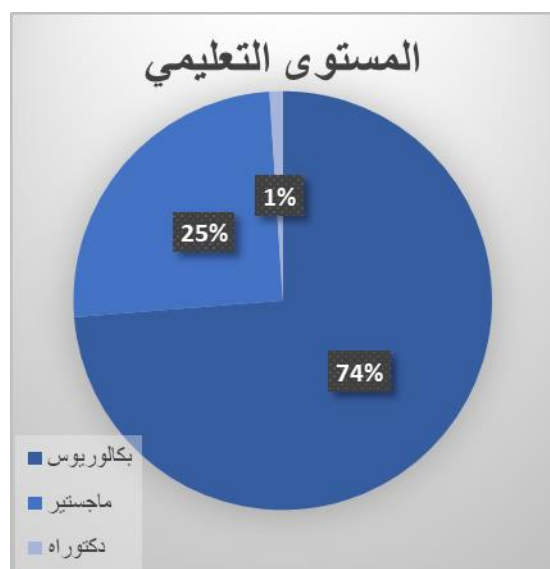
شكل 2: توزيع العينة وفق العمر



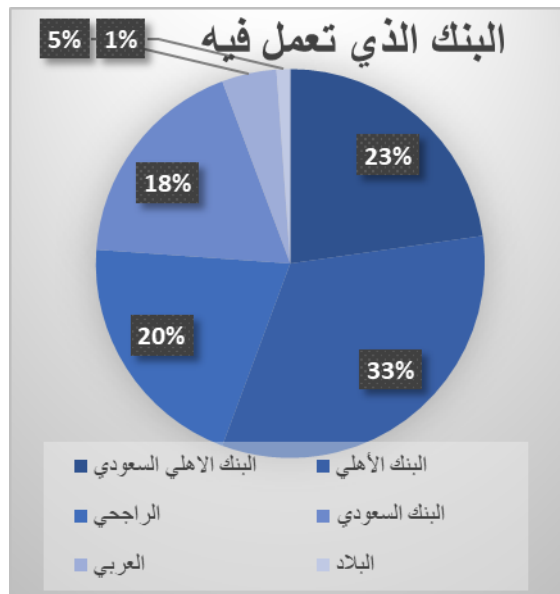
شكل 1: توزيع العينة وفق الجنس



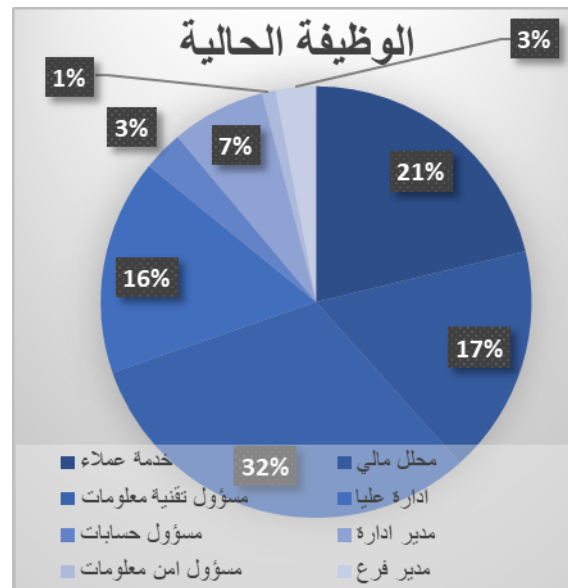
شكل 4: توزيع العينة وفق سنوات الخبرة



شكل 3: توزيع العينة وفق المستوى التعليمي



شكل 6: توزيع أفراد العينة وفق البنك



شكل 5: توزيع أفراد العينة وفق الوظيفة

3.2 أدوات جمع البيانات ومقاييس الدراسة

تتكون أداة جمع البيانات في هذه الدراسة الاستبانة. تتضمن الاستبانة مجموعة من المحاور للوصول إلى أهداف الدراسة. تعتمد الأسئلة على مقياس ليكرت الخماسي. وتكونت محاور الاستبانة مما يلي:

1. الوعي بالتهديدات السيبرانية:
 - مستوى الإدراك بالتهديدات الحالية والناشئة
 - فهم كيفية استغلال الذكاء الاصطناعي في الهجمات السيبرانية
2. استخدام الذكاء الاصطناعي في أمن البيانات:
 - مدى استخدام تقنيات الذكاء الاصطناعي في حماية البيانات
 - فعالية الحلول القائمة على الذكاء الاصطناعي في كشف التهديدات
3. تقييم الاستراتيجيات الحالية:
 - فعالية السياسات والإجراءات الحالية لأمن البيانات
 - تحديات تطبيق استراتيجيات الأمن السيبراني

صدق وثبات الاستبيان

صدق الاتساق الداخلي:

نقوم بحساب صدق الاتساق الداخلي عن طريق حساب معامل الارتباط بيرسون بين درجة كل عبارة ودرجة

المحور الذي تنتمي إليه، والجدول التالي يوضح النتائج:

جدول 2: معاملات الاتساق الداخلي بين العبارة والمحور الذي تنتمي إليه

السؤال	معامل بيرسون	فهم كيفية استغلال الذكاء الاصطناعي		مدى استخدام تقنية الذكاء الاصطناعي في حماية البيانات	
		السيبرانية	الهجمات	الاصطناعي	البيانات
1	0.804	1	0.888	1	0.919
2	0.891	2	0.967	2	0.926
3	0.727	3	0.942	3	0.860
4	0.943	4	0.950	4	0.887
5	0.676	5	0.963	5	0.877
فعالية الحلول القائمة على الذكاء الاصطناعي في كشف التهديدات					
فعالية الإجراءات والبيانات					
الحالية لأمن					
السيبرانية					
1	0.723	1	0.978	1	0.851
2	0.944	2	0.895	2	0.814
3	0.945	3	0.898	3	0.830
4	0.953	4	0.847	4	0.853
5	0.930	5	0.949	5	0.531

نلاحظ من الجدول أن جميع معاملات الترابط قوية موجبة وأكبر من 0.6 مما يدل على صدق جيد للاتساق

الداخلي.

جرى حساب ثبات الاستبيان عن طريق معاملات ألفا كرونباخ لكل محور من المحاور والجدول التالي يوضح

النتائج:

جدول 3: معاملات الثبات ألفا كرونباخ

المحاور	عدد العبارات	Alpha Cronbach
	5	0.85
مستوى الإدراك بالتهديدات الحالية والناشئة	5	0.96
فهم كيفية استغلال الذكاء الاصطناعي في الهجمات السيبرانية	6	0.96
مدى استخدام تقنيات الذكاء الاصطناعي في حماية البيانات	5	0.94
فعالية الحلول القائمة على الذكاء الاصطناعي في كشف التهديدات	5	0.96
فعالية السياسات والإجراءات الحالية لأمن البيانات	5	0.76
تحديات تطبيق استراتيجيات الأمن السيبراني	5	0.90

يظهر من الجدول أن معاملات ألفا كرونباخ مقوية وأكبر من 0.6 مما يدل على ثبات جيد للاستبانة.

3.3 مجالات الدراسة

المجال المكاني: البنوك العامة في المملكة العربية السعودية في منطقة الرياض.

