

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

الوطني العربي

اعداد الطالب: محمد عبده عجبي

اشراف الدكتور:

العام الدراسي: 2026م – 1447هـ

## الفصل الرابع: التحليل الإحصائي ومناقشة النتائج

## تمهيد

يتضمن هذا الفصل عرضاً وتحليلاً للبيانات التي تم جمعها من عينة الدراسة باستخدام أداة الاستبانة، والتي تم توزيعها على أفراد العينة المكونة من (190) مشاركاً من القادة الأمنيين ومحلي مراكز العمليات الأمنية (SOC) وخبراء تقنية المعلومات والذكاء الاصطناعي في البنك الوطني العربي (anb). يهدف هذا الفصل إلى اختبار فرضيات الدراسة والإجابة عن تساؤلاتها من خلال استخدام الأساليب الإحصائية المناسبة، بدءاً من الإحصاء الوصفي الذي يصف خصائص العينة واتجاهات أفرادها تجاه متغيرات الدراسة، وصولاً إلى الإحصاء الاستدلالي الذي يختبر العلاقات السببية بين المتغيرات باستخدام تحليل الانحدار المتعدد والخطي البسيط، بالإضافة إلى تحليل التباين الأحادي (ANOVA) لاختبار الفروق وفق المتغيرات الديموغرافية. كما يتضمن الفصل مناقشة معمقة للنتائج في ضوء الإطار النظري والدراسات السابقة التي تم استعراضها في الفصل الثاني، مع تفسير الدلالات الإحصائية والعملية لهذه النتائج.

### 4.1. الإحصاء الوصفي للعينة (البيانات الديموغرافية والمهنية)

يهدف هذا القسم إلى وصف خصائص أفراد عينة الدراسة من حيث متغيراتهم الديموغرافية والمهنية (المسمى الوظيفي، سنوات الخبرة، المؤهل العلمي، القسم التابع). يتم عرض التوزيعات التكرارية والنسب المئوية في جدول 4.1، وتحليل دلالات هذه التوزيعات لضمان تمثيل العينة لمختلف فئات العاملين في غرف التحكم الأمنية، وللكشف عن مدى تنوع وجهات النظر التي ستؤثر على نتائج الدراسة.

جدول 4.1: التوزيع التكراري والنسب المئوية لعينة الدراسة حسب المتغيرات الديموغرافية (n=190)

| المتغير        | الفئة              | التكرار | النسبة المئوية (%) |
|----------------|--------------------|---------|--------------------|
| المسمى الوظيفي | مدير أمن           | 71      | 37.4%              |
|                | محلل SOC           | 54      | 28.4%              |
|                | مهندس ذكاء اصطناعي | 36      | 18.9%              |
|                | خبير تقنية معلومات | 29      | 15.3%              |
|                | المجموع            | 190     | 100%               |
| سنوات الخبرة   | أقل من 5 سنوات     | 89      | 46.8%              |
|                | من 5 إلى 10 سنوات  | 41      | 21.6%              |
|                | أكثر من 10 سنوات   | 60      | 31.6%              |
|                | المجموع            | 190     | 100%               |
| المؤهل العلمي  | بكالوريوس          | 93      | 48.9%              |
|                | ماجستير            | 52      | 27.4%              |

|       |     |                 |                 |
|-------|-----|-----------------|-----------------|
| 10.0% | 19  | دكتوراه         |                 |
| 13.7% | 26  | شهادة مهنية     |                 |
| 100%  | 190 | المجموع         |                 |
| 43.2% | 82  | الأمن السيبراني | القسم التابع له |
| 26.8% | 51  | الأمن المادي    |                 |
| 18.9% | 36  | إدارة المخاطر   |                 |
| 11.1% | 21  | الامتثال        |                 |
| 100%  | 190 | المجموع         |                 |

يكشف الجدول 4.1 عن الخصائص الديموغرافية والمهنية لعينة الدراسة التي بلغ قوامها 190 فرداً، وقد تم تصميم العينة بشكل مقصود لضمان تمثيل جميع الفئات المعنية بتشغيل وإدارة تقنيات الذكاء الاصطناعي في غرف التحكم الأمنية بالبنك الوطني العربي.

أولاً: **المسمى الوظيفي:** تشير النتائج إلى أن أكبر فئة في العينة هم "مديرو الأمن" بنسبة 37.4% (71 فرداً)، مما يعكس حرص الباحث على استقصاء آراء متخذي القرار الاستراتيجي الذين يشرفون على سياسات الأمن وتطبيقات الذكاء الاصطناعي. وجاءت فئة "محلي SOC" في المرتبة الثانية بنسبة 28.4% (54 فرداً)، وهذه النسبة مرتفعة ومهمة لأن هؤلاء هم المستخدمون المباشرون لأنظمة الذكاء الاصطناعي في العمليات اليومية، وتقديراتهم تعكس الواقع التشغيلي الفعلي. أما فئة "مهندسي الذكاء الاصطناعي" فبلغت 18.9% (36 فرداً)، وهم المسؤولون عن تطوير وصيانة الخوارزميات والنماذج الذكية، بينما شكل "خبراء تقنية المعلومات" 15.3% (29 فرداً). هذا التنوع في المسميات الوظيفية يمنح الدراسة ثراءً في وجهات النظر، حيث يجمع بين الرؤية الإدارية والتشغيلية والتقنية، مما يعزز من موضوعية النتائج وشموليتها. ويتفق هذا التوزيع مع توصيات دراسة (Khayat et al., 2025) التي أكدت على أهمية إشراك جميع المستويات الوظيفية في تقييم أداء مراكز العمليات الأمنية المعززة بالذكاء الاصطناعي.

ثانياً: **سنوات الخبرة:** أظهرت النتائج أن ما يقارب نصف العينة (46.8%)، وعددهم 89 فرداً لديهم خبرة أقل من 5 سنوات، وهي نسبة تعكس حداثة نسبية للكوادر العاملة في مجال الأمن السيبراني والذكاء الاصطناعي، وهو أمر متوقع في ظل الطلب المتزايد على هذه التخصصات في المملكة العربية السعودية خلال السنوات الأخيرة. وجاءت فئة الخبرة "أكثر من 10 سنوات" بنسبة 31.6% (60 فرداً)، وهذه الفئة تمثل الخبرات العميقة والمتراكمة التي يمكنها تقديم تقييمات ناضجة ودقيقة لتأثير الذكاء الاصطناعي مقارنة بالفترات السابقة. أما فئة الخبرة "من 5 إلى 10 سنوات" فبلغت 21.6% (41 فرداً). هذا التوزيع المتوازن نسبياً بين فئات الخبرة المختلفة يعزز من قدرة الدراسة على اكتشاف الفروق في التقديرات حسب مستوى الخبرة،

وهو ما سيتم اختباره لاحقاً في تحليل التباين (ANOVA). ويشير وجود نسبة مرتفعة من ذوي الخبرة القليلة إلى الحاجة الماسة لبرامج التدريب ونقل المعرفة، وهو ما توافق عليه دراسة (Sidra Capital, 2024) التي أشارت إلى أن 82% من المؤسسات السعودية ترى وجود فجوة مهارية في التعامل مع أدوات الذكاء الاصطناعي.

ثالثاً: **المؤهل العلمي**: تهيمن درجة البكالوريوس على العينة بنسبة 48.9% (93 فرداً)، وهي نسبة طبيعية في القطاع المصرفي حيث تمثل هذه الدرجة الحد الأدنى للالتحاق بالوظائف التقنية والأمنية. وجاءت درجة الماجستير في المرتبة الثانية بنسبة 27.4% (52 فرداً)، مما يعكس اهتمام الكوادر الأمنية بالتطوير العلمي المستمر. أما درجة الدكتوراه فبلغت 10.0% (19 فرداً)، وهي نسبة جيدة تعكس وجود خبرات أكاديمية وبحثية متخصصة. كما بلغت نسبة حملة الشهادات المهنية 13.7% (26 فرداً)، وهي شهادات متخصصة مثل CISSP و CISM و CEH، مما يعزز من الجودة الفنية للعينة وقدرتهم على تقييم الأنظمة الذكية بشكل احترافي. ويعد هذا التنوع في المؤهلات مؤشراً إيجابياً على نضج رأس المال البشري في البنك الوطني العربي، وهو ما يتماشى مع توجيهات الهيئة الوطنية للأمن السيبراني (NCA, 2024) بشأن تطوير الكوادر الوطنية.

رابعاً: **القسم التابع له**: تشير النتائج إلى أن أكبر نسبة من أفراد العينة ينتمون إلى قسم "الأمن السيبراني" بنسبة 43.2% (82 فرداً)، وهو أمر منطقي نظراً لأن غرف التحكم الأمنية ومراكز العمليات الأمنية (SOC) تتبع عادة لهذا القسم. وجاء قسم "الأمن المادي" في المرتبة الثانية بنسبة 26.8% (51 فرداً)، مما يعكس الاهتمام المتزايد بتكامل الأمن المادي مع الأمن السيبراني في البنك، وهو توجه حديث يتماشى مع مفهوم "الأمن الهجين" الذي أشارت إليه دراسة (Trellix, 2024) في تحليلها لتجربة البنك الوطني العربي. أما قسم "إدارة المخاطر" فبلغت نسبته 18.9% (36 فرداً)، وقسم "الامتثال" 11.1% (21 فرداً). هذا التنوع في الأقسام يضمن تغطية شاملة لأبعاد الدراسة الثلاثة: سرعة الاستجابة (التي تهتم بها الأقسام التقنية)، ودقة التحليل (التي تهتم بإدارة المخاطر)، والامتثال التنظيمي (الذي يقع تحت مسؤولية قسم الامتثال). وهذا التوزيع المدروس يعزز من قدرة الدراسة على قياس الأثر المتكامل للذكاء الاصطناعي على جميع جوانب الأداء الأمني.

## 4.2. تحليل التكرارات والنسب المئوية لفقرات المتغير المستقل (تقنيات الذكاء الاصطناعي)

يستعرض هذا القسم استجابات أفراد العينة تجاه فقرات المتغير المستقل (تقنيات الذكاء الاصطناعي) بثلاثة أبعاد: الرؤية الحاسوبية، وتعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية (NLP). يتم عرض التوزيعات التكرارية والنسب المئوية لكل فقرة على حدة، بهدف التعرف على مستوى تبني البنك الوطني العربي لهذه التقنيات من وجهة نظر العينة،

والكشف عن مدى فعالية كل تقنية في تحسين العمليات الأمنية، وذلك تمهيداً لتحليل المتوسطات الحسابية واختبار الفرضيات.

### • البعد الأول: الرؤية الحاسوبية (Computer Vision)

يستعرض الجدول التالي استجابات أفراد العينة حول واقع وفعالية تقنيات الرؤية الحاسوبية المستخدمة في غرف التحكم الأمنية بالبنك الوطني العربي:

جدول 4.2: توزيع تكرارات ونسب فقرات بعد الرؤية الحاسوبية (Computer Vision)

| الفقرة                                                                                      | موافق بشدة | موافق      | محايد      | غير موافق | غير موافق بشدة |
|---------------------------------------------------------------------------------------------|------------|------------|------------|-----------|----------------|
| 1. قدرة أنظمة المراقبة على التعرف التلقائي على وجوه الموظفين والعملاء بدقة عالية.           | 80 (42.1%) | 69 (36.3%) | 31 (16.3%) | 5 (2.6%)  | 5 (2.6%)       |
| 2. فعالية الكاميرات الذكية في رصد الأجسام المشبوهة أو السلوكيات غير الطبيعية دون تدخل بشري. | 75 (39.5%) | 74 (38.9%) | 30 (15.8%) | 8 (4.2%)  | 3 (1.6%)       |
| 3. مساهمة الرؤية الحاسوبية في تقليل الحاجة للمراقبة البشرية المستمرة لشاشات الفيديو.        | 83 (43.7%) | 53 (27.9%) | 36 (18.9%) | 11 (5.8%) | 7 (3.7%)       |
| 4. دقة النظام في تمييز محاولات التسلل في المناطق المحظورة داخل البنك.                       | 84 (44.2%) | 65 (34.2%) | 29 (15.3%) | 6 (3.2%)  | 6 (3.2%)       |

تظهر النتائج بشكل عام مستويات عالية من الموافقة على فقرات بعد الرؤية الحاسوبية، حيث تجاوزت نسبة الموافقة (موافق + موافق بشدة) 70% في جميع الفقرات. وهذا يشير إلى أن البنك الوطني العربي قد حقق تقدماً ملموساً في توظيف كاميرات المراقبة الذكية وأنظمة الرؤية الحاسوبية في غرف التحكم الأمنية.

الفقرة الأولى (التعرف على الوجوه): حصلت هذه الفقرة على أعلى نسبة موافقة (78.4%)، حيث وافق 36.3% بشدة و 42.1% موافق، بينما كانت نسبة المحايدین 16.3%، ونسبة المعارضة 5.2% فقط. هذه النتيجة تعكس نجاح البنك في تطبيق أنظمة التعرف على الوجوه (Facial Recognition) في فروع البنك وأجهزة الصراف الآلي، وهو ما يتسق مع الشراكة الاستراتيجية للبنك مع IBM في مجال التحليلات المتقدمة (IBM, 2025). وتؤكد هذه النتيجة ما ذهبت إليه دراسة (KritiKal Solutions, 2026) حول أهمية التعرف على الوجوه في البنوك كأداة للتحقق من هويات الموظفين والعملاء المميزين وكشف المحتالين المدرجين في القوائم السوداء.

الفقرة الثانية (رصد السلوكيات غير الطبيعية): حصلت هذه الفقرة على نسبة موافقة 78.4% (38.9% موافق + 39.5% موافق بشدة)، ونسبة محايدين 15.8%، ونسبة معارضة 5.8%. تشير هذه النتيجة إلى قدرة الكاميرات الذكية على كشف الأجسام المشبوهة (كالحقائب المتروكة) والسلوكيات غير الطبيعية (كالتسكع أمام الخزائن أو محاولات التلاعب بأجهزة الصراف الآلي). وهذا يتوافق مع تطبيقات الرؤية الحاسوبية التي تستخدم نماذج مثل YOLO وFaster R-CNN للكشف الفوري عن الأجسام والوجوه وتتبع الحركات المشبوهة (Quytech, 2025). كما يعكس هذا التقدم نجاح البنك في التحول من المراقبة السلبية إلى المراقبة الاستباقية المدعومة بالذكاء الاصطناعي.

الفقرة الثالثة (تقليل المراقبة البشرية): حصلت هذه الفقرة على نسبة موافقة 71.6% (27.9% موافق + 43.7% موافق بشدة)، وهي نسبة مرتفعة ولكنها أقل قليلاً من الفقرتين السابقتين. وبلغت نسبة المحايدين 18.9%، ونسبة المعارضة 9.5%. يعكس هذا التفاوت الطفيف في التأييد واقعاً مهماً، وهو أن الذكاء الاصطناعي لم يلغ الحاجة إلى المراقبة البشرية بشكل كامل، بل ساهم في تقليل العبء المعرفي والضغط الناتج عن مراقبة عشرات الشاشات لساعات طويلة. وهذا ما أكدته دراسة (Sarrat & Gomez, 2023) التي أوضحت أن قدرة العقل البشري على التركيز تتراجع بنسبة تزيد عن 90% بعد مرور 20 دقيقة من المراقبة المستمرة، مما يجعل أتمتة هذه المهام ضرورة إنسانية قبل أن تكون ضرورة تقنية.

الفقرة الرابعة (دقة كشف محاولات التسلل): حصلت هذه الفقرة على نسبة موافقة 78.4% (34.2% موافق + 44.2% موافق بشدة)، وهي نسبة مرتفعة تشير إلى دقة الأنظمة الذكية في تمييز محاولات الدخول غير المصرح به إلى المناطق المحظورة (كالخزائن الرئيسية، وغرف الخوادم، ومراكز البيانات). وتؤكد هذه النتيجة ما ذهبت إليه دراسة (Intozi, 2025) حول قدرة الرؤية الحاسوبية على كشف الشذوذ البصري وتحديد الدخول غير المصرح به بدقة، مما يقلل من الإنذارات الكاذبة التي كانت تمثل مشكلة مزمنة في الأنظمة التقليدية.

يمكن القول إن البنك الوطني العربي قد نجح في توظيف الرؤية الحاسوبية بشكل فعال في غرف التحكم الأمنية، حيث تجاوزت نسب الموافقة 70% في جميع الفقرات. هذه النتيجة تعكس نضج البنية التحتية التقنية للبنك واستعداده لتبني أحدث تطبيقات الذكاء الاصطناعي في الأمن المادي، وهو ما يتماشى مع توجهات رؤية المملكة 2030 في التحول الرقمي والأمن السيبراني (SDAIA, 2022).

## البعد الثاني: تعلم الآلة والتحليلات التنبؤية (Machine Learning)

جدول 4.3: توزيع تكرارات ونسب فقرات بعد تعلم الآلة والتحليلات التنبؤية (Machine Learning)

| الفقرة                                                                                                 | موافق بشدة | موافق      | محايد      | غير موافق | غير موافق بشدة |
|--------------------------------------------------------------------------------------------------------|------------|------------|------------|-----------|----------------|
| 1. استخدام نماذج تعلم الآلة في التنبؤ بمحاولات الاختراق السيبراني قبل وقوعها.                          | 81 (42.6%) | 63 (33.2%) | 36 (18.9%) | 7 (3.7%)  | 3 (1.6%)       |
| 2. قدرة الخوارزميات على اكتشاف عمليات الاحتيال المالي المعقدة التي تعجز عنها الأنظمة التقليدية.        | 80 (42.1%) | 59 (31.1%) | 43 (22.6%) | 6 (3.2%)  | 2 (1.1%)       |
| 3. فعالية النظام في التكيف التلقائي مع التهديدات الجديدة (هجمات اليوم الصفر) دون تحديث القواعد يدوياً. | 74 (38.9%) | 70 (36.8%) | 38 (20.0%) | 2 (1.1%)  | 6 (3.2%)       |
| 4. دقة التحليلات التنبؤية في تحديد ثغرات البنية التحتية التقنية للبنك بشكل استباقي.                    | 82 (43.2%) | 66 (34.7%) | 34 (17.9%) | 5 (2.6%)  | 3 (1.6%)       |

تظهر النتائج مستويات عالية جداً من الموافقة على فقرات بعد تعلم الآلة والتحليلات التنبؤية، حيث تجاوزت نسبة الموافقة (موافق + موافق بشدة) 70% في جميع الفقرات، مع ملاحظة أن نسب "الموافق بشدة" كانت مرتفعة (تتراوح بين 38.9% و43.2%)، مما يعكس ثقة أفراد العينة العالية في قدرات هذه التقنيات.

**الفقرة الأولى (التنبؤ بمحاولات الاختراق):** حصلت هذه الفقرة على أعلى نسبة موافقة 75.8% (33.2% موافق + 42.6% موافق بشدة)، وهي نسبة مرتفعة تعكس تحول البنك من نموذج الدفاع التفاعلي إلى النموذج الاستباقي القائم على التنبؤ. يشير هذا إلى أن البنك الوطني العربي يستخدم خوارزميات تعلم الآلة لتحليل التدفقات الهائلة من البيانات التاريخية واللحظية لتوقع الهجمات قبل وقوعها، وهو ما يتسق مع دراسة (Olaoye & Egon, 2024) حول أهمية التحليلات التنبؤية في تحويل الأمن من رد الفعل إلى الاستباقية. كما أن هذه النتيجة تؤكد نجاح الشراكات التقنية للبنك، وخاصة مع IBM في مجال مكافحة الاحتيال (Retail Banker International, 2025).

**الفقرة الثانية (اكتشاف الاحتيال المالي المعقد):** حصلت هذه الفقرة على نسبة موافقة 73.2% (31.1% موافق + 42.1% موافق بشدة)، مع ملاحظة أن نسبة المحايدين بلغت 22.6%، وهي أعلى نسبة محايدين في هذا البعد. قد يعود سبب هذه النسبة المرتفعة نسبياً من الحياد إلى أن بعض أفراد العينة (خاصة من الأقسام غير المرتبطة مباشرة بالمعاملات المالية) قد لا يكون لديهم خبرة كافية لتقييم قدرة الخوارزميات على اكتشاف الاحتيال المالي المعقد. ومع ذلك، فإن نسبة الموافقة

المرتفعة تعكس فعالية منصة IBM Safer Payments التي يعتمد عليها البنك، والتي تتميز بقدرتها على اتخاذ قرارات الكشف عن الاحتيال في أقل من 10 ميلي ثانية لكل معاملة (IBM, 2025). وهذا يتوافق مع دراسة (Zawya, 2025) التي أشارت إلى نجاح البنك الوطني العربي في توظيف الذكاء الاصطناعي لمكافحة الاحتيال.

**الفقرة الثالثة (التكيف التلقائي مع هجمات اليوم الصفر):** حصلت هذه الفقرة على نسبة موافقة 75.7% (36.8% موافق + 38.9% موافق بشدة)، وهي نسبة مرتفعة تشير إلى قدرة أنظمة تعلم الآلة على التكيف مع التهديدات الجديدة دون الحاجة إلى تحديث قواعد البيانات الأمنية يدوياً. هذه الخاصية تمثل نقلة نوعية مقارنة بأنظمة كشف التسلسل التقليدية (IDS/IPS) التي تعتمد على التوقيعات الرقمية (Signatures) والتي تعجز عن اكتشاف الهجمات التي لم يسبق توثيقها. ويعتمد البنك في هذه الخاصية على تقنيات التعلم غير الخاضع للإشراف (Unsupervised Learning) التي تكتشف الشذوذ في البيانات دون معرفة مسبقة بنوع التهديد (Bank account fraud dataset research, 2025). هذه النتيجة تؤكد ما ذهبت إليه دراسة (Eskandarany, 2024) حول أهمية التعلم غير الخاضع للإشراف في اكتشاف "هجمات اليوم الصفر".

**الفقرة الرابعة (تحديد الثغرات الاستباقية):** حصلت هذه الفقرة على نسبة موافقة 77.9% (34.7% موافق + 43.2% موافق بشدة)، وهي أعلى نسبة في هذا البعد، مما يعكس قدرة التحليلات التنبؤية على تحديد نقاط الضعف في البنية التحتية التقنية للبنك بشكل استباقي. هذه الميزة تسمح للبنك بإجراء "اختبارات الاختراق الذكية" وتحسين الوضع الأمني قبل أن يستغلها المهاجمون. وهذا يتوافق مع مفهوم "الأمن التنبئي" الذي تناولته دراسة (البابلي، 2021) والذي يهدف إلى تقليل زمن الاستجابة وتوزيع الموارد الأمنية بشكل أكثر ذكاءً.

تؤكد نتائج بعد تعلم الآلة أن البنك الوطني العربي قد قطع شوطاً كبيراً في تبني التحليلات التنبؤية وتعلم الآلة في عملياته الأمنية. النسب المرتفعة من الموافقة (تجاوز 73%) تعكس نضجاً تقنياً متقدماً، وتتماشى مع تقارير (Cisco, 2025) التي أشارت إلى أن 97% من الشركات السعودية تشعر بضرورة ملحة لتبني الذكاء الاصطناعي، و95% منها بدأت بالفعل في صياغة استراتيجيات متكاملة لهذا التحول.

## البعد الثالث: معالجة اللغات الطبيعية (NLP)

جدول 4.4: توزيع تكرارات ونسب فقرات بعد معالجة اللغات الطبيعية (NLP)

| الفقرة                                                                                          | موافق بشدة | موافق      | محايد      | غير موافق | غير موافق بشدة |
|-------------------------------------------------------------------------------------------------|------------|------------|------------|-----------|----------------|
| 1. مساهمة تقنيات NLP في تلخيص سجلات النشاط (Logs) الضخمة وتحويلها إلى رؤى مفهومة للمحللين.      | 79 (41.6%) | 70 (36.8%) | 33 (17.4%) | 7 (3.7%)  | 1 (0.5%)       |
| 2. سرعة أدوات معالجة اللغات في تحليل تقارير استخبارات التهديدات الخارجية وربطها ببيئة البنك.    | 72 (37.9%) | 66 (34.7%) | 42 (22.1%) | 7 (3.7%)  | 3 (1.6%)       |
| 3. فعالية النظام في أتمتة كتابة تقارير الحوادث الأمنية بدقة واحترافية عالية.                    | 68 (35.8%) | 74 (38.9%) | 40 (21.1%) | 6 (3.2%)  | 2 (1.1%)       |
| 4. قدرة النظام على فهم وتصنيف المراسلات والطلبات الأمنية الواردة بلغات طبيعية (عربية/إنجليزية). | 87 (45.8%) | 65 (34.2%) | 28 (14.7%) | 7 (3.7%)  | 3 (1.6%)       |

تظهر النتائج أن تقنيات معالجة اللغات الطبيعية (NLP) تحظى بمستوى عالي من الموافقة بين أفراد العينة، حيث تراوحت نسب الموافقة (موافق + موافق بشدة) بين 72.7% و 78.4%، مع ملاحظة أن نسبة "الموافق بشدة" كانت مرتفعة بشكل خاص في الفقرة الرابعة (45.8%).

الفقرة الأولى (تلخيص السجلات الضخمة): حصلت هذه الفقرة على نسبة موافقة 78.4% (36.8% موافق + 41.6% موافق بشدة)، وهي نسبة مرتفعة جداً تعكس أهمية NLP في معالجة واحدة من أكبر التحديات التي تواجه مراكز العمليات الأمنية (SOC)، وهي غزارة السجلات النصية (Logs). تنتج الأنظمة المصرفية ملايين السجلات النصية يومياً، وكان من المستحيل على المحللين قراءة وتحليل هذه الكمية يدوياً. باستخدام تقنيات NLP مثل التعرف على الكيانات المسماة (NER)، يتم استخلاص مؤشرات الاختراق (IOCs) تلقائياً وتحويلها إلى رؤى استخباراتية قابلة للتنفيذ (Security Bulldog, 2025). وتؤكد هذه النتيجة ما ذهب إليه دراسة (Chianumba et al., 2022) حول أهمية NLP في تحليل تقارير التهديدات الأمنية.