المجال الزمني: العام الدراسي 2023-2024.

المجال البشري: الموظفين في البنوك العامة في الرياض.

3.4 المقاييس والاختبارات الإحصائية المقترح استخدامها

جرى استخدام برنامج Excel وبرنامج SPSS لتحليل البيانات التي تم جمعها في هذه الدراسة ومن الأساليب

الإحصائية اللازمة للوصول للنتائج ما يلي :

- المتوسطات الحسابية والانحرافات المعيارية والرتبة
- معاملات الارتباط بيرسون لحساب صدق الاتساق الداخلي للاستبيان
- معاملات ألفا كرونباخ لحساب ثبات الاستبيان
- التكرارات والنسب المئوية ومقاييس العلاقة أو الفروق بين المتغيرات

4 الفصل الرابع: تحليل البيانات والنتائج

عرض وتفسير النتائج:

الإجابة على تساؤلات الدراسة:

السؤال الأول: ما هي التهديدات السيبرانية الحالية والمستقبلية التي تواجه البنوك السعودية في مجال أمن

البيانات؟

للإجابة على هذا السؤال جرى تحليل بيانات المحور الأول من محاور الاستبيان، حيث تم حساب المتوسط

الحسابي والنسبة المئوية ودرجة ورتبة كل عبارة والجدول التالي يوضح نتائج التحليل:

جدول 4: مستوى الادراك بالتهديدات الحالية والناشئة

الرتبة	درجة التحقق	المتوسط الحسابي	مستوى الادراك بالتهديدات الحالية والناشئة
2	مرتفعة جداً	4.55	أنا على دراية بالتهديدات السيبرانية الحالية مثل هجمات الفدية (Ransomware) وهجمات التصيد الاحتيالي (Phishing).
3	مرتفعة جداً	4.46	أنا على دراية بالتهديدات السيبرانية المستقبلية المحتملة مثل الهجمات باستخدام الذكاء الاصطناعي لتوليد برامج ضارة متقدمة.
5	مرتفعة	4.15	مؤسستي توفر تدريبات منتظمة حول التهديدات السيبرانية بما في ذلك استخدام الذكاء الاصطناعي في الهجمات.
4	مرتفعة جداً	4.30	أنا على علم بالتهديدات السيبرانية التي تستهدف البنية التحتية المصرفية مثل هجمات DDoS (Service (Distributed Denial of
1	مرتفعة جداً	4.62	أدرك تأثير الهجمات السيبرانية على السمعة والثقة العامة بالبنك.
	مرتفعة	4.41	المحور الكلي

يتبين من الجدول بأن مستوى الادراك لدى موظفي الشركة للتهديدات الحالية والناشئة كان عالي حيث تحقق بدرجات مرتفعة لدى عبارات المحور حيث تحقق ذلك في العبارة الأخيرة بمتوسط حسابي 4.62 أما العبارة الأولى كانت بمتوسط أقل 4.55 ومن ثم العبارة الثانية بمتوسط 4.55 وبمتوسط يلها كان لصالح العبارة الرابعة حيث كانت قيمته 4.30 وأخيراً وأقل متوسط كان للعبارة الثالثة بقيمة 4.15 مما يدل على دراية الموظفين لتأثير الهجمات السيبرانية على السمعة والثقة كما رأينا في متوسط العبارة الأولى لهذا كان الموظفون غير موافقين على وجود تدريبات منتظمة وبالتالي الشركات تفتقر لتدريبات تتحدث حول التهديدات السيبرانية.

السؤال الثاني: ما هي التهديدات السيبرانية الحالية والمستقبلية التي تواجه البنوك السعودية في مجال أمن البيانات؟

للإجابة على هذا السؤال جرى تحليل بيانات المحور الأول من محاور الاستبيان، حيث تم حساب المتوسط الحسابي والنسبة المئوية ودرجة ورتبة كل عبارة والجدول التالي يوضح نتائج التحليل:

جدول 5: فهم كيفية استغلال الذكاء الاصطناعي للهجمات السيبرانية

الرتبة	درجة الأهمية	الانحراف المعياري	المتوسط الحسابي	فهم كيفية استغلال الذكاء الاصطناعي للهجمات السيبرانية
1	مرتفعة جداً	0.813	4.49	أدرك أن الذكاء الاصطناعي يمكن أن يستخدم لتوليد هجمات تصيد احتيالي (Phishing) ذكية وشخصية.
3.5	مرتفعة جداً	0.831	4.27	أفهم الطرق التي يمكن أن يستخدم فيها الذكاء الاصطناعي لاختراق الأنظمة المصرفية من خلال تحليل الثغرات بشكل سريع وذكي.

2	مرتفعة جداً	0.826	4.30	أعتقد أن استخدام الذكاء الاصطناعي يمكن أن يجعل هجمات القوة العمياء (Brute Force) أكثر فعالية وتعقيداً.
4	مرتفعة	0.915	4.20	أنا على علم بكيفية استخدام الذكاء الاصطناعي لتجاوز أنظمة الحماية التقليدية مثل الجدران النارية (Firewalls).
3.5	مرتفعة جداً	0.879	4.27	أفهم كيفية استخدام الذكاء الاصطناعي لتحليل بيانات العملاء واستهدافهم بشكل أكثر دقة في الهجمات السيبرانية.
	مرتفعة جداً	0.803	4.30	المقياس الكلي للعبارات الخاصة بفهم كيفية استغلال الذكاء الاصطناعي للهجمات السيبرانية

يتبين من الجدول بأن فهم كيفية استغلال الذكاء الاصطناعي للتهديدات الحالية والناشئة كان عالي حيث سجل أعلى مرتبة لدى عبارات المحور فكانت بمتوسط حسابي 4.49 تليه العبارة الثالثة بمتوسط 4.30 أما بالنسبة للعبارات الثانية والخامسة كانتا بمتوسطتين متساويتين 4.27 ومن ثم العبارة الثانية بمتوسط 4.55 وبمتوسط يلها كان لصالح العبارة الرابعة حيث كانت قيمته 4.30 وأخيراً وأقل متوسط كان للعبارة الرابعة بقيمة 4.20 مما يدل على ادراك الموظفين بأن الذكاء الاصطناعي يستخدم هجمات تصيد ذكية كما رأينا ذلك في العبارة الأولى ولكنهم لا يعلمون كيفية استخدام الذكاء الاصطناعي لتجاوز أنظمة الحماية.

السؤال الثالث: ما هي التهديدات السيبرانية الحالية والمستقبلية التي تواجه البنوك السعودية في مجال أمن

البيانات؟

للإجابة على هذا السؤال جرى تحليل بيانات المحور الأول من محاور الاستبيان، حيث تم حساب المتوسط

الحسابي والنسبة المئوية ودرجة ورتبة كل عبارة والجدول التالي يوضح نتائج التحليل:

جدول 6: مدى استخدام تقنية الذكاء الاصطناعي في حماية البيانات

الرتبة	درجة الأهمية	الانحراف المعياري	المتوسط الحسابي	مدى استخدام تقنية الذكاء الاصطناعي في حماية البيانات
3	مرتفعة	0.951	4.21	مؤسستي تستخدم تقنيات الذكاء الاصطناعي مثل التعلم الآلي (Machine Learning) للكشف عن النشاط غير المعتاد.
1	مرتفعة جداً	0.843	4.27	نستخدم أنظمة كشف التسلل (Intrusion Detection Systems) القائمة على الذكاء الاصطناعي لتحليل الأنشطة المشبوهة بشكل مستمر.
2	مرتفعة جداً	0.815	4.26	تساهم حلول الذكاء الاصطناعي في تحسين قدرة البنك على كشف التهديدات السيبرانية مثل هجمات الحرمان من الخدمة (DDoS) وهجمات الهندسة الاجتماعية (Social Engineering).
6	مرتفعة	0.888	3.81	لدينا تطبيقات ذكاء اصطناعي تعمل على تحليل البيانات في الوقت الحقيقي لرصد التهديدات السيبرانية المحتملة.
4	مرتفعة	0.728	4.00	نعتمد على تقنيات الذكاء الاصطناعي لتقييم نقاط الضعف في أنظمة الأمان وتحسينها بشكل مستمر.
5	مرتفعة	0.825	3.95	نستخدم الذكاء الاصطناعي لتحليل سلوك المستخدمين وكشف الأنماط الغير عادية التي قد تشير إلى اختراقات.
	مرتفعة	0.756	4.08	المحور ككل

يتبين من الجدول بأن مدى استخدام تقنية الذكاء الاصطناعي في حماية البيانات كان عالي حيث تحقق بدرجات جيدة لدى عبارات المحور حيث تحقق ذلك بالمرتبة الأولى في العبارة الثانية بمتوسط حسابي 4.27 وبمتوسط أقل نسبيا كان صالح العبارة الثالثة بقيمة 4.2 ومن ثم العبارة الخامسة بمتوسط 4.00 وبمتوسط يليها كان لصالح العبارة السادسة حيث كانت قيمته 3.95 وأخيرا وأقل متوسط كان للعبارة الرابعة بقيمة 3.81 مما يدل على استخدام أنظمة كشف التسلل (Intrusion Detection Systems) القائمة على الذكاء الاصطناعي لتحليل الأنشطة المشبوهة بشكل مستمر كما رأينا في متوسط العبارة الثانية لكن لا يوجد تطبيقات ذكاء تعمل على تحليل البيانات في الوقت الحقيقي لرصد التهديدات السيبرانية المحتملة كما رأينا ذلك في متوسط العبارة الرابعة.

السؤال الرابع: ما هي التهديدات السيبرانية الحالية والمستقبلية التي تواجه البنوك السعودية في مجال أمن البيانات؟

للإجابة على هذا السؤال جرى تحليل بيانات المحور الأول من محاور الاستبيان، حيث تم حساب المتوسط الحسابي والنسبة المئوية ودرجة ورتبة كل عبارة والجدول التالي يوضح نتائج التحليل:

جدول 7: فعالية الحلول القائمة على الذكاء الاصطناعي في كشف التهديدات

الرتبة	درجة الأهمية	الانحراف المعياري	المتوسط الحسابي	فعالية الحلول القائمة على الذكاء الاصطناعي في كشف التهديدات
5	مرتفعة	0.767	3.94	الحلول القائمة على التعلم العميق (Deep Learning) التي نستخدمها فعالة في كشف الهجمات السيبرانية المعقدة.

3.5	مرتفعة	0.903	4.20	تقنيات الذكاء الاصطناعي تساعدنا في التعرف على أنماط الهجمات السيبرانية قبل حدوثها.
1	مرتفعة	0.790	4.37	أشعر بأن استخدام الذكاء الاصطناعي في نظام إدارة المعلومات الأمنية (SIEM) يساهم بشكل كبير في تأمين بياناتنا المصرفية.
2	مرتفعة جداً	0.787	4.35	الحلول الأمنية القائمة على الذكاء الاصطناعي تتفوق على الحلول التقليدية في الكشف عن تهديدات يوم الصفر (Day Zero).
3.5	مرتفعة	0.926	4.20	تقنيات الذكاء الاصطناعي تمكننا من الاستجابة للهجمات السيبرانية بشكل أسرع وأكثر فعالية.
	مرتفعة	0.75	4.21	المقياس الكلي للعبارات الخاصة بفعالية الحلول القائمة على الذكاء الاصطناعي في كشف التهديدات

يتبين من الجدول بأن الحلول القائمة على الذكاء الاصطناعي كان فعالة بشكل كبير بالنسبة لرأي الموظفين حيث تحقق بدرجات جيدة لدى عبارات المحور تحقق ذلك بالمرتبة الأولى في العبارة الثالثة بمتوسط حسابي 4.37 وبمتوسط أقل نسبياً كان صالح العبارة الرابعة بقيمة 4.35 ومن ثم العبارات الثانية والخامسة بمتوسط 4.20 مما يدل على أن استخدام الذكاء الاصطناعي في نظام إدارة المعلومات الأمنية (SIEM) يساهم بشكل كبير في تأمين بياناتنا المصرفية ولكن الحلول القائمة على التعلم العميق (Deep Learning) التي نستخدمها غير فعالة كثيراً في كشف الهجمات السيبرانية المعقدة.

السؤال الخامس: ما هي التهديدات السيبرانية الحالية والمستقبلية التي تواجه البنوك السعودية في مجال

أمن البيانات؟

للإجابة على هذا السؤال جرى تحليل بيانات المحور الأول من محاور الاستبيان، حيث تم حساب المتوسط

الحسابي والنسبة المئوية ودرجة ورتبة كل عبارة والجدول التالي يوضح نتائج التحليل:

جدول 8: فعالية السياسات والإجراءات الحالية لأمن البيانات

الرتبة	درجة الأهمية	الانحراف المعياري	المتوسط الحسابي	فعالية السياسات والإجراءات الحالية لأمن البيانات
4	مرتفعة	0.741	4.04	السياسات الحالية لأمن البيانات في مؤسستي فعالة في حماية المعلومات من تهديدات الفدية (Ransomware).
1	مرتفعة جداً	0.757	4.24	إجراءات الأمن السيبراني المتبعة في مؤسستي قوية بما يكفي للتصدي لهجمات التصيد الاحتيالي (Phishing).
2	مرتفعة	0.769	4.20	لدينا سياسات واضحة ومحددة للتعامل مع هجمات القوة العمياء (Brute Force) وغيرها من التهديدات السيبرانية.
5	مرتفعة	0.868	3.89	السياسات الحالية تضمن سلامة البيانات أثناء النقل (Data in Transit) وأثناء التخزين (Data at Rest).
3	مرتفعة	0.747	4.05	أعتقد أن سياسات الأمان لدينا شاملة بما يكفي لتغطية جميع جوانب الأمان السيبراني في البنك.
	مرتفعة	0.707	4.08	المقياس الكلي للعبارة الخاصة بفعالية السياسات والإجراءات الحالية لأمن البيانات

يتبين من الجدول بأن فعالية السياسات والإجراءات الحالية لأمن البيانات تحققت بدرجات عالية لدى عبارات المحور حيث تحقق ذلك بالمرتبة الأولى في العبارة الثانية بمتوسط حسابي 4.24 وبمتوسط أقل كان صالح العبارة الثانية بقيمة 4.20 ومن ثم العبارات الأولى والخامسة بمتوسط 4.04 و 4.05 وبمتوسط أقل كان لصالح العبارة الرابعة بقيمة 3.89 مما يدل على أن إجراءات الأمن السيبراني المتبعة قوية بما يكفي للتصدي لهجمات التصيد الاحتيالي. ولكن السياسات الحالية لا تضمن سلامة البيانات أثناء النقل وأثناء التخزين بشكل كبير.