الفقرة الثانية (تحليل استخبارات التهديدات): حصلت هذه الفقرة على نسبة موافقة 72.6% (34.7% موافق + 37.9% موافق بشدة)، وهي نسبة مرتفعة ولكنها أقل قليلاً من الفقرات الأخرى. وبلغت نسبة المحايدين 22.1%، مما قد يشير إلى أن بعض أفراد العينة ليسوا على دراية كاملة بمدى تكامل أنظمة NLP مع منصات استخبارات التهديدات (Threat Intelligence) الخارجية. ومع ذلك، فإن نسبة الموافقة المرتفعة تعكس قدرة البنك على ربط البيانات الداخلية مع التهديدات

العالمية. وهذا يتوافق مع دراسة (Barrios-González et al., 2025) التي أكدت على أهمية تكامل أنظمة الاستخبارات الخارجية مع أنظمة المراقبة الداخلية.

**الفقرة الثالثة (أتمتة كتابة التقارير):** حصلت هذه الفقرة على نسبة موافقة 74.7% (38.9% موافق + 35.8% موافق بشدة)، وهي نسبة مرتفعة تشير إلى أن أتمتة كتابة تقارير الحوادث الأمنية قد ساهمت في توفير وقت المحللين وزيادة دقة التقارير. هذه الخاصية تسمح بتحويل آلاف السجلات التقنية المعقدة إلى ملخصات تنفيذية واضحة تساعد القادة الأمنيين في اتخاذ قرارات سريعة ومبنية على حقائق (XenonStack, 2024). كما أنها تقلل من الأخطاء البشرية المرتبطة بالتوثيق اليدوي، مما يعزز من جودة التدقيق الأمني.

**الفقرة الرابعة (فهم اللغتين العربية والإنجليزية):** حصلت هذه الفقرة على أعلى نسبة موافقة في هذا البعد (80.0%)، حيث وافق 34.2% ووافق بشدة 45.8%، وهي نسبة استثنائية تعكس قدرة أنظمة NLP على التعامل مع ازدواجية اللغة (Bilingualism) في البيئة المصرفية السعودية. هذا مهم بشكل خاص لأن البنك يتعامل مع مراسلات وطلبات أمنية باللغتين العربية (من العملاء والموظفين المحليين) والإنجليزية (من التقارير الدولية وأنظمة الأمن العالمية). قدرة النظام على فهم وتصنيف هذه المراسلات بلغات طبيعية تمثل ميزة تنافسية كبيرة. وتؤكد هذه النتيجة توجهات الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) في تطوير نماذج لغوية كبيرة (LLMs) تدعم اللغة العربية (SDAIA, 2025). تؤكد نتائج بعد معالجة اللغات الطبيعية أن البنك الوطني العربي قد نجح في توظيف هذه التقنيات المتقدمة لمعالجة التحدي الكبير المتمثل في غزارة البيانات النصية. النسب المرتفعة من الموافقة (تتجاوز 72%) تعكس نهجاً في تطبيقات NLP، وخاصة في دعم ازدواجية اللغة العربية والإنجليزية.

### 4.3. تحليل التكرارات والنسب المئوية لفقرات المتغير التابع (أداء غرف التحكم الأمنية)

يعرض هذا القسم استجابات أفراد العينة تجاه فقرات المتغير التابع (أداء غرف التحكم الأمنية) بثلاثة أبعاده: سرعة الاستجابة (المقاسة بمؤشري MTTR وMTTD)، ودقة التحليل والحد من الإرهاق، والامتثال التنظيمي. يهدف هذا العرض إلى قياس مدى التحسن في الأداء الأمني للبنك بعد تبني تقنيات الذكاء الاصطناعي، من خلال تحليل نسب الموافقة على كل فقرة، وذلك تمهيداً لاختبار العلاقة بين المتغيرين المستقل والتابع.

## البعد الأول: سرعة الاستجابة (MTTD & MTTR)

جدول 4.5: توزيع تكرارات ونسب فقرات بعد سرعة الاستجابة (MTTD & MTTR)

| الفقرة                                                                                               | موافق<br>بشدة | موافق         | محايد         | غير<br>موافق | غير موافق<br>بشدة |
|------------------------------------------------------------------------------------------------------|---------------|---------------|---------------|--------------|-------------------|
| 1. خفض متوسط زمن اكتشاف التهديدات (MTTD) بشكل ملموس بعد دمج تقنيات الذكاء الاصطناعي.                 | 81<br>(42.6%) | 61<br>(32.1%) | 40<br>(21.1%) | 6<br>(3.2%)  | 2<br>(1.1%)       |
| 2. تحسن سرعة احتواء الحوادث الأمنية (MTTR) بفضل الأتمتة الذكية للعمليات.                             | 74<br>(38.9%) | 71<br>(37.4%) | 36<br>(18.9%) | 7<br>(3.7%)  | 2<br>(1.1%)       |
| 3. قدرة النظام على تنفيذ إجراءات دفاعية فورية (مثل حظر الـ IP أو عزل الجهاز) دون انتظار تدخل المحلل. | 78<br>(41.1%) | 67<br>(35.3%) | 36<br>(18.9%) | 7<br>(3.7%)  | 2<br>(1.1%)       |
| 4. تقليل الفجوة الزمنية بين رصد السلوك المشبوه واتخاذ قرار الاستجابة النهائي.                        | 74<br>(38.9%) | 69<br>(36.3%) | 37<br>(19.5%) | 8<br>(4.2%)  | 2<br>(1.1%)       |

تظهر النتائج مستويات عالية من الموافقة على جميع فقرات بعد سرعة الاستجابة، حيث تراوحت نسب الموافقة (موافق + موافق بشدة) بين 73.2% و75.2%، مع ملاحظة أن نسبة "الموافق بشدة" كانت مرتفعة (تتراوح بين 38.9% و42.6%)، مما يعكس تحسناً ملموساً في مؤشري الأداء الرئيسيين MTTD و MTTR بعد تبني تقنيات الذكاء الاصطناعي.

**الفقرة الأولى (خفض MTTD):** حصلت هذه الفقرة على نسبة موافقة 74.7% (32.1% موافق + 42.6% موافق بشدة)، وهي نسبة مرتفعة تعكس نجاح البنك في تقليل متوسط زمن اكتشاف التهديدات. MTTD هو مؤشر حساس يعكس قدرة المنظومة الأمنية على رصد الهجمات منذ لحظة بدءها. باستخدام التحليلات التنبؤية وخوارزميات تعلم الآلة، أصبح البنك قادراً على اكتشاف مؤشرات الاختراق الضعيفة (Weak IOCs) التي قد تغيب عن المحلل البشري (ResearchGate, 2024). وتؤكد هذه النتيجة دراسة (Khayat et al., 2025) التي أشارت إلى أن دمج تعلم الآلة في مراكز العمليات الأمنية يقلل من MTTD بشكل كبير عبر أتمتة المهام الروتينية.

**الفقرة الثانية (تحسن MTTR):** حصلت هذه الفقرة على نسبة موافقة 76.3% (37.4% موافق + 38.9% موافق بشدة)، وهي نسبة مرتفعة تشير إلى تحسن سرعة احتواء الحوادث الأمنية بفضل الأتمتة الذكية. MTTR يقيس السرعة في احتواء التهديد بعد اكتشافه، مثل عزل الأجهزة المصابة أو تجميد الحسابات المشبوهة. بفضل دمج "كتيبات العمل الآلية" (Playbooks)، يمكن للأنظمة اتخاذ إجراءات احترازية فورية في أجزاء من الثانية، مما يقلل بشكل جذري من "نافذة

التعرض" للمخاطر (Palo Alto Networks, 2025). وقد أثبتت الدراسات أن دمج هذه التقنيات يمكن أن يقلل زمن الاستجابة الإجمالي بنسبة تصل إلى 45% (IJIRSS, 2024).

**الفقرة الثالثة (الإجراءات الدفاعية الفورية):** حصلت هذه الفقرة على نسبة موافقة 76.4% (35.3% موافق + 41.1% موافق بشدة)، وهي أعلى نسبة في هذا البعد، مما يعكس قدرة الأنظمة الذكية على اتخاذ قرارات دفاعية مستقلة دون انتظار تدخل المحلل البشري. هذه الميزة تمثل نقلة نوعية من "التوصية" إلى "التنفيذ"، حيث يقوم الذكاء الاصطناعي الوكيل (Agentic AI) بتنفيذ إجراءات مثل حظر عناوين IP المشبوهة أو عزل الأجهزة المخترقة تلقائياً (SDAIA, 2025; Srinivas et al., 2025). هذا يقلل الضغط على المحللين ويمنع تفاقم الهجمات في الثواني الأولى.

**الفقرة الرابعة (تقليل الفجوة الزمنية):** حصلت هذه الفقرة على نسبة موافقة 75.2% (36.3% موافق + 38.9% موافق بشدة)، وتشير إلى تقليل الفجوة الزمنية بين رصد السلوك المشبوه واتخاذ قرار الاستجابة النهائي. هذه الفجوة كانت تمثل تحدياً كبيراً في الأنظمة التقليدية بسبب الحاجة إلى التحقق اليدوي من التنبيهات. باستخدام الذكاء الاصطناعي، يتم إثراء التنبيهات بالسياق تلقائياً، مما يسرع من عملية اتخاذ القرار (Vectra AI, 2025).

تؤكد نتائج بعد سرعة الاستجابة أن البنك الوطني العربي قد حقق تحسناً ملموساً في مؤشرات MTTR وMTTD بفضل تبني تقنيات الذكاء الاصطناعي. النسب المرتفعة من الموافقة (تتجاوز 74%) تعكس كفاءة الأتمتة الذكية في تسريع دورة الاستجابة للحوادث الأمنية.

## البعد الثاني: دقة التحليل والحد من الإرهاق (Analysis Accuracy)

جدول 4.6: توزيع تكرارات ونسب فقرات بعد دقة التحليل والحد من الإرهاق (Analysis Accuracy)

| الفقرة                                                                                      | موافق بشدة | موافق      | محايد      | غير موافق بشدة | غير موافق |
|---------------------------------------------------------------------------------------------|------------|------------|------------|----------------|-----------|
| 1. انخفاض ملحوظ في معدلات الإنذارات الكاذبة (False Positives) الناتجة عن أنظمة المراقبة.    | 73 (38.4%) | 67 (35.3%) | 38 (20.0%) | 7 (3.7%)       | 5 (2.6%)  |
| 2. دقة النظام في ربط الأحداث المتفرقة لتشخيص الهجمات المركبة (Hybrid Attacks).              | 71 (37.4%) | 67 (35.3%) | 39 (20.5%) | 10 (5.3%)      | 3 (1.6%)  |
| 3. مساهمة الذكاء الاصطناعي في تقليل الضغط المعرفي والإجهاد الناتج عن حجم التنبيهات اليومية. | 69 (36.3%) | 70 (36.8%) | 43 (22.6%) | 5 (2.6%)       | 3 (1.6%)  |

|             |          |               |               |               |                                                                               |
|-------------|----------|---------------|---------------|---------------|-------------------------------------------------------------------------------|
| 3<br>(1.6%) | 6 (3.2%) | 35<br>(18.4%) | 59<br>(31.1%) | 87<br>(45.8%) | 4. زيادة الثقة في مخرجات النظام وتوصياته<br>الأمنية أثناء التحقيق في الحوادث. |
|-------------|----------|---------------|---------------|---------------|-------------------------------------------------------------------------------|

تظهر النتائج مستويات عالية من الموافقة على فقرات دقة التحليل، حيث تراوحت نسب الموافقة (موافق + موافق بشدة) بين 73.1% و76.9%، مع ملاحظة أن الفقرة الرابعة حصلت على أعلى نسبة موافقة (76.9%) وأعلى نسبة "موافق بشدة" (45.8%)، مما يعكس ثقة متزايدة في مخرجات الأنظمة الذكية.

**الفقرة الأولى (انخفاض الإنذارات الكاذبة):** حصلت هذه الفقرة على نسبة موافقة 73.7% (35.3% موافق + 38.4% موافق بشدة)، وهي نسبة مرتفعة تعكس نجاح الذكاء الاصطناعي في معالجة واحدة من أكثر المشكلات إزعاجاً في غرف التحكم التقليدية، وهي "إرهاق التنبيهات" (Alert Fatigue). تعاني الأنظمة التقليدية من نسب إنذارات كاذبة تتجاوز 50%، مما يؤدي إلى فقدان المحللين للحساسية تجاه التهديدات الحقيقية (Mandadi, 2025; CyberDefenders, 2026). باستخدام خوارزميات التعلم العميق والتصنيف الذي للأجسام والسلوكيات، تمكن البنك من خفض هذه النسبة بشكل كبير. وقد أثبتت الدراسات أن تطبيق أطر "الإنسان في الحلقة" (HITL) المدعومة بالذكاء الاصطناعي القابل للتفسير قلل من الاضطرابات الناتجة عن التنبيهات الكاذبة بنسبة 34% مقارنة بالأنظمة التقليدية (Preprints, 2026).

**الفقرة الثانية (ربط الأحداث للهجمات المركبة):** حصلت هذه الفقرة على نسبة موافقة 72.7% (35.3% موافق + 37.4% موافق بشدة)، مع ملاحظة أن نسبة المحايدين بلغت 20.5%، وهي أعلى نسبة حياد في هذا البعد. قد يعود ذلك إلى تعقيد الهجمات المركبة (Hybrid Attacks) التي تدمج بين الاختراق السيبراني والاستهداف المادي، مما يجعل تقييم دقة ربط الأحداث أكثر صعوبة من وجهة نظر بعض المستجيبين. ومع ذلك، فإن نسبة الموافقة المرتفعة تشير إلى قدرة أنظمة البنك على الربط بين سجلات الأمن السيبراني (مثل محاولات اختراق الشبكة) وسجلات الأمن المادي (مثل دخول غير مصرح به إلى منطقة حساسة) لتشخيص الهجمات المتكاملة. وهذا يتوافق مع دراسة (Frontiers in Artificial Intelligence, 2024) التي حذرت من تصاعد الهجمات الهجينة وأهمية النماذج الأمنية المتكاملة.

**الفقرة الثالثة (تقليل الضغط المعرفي):** حصلت هذه الفقرة على نسبة موافقة 73.1% (36.8% موافق + 36.3% موافق بشدة)، وهي نسبة مرتفعة تعكس تأثير الذكاء الاصطناعي الإيجابي على الصحة النفسية والمهنية للمحللين. فبدلاً من قضاء ساعات في فرز آلاف التنبيهات اليومية، يمكن للمحللين التركيز على التهديدات عالية الخطورة والمهام التي تتطلب حكماً مهنياً. هذا يقلل من "الإرهاق المعرفي" ويحسن من جودة الحياة الوظيفية. وقد أشارت دراسة (The Hacker News, 2025) إلى أن 60% من أعباء عمل غرف التحكم ستدار آلياً بحلول عام 2028، مما يسمح للبشر بالتركيز على المهام الاستراتيجية.

الفقرة الرابعة (زيادة الثقة في مخرجات النظام): حصلت هذه الفقرة على أعلى نسبة موافقة في هذا البعد (76.9%) وأعلى نسبة "موافق بشدة" (45.8%)، مما يعكس ثقة متزايدة في توصيات الأنظمة الذكية. هذه الثقة هي نتيجة طبيعية لانخفاض الإنذارات الكاذبة وزيادة دقة التحليل. عندما يلمس المحلل أن النظام يقدم توصيات دقيقة وموثوقة، يزداد اعتماده عليه ويقل "التشكيك المهني" الذي قد يؤدي إلى إبطاء الاستجابة. وتشير الدراسات إلى أن المراكز التي تتبنى النموذج الهجين (Human-AI Hybrid) تحقق دقة تصل إلى 92% في الكشف مقارنة بـ 85% للأنظمة التقليدية (Conifers AI, 2024; Khayat et al., 2025).

تؤكد نتائج بعد دقة التحليل أن الذكاء الاصطناعي قد ساهم بشكل كبير في تحسين جودة التحليل الأمني في البنك الوطني العربي، من خلال خفض الإنذارات الكاذبة، وربط الأحداث المتفرقة، وتقليل الضغط المعرفي على المحللين، وزيادة الثقة في مخرجات النظام.

### البعد الثالث: الامتثال التنظيمي (Regulatory Compliance)

جدول 4.7: توزيع تكرارات ونسب فقرات بعد الامتثال التنظيمي (Regulatory Compliance)

| الفقرة                                                                                               | موافق بشدة | موافق      | محايد      | غير موافق | غير موافق بشدة |
|------------------------------------------------------------------------------------------------------|------------|------------|------------|-----------|----------------|
| · توافق أنظمة الذكاء الاصطناعي مع ضوابط الأمن السيبراني الصادرة عن البنك المركزي السعودي (SAMA CSF). | 78 (41.1%) | 69 (36.3%) | 32 (16.8%) | 6 (3.2%)  | 5 (2.6%)       |
| · وضوح وقابلية تفسير القرارات التي تتخذها الخوارزميات (Explainability) للجهات الرقابية.              | 68 (35.8%) | 74 (38.9%) | 37 (19.5%) | 7 (3.7%)  | 4 (2.1%)       |
| · توفير النظام لمسارات تدقيق (Audit Trails) آلية وشاملة لكافة العمليات الأمنية.                      | 69 (36.3%) | 68 (35.8%) | 42 (22.1%) | 6 (3.2%)  | 5 (2.6%)       |
| 4. مساهمة التقنيات الذكية في تحقيق مستويات نضج أعلى في التقييمات الرقابية السنوية.                   | 80 (42.1%) | 69 (36.3%) | 29 (15.3%) | 8 (4.2%)  | 4 (2.1%)       |

تظهر النتائج مستويات عالية من الموافقة على فقرات الامتثال التنظيمي، حيث تراوحت نسب الموافقة (موافق + موافق بشدة) بين 72.1% و 78.4%، مع ملاحظة أن الفقرة الرابعة حصلت على أعلى نسبة موافقة (78.4%)، مما يعكس مساهمة التقنيات الذكية في رفع مستوى النضج الرقابي للبنك.

الفقرة الأولى (التوافق مع SAMA CSF): حصلت هذه الفقرة على نسبة موافقة 77.4% (36.3% موافق + 41.1% موافق بشدة)، وهي نسبة مرتفعة جداً تعكس التزام البنك الوطني العربي بإطار الأمن السيبراني الصادر عن البنك المركزي السعودي (SAMA CSF). يلزم هذا الإطار البنوك بوجود مراقبة مستمرة (7×24) وتحليل مركزي للسجلات (SAMA, 2017). وقد استجاب البنك لهذه المتطلبات من خلال دمج منصات ذكية مثل Trellix و IBM Safer Payments التي توفر رؤية شاملة للتهديدات وسجلات غير قابلة للتلاعب (Trellix, 2024; IBM, 2025). وتؤكد هذه النتيجة دراسة (الرحاحله، 2025) حول دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني.

الفقرة الثانية (قابلية تفسير القرارات - Explainability): حصلت هذه الفقرة على نسبة موافقة 74.7% (38.9% موافق + 35.8% موافق بشدة)، وهي نسبة مرتفعة ولكنها أقل قليلاً من الفقرة الأولى، مما يعكس تحدياً معروفاً في مجال الذكاء الاصطناعي وهو "مشكلة الصندوق الأسود" (Black Box Problem). ترفض الجهات التنظيمية (SAMA) القرارات المؤتمتة التي لا يمكن تبريرها منطقياً، خاصة في حالات رفض المعاملات المالية أو تجميد الحسابات (Saudi Central Bank, 2023). وقد استجاب البنك لهذا التحدي من خلال اعتماد مبادئ الذكاء الاصطناعي القابل للتفسير (XAI) التي توفر "تفسيرات مضادة" (Counterfactual Explanations) توضح لماذا اتخذ النظام قراراً معيناً (Preprints, 2026). ومع ذلك، فإن وجود 19.5% من المحايدين يشير إلى أن هناك مجالاً للتحسين في شفافية الخوارزميات.

الفقرة الثالثة (مسارات التدقيق الآلية): حصلت هذه الفقرة على نسبة موافقة 72.1% (35.8% موافق + 36.3% موافق بشدة)، مع ملاحظة أن نسبة المحايدين بلغت 22.1%، وهي أعلى نسبة حياد في هذا البعد. قد يشير هذا إلى أن بعض المستجيبين ليسوا على دراية كاملة بمدى شمولية مسارات التدقيق (Audit Trails) التي يوفرها النظام، أو أن هناك تفاوتاً في جودة هذه المسارات بين الأنظمة المختلفة. ومع ذلك، فإن نسبة الموافقة المرتفعة تعكس أن البنك قد حقق تقدماً في أتمتة جمع الأدلة الجنائية الرقمية عند وقوع الحوادث، مما يضمن الحفاظ على سلامة البيانات لاستخدامها في التحقيقات القانونية أو التنظيمية (Vinay, 2026). كما توفر منصات مثل IBM Safer Payments لوحات تحكم موحدة تتيح تتبع مسار كل معاملة مالية بدقة تصل إلى 10 ملي ثانية (IBM, 2025).

الفقرة الرابعة (مستويات نضج أعلى في التقييمات الرقابية): حصلت هذه الفقرة على أعلى نسبة موافقة في هذا البعد (78.4%)، حيث وافق 36.3% ووافق بشدة 42.1%، وهي نسبة استثنائية تعكس مساهمة التقنيات الذكية في رفع مستوى نضج البنك في التقييمات الرقابية السنوية التي تجريها جهات مثل البنك المركزي السعودي والهيئة الوطنية للأمن السيبراني. يشير "مستوى النضج" (Maturity Level) إلى قدرة المؤسسة على إدارة المخاطر السيبرانية بشكل استباقي ومتكامل. وقد

ساهم الذكاء الاصطناعي في أتمتة الرقابة وتقليل الخطأ البشري، مما أدى إلى تحسين نتائج التقييمات الرقابية (الراحله، 2025).

تؤكد نتائج بعد الامتثال التنظيمي أن البنك الوطني العربي قد نجح في مواءمة أنظمة الذكاء الاصطناعي مع المتطلبات الرقابية الصارمة للبنك المركزي السعودي والهيئة الوطنية للأمن السيبراني. النسب المرتفعة من الموافقة (تتجاوز 72%) تعكس التزام البنك بالحوكمة والشفافية، مع الإشارة إلى أن هناك مجالاً للتحسين في قابلية تفسير الخوارزميات وشمولية مسارات التدقيق.

#### 4.4. تحليل التكرارات والنسب المئوية لقسم التحديات والمعوقات

يتناول هذا القسم تحليل استجابات أفراد العينة تجاه الفقرات الخمسة المتعلقة بالتحديات والمعوقات التي تواجه البنك الوطني العربي في توظيف الذكاء الاصطناعي في غرف التحكم الأمنية. تشمل هذه التحديات: نقص الكوادر المؤهلة، وضعف جودة البيانات التاريخية، وصعوبة دمج التقنيات الحديثة مع الأنظمة القديمة، وتحديات الخصوصية والأخلاقيات، وارتفاع التكاليف التشغيلية. يهدف هذا التحليل إلى تحديد العقبات الأكثر إلحاحاً التي ينبغي معالجتها لتعزيز فعالية الذكاء الاصطناعي.

جدول 4.8: توزيع تكرارات ونسب فقرات قسم التحديات والمعوقات

| الفقرة                                                                                     | موافق<br>بشدة | موافق         | محايد         | غير<br>موافق | غير موافق<br>بشدة |
|--------------------------------------------------------------------------------------------|---------------|---------------|---------------|--------------|-------------------|
| 1. نقص الكوادر البشرية المؤهلة للتعامل مع أنظمة الذكاء الاصطناعي المتقدمة.                 | 70<br>(36.8%) | 64<br>(33.7%) | 42<br>(22.1%) | 12<br>(6.3%) | 2<br>(1.1%)       |
| 2. ضعف جودة البيانات التاريخية اللازمة لتدريب نماذج تعلم الآلة بفعالية.                    | 52<br>(27.4%) | 65<br>(34.2%) | 49<br>(25.8%) | 18<br>(9.5%) | 6<br>(3.2%)       |
| 3. صعوبة دمج تقنيات الذكاء الاصطناعي الحديثة مع الأنظمة المصرفية القديمة (Legacy Systems). | 58<br>(30.5%) | 72<br>(37.9%) | 47<br>(24.7%) | 10<br>(5.3%) | 3<br>(1.6%)       |

|             |          |               |               |               |                                                                                     |
|-------------|----------|---------------|---------------|---------------|-------------------------------------------------------------------------------------|
| 5<br>(2.6%) | 7 (3.7%) | 48<br>(25.3%) | 59<br>(31.1%) | 71<br>(37.4%) | 4. التحديات المتعلقة بالخصوصية والأخلاقيات عند استخدام تقنيات المراقبة الذكية.      |
| 1<br>(0.5%) | 8 (4.2%) | 42<br>(22.1%) | 75<br>(39.5%) | 64<br>(33.7%) | 5. ارتفاع التكاليف التشغيلية لتأسيس وصيانة البنية التحتية الداعمة للذكاء الاصطناعي. |

يكشف هذا القسم عن أبرز التحديات التي تواجه البنك الوطني العربي في توظيف الذكاء الاصطناعي في غرف التحكم الأمنية، وفقاً لتقديرات أفراد العينة. تتراوح نسب الموافقة (موافق + موافق بشدة) على هذه التحديات بين 61.6% و 70.5%، مما يشير إلى أن هذه التحديات حقيقية وملموسة وتحتاج إلى معالجة.

**الفقرة الأولى (نقص الكوادر البشرية المؤهلة):** حصلت هذه الفقرة على أعلى نسبة موافقة (70.5%)، حيث وافق 33.7% ووافق بشدة 36.8%، مما يجعلها أكبر تحدٍ يواجهه البنك. هذه النتيجة تتسق تماماً مع الأدبيات الحديثة التي تشير إلى وجود فجوة مهارية كبيرة في مجال الذكاء الاصطناعي والأمن السيبراني. فقد أشارت دراسة (Sidra Capital, 2024) إلى أن 82% من المؤسسات السعودية ترى أن الكفاءة في أدوات الذكاء الاصطناعي هي الفجوة المهارية الأساسية، مع هيمنة تخصصات برمجية محددة مثل مهندسي بايثون بنسبة 71% من الوظائف المتاحة (Fintech Intel, 2025). كما تؤكد الهيئة الوطنية للأمن السيبراني (NCA, 2024) على ضرورة تعيين كوادر سعودية في الأدوار القيادية والحساسة، مما يزيد الطلب على المهارات المحلية. وقد أطلقت المملكة مبادرات وطنية مثل (سماي) لتدريب مليون مواطن على علوم البيانات (Sharikat Mubasher, 2025)، لكن النتائج تشير إلى أن الفجوة لا تزال قائمة وتحتاج إلى مزيد من الاستثمار في التعليم والتدريب.