السؤال السادس: ما هي التهديدات السيبرانية الحالية والمستقبلية التي تواجه البنوك السعودية في مجال

أمن البيانات؟

للإجابة على هذا السؤال جرى تحليل بيانات المحور الأول من محاور الاستبيان، حيث تم حساب المتوسط

الحسابي والنسبة المئوية ودرجة ورتبة كل عبارة والجدول التالي يوضح نتائج التحليل:

جدول 9: فعالية السياسات والإجراءات الحالية لأمن البيانات

الرتبة	درجة الأهمية		المتوسط الحسابي	تحديات تطبيق استراتيجيات الأمن السيبراني
5	مرتفعة	1.172	3.25	أواجه صعوبات في تطبيق استراتيجيات الأمن السيبراني الحالية عند التعامل مع هجمات التصيد الاحتيالي (Phishing) المتطورة.
3	مرتفعة جداً	0.771	4.34	هناك تحديات في تحديث السياسات والإجراءات لمواكبة تهديدات الذكاء الاصطناعي المستجدة.
1	مرتفعة جداً	0.500	4.55	أعتقد أن هناك حاجة لتطوير استراتيجيات جديدة لمواجهة التهديدات السيبرانية التي يستخدم فيها الذكاء الاصطناعي بشكل متزايد.
2	مرتفعة جداً	0.652	4.39	هناك صعوبات في تخصيص ميزانية كافية لتطبيق أحدث تقنيات الذكاء الاصطناعي في الأمن السيبراني.
4	مرتفعة	0.955	4.08	أواجه تحديات في توظيف وتدريب الكوادر المتخصصة في أمن المعلومات والذكاء الاصطناعي.
	مرتفعة	0.607	4.12	المقياس الكلي للعبارات الخاصة بتحديات تطبيق استراتيجيات الأمن السيبراني

يتبين من الجدول بأن تحديات تطبيق استراتيجيات الأمن السيبراني كانت متواجدة بدرجات عالية لدى عبارات المحور حيث تحقق ذلك بالمرتبة الأولى في العبارة الثالثة بمتوسط حسابي 4.55 وبمتوسط أقل كان صالح العبارة الرابعة بقيمة 4.39 ومن ثم العبارة الثانية بمتوسط 4.34 وبمتوسط أقل كان لصالح العبارة الثانية بقيمة 4.08 وبالمرتبة الأخيرة كانت متوسط العبارة الأولى بقيمة 3.25 مما يدل على أن هناك حاجة لتطوير استراتيجيات جديدة لمواجهة التهديدات السيبرانية التي يستخدم فيها الذكاء الاصطناعي بشكل متزايد ولا يوجد صعوبات في تطبيق استراتيجيات الأمن السيبراني الحالية عند التعامل مع هجمات التصيد الاحتيالي (Phishing) المتطورة.

4.1 اختبار فرضيات الدراسة:

الفرضية الأولى: يسهم الذكاء الاصطناعي في تعزيز قدرات الهجمات السيبرانية على البنوك العامة السعودية من خلال تطوير أساليب اختراق أكثر تعقيداً وصعوبة في الكشف عنها. لاختبار هذه الفرضية قمنا باستخدام اختبار **One-Sample Test** الذي يقوم بمقارنة العينة مع قيمة محددة وبحسب مدى فروق هذه العينة عن تلك القيمة

جدول 10: اختبارات لإسهام الذكاء الاصطناعي في تعزيز قدرات الهجمات السيبرانية

Mean Difference	Sig. (2-tailed)	df	t	
1.36	.000	98	19.90	الوعي بالتهديدات_السيبرانية

-نلاحظ من خلال الجدول السابق أن قيمة $\text{sig}=0.00$ وهي أصغر من مستوى الدلالة المعنوية 0.05 وبالتالي نرفض الفرضية الابتدائية ونقبل الفرضية البديلة التي تنص على " يوجد فروق معنوية بين متوسط الإجابات على السؤال " يسهم الذكاء الاصطناعي في تعزيز قدرات الهجمات السيبرانية على البنوك العامة السعودية من

خلال تطوير أساليب اختراق أكثر تعقيداً وصعوبة في الكشف عنها" ومتوسط درجات الإجابات وهو القيمة 3" وبما أن متوسط العينة هو 4.36 وبالتالي أغلب المجيبين كانت لديهم موافقة على أن الذكاء الاصطناعي له دور تعزيز الهجمات السيبرانية

الفرضية الثانية: يمكن استخدام تقنيات الذكاء الاصطناعي بفعالية لتعزيز أمن البيانات وكشف التهديدات بشكل استباقي في البنوك السعودية.

لاختبار هذه الفرضية قمنا باستخدام اختبار One-Sample Test الذي يقوم بمقارنة العينة مع قيمة محددة وحسب مدى فروق هذه العينة عن تلك القيمة

جدول 11: اختبار استخدام الذكاء الاصطناعي في تعزيز أمن البيانات

Mean Difference	Sig. (2-tailed)	df	t	
1.143	.000	98	15.58	استخدام الذكاء في أمن البيانات

-نلاحظ من خلال الجدول السابق أن قيمة sig=0.00 وهي أصغر من مستوى الدلالة المعنوية 0.05 وبالتالي نرفض الفرضية الابتدائية ونقبل الفرضية البديلة التي تنص على " يوجد فروق معنوية بين متوسط الإجابات على السؤال " يمكن استخدام تقنيات الذكاء الاصطناعي بفعالية لتعزيز أمن البيانات وكشف التهديدات بشكل استباقي في البنوك السعودية" ومتوسط درجات الإجابات وهو القيمة 3" وبما أن متوسط العينة هو 4.14 وبالتالي أغلب المجيبين كانت لديهم موافقة على أن تقنيات الذكاء الاصطناعي لها دور في تعزيز أمن البيانات وكشف التهديدات.

الفرضية الثالثة: الاستراتيجيات الحالية التي تتبعها البنوك السعودية في حماية البيانات من التهديدات السيبرانية غير كافية لمواجهة التحديات الناشئة عن تطور تقنيات الذكاء الاصطناعي.

لاختبار هذه الفرضية قمنا باستخدام اختبار **One-Sample Test** الذي يقوم بمقارنة العينة مع متوسط (قيمة محددة) ويحسب مدى فروق هذه العينة عن المتوسط

جدول 12: اختبارات لاستراتيجيات البنوك السعودية في حماية البيانات

Mean Difference	Sig. (2-tailed)	df	t	تحديات تطبيق استراتيجيات الأمن
1.12	.000	98	18.38	

نلاحظ من خلال الجدول السابق أن قيمة $\text{sig}=0.00$ وهي أصغر من مستوى الدلالة المعنوية 0.05 وبالتالي نرفض الفرضية الابتدائية ونقبل الفرضية البديلة التي تنص على "يوجد فروق معنوية بين متوسط الإجابات على السؤال "الاستراتيجيات الحالية التي تتبعها البنوك السعودية في حماية البيانات من التهديدات السيبرانية غير كافية لمواجهة التحديات الناشئة عن تطور تقنيات الذكاء الاصطناعي" ومتوسط درجات الإجابات وهو القيمة 3" وبما أن متوسط العينة هو 4.12 مما يدل على عدم موافقة أغلب المجيبين على أن الاستراتيجيات الحالية غير كافية وبالتالي مما يدل على كفاية وجهوية البنوك السعودية في الرياض للتصدي لأي تهديد سيبراني.

4.2 مناقشة النتائج والتوصيات

السؤال الأول: التهديدات السيبرانية الحالية والمستقبلية

تشير النتائج إلى أن مستوى الوعي بالتهديدات السيبرانية الحالية والمستقبلية في البنوك السعودية مرتفع جداً. إذ يتضح أن المشاركين مدركون بشكل جيد للتهديدات الحالية مثل هجمات الفدية وهجمات التصيد الاحتيالي، كما أن لديهم إدراكاً عالياً للتهديدات المستقبلية المحتملة التي قد تستخدم الذكاء الاصطناعي لتوليد برامج ضارة متقدمة. كما أن المؤسسات توفر تدريبات منتظمة حول هذه التهديدات، مما يعزز من استعدادها لمواجهة التهديدات السيبرانية.

السؤال الثاني: استغلال الذكاء الاصطناعي في الهجمات السيبرانية

تشير البيانات إلى أن هناك وعياً عالياً بفهم كيفية استغلال الذكاء الاصطناعي في الهجمات السيبرانية. يدرك المشاركون أن الذكاء الاصطناعي يمكن أن يستخدم لتوليد هجمات تصيد احتيالي ذكية، وتحليل الثغرات بسرعة، وجعل هجمات القوة العمياء أكثر فعالية وتعقيداً. هذا الوعي يبرز الحاجة الملحة لتعزيز قدرات الدفاع السيبراني لمواجهة هذه التهديدات المتقدمة.

السؤال الثالث: استخدام الذكاء الاصطناعي في حماية البيانات

توضح النتائج أن البنوك السعودية تستخدم تقنيات الذكاء الاصطناعي بشكل كبير في حماية البيانات. تشمل هذه التقنيات أنظمة كشف التسلل القائمة على الذكاء الاصطناعي، وتحليل النشاط غير المعتاد، وتحليل البيانات في الوقت الحقيقي. هذه الاستخدامات تظهر أن الذكاء الاصطناعي يلعب دوراً محورياً في تحسين قدرات البنوك على كشف التهديدات السيبرانية والاستجابة لها بشكل فعال.

السؤال الرابع: فعالية الحلول القائمة على الذكاء الاصطناعي في كشف التهديدات

تشير النتائج إلى أن الحلول الأمنية القائمة على الذكاء الاصطناعي فعالة في كشف الهجمات السيبرانية المعقدة، والتعرف على أنماط الهجمات قبل حدوثها، والاستجابة السريعة للهجمات. يساهم الذكاء الاصطناعي في نظام إدارة المعلومات الأمنية بشكل كبير في تأمين البيانات المصرفية، مما يعزز من فعالية الاستراتيجيات الأمنية.

السؤال الخامس: فعالية السياسات والإجراءات الحالية لأمن البيانات

توضح البيانات أن السياسات والإجراءات الحالية لأمن البيانات في البنوك السعودية فعالة إلى حد كبير. تشمل هذه السياسات الحماية من هجمات الفدية والتصيد الاحتيالي، والتعامل مع هجمات القوة العمياء، وضمان سلامة البيانات أثناء النقل والتخزين. ومع ذلك، تبين النتائج أن هناك تحديات في تحديث السياسات والإجراءات لمواكبة التهديدات المستجدة.

السؤال السادس: تحديات تطبيق استراتيجيات الأمن السيبراني

تكشف النتائج أن هناك تحديات ملحوظة في تطبيق استراتيجيات الأمن السيبراني. تشمل هذه التحديات التعامل مع هجمات التصيد الاحتيالي المتطورة، تحديث السياسات لمواكبة تهديدات الذكاء الاصطناعي، تخصيص ميزانية كافية لتطبيق أحدث التقنيات، وتوظيف وتدريب الكوادر المتخصصة.

تعكس النتائج وعيًا عاليًا لدى البنوك السعودية بالتهديدات السيبرانية الحالية والمستقبلية، وتوضح أن هناك استخدامًا واسعًا لتقنيات الذكاء الاصطناعي في حماية البيانات. ومع ذلك، تواجه هذه البنوك تحديات كبيرة في مواكبة التطورات السريعة في تقنيات الهجوم والدفاع السيبراني. يشير الاختبار الاحصائي لفرضيات الدراسة إلى وجود تأثير كبير للذكاء الاصطناعي في تعزيز قدرات الهجمات السيبرانية وكذلك في تعزيز الأمن السيبراني .

التوصيات

تقدم الدراسة التوصيات الآتية:

- تعزيز التدريب والتوعية: يجب على البنوك زيادة جهود التدريب والتوعية حول التهديدات السيبرانية المتقدمة، بما في ذلك استخدام الذكاء الاصطناعي في الهجمات.
- تطوير السياسات والإجراءات: ينبغي مراجعة وتحديث السياسات والإجراءات الأمنية بشكل مستمر لمواكبة التطورات التقنية والتهديدات السيبرانية الجديدة.
- استثمار في التقنيات المتقدمة: زيادة الاستثمارات في تقنيات الذكاء الاصطناعي والأمن السيبراني لضمان فعالية الكشف عن التهديدات والاستجابة لها بسرعة.
- توظيف وتدريب الكوادر المتخصصة: تعزيز الجهود في توظيف وتدريب المتخصصين في مجال أمن المعلومات والذكاء الاصطناعي لضمان توفر المهارات اللازمة لمواجهة التحديات الأمنية.
- تخصيص ميزانية كافية: التأكيد على تخصيص ميزانية كافية لتطبيق أحدث تقنيات الذكاء الاصطناعي في الأمن السيبراني، مما يساهم في تحسين البنية التحتية الأمنية بشكل كبير.
- التعاون مع الجهات المعنية: تعزيز التعاون مع الجهات الحكومية والخاصة في مجال الأمن السيبراني لتبادل المعرفة والخبرات، مما يساهم في تعزيز القدرات الدفاعية المشتركة ضد التهديدات السيبرانية.