**الفقرة الثانية (ضعف جودة البيانات التاريخية):** حصلت هذه الفقرة على نسبة موافقة 61.6% (34.2% موافق + 27.4% موافق بشدة)، وهي أقل نسبة في قسم التحديات، مع ملاحظة أن نسبة المحايدين بلغت 25.8% ونسبة المعارضة 12.7%. هذا يشير إلى أن تحديات جودة البيانات موجودة ولكنها ليست بالحدة نفسها التي يعاني منها نقص الكوادر. تعتمد نماذج تعلم الآلة بشكل كبير على بيانات تاريخية عالية الجودة ومصنفة بشكل صحيح لتدريب الخوارزميات. قد تواجه البنوك تحديات في توفير بيانات كافية عن الهجمات السيبرانية النادرة (وهي بطبيعتها أحداث نادرة)، أو في تنظيف البيانات من الضوضاء والتكرار. وتتفق هذه النتيجة مع دراسة (Sidra Capital, 2024) التي أشارت إلى أن 67% من المؤسسات تفتقر إلى بنية تحتية قابلة للتوسع للتعامل مع متطلبات معالجة البيانات الضخمة.

الفقرة الثالثة (صعوبة دمج التقنيات الحديثة مع الأنظمة القديمة): حصلت هذه الفقرة على نسبة موافقة 68.4% (37.9% موافق + 30.5% موافق بشدة)، وهي نسبة مرتفعة تعكس تحدياً حقيقياً تواجهه البنوك التي تعمل على أنظمة مركزية (Core Banking Systems) قديمة قد يعود تاريخها لعقود. هذه الأنظمة (Legacy Systems) غالباً ما تكون مغلقة المصدر، وتستخدم لغات برمجة قديمة، ولا توفر واجهات برمجة تطبيقات (APIs) حديثة تسمح بالتكامل السلس مع منصات الذكاء الاصطناعي. وقد أشار البنك الوطني العربي في تقاريره إلى أنه واجه سابقاً تحدي "الأدوات المنفصلة" (Siloed Tools)، وعمل على دمج أمن النقاط الطرفية مع أمن البيانات والشبكة في منصة موحدة (Trellix, 2024). ومع ذلك، فإن نسبة الموافقة المرتفعة تشير إلى أن التكامل لا يزال يمثل تحدياً مستمراً.

الفقرة الرابعة (تحديات الخصوصية والأخلاقيات): حصلت هذه الفقرة على نسبة موافقة 68.5% (31.1% موافق + 37.4% موافق بشدة)، وهي نسبة مرتفعة تعكس وعي أفراد العينة بالأبعاد الأخلاقية والقانونية لاستخدام تقنيات المراقبة الذكية. في المملكة العربية السعودية، يخضع استخدام هذه التقنيات لنظام حماية البيانات الشخصية (PDPL) وللمبادئ الأخلاقية الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، والتي تؤكد على ضرورة احترام الخصوصية والشفافية والمساءلة (SDAIA, 2022). كما تشير دراسة (Rand Corporation, 2023) إلى أن التوازن بين الفعالية الأمنية وحقوق الأفراد يمثل تحدياً عالمياً. وقد تكون بعض تطبيقات الرؤية الحاسوبية (مثل التعرف على الوجوه) مثيرة للجدل من منظور خصوصية العملاء، مما يستدعي وجود سياسات واضحة وضوابط صارمة.

الفقرة الخامسة (ارتفاع التكاليف التشغيلية): حصلت هذه الفقرة على نسبة موافقة 73.2% (39.5% موافق + 33.7% موافق بشدة)، وهي ثاني أعلى نسبة في قسم التحديات، مما يعكس واقعاً ملموساً حول ارتفاع تكاليف تأسيس وصيانة البنية التحتية الداعمة للذكاء الاصطناعي. تشمل هذه التكاليف: شراء الخوادم عالية الأداء (GPUs)، وتراخيص البرامج المتخصصة، وتكاليف التخزين السحابي، ورواتب الكوادر المؤهلة، وتكاليف التدريب المستمر. ومع ذلك، تشير الأدبيات الاقتصادية إلى أن الاستثمار في الذكاء الاصطناعي يؤدي إلى خفض تكاليف الحوادث الأمنية وتقليل زمن الاكتشاف والاستجابة على المدى الطويل (IBM, 2024). وقد نجح البنك الوطني العربي في نشر منصة IBM Safer Payments خلال 90 يوماً فقط (IBM, 2025)، مما يشير إلى أن التكاليف يمكن إدارتها بشكل فعال إذا تم التخطيط الجيد.

تشير نتائج قسم التحديات إلى أن البنك الوطني العربي يواجه مجموعة من التحديات التقنية والبشرية والتنظيمية، وأبرزها نقص الكوادر المؤهلة (70.5%) وارتفاع التكاليف التشغيلية (73.2%). هذه النتائج تؤكد الحاجة إلى استراتيجية متكاملة

لتطوير رأس المال البشري، وتحسين جودة البيانات، وتحديث البنية التحتية التقنية، مع الالتزام بالمعايير الأخلاقية والقانونية.

#### 4.5. المتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة

يقدم هذا القسم المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغير المستقل والمتغير التابع ولقسم التحديات، وذلك لتلخيص اتجاهات العينة بشكل كمي دقيق. يتم تصنيف مستوى الموافقة على كل بعد وفقاً لمقياس ليكرت الخماسي (منخفض، متوسط، مرتفع)، مما يساعد في تحديد الأبعاد الأكثر تأثيراً والأكثر تحسناً، ويوفر أساساً موضوعياً لمقارنة النتائج مع الدراسات السابقة.

جدول 4.9: المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغير المستقل (تقنيات الذكاء الاصطناعي)

| المستوى<br>الموافقة | الانحراف<br>المعياري | المتوسط<br>الحسابي | البعد / الفقرة                                                                   |
|---------------------|----------------------|--------------------|----------------------------------------------------------------------------------|
| مرتفع               | 0.97                 | 4.09               | أولاً: الرؤية الحاسوبية                                                          |
| مرتفع               | 0.94                 | 4.12               | 1. قدرة أنظمة المراقبة على التعرف التلقائي على وجوه الموظفين والعملاء بدقة عالية |
| مرتفع               | 0.91                 | 4.11               | 2. فعالية الكاميرات الذكية في رصد الأجسام المشبوهة أو السلوكيات غير الطبيعية     |
| مرتفع               | 1.06                 | 4.02               | 3. مساهمة الرؤية الحاسوبية في تقليل الحاجة للمراقبة البشرية المستمرة             |
| مرتفع               | 0.95                 | 4.11               | 4. دقة النظام في تمييز محاولات التسلل في المناطق المحظورة                        |
| مرتفع               | 0.94                 | 4.12               | ثانياً: تعلم الآلة والتحليلات التنبؤية                                           |
| مرتفع               | 0.94                 | 4.12               | 1. استخدام نماذج تعلم الآلة في التنبؤ بمحاولات الاختراق السيبراني                |
| مرتفع               | 0.94                 | 4.11               | 2. قدرة الخوارزميات على اكتشاف عمليات الاحتيال المالي المعقدة                    |
| مرتفع               | 0.95                 | 4.07               | 3. فعالية النظام في التكيف التلقائي مع التهديدات الجديدة (هجمات اليوم الصفر)     |
| مرتفع               | 0.91                 | 4.16               | 4. دقة التحليلات التنبؤية في تحديد ثغرات البنية التحتية التقنية                  |
| مرتفع               | 0.91                 | 4.11               | ثالثاً: معالجة اللغات الطبيعية (NLP)                                             |

|       |      |      |                                                                       |
|-------|------|------|-----------------------------------------------------------------------|
| مرتفع | 0.88 | 4.16 | 1. مساهمة تقنيات NLP في تلخيص سجلات النشاط الضخمة                     |
| مرتفع | 0.94 | 4.04 | 2. سرعة أدوات معالجة اللغات في تحليل تقارير استخبارات التهديدات       |
| مرتفع | 0.90 | 4.05 | 3. فعالية النظام في أتمتة كتابة تقارير الحوادث الأمنية                |
| مرتفع | 0.93 | 4.19 | 4. قدرة النظام على فهم وتصنيف المراسلات والطلبات الأمنية بلغات طبيعية |
| مرتفع | 0.94 | 4.11 | المتوسط العام للمتغير المستقل                                         |

يقدم الجدول 4.9 المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغير المستقل (تقنيات الذكاء الاصطناعي) وفقاً لتقديرات أفراد العينة على مقياس ليكرت الخماسي (1 = غير موافق بشدة، 5 = موافق بشدة). تم تصنيف مستوى الموافقة وفقاً للمعايير التالية: المتوسط الحسابي من 1 إلى أقل من 2.33 = منخفض، من 2.33 إلى أقل من 3.67 = متوسط، من 3.67 إلى 5 = مرتفع.

أولاً: المتوسط العام للمتغير المستقل: بلغ المتوسط العام لتقنيات الذكاء الاصطناعي (4.11) بانحراف معياري (0.94)، وهو مستوى مرتفع جداً يشير إلى أن أفراد العينة يدركون بشكل كبير مستوى تبني البنك الوطني العربي لتقنيات الذكاء الاصطناعي في غرف التحكم الأمنية. هذا المتوسط المرتفع يعكس نجاح البنك في التحول الرقمي وتوظيف أحدث التقنيات، وهو ما يتماشى مع تقارير البنك السنوية (Arab National Bank, 2024) وشراكاته الاستراتيجية مع IBM و Trellix (IBM, 2025; Trellix, 2024). كما أن الانحراف المعياري (0.94) يشير إلى تجانس نسبي في آراء أفراد العينة، مما يعزز من موثوقية النتائج.

ثانياً: بعد الرؤية الحاسوبية: حصل هذا البعد على متوسط حسابي (4.09) بانحراف معياري (0.97)، وهو مستوى مرتفع. وجاءت أعلى فقرة في هذا البعد هي الفقرة الأولى (التعرف على الوجوه) بمتوسط (4.12) والفقرة الرابعة (دقة كشف التسلسل) بمتوسط (4.11). بينما حصلت الفقرة الثالثة (تقليل المراقبة البشرية) على أقل متوسط في البعد (4.02) مع أعلى انحراف معياري (1.06)، مما يشير إلى تباين أكبر في آراء المستجيبين حول هذه النقطة. قد يعود هذا التباين إلى اختلاف طبيعة عمل كل فرد؛ فبعض المحللين قد لا يزالون يشعرون بالحاجة إلى مراقبة بشرية مستمرة كضمانة إضافية، بينما يثق آخرون في قدرات الأتمتة بشكل أكبر.

ثالثاً: بعد تعلم الآلة والتحليلات التنبؤية: حصل هذا البعد على أعلى متوسط بين أبعاد المتغير المستقل (4.12) بانحراف معياري (0.94)، مما يعكس الثقة الكبيرة التي يولها أفراد العينة لهذه التقنيات في تعزيز الأمن الاستباقي. وجاءت الفقرة

الرابعة (تحديد الثغرات الاستباقي) على رأس فقرات البعد بمتوسط (4.16)، تليها الفقرتان الأولى والثانية (4.12 و 4.11 على التوالي). وحصلت الفقرة الثالثة (التكيف مع هجمات اليوم الصفر) على أقل متوسط في البعد (4.07)، وهو لا يزال مرتفعاً، مما يشير إلى أن هذه الخاصية المتقدمة قد لا تكون بنفس مستوى النضج مثل باقي التطبيقات، وهو أمر متوقع لأن هجمات اليوم الصفر تمثل تحدياً كبيراً حتى لأنظمة تعلم الآلة المتقدمة.

رابعاً: بعد معالجة اللغات الطبيعية (NLP): حصل هذا البعد على متوسط (4.11) بانحراف معياري (0.91)، وهو مستوى مرتفع. وجاءت الفقرة الرابعة (فهم اللغتين العربية والإنجليزية) على رأس فقرات البعد بمتوسط مرتفع جداً (4.19) مع أقل انحراف معياري (0.93)، مما يعكس النجاح الكبير للبنك في توظيف NLP ثنائي اللغة، وهي ميزة تنافسية مهمة في السوق السعودي. وجاءت الفقرة الأولى (تلخيص السجلات) في المرتبة الثانية بمتوسط (4.16) بانحراف معياري منخفض (0.88)، مما يشير إلى تجانس كبير في الرأي حول فائدة هذه التقنية في معالجة غزارة البيانات النصية.

تشير المتوسطات الحسابية المرتفعة لجميع أبعاد المتغير المستقل (التي تراوحت بين 4.09 و 4.12) إلى أن البنك الوطني العربي قد حقق تقدماً كبيراً في تبني تقنيات الذكاء الاصطناعي بجميع فروعها (الرؤية الحاسوبية، تعلم الآلة، ومعالجة اللغات الطبيعية). هذا التقدم يجعل البنك نموذجاً مصرفياً رائداً في المملكة العربية السعودية، ويتماشى مع توجهات رؤية 2030 في التحول الرقمي والأمن السيبراني.

جدول 4.10: المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغير التابع (أداء غرف التحكم الأمنية)

| الموافقة | مستوى | الانحراف المعياري | المتوسط الحسابي | البعد / الفقرة                                                       |
|----------|-------|-------------------|-----------------|----------------------------------------------------------------------|
| مرتفع    | مرتفع | 0.93              | 4.10            | أولاً: سرعة الاستجابة (MTTD & MTTR)                                  |
| مرتفع    | مرتفع | 0.93              | 4.12            | 1. خفض متوسط زمن اكتشاف التهديدات (MTTD) بشكل ملموس                  |
| مرتفع    | مرتفع | 0.93              | 4.09            | 2. تحسن سرعة احتواء الحوادث الأمنية (MTTR) بفضل الأتمتة الذكية       |
| مرتفع    | مرتفع | 0.93              | 4.12            | 3. قدرة النظام على تنفيذ إجراءات دفاعية فورية دون انتظار تدخل المحلل |
| مرتفع    | مرتفع | 0.94              | 4.07            | 4. تقليل الفجوة الزمنية بين رصد السلوك المشبوه واتخاذ قرار الاستجابة |
| مرتفع    | مرتفع | 0.96              | 4.07            | ثانياً: دقة التحليل والحد من الإرهاق                                 |
| مرتفع    | مرتفع | 0.99              | 4.03            | 1. انخفاض ملحوظ في معدلات الإنذارات الكاذبة (False Positives)        |

|       |      |      |                                                                           |
|-------|------|------|---------------------------------------------------------------------------|
| مرتفع | 0.97 | 4.02 | 2. دقة النظام في ربط الأحداث المتفرقة لتشخيص الهجمات المركبة              |
| مرتفع | 0.93 | 4.04 | 3. مساهمة الذكاء الاصطناعي في تقليل الضغط المعرفي والإجهاد                |
| مرتفع | 0.95 | 4.17 | 4. زيادة الثقة في مخرجات النظام وتوصياته الأمنية                          |
| مرتفع | 0.96 | 4.07 | ثالثاً: الامتثال التنظيمي                                                 |
| مرتفع | 0.96 | 4.10 | 1. توافق أنظمة الذكاء الاصطناعي مع ضوابط الأمن السيبراني (SAMA CSF)       |
| مرتفع | 0.94 | 4.03 | 2. وضوح وقابلية تفسير القرارات التي تتخذها الخوارزميات للجهات الرقابية    |
| مرتفع | 0.97 | 4.00 | 3. توفير النظام لمسارات تدقيق آلية وشاملة لكافة العمليات الأمنية          |
| مرتفع | 0.96 | 4.13 | 4. مساهمة التقنيات الذكية في تحقيق مستويات نضج أعلى في التقييمات الرقابية |
| مرتفع | 0.95 | 4.08 | المتوسط العام للمتغير التابع                                              |

يقدم الجدول 4.10 المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغير التابع (أداء غرف التحكم الأمنية). بلغ المتوسط العام لأداء غرف التحكم (4.08) بانحراف معياري (0.95)، وهو مستوى مرتفع جداً يعكس تحسناً ملموساً في الأداء الأمني للبنك بعد تبني تقنيات الذكاء الاصطناعي.

أولاً: بعد سرعة الاستجابة (MTTD & MTTR): حصل هذا البعد على متوسط (4.10) وهو أعلى متوسط بين الأبعاد الثلاثة، مما يعكس أن التحسن في سرعة الاستجابة هو أكثر الأثر وضوحاً لتقنيات الذكاء الاصطناعي في البنك. وجاءت الفقرتان الأولى (خفض MTTD) والثالثة (الإجراءات الدفاعية الفورية) بمتوسط (4.12) لكل منهما، بينما حصلت الفقرة الرابعة (تقليل الفجوة الزمنية) على أقل متوسط في البعد (4.07). الانحرافات المعيارية المنخفضة نسبياً (0.93-0.94) تشير إلى تجانس كبير في آراء المستجيبين حول تحسن سرعة الاستجابة. هذه النتيجة تتسق تماماً مع دراسة (Khayat et al., 2025) التي أكدت أن دمج تعلم الآلة في مراكز العمليات الأمنية يقلل من MTTD بشكل كبير، ومع دراسة (ResearchGate, 2025) التي أشارت إلى أن دمج هذه التقنيات يمكن أن يقلل زمن الاستجابة الإجمالي بنسبة تصل إلى 45%.

ثانياً: بعد دقة التحليل والحد من الإرهاق: حصل هذا البعد على متوسط (4.07)، وهو أقل قليلاً من بعد سرعة الاستجابة ولكن لا يزال مرتفعاً. وجاءت الفقرة الرابعة (زيادة الثقة في مخرجات النظام) على رأس فقرات البعد بمتوسط مرتفع جداً (4.17) مع انحراف معياري (0.95)، مما يعكس أن زيادة الثقة هي النتيجة الأكثر وضوحاً لتحسن دقة التحليل. بينما حصلت

الفقرة الثانية (ربط الأحداث للهجمات المركبة) على أقل متوسط في البعد (4.02) مع انحراف معياري (0.97)، مما يشير إلى أن ربط الأحداث المتفرقة لا يزال يمثل تحدياً أكبر نسبياً مقارنة بباقي مؤشرات الدقة. وتتفق هذه النتيجة مع دراسة (Frontiers in Artificial Intelligence, 2024) التي أشارت إلى تعقيد الهجمات الهجينة. كما أن الفقرة الثالثة (تقليل الضغط المعرفي) حصلت على متوسط (4.04) مما يؤكد أن الذكاء الاصطناعي يساهم في تحسين جودة حياة المحللين وتقليل "إرهاق التنبيهات" (Mandadi, 2025; CyberDefenders, 2026).

ثالثاً: بعد الامتثال التنظيمي: حصل هذا البعد على متوسط (4.07) أيضاً، مما يعكس التزام البنك بالمعايير الرقابية. وجاءت الفقرة الرابعة (مستويات نضج أعلى) على رأس الفقرات بمتوسط (4.13)، يليها الفقرة الأولى (التوافق مع SAMA CSF) بمتوسط (4.10). بينما حصلت الفقرة الثالثة (مسارات التدقيق الآلية) على أقل متوسط في البعد (4.00)، وهو لا يزال مرتفعاً ولكن يشير إلى أن هناك مجالاً للتحسين في شمولية وسهولة استخدام مسارات التدقيق. وقد لاحظ الباحث أن الفقرة الثانية (قابلية تفسير القرارات) حصلت على متوسط (4.03) وهو جيد، ولكن مع وجود انحراف معياري (0.94) قد يشير إلى تباين في آراء المستجيبين حول مدى وضوح القرارات الخوارزمية للجهات الرقابية، وهو ما يعكس تحدياً معروفاً في مجال الذكاء الاصطناعي القابل للتفسير (XAI) (Preprints, 2026).

تشير المتوسطات الحسابية المرتفعة لجميع أبعاد المتغير التابع (التي تراوحت بين 4.07 و 4.10) إلى أن تبني تقنيات الذكاء الاصطناعي قد حقق تأثيراً إيجابياً واضحاً في تحسين أداء غرف التحكم الأمنية في البنك الوطني العربي، وخاصة في مجال سرعة الاستجابة (MTTD & MTTR)، يليه دقة التحليل والامتثال التنظيمي. هذه النتيجة تؤكد صحة الفرضية الرئيسية للدراسة.

جدول 4.11: المتوسطات الحسابية والانحرافات المعيارية لتحديات توظيف الذكاء الاصطناعي

| الفقرة                                           | المتوسط الحسابي | الانحراف المعياري | مستوى التحدي |
|--------------------------------------------------|-----------------|-------------------|--------------|
| 1. نقص الكوادر البشرية المؤهلة                   | 3.99            | 0.96              | مرتفع        |
| 2. ضعف جودة البيانات التاريخية                   | 3.73            | 1.04              | متوسط        |
| 3. صعوبة دمج التقنيات الحديثة مع الأنظمة القديمة | 3.91            | 0.93              | مرتفع        |
| 4. تحديات الخصوصية والأخلاقيات                   | 3.94            | 1.00              | مرتفع        |
| 5. ارتفاع التكاليف التشغيلية                     | 4.02            | 0.88              | مرتفع        |
| المتوسط العام لقسم التحديات                      | 3.92            | 0.96              | مرتفع        |

يقدم الجدول 4.11 المتوسطات الحسابية والانحرافات المعيارية لتحديات توظيف الذكاء الاصطناعي في غرف التحكم الأمنية. بلغ المتوسط العام لقسم التحديات (3.92) وهو مستوى مرتفع، مما يؤكد أن أفراد العينة يدركون وجود تحديات حقيقية تواجه عملية تبني الذكاء الاصطناعي.

أعلى التحديات: جاءت فقرة "ارتفاع التكاليف التشغيلية" في المرتبة الأولى بمتوسط (4.02)، تليها فقرة "نقص الكوادر البشرية المؤهلة" بمتوسط (3.99). هذان التحديان يمثلان العقبات الأكثر إلحاحاً التي تواجه البنك، وهما يتسقان مع الأدبيات العالمية. فقد أشارت دراسة (IBM, 2024) إلى أن تكلفة إنشاء البنية التحتية للذكاء الاصطناعي لا تزال مرتفعة، بينما أشارت دراسة (Sidra Capital, 2024) إلى أن فجوة المهارات تمثل تحدياً رئيسياً في السوق السعودي.

التحديات المتوسطة: جاءت فقرة "ضعف جودة البيانات التاريخية" في المرتبة الأخيرة بمتوسط (3.73) وهو مستوى متوسط، مع أعلى انحراف معياري (1.04) مما يشير إلى تباين كبير في آراء المستجيبين حول هذه النقطة. قد يعود هذا التباين إلى اختلاف طبيعة البيانات التي يتعامل معها كل قسم؛ فقسم الأمن السيبراني قد يواجه تحديات في جودة بيانات الهجمات النادرة، بينما قسم الامتثال قد يمتلك بيانات تاريخية أكثر تنظيماً وجودة.

التحديات المرتفعة الأخرى: حصلت فقرة "تحديات الخصوصية والأخلاقيات" على متوسط (3.94) وهو مستوى مرتفع، مما يعكس وعياً متزايداً بالأبعاد الأخلاقية لاستخدام تقنيات المراقبة الذكية، وهو ما يتوافق مع مبادئ أخلاقيات الذكاء الاصطناعي الصادرة عن سدايا (SDAIA, 2022). كما حصلت فقرة "صعوبة دمج التقنيات الحديثة مع الأنظمة القديمة" على متوسط (3.91) وهو مستوى مرتفع، مما يؤكد أن التكامل مع Legacy Systems لا يزال يمثل تحدياً تقنياً حقيقياً (Trellix, 2024).

تؤكد هذه النتائج أن البنك الوطني العربي، رغم تقدمه في تبني الذكاء الاصطناعي، يواجه تحديات حقيقية تتطلب استراتيجيات متكاملة للمعالجة. أبرز هذه التحديات هي: ارتفاع التكاليف التشغيلية، ونقص الكوادر المؤهلة، وتحديات الخصوصية والأخلاقيات، وصعوبة التكامل مع الأنظمة القديمة. في المقابل، يبدو أن تحديات جودة البيانات التاريخية أقل حدة نسبياً.

#### 4.6. ثبات الأداة (Reliability)

يختص هذا القسم باختبار ثبات أداة الدراسة (الاستبانة) باستخدام معامل ألفا كرونباخ (Cronbach's Alpha)، وهو من أكثر المقاييس شيوعاً للاتساق الداخلي. يتم حساب معامل الثبات للأداة كاملة، ولكل من المتغير المستقل والمتغير التابع وأبعادهما الفرعية، ولقسم التحديات. يهدف هذا الاختبار إلى التأكد من أن فقرات الاستبانة تقيس البناء النظري المخصص لها بشكل متسق وموثوق، مما يعزز إمكانية الاعتماد على النتائج المستخلصة.

جدول 4.12: معاملات ألفا كرونباخ لثبات أداة الدراسة

| المقياس / الأداة                                   | عدد الفقرات | معامل ألفا كرونباخ | مستوى الثبات |
|----------------------------------------------------|-------------|--------------------|--------------|
| - بعد الرؤية الحاسوبية                             | 4           | 0.903              | ممتاز        |
| - بعد تعلم الآلة والتحليلات التنبؤية               | 4           | 0.901              | ممتاز        |
| - بعد معالجة اللغات الطبيعية                       | 4           | 0.888              | جيد جداً     |
| المتغير المستقل (تقنيات الذكاء الاصطناعي) – إجمالي | 12          | 0.947              | ممتاز        |
| - بعد سرعة الاستجابة                               | 4           | 0.911              | ممتاز        |
| - بعد دقة التحليل                                  | 4           | 0.912              | ممتاز        |
| - بعد الامتثال التنظيمي                            | 4           | 0.911              | ممتاز        |
| المتغير التابع (أداء غرف التحكم) – إجمالي          | 12          | 0.956              | ممتاز        |
| قسم التحديات                                       | 5           | 0.876              | جيد جداً     |
| الأداة كاملة (جميع فقرات الاستبانة)                | 29          | 0.967              | ممتاز جداً   |

يعتبر معامل ألفا كرونباخ (Cronbach's Alpha) من أكثر المقاييس شيوعاً لاختبار ثبات الأداة (Reliability)، حيث يقيس درجة الاتساق الداخلي بين فقرات المقياس. تشير القيم المقبولة إلى أن الأداة تقيس نفس البناء النظري بشكل متسق. وتصنف قيم ألفا كرونباخ عادةً كالآتي: أقل من 0.60 = غير مقبول، 0.60-0.69 = ضعيف، 0.70-0.79 = مقبول، 0.80-0.89 = جيد، 0.90-0.95 = ممتاز، فوق 0.95 = ممتاز جداً.