المراجع العربية

- احمد الخطيب خالد زيفان. (2009). إدارة المعرفة ونظم المعلومات ، الطبعة 1، دار الكتاب العالمي ، عمان ، الأردن.
- أحمد عثمان ادم، (2009). دور ادارة المعرفة والأصول الفكرية في تحقيق المنظمة الاقتصادية للمكتبات الجامعية ، الطبعة 1، المجموعة العربية للتدريب ، القاهرة، مصر
- أحمد علي صالح، (2012). إدارة الأعمال الدولية، مدخل منهج متكامل، ط1، دار وائل، عمان، الأردن.
- أحمد ماهر. (2002). دليل المدير خطوة بخطوة في الإدارة الاستراتيجية، الدار الجامعية، الإسكندرية، مصر.
- إسماعيل محمد السيد، (1999). الإدارة الاستراتيجية، مفاهيم وحالات تطبيقيا، مكتب العربي الحديث، إسكندرية، مصر.
- ايهاب زهران. (2020). الجودة والتحول الرقمي، خبير الجودة في إدارة المستشفيات.
- بدروني، هدى. وكواريش، نصيرة. (مايو 2024). دور الذكاء الاصطناعي في تحسين وتطوير الخدمات المالية على مستوى البنوك - عرض تجارب بنكية دولية. الملتقى الوطني حول الذكاء الاصطناعي وتطبيقاته في مجال الأعمال في الجزائر.
- بشير علاق (2008) مبادئ الإدارة، دار اليازوري، عمان، الأردن.
- ثابت عبد الرحمان إدريس، جمال الدين محمد المرسي، (2003). الإدارة الاستراتيجية، مفاهيم ونماذج تطبيقية، ط1، دار الجامعة، عمان، الأردن.
- جمال الدين محمد مرسي . (2007). التفكير الاستراتيجي والإدارة الاستراتيجية (منهج تطبيقي) ، الدار الجامعية، الإسكندرية، مصر.
- جمعة، أميرة. (2023). آليات التحول الرقمي وأثره على سلامة البيانات المالية (دراسة حالة مصرف الراجحي). المجلة الأكاديمية لنشر البحث العلمي. 5 (56)، 121-140. DOI: [10.52132/Ajrsp/v5.56.5](https://doi.org/10.52132/Ajrsp/v5.56.5)
- حسن حريم، (2006). مبادئ الإدارة الحديثة، النظريات العمليات الإدارية وظائف المنظمة، ط1، ار حامد، عمان، الأردن.
- حسن علي الزغبى، (2005). نظم المعلومات الاستراتيجية، مدخل استراتيجي، ط1، دار وائل، عمان، الأردن.

خالد محمد بني حمدان، وائل محمد صبيحي ادريس، الاستراتيجية والتخطيط الاستراتيجي، المنهج المعاصر، ط1، دار اليازوري، عمان، الأردن، 2007

خضير مصباح الطيطي (2013). الإدارة الاستراتيجية، دار الحامد، عمان، الأردن.

خليل محمد حسن السماع (1999) مبادئ الإدارة مع التركيز على إدارة الأعمال، دار المسيرة، عمان، الأردن.

خليل محمد حسن السماع، (2007) مبادئ الإدارة مع التركيز على إدارة الأعمال، ط1، دار المسيرة، عمان، الأردن.

الديبسي، عبد الكريم. (2021). الإعلام الرقمي وتحديات الذكاء الاصطناعي. المسيرة للنشر، عمان الأردن.

دلال صادق، د. حميد ناصر. (2008). أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، الاردن، عمان

رافدة عمر الحريري (2010) القيادة وإدارة الجودة في التعليم العالي، ط1، دار الثقافة، عمان، الأردن،

رقية منصور، (2015). توافق التخطيط الاستراتيجي للمنظمة والتخطيط الاستراتيجي لنظم المعلومات وأثره على تحقيق عوامل التفوق التنافسي، رسالة دكتوراه غير منشورة، جامعة محمد خيضر،

السعيد مبروك إبراهيم، (2012). المعلومات ودورها في دعم واتخاذ القرار الاستراتيجي، الطبعة 1، دار الكتب المصرية، القاهرة، مصر.

عدنان تايه النعيمي & أرشد فؤاد التميمي، (2011). التحليل والتخطيط المالي اتجاهات معاصرة، دار اليازوري العلمية للنشر والتوزيع، الأردن، عمان .

عدنان مصطفى البار، تقنيات التحول الرقمي، (2018). جامعة الملك عبد العزيز، كليات الحاسب وتقنية المعلومات

علي بن صالح آل صمع، (2018) التحول الرقمي كمرتكز استراتيجي لقيادة التحول الاقتصادي.

علي خلف عبد الله & وليد ناجي الحياي، (2015). التحليل المالي للرقابة على الأداء والكشف عن الانحرافات، مركز الكتاب الأكاديمي، عمان، الاردن.

علي عبد المحسن عباس حسن الفتالوي، (2020). نظرة عامة على تحليل البيانات المالية، جامعة كربلاء كلية الإدارة والاقتصاد قسم المحاسبة.

عمر النور، كريم الدين عمر. (2023). دور الاتجاهات الحديثة للمراجعة الداخلية في الحد من مخاطر أمن المعلومات المحاسبية، دراسة ميدانية على بنك الخرطوم. *المجلة الدولية لنشر البحوث والدراسات*،

DOI: [10.52133/ijrsp.v4.39.18](https://doi.org/10.52133/ijrsp.v4.39.18). 552-530، (39) 4

عمرو وصفي عقيلي، (2013). دليل المصطلحات والمفاهيم الأساسية في العلوم الإدارية، المالية والمصرفية، التسويق إثراء للنشر والتوزيع، الأردن.

غريد، صباح. ونصري، وهيبة. (نوفمبر، 2023). دور تحليل البيانات الضخمة المدعم بالذكاء الاصطناعي في تحسين عملية التدقيق المالي _ دراسة حالة شركة Presight لحلول الذكاء الاصطناعي . الملتقى الدولي الحضوري – الافتراضي حول: الذكاء الاصطناعي وتطبيقاته في المحاسبة والتدقيق جامعة باجي مختار - عنابة

غوانمة، أسماء. رملي، أشرف بن محمد. بن جليل، عبد الله. وعلاونة، مؤيد فضل. (2023). أثر نظم الذكاء الاصطناعي على تحسين جودة الخدمات المصرفية في المصارف الإسلامية الأردنية. مجلة النظم الذكية في الخدمات المصرفية. 8(2)، 79-390. doi:10.31559/SIS2023.8.2.390-79 .

فيصل محمود الشواورة، (2013). مبادئ الادارة المالية، دار المسيرة للنشر والتوزيع والطباعة، عمان، الاردن.

قشي، مريم. (نوفمبر 2023). الذكاء الاصطناعي في الصناعة 4.0، الفرص والتحديات المستقبلية. الملتقى الدولي الأول: نحو اعتماد استراتيجيات الذكاء الاصطناعي. جامعة 10 أوت 1955 سكيكدة. 7-8 نوفمبر.

كاظم، يحيى. وعلائي، صفاء. (كانون الثاني 2023). تقنيات الذكاء الاصطناعي ودورها في الحد من الاحتيال المحاسبي. المؤتمر الدولي الرابع لعلوم الإدارة والمحاسبة. DOI: [10.24086/ICAFS2023/paper.927](https://doi.org/10.24086/ICAFS2023/paper.927)

معاندي، أمينة. وشابي، حليلة. (ديسمبر 2021). دور تقنيات التكنولوجيا المالية في تعميم الخدمات المالية وتعزيز الشمول المالي، الذكاء الاصطناعي نموذجاً. الملتقى الوطني حول التكنولوجيا المالية والذكاء الاصطناعي كتوجه في النشاط المالي والبنكي وموقع الأنظمة المالية لدول شمال افريقيا والشرق الأوسط، 16 ديسمبر.