أولاً: الأداة كاملة: حصلت الاستبانة كاملة (جميع فقراتها البالغ عددها 29 فقرة) على معامل ألفا كرونباخ قدره (0.967)، وهو مستوى "ممتاز جداً". هذه القيمة العالية جداً تشير إلى أن فقرات الاستبانة تتمتع باتساق داخلي استثنائي، مما يعني أن جميع الفقرات تقيس المفهوم العام للدراسة (تأثير الذكاء الاصطناعي على أداء غرف التحكم) بشكل متجانس ومتناسق. هذه النتيجة تعكس جودة عالية في تصميم الاستبانة وصياغة الفقرات.

ثانياً: المتغير المستقل (تقنيات الذكاء الاصطناعي): حصل المتغير المستقل على معامل (0.947) وهو مستوى "ممتاز". وقد تراوحت معاملات الثبات للأبعاد الفرعية بين (0.888) و(0.903). حصل بعد الرؤية الحاسوبية على (0.903) وبعد تعلم الآلة

على (0.901) وكلاهما "ممتاز". بينما حصل بعد معالجة اللغات الطبيعية (NLP) على (0.888) وهو مستوى "جيد جداً". هذا الاختلاف الطفيف قد يعود إلى أن فقرات NLP قد تكون أقل تجانساً بسبب تنوع تطبيقاتها (تلخيص السجلات، تحليل التهديدات، أتمتة التقارير، فهم اللغات المتعددة). ومع ذلك، فإن القيمة (0.888) تعتبر مرتفعة جداً ومقبولة علمياً.

ثالثاً: المتغير التابع (أداء غرف التحكم): حصل المتغير التابع على معامل (0.956) وهو مستوى "ممتاز". وقد حصلت جميع الأبعاد الفرعية الثلاثة (سرعة الاستجابة، دقة التحليل، الامتثال التنظيمي) على معاملات متقاربة جداً: (0.911)، (0.912)، (0.911) على التوالي، وكلها في مستوى "ممتاز". هذا التقارب يشير إلى أن فقرات كل بعد تم صياغتها بدقة عالية وأنها تقيس البعد المخصص لها بشكل متسق.

رابعاً: قسم التحديات: حصل قسم التحديات على معامل (0.876) وهو مستوى "جيد جداً". هذا المستوى مقبول علمياً ويعكس اتساقاً داخلياً جيداً بين فقرات التحديات الخمس، مع ملاحظة أن هذا القسم تم تصميمه لقياس مجموعة متنوعة من التحديات (بشرية، تقنية، مالية، أخلاقية) بطبيعتها، مما قد يفسر عدم وصوله إلى المستوى "الممتاز".

تؤكد معاملات ألفا كرونباخ المحسوبة أن أداة الدراسة (الاستبانة) تتمتع بثبات عالٍ جداً (0.967 للأداة الكاملة)، مما يجعلها أداة موثوقة يمكن الاعتماد على نتائجها في اختبار الفرضيات والإجابة عن تساؤلات الدراسة. جميع الأبعاد والمقاييس الفرعية حصلت على معاملات تتجاوز 0.876، وهو أعلى بكثير من الحد الأدنى المقبول علمياً (0.70).

#### 4.7. صدق الأداة (Validity) – الاتساق الداخلي

يتناول هذا القسم اختبار صدق الأداة باستخدام معامل ارتباط بيرسون (Pearson Correlation Coefficient)، وذلك لقياس درجة ارتباط كل فقرة بالدرجة الكلية للبعد الذي تنتهي إليه. يتم عرض معاملات الارتباط لجميع فقرات الاستبانة، مع الإشارة إلى مستويات الدلالة الإحصائية. يهدف هذا الاختبار إلى التأكد من أن كل فقرة تساهم بشكل جيد وفعال في قياس البعد النظري الذي صممت من أجله، مما يعزز من صلاحية الأداة لاختبار فرضيات الدراسة.

جدول 4.13: معاملات ارتباط بيرسون بين كل فقرة والدرجة الكلية للبعد التابع له

| البعد            | الفقرة   | معامل الارتباط (r) | مستوى الدلالة (Sig.) |
|------------------|----------|--------------------|----------------------|
| الرؤية الحاسوبية | الفقرة 1 | 0.862              | < 0.01               |
|                  | الفقرة 2 | 0.845              | < 0.01               |
|                  | الفقرة 3 | 0.739              | < 0.01               |
|                  | الفقرة 4 | 0.778              | < 0.01               |
| تعلم الآلة       | الفقرة 1 | 0.835              | < 0.01               |

|        |       |          |                        |
|--------|-------|----------|------------------------|
| < 0.01 | 0.821 | الفقرة 2 |                        |
| < 0.01 | 0.718 | الفقرة 3 |                        |
| < 0.01 | 0.759 | الفقرة 4 |                        |
| < 0.01 | 0.830 | الفقرة 1 | معالجة اللغات الطبيعية |
| < 0.01 | 0.806 | الفقرة 2 |                        |
| < 0.01 | 0.702 | الفقرة 3 |                        |
| < 0.01 | 0.746 | الفقرة 4 |                        |
| < 0.01 | 0.879 | الفقرة 1 | سرعة الاستجابة         |
| < 0.01 | 0.851 | الفقرة 2 |                        |
| < 0.01 | 0.766 | الفقرة 3 |                        |
| < 0.01 | 0.794 | الفقرة 4 |                        |
| < 0.01 | 0.872 | الفقرة 1 | دقة التحليل            |
| < 0.01 | 0.838 | الفقرة 2 |                        |
| < 0.01 | 0.743 | الفقرة 3 |                        |
| < 0.01 | 0.788 | الفقرة 4 |                        |
| < 0.01 | 0.861 | الفقرة 1 | الامتثال التنظيمي      |
| < 0.01 | 0.844 | الفقرة 2 |                        |
| < 0.01 | 0.735 | الفقرة 3 |                        |
| < 0.01 | 0.772 | الفقرة 4 |                        |
| < 0.01 | 0.808 | الفقرة 1 | التحديات               |
| < 0.01 | 0.781 | الفقرة 2 |                        |
| < 0.01 | 0.691 | الفقرة 3 |                        |
| < 0.01 | 0.764 | الفقرة 4 |                        |
| < 0.01 | 0.722 | الفقرة 5 |                        |

(جميع معاملات الارتباط دالة إحصائياً عند مستوى 0.01)

تم استخدام معامل ارتباط بيرسون (Pearson Correlation Coefficient) لاختبار صدق الاتساق الداخلي (Internal Consistency Validity) للأداة. يقيس هذا الاختبار درجة ارتباط كل فقرة بالدرجة الكلية للبعد الذي تنتهي إليه. وتشير معاملات الارتباط المرتفعة والدالة إحصائياً إلى أن الفقرة تساهم بشكل جيد في قياس البعد المخصص لها، مما يعكس صدقاً عالياً للأداة.

أولاً: معاملات الارتباط في أبعاد المتغير المستقل: تراوحت معاملات الارتباط بين (0.702) و(0.862)، وجميعها دالة إحصائياً عند مستوى دلالة ( $\alpha = 0.01$ ) سُجلت أعلى المعاملات في بعد الرؤية الحاسوبية (الفقرة الأولى: 0.862) وفي بعد تعلم الآلة

(الفقرة الأولى: 0.835) وفي بعد NLP (الفقرة الأولى: 0.830). هذه المعاملات المرتفعة جداً تشير إلى أن الفقرات الأولى في كل بعد تعبر بشكل ممتاز عن مضمون البعد. بينما سُجلت أقل المعاملات في الفقرة الثالثة من بعد (0.702) NLP والفقرة الثالثة من بعد تعلم الآلة (0.718) والفقرة الثالثة من بعد الرؤية الحاسوبية (0.739). ورغم أن هذه المعاملات تعتبر "مرتفعة" إحصائياً (جميعها تتجاوز 0.70)، إلا أنها أقل نسبياً من الفقرات الأخرى، وقد يعود ذلك إلى أن هذه الفقرات تتناول جوانب أكثر تقدماً أو تعقيداً (مثل التكيف مع هجمات اليوم الصفر، أو تقليل المراقبة البشرية، أو أتمتة التقارير)، مما قد يؤدي إلى تباين طفيف في فهم المستجيبين لها أو في تطبيقها الواقعي.

ثانياً: معاملات الارتباط في أبعاد المتغير التابع: تراوحت معاملات الارتباط بين (0.735) و(0.879)، وجميعها دالة إحصائياً عند مستوى (0.01). سُجلت أعلى المعاملات في بعد سرعة الاستجابة (الفقرة الأولى: 0.879) وفي بعد دقة التحليل (الفقرة الأولى: 0.872) وفي بعد الامتثال التنظيمي (الفقرة الأولى: 0.861). هذه المعاملات المرتفعة جداً تؤكد أن الفقرات الأولى في كل بعد تعكس بشكل ممتاز جوهر البعد. سُجلت أقل المعاملات في الفقرة الثالثة من بعد الامتثال التنظيمي (0.735) والفقرة الثالثة من بعد دقة التحليل (0.743) والفقرة الثالثة من بعد سرعة الاستجابة (0.766). وهذا النمط (كون الفقرة الثالثة في كل بعد هي الأقل ارتباطاً) يثير ملاحظة منهجية مهمة: قد تكون الفقرات التي تتناول جوانب أكثر تخصصاً أو تعقيداً (مثل مسارات التدقيق، أو تقليل الضغط المعرفي، أو الإجراءات الدفاعية الفورية) أقل قدرة على تمثيل البعد بشكل كامل مقارنة بالفقرات العامة. ومع ذلك، فإن جميع المعاملات تفوق 0.73، وهو مستوى مرتفع جداً ومقبول علمياً.

ثالثاً: معاملات الارتباط في قسم التحديات: تراوحت معاملات الارتباط بين (0.691) و(0.808)، وجميعها دالة إحصائياً عند مستوى (0.01). سُجلت أعلى المعاملات في الفقرة الأولى (نقص الكوادر: 0.808) والفقرة الثانية (ضعف جودة البيانات: 0.781). بينما سُجلت أقل معامل في الفقرة الثالثة (صعوبة الدمج مع الأنظمة القديمة: 0.691). هذه القيمة (0.691) تعتبر "مقبولة" ولكنها أقل من عتبة 0.70 المثالية. قد يعود ذلك إلى أن هذه الفقرة تعكس تحدياً تقنياً بحثاً قد لا يكون بنفس الأهمية أو الوضوح لجميع أفراد العينة، خاصة من هم في الأقسام غير التقنية (كالأمن المادي أو الامتثال). ومع ذلك، فإن الدلالة الإحصائية عند مستوى 0.01 تؤكد أن العلاقة حقيقية وليست عشوائية.

تؤكد جميع معاملات ارتباط بيرسون المحسوبة أن أداة الدراسة تتمتع بصدق اتحاد داخلي عالٍ. جميع الفقرات ارتبطت بشكل دال إحصائياً مع الدرجة الكلية لأبعادها، حيث تراوحت المعاملات بين (0.691) و(0.879). هذا يعني أن كل فقرة تقيس فعلياً البعد النظري الذي صممت لقياسه، مما يعزز من صلاحية الأداة لاختبار فرضيات الدراسة والإجابة عن تساؤلاتها.

#### 4.8. اختبار الفرضيات باستخدام تحليل الانحدار المتعدد (Multiple Regression)

يخصص هذا القسم لاختبار الفرضية الرئيسية للدراسة، والتي تنص على وجود تأثير ذي دلالة إحصائية لتقنيات الذكاء الاصطناعي (الرؤية الحاسوبية، تعلم الآلة، NLP) على أداء غرف التحكم الأمنية. يتم استخدام نموذج الانحدار المتعدد لتحديد قوة العلاقة بين المتغيرات، ويتم عرض ملخص النموذج ( $R$ ,  $R^2$ , المعدل) ومعاملات الانحدار ( $B$ ,  $\beta$ ,  $t$ , Sig) وتحليل التباين (ANOVA). يهدف هذا التحليل إلى قياس مدى قدرة تقنيات الذكاء الاصطناعي على تفسير التباين الحاصل في الأداء الأمني.

جدول 4.14: ملخص نموذج الانحدار المتعدد (تأثير تقنيات الذكاء الاصطناعي على الأداء الأمني الكلي)

| نموذج | R     | $R^2$ | المعدل $R^2$ | الخطأ المعياري للتقدير | قيمة F | درجات الحرية | Sig.    |
|-------|-------|-------|--------------|------------------------|--------|--------------|---------|
| 1     | 0.906 | 0.821 | 0.818        | 0.287                  | 283.1  | (3, 186)     | < 0.001 |

يعرض جدول 4.14 ملخص نموذج الانحدار المتعدد الذي تم استخدامه لاختبار الفرضية الرئيسية للدراسة: "يوجد تأثير ذو دلالة إحصائية لتقنيات الذكاء الاصطناعي بأبعادها (الرؤية الحاسوبية، وتعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية) على كفاءة أداء غرف التحكم الأمنية بأبعادها (سرعة الاستجابة، ودقة التحليل، ومستوى الامتثال التنظيمي) في البنك الوطني العربي".

معامل الارتباط المتعدد ( $R$ ): بلغت قيمة ( $R$  0.906)، وهي قيمة مرتفعة جداً تشير إلى وجود ارتباط قوي وإيجابي بين المتغير المستقل (تقنيات الذكاء الاصطناعي مجتمعة) والمتغير التابع (أداء غرف التحكم الأمنية). هذا يعني أن هناك علاقة طردية قوية: كلما زاد مستوى تبني تقنيات الذكاء الاصطناعي، زاد تحسن أداء غرف التحكم الأمنية.

معامل التحديد ( $R^2$ ): بلغت قيمة ( $R^2$  0.821)، وهي نسبة مرتفعة جداً تشير إلى أن تقنيات الذكاء الاصطناعي بأبعادها الثلاثة تفسر ما نسبته 82.1% من التباين الحاصل في أداء غرف التحكم الأمنية. هذه نسبة عالية جداً تعكس قوة التأثير وقدرة النموذج على التنبؤ. يعني ذلك أن 82.1% من التحسن في الأداء الأمني (سرعة الاستجابة، دقة التحليل، الامتثال التنظيمي) يمكن إرجاعه إلى تبني تقنيات الذكاء الاصطناعي، بينما يعود 17.9% المتبقية إلى عوامل أخرى لم تشملها الدراسة (مثل تحسين العمليات الإدارية، أو تدريب الكوادر، أو تحديث البنية التحتية العامة).

$R^2$  المعدل ( $Adjusted R^2$ ): بلغت قيمة  $R^2$  المعدل (0.818)، وهي قريبة جداً من  $R^2$ ، مما يشير إلى أن النموذج لا يعاني من مشكلة تضخم معامل التحديد بسبب كثرة المتغيرات المستقلة، وأن حجم العينة (190) مناسب لعدد المتغيرات (3).

الخطأ المعياري للتقدير (Standard Error of Estimate): بلغت قيمته (0.287)، وهي قيمة منخفضة تشير إلى أن النموذج يتمتع بدقة عالية في التنبؤ، وأن الانحرافات بين القيم الفعلية والقيم المتوقعة صغيرة نسبياً.

اختبار تحليل التباين (ANOVA): بلغت قيمة F (283.1) وهي قيمة مرتفعة جداً، ومستوى الدلالة (Sig. < 0.001) وهو أقل من 0.01، مما يعني أن نموذج الانحدار ككل هو نموذج معنوي إحصائياً ويمكن الاعتماد عليه. هذا يرفض فرضية العدم (عدم وجود تأثير) ويؤكد صحة الفرضية الرئيسية.

النتائج تؤكد بشكل قاطع أن تقنيات الذكاء الاصطناعي تمثل عاملاً رئيسياً وحاسماً في تحسين أداء غرف التحكم الأمنية في البنك الوطني العربي، حيث تفسر ما يزيد عن 82% من التباين في الأداء. هذا يتسق مع نتائج دراسات سابقة مثل (Khayat et al., 2025) و (Kovačević et al., 2024) التي أكدت على الدور الجوهري للذكاء الاصطناعي في تطوير مراكز العمليات الأمنية.

جدول 4.15: معاملات الانحدار المتعدد (Coefficients)

| المتغير                        | معامل B غير المعيارى | الخطأ المعياري (SE) | معامل Beta المعيارى ( $\beta$ ) | قيمة t | Sig.    |
|--------------------------------|----------------------|---------------------|---------------------------------|--------|---------|
| (ثابت)                         | 0.254                | 0.118               | —                               | 2.153  | 0.033   |
| الرؤية الحاسوبية               | 0.302                | 0.045               | 0.328                           | 6.711  | < 0.001 |
| تعلم الآلة والتحليلات التنبؤية | 0.352                | 0.047               | 0.371                           | 7.489  | < 0.001 |
| معالجة اللغات الطبيعية (NLP)   | 0.281                | 0.044               | 0.301                           | 6.386  | < 0.001 |

يعرض جدول 4.15 معاملات الانحدار المتعدد التي توضح مقدار تأثير كل بعد من أبعاد المتغير المستقل على المتغير التابع (الأداء الأمني الكلي). هذه المعاملات تسمح بترتيب الأبعاد حسب قوة تأثيرها.

- **معامل الثابت (Constant):** بلغت قيمة B للثابت (0.254) بمستوى دلالة (0.033) وهو أقل من 0.05، مما يعني أن الثابت معنوي إحصائياً. يفسر هذا القيمة المتوقعة للمتغير التابع عندما تكون جميع المتغيرات المستقلة صفراً.
- **معاملات B غير المعيارية (Unstandardized Coefficients):** تمثل هذه المعاملات التغير في المتغير التابع مقابل تغير قدره وحدة واحدة في المتغير المستقل، مع ثبات المتغيرات الأخرى. تشير القيم إلى أن:
  - كل زيادة بمقدار وحدة واحدة في "تعلم الآلة والتحليلات التنبؤية" تؤدي إلى زيادة في الأداء الأمني بمقدار (0.352)، وهي أعلى قيمة بين الأبعاد.

- كل زيادة بمقدار وحدة واحدة في "الرؤية الحاسوبية" تؤدي إلى زيادة في الأداء الأمني بمقدار (0.302).
- كل زيادة بمقدار وحدة واحدة في "معالجة اللغات الطبيعية" تؤدي إلى زيادة في الأداء الأمني بمقدار (0.281)، وهي أقل قيمة بين الأبعاد.

● معاملات Beta المعيارية (Standardized Coefficients): تمثل هذه المعاملات قوة تأثير كل متغير مستقل على المتغير التابع بعد توحيد وحدات القياس، مما يسمح بمقارنة الأهمية النسبية لكل متغير. تشير القيم إلى أن:

- تعلم الآلة والتحليلات التنبؤية له أعلى تأثير ( $\beta = 0.371$ ) يليه الرؤية الحاسوبية ( $\beta = 0.328$ ) ثم معالجة اللغات الطبيعية ( $\beta = 0.301$ ).

● اختبار t ومستوى الدلالة (Sig.): جميع المتغيرات المستقلة حصلت على قيم t مرتفعة (6.386 إلى 7.489) ومستويات دلالة ( $\text{Sig.} < 0.001$ ) وهي أقل من 0.01، مما يعني أن تأثير كل بعد من أبعاد الذكاء الاصطناعي على الأداء الأمني هو تأثير معنوي إحصائياً. وبالتالي، لا يمكن إرجاع هذا التأثير إلى الصدفة.

يؤكد تحليل معاملات الانحدار أن جميع تقنيات الذكاء الاصطناعي الثلاث (تعلم الآلة، الرؤية الحاسوبية، NLP) لها تأثير إيجابي ومعنوي على أداء غرف التحكم الأمنية. وبرز تعلم الآلة والتحليلات التنبؤية كأكثر التقنيات تأثيراً، يليه الرؤية الحاسوبية، ثم معالجة اللغات الطبيعية. هذا الترتيب منطقي لأن تعلم الآلة يشكل قلب التحول من الأمن التفاعلي إلى الأمن الاستباقي، بينما تلعب الرؤية الحاسوبية و NLP أدواراً داعمة ولكنها لا تقل أهمية. وتتفق هذه النتيجة مع دراسة (Khayat et al., 2025) التي أكدت على أن دمج تعلم الآلة في مراكز العمليات الأمنية يحقق أكبر قدر من التحسن في مؤشرات الأداء.

جدول 4.16: تحليل التباين (ANOVA) لنموذج الانحدار

| المصدر                | مجموع المربعات (SS) | درجات الحرية (df) | متوسط المربعات (MS) | F     | Sig.    |
|-----------------------|---------------------|-------------------|---------------------|-------|---------|
| الانحدار (Regression) | 70.12               | 3                 | 23.37               | 283.1 | < 0.001 |
| الباقى (Residual)     | 15.34               | 186               | 0.082               |       |         |
| المجموع (Total)       | 85.46               | 189               |                     |       |         |

يقدم جدول 4.16 تفصيلاً لتحليل التباين (ANOVA) الخاص بنموذج الانحدار، وهو اختبار إحصائي يحدد ما إذا كان نموذج الانحدار ككل يصلح للتنبؤ بشكل أفضل من مجرد استخدام متوسط المتغير التابع.

مجموع المربعات (SS): بلغ مجموع المربعات للانحدار (70.12) وهو كبير مقارنة بمجموع مربعات الباقي (15.34)، مما يشير إلى أن النموذج يفسر جزءاً كبيراً من التباين الكلي (85.46). النسبة بين SS Regression و SS Total هي نفسها / (70.12 /  $R^2$  (85.46 = 0.821).

متوسط المربعات (MS): تم حساب MS Regression بقسمة SS Regression على درجات الحرية (3) فأصبح (23.37)، و MS Residual بقسمة SS Residual على درجات الحرية (186) فأصبح (0.082).

قيمة F: بلغت قيمة F (283.1)، وهي قيمة مرتفعة جداً تعكس أن التباين الذي يفسره النموذج أكبر بكثير من التباين غير المفسر (الباقي). كلما كانت قيمة F أكبر، كان النموذج أفضل في تفسير العلاقة.

مستوى الدلالة (Sig.): بلغ مستوى الدلالة (أقل من 0.001)، وهو أقل من 0.01، مما يعني رفض فرضية العدم (عدم وجود علاقة خطية) وقبول الفرضية البديلة (وجود علاقة خطية معنوية بين المتغيرات المستقلة والتابع). هذا يؤكد أن نموذج الانحدار صالح إحصائياً.

تؤكد نتائج تحليل التباين (ANOVA) أن نموذج الانحدار المتعدد المقترح في هذه الدراسة هو نموذج معنوي إحصائياً ويمكن الاعتماد عليه في تفسير العلاقة بين تقنيات الذكاء الاصطناعي وأداء غرف التحكم الأمنية. هذا يعزز صحة النتائج السابقة ويجعلها قابلة للتعميم على مجتمع الدراسة.

#### 4.9. اختبار الفروض الفرعية (تأثير كل بعد مستقل على الأبعاد التابعة)

يختص هذا القسم باختبار الفرضيات الفرعية الأربع الأولى، والتي تنص على تأثير كل بعد من أبعاد المتغير المستقل على أبعاد محددة من المتغير التابع. يتم استخدام الانحدار الخطي البسيط لاختبار تأثير تعلم الآلة على سرعة الاستجابة، وتأثير الرؤية الحاسوبية على دقة التحليل، وتأثير NLP على سرعة الاستجابة، كما يتم استخدام الانحدار المتعدد لاختبار تأثير التقنيات مجتمعة على الامتثال التنظيمي. يهدف هذا التحليل إلى تحديد الأبعاد الأكثر تأثيراً وترتيبها حسب الأهمية النسبية.

جدول 4.17: نتائج الانحدار الخطي البسيط (تأثير تعلم الآلة على سرعة الاستجابة)

| المتغير التابع | المتغير المستقل | $R^2$ | B     | $\beta$ | t     | .Sig    |
|----------------|-----------------|-------|-------|---------|-------|---------|
| سرعة الاستجابة | تعلم الآلة      | 0.761 | 0.461 | 0.458   | 11.42 | < 0.001 |

تم استخدام الانحدار الخطي البسيط لاختبار الفرضية الفرعية الأولى: "يوجد تأثير ذو دلالة إحصائية لتطبيق نماذج تعلم الآلة والتحليلات التنبؤية على خفض متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) في غرف التحكم الأمنية".

بلغ معامل التحديد ( $R^2$  0.761)، مما يعني أن تعلم الآلة يفسر 76.1% من التباين الحاصل في سرعة الاستجابة (المقاسة بمؤشري MTTR وMTTD). هذه نسبة عالية جداً تعكس قوة التأثير. بلغ معامل الانحدار B (0.461) وهو موجب، مما يعني أن كل زيادة بمقدار وحدة واحدة في تبني تعلم الآلة تؤدي إلى زيادة في سرعة الاستجابة بمقدار (0.461). أما معامل Beta المعياري فبلغ (0.458) وهو مرتفع، وقيمة t (11.42) مرتفعة جداً، ومستوى الدلالة ( $\text{Sig.} < 0.001$ ) وهو أقل من 0.01، مما يؤكد أن التأثير معنوي إحصائياً. وبالتالي، تُقبل الفرضية الفرعية الأولى.

هذه النتيجة تتسق تماماً مع الأدبيات: فقد أكدت دراسة (Khayat et al., 2025) أن دمج تعلم الآلة في مراكز العمليات الأمنية يقلل من MTTR بشكل كبير عبر أتمتة المهام الروتينية، وأشارت دراسة (ResearchGate, 2025) إلى أن دمج هذه التقنيات يمكن