النعساني، أحمد. (2024). أثر استخدام تطبيقات الذكاء الاصطناعي في تخفيف المخاطر في العمليات المصرفية: دراسة ميدانية بالتطبيق على بنك الراجحي والأهلي.

- Al-Baity, Heyam H. 2023. "The Artificial Intelligence Revolution in Digital Finance in Saudi Arabia: A Comprehensive Review and Proposed Framework" *Sustainability* 15, no. 18: 13725. <https://doi.org/10.3390/su151813725>
- Almonte, R.G.; Lacatan, L.L. Sentiment Analysis of Facebook Posts Towards Good Governance Using SVM Algorithm: A Framework Proposal. In Proceedings of the 2021 the 4th International Conference on [31] Machine Learning and Machine Intelligence, Hangzhou, China, 17–19 September 2021; pp. 140–144
- Al-Nasani, A. (2024). The Impact of Using Artificial Intelligence Applications on Mitigating Risks in Banking Operations: A Field Study Applied to Al Rajhi and Al Ahli Banks. *Innovations Journal of Humanities and Social Studies*. 2 (spc), 1-25. DOI:[10.61856/ijhss.v2ispc..155](https://doi.org/10.61856/ijhss.v2ispc..155)
- Banitaan, S., Al-refai, G., Almatarnah, S., & Alquran, H. (2023). A Review on Artificial Intelligence in the Context of Industry 4.0. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 14.(02)
- Brundage, Miles & Avin, Shahar & Clark, Jack & Toner, Helen & Eckersley, Peter & Garfinkel, Ben & Dafoe, Allan & Scharre, Paul & Zeitzoff, Thomas. Et al. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Oxford university report.
- Capgemini. (2019). *Scaling AI in Manufacturing Operations: A Practitioners' Perspective*. Capgemini.
- Chinea, A. Understanding the Principles of Recursive Neural Networks: A Generative Approach to Tackle Model Complexity. *Int. Conf. Artif. Neural Netw.* 2009, 5768, 952–963.
- Chopra, M., Singh, S., Sharma, S., & Mahto, D. (2021). Impact and Usability of Artificial Intelligence in Manufacturing workflow to empower Industry 4.0. *1International Conference on Smart Systems and Advanced Computing (Syscom-2021)*, December 25–26, 2021.
- Chui, M., Henke, N., & Miremadi, M. (2018, July 20). Most of AI's Business Uses Will Be in Two Areas.

- Duarte, D.L.; de Moraes Barboza, F.L. Forecasting Financial Distress with Machine Learning—A Review. *Future Stud. Res. J. Trends Strateg.* 2020, 12, 528–574
- Durairaj, D.M.; Mohan, B.H.K. A convolutional neural network-based approach to financial time series prediction. *Neural. Comput. Appl.* 2022, 34, 13319–13337
- El-Adawy, A. (2023). Artificial Superintelligence and Arab National Security. Security Research Center. DOI:[10.26735/XZPJ8837](https://doi.org/10.26735/XZPJ8837)
- Fadlullah, Zubair & Tang, Fengxiao & Mao, Bomin & Kato, Nei & Akashi, Osamu & Inoue, Takeru & Mizutani, Kimihiro. (2017). State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems. *IEEE Communications Surveys & Tutorials*. PP. 1-
<https://doi.org/10.1109/COMST.2017.2707140>.
- Hinge, D. (2022). Impact of Artificial Intelligence in Banking Sector. *International Journal of Advanced Research*. 10(02):301-305.DOI:[10.21474/IJAR01/14208](https://doi.org/10.21474/IJAR01/14208)
- Huang, J.; Chai, J.; Cho, S. Deep learning in finance and banking: A literature review and classification. *Front. Bus. Res. China* 2020, 14, 13
- Johri, S.; Qureshi, N.I.; Mehta, K.; Othman, B.; Waghmare, S.; Pant, B. A Critical Significance of Using Machine Learning in Strengthening Financial Risk Management in Banking Firms. In *Proceedings of the 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Greater Noida, India, 28–29 April 2022; pp. 1933–1937.
- Kshetri, Nir & Voas, Jeffrey. (2018). Blockchain-Enabled E-Voting. *IEEE Software*. 35. 95-99.
<https://doi.org/10.1109/MS.2018.2801546>.
- Maree, C.; Omlin, C.W. Understanding Spending Behavior: Recurrent Neural Network Explanation and Interpretation. 2021.
- Zimmermann, H.G.; Tietz, C.; Grothmann, R.; Runkler, T. Recurrent Neural Networks for Industrial Procurement Decisions. *KI—Kunstl. Intell.* 2012, 26, 403–406

5 الملاحق

استبيان حول مخاطر الذكاء الاصطناعي على أمن البيانات في البنوك السعودية

بسم الله الرحمن الرحيم

السلام عليكم ورحمة الله وبركاته،

عزيزي المشارك / عزيزتي المشاركة،

أتقدم إليكم بجزيل الشكر على تخصيص جزء من وقتكم الثمين للمشاركة في هذه الدراسة البحثية الهامة. أنا باحث في مرحلة الماجستير، وأقوم بإجراء دراسة بعنوان:

"دراسة مخاطر الذكاء الاصطناعي على أمن البيانات في قطاع الخدمات المالية والبنوك: دراسة حالة البنوك العامة في المملكة العربية السعودية"

يهدف هذا الاستبيان إلى جمع معلومات قيّمة حول التحديات الأمنية الحالية والمستقبلية التي تواجهها البنوك السعودية في ظل التطور السريع لتقنيات الذكاء الاصطناعي. كما يسعى إلى فهم مدى استعداد القطاع المصرفي لمواجهة هذه التحديات واستغلال الفرص التي يقدمها الذكاء الاصطناعي في تعزيز أمن البيانات. مشاركتكم في هذا الاستبيان تعتبر تطوعية بالكامل، ونؤكد لكم أن جميع المعلومات التي ستقدمونها ستعامل بسرية تامة ولن تستخدم إلا لأغراض البحث العلمي. لن يتم الإشارة إلى أي معلومات شخصية في نتائج الدراسة.

يتكون الاستبيان من خمسة محاور رئيسية، ويستغرق إكماله حوالي 15-20 دقيقة. نرجو منكم الإجابة على جميع الأسئلة بصدق وموضوعية قدر الإمكان، حيث أن دقة إجاباتكم ستساهم بشكل كبير في تحقيق أهداف الدراسة وتقديم توصيات قيّمة لتعزيز أمن البيانات في القطاع المصرفي السعودي.

شاكرين ومقدرين تعاونكم،

معتر السبيعي

باحث ماجستير - جامعة ميدأوشن

يرجى الإجابة على العبارات التالية باستخدام المقياس: (1) غير موافق بشدة، (2) غير موافق، (3) محايد، (4) موافق، (5) موافق بشدة

الجزء الأول: الوعي بالتهديدات السيبرانية					
1. مستوى الإدراك بالتهديدات الحالية والناشئة:					
1	2	3	4	5	
					- أنا على دراية بالتهديدات السيبرانية الحالية مثل هجمات الفدية (Ransomware) وهجمات التصيد الاحتيالي (Phishing).
					- أنا على دراية بالتهديدات السيبرانية المستقبلية المحتملة مثل الهجمات باستخدام الذكاء الاصطناعي لتوليد برامج ضارة متقدمة.
					- مؤسستي توفر تدريبات منتظمة حول التهديدات السيبرانية بما في ذلك استخدام الذكاء الاصطناعي في الهجمات.
					- أنا على علم بالتهديدات السيبرانية التي تستهدف البنية التحتية المصرفية مثل هجمات (DDoS (Distributed Denial of Service.
					- أدرك تأثير الهجمات السيبرانية على السمعة والثقة العامة بالبنك.
2. فهم كيفية استغلال الذكاء الاصطناعي في الهجمات السيبرانية:					
					- أدرك أن الذكاء الاصطناعي يمكن أن يستخدم لتوليد هجمات تصيد احتيالي (Phishing) ذكية وشخصية.
					- أفهم الطرق التي يمكن أن يستخدم فيها الذكاء الاصطناعي لاختراق الأنظمة المصرفية من خلال تحليل الثغرات بشكل سريع وذكي.
					- أعتقد أن استخدام الذكاء الاصطناعي يمكن أن يجعل هجمات القوة العمياء (Brute Force) أكثر فعالية وتعقيدًا.
					- أنا على علم بكيفية استخدام الذكاء الاصطناعي لتجاوز أنظمة الحماية التقليدية مثل الجدران النارية (Firewalls).
					- أفهم كيفية استخدام الذكاء الاصطناعي لتحليل بيانات العملاء واستهدافهم بشكل أكثر دقة في الهجمات السيبرانية.
الجزء الثاني: استخدام الذكاء الاصطناعي في أمن البيانات					
3. مدى استخدام تقنيات الذكاء الاصطناعي في حماية البيانات:					
					- مؤسستي تستخدم تقنيات الذكاء الاصطناعي مثل التعلم الآلي (Machine Learning) للكشف عن النشاط غير المعتاد.

					- نستخدم أنظمة كشف التسلل (Intrusion Detection Systems) القائمة على الذكاء الاصطناعي لتحليل الأنشطة المشبوهة بشكل مستمر.
					تساهم حلول الذكاء الاصطناعي في تحسين قدرة البنك على كشف التهديدات السيبرانية مثل هجمات الحرمان من الخدمة (DDoS) وهجمات الهندسة الاجتماعية (Social Engineering).
					- لدينا تطبيقات ذكاء اصطناعي تعمل على تحليل البيانات في الوقت الحقيقي لرصد التهديدات السيبرانية المحتملة.
					- نعتمد على تقنيات الذكاء الاصطناعي لتقييم نقاط الضعف في أنظمة الأمان وتحسينها بشكل مستمر.
					- نستخدم الذكاء الاصطناعي لتحليل سلوك المستخدمين وكشف الأنماط الغير عادية التي قد تشير إلى اختراقات.
4. فعالية الحلول القائمة على الذكاء الاصطناعي في كشف التهديدات:					
					- الحلول القائمة على التعلم العميق (Deep Learning) التي نستخدمها فعالة في كشف الهجمات السيبرانية المعقدة.
					- تقنيات الذكاء الاصطناعي تساعدنا في التعرف على أنماط الهجمات السيبرانية قبل حدوثها.
					- أشعر بأن استخدام الذكاء الاصطناعي في نظام إدارة المعلومات الأمنية (SIEM) يساهم بشكل كبير في تأمين بياناتنا المصرفية.
					- الحلول الأمنية القائمة على الذكاء الاصطناعي تتفوق على الحلول التقليدية في الكشف عن تهديدات يوم الصفر (Zero-Day).
					- تقنيات الذكاء الاصطناعي تمكننا من الاستجابة للهجمات السيبرانية بشكل أسرع وأكثر فعالية.
الجزء الثالث: تقييم الاستراتيجيات الحالية					
5. فعالية السياسات والإجراءات الحالية لأمن البيانات:					
					- السياسات الحالية لأمن البيانات في مؤسستي فعالة في حماية المعلومات من تهديدات الفدية (Ransomware).
					- إجراءات الأمن السيبراني المتبعة في مؤسستي قوية بما يكفي للتصدي لهجمات التصيد الاحتيالي (Phishing).
					- لدينا سياسات واضحة ومحددة للتعامل مع هجمات القوة العمياء (Brute Force) وغيرها من التهديدات السيبرانية.

					- السياسات الحالية تضمن سلامة البيانات أثناء النقل (Data in Transit) وأثناء التخزين (Data at Rest).
					- أعتقد أن سياسات الأمان لدينا شاملة بما يكفي لتغطية جميع جوانب الأمان السيبراني في البنك.
6. تحديات تطبيق استراتيجيات الأمن السيبراني:					
					- أواجه صعوبات في تطبيق استراتيجيات الأمن السيبراني الحالية عند التعامل مع هجمات التصيد الاحتيالي (Phishing) المتطورة.
					- هناك تحديات في تحديث السياسات والإجراءات لمواكبة تهديدات الذكاء الاصطناعي المستجدة.
					- أعتقد أن هناك حاجة لتطوير استراتيجيات جديدة لمواجهة التهديدات السيبرانية التي يستخدم فيها الذكاء الاصطناعي بشكل متزايد.
					- هناك صعوبات في تخصيص ميزانية كافية لتطبيق أحدث تقنيات الذكاء الاصطناعي في الأمن السيبراني.
					- أواجه تحديات في توظيف وتدريب الكوادر المتخصصة في أمن المعلومات والذكاء الاصطناعي.

الأسئلة الديموغرافية :

1. العمر:

☐ أقل من 25 سنة

☐ 25 - 34 سنة

☐ 35 - 44 سنة

☐ 45 - 54 سنة

☐ 55 سنة فأكثر

2. الجنس:

☐ ذكر

☐ أنثى

3. المستوى التعليمي:

☐ ثانوية عامة أو ما يعادلها

☐ دبلوم

☐ بكالوريوس

☐ ماجستير

☐ دكتوراه

4. عدد سنوات الخبرة في المجال المصرفي:

☐ أقل من سنة

☐ 1 - 5 سنوات

☐ 6 - 10 سنوات

☐ 11 - 15 سنة

☐ 16 - 20 سنة

☐ أكثر من 20 سنة

5. الوظيفة الحالية:

☐ موظف خدمة عملاء

☐ مسؤول حسابات

☐ محلل مالي

☐ مدير فرع

☐ مسؤول تقنية معلومات

☐ مسؤول أمن معلومات

☐ مدير إدارة

☐ إدارة عليا

☐ أخرى (يرجى التحديد): _____

البنك الذي تعمل به:

Midocean University

College of Management



**Study of the Risks of Artificial Intelligence on Data Security in the Financial
Services and Banking Sector
A Case Study of Public Banks in the Al Riyadh Area**

Prepared by:

Mutaz Saad Alsubaie

233000952

Supervised by:

Dr. Al-Faisal Abdulhamid

Dr. Fayez Jarrad

Year:2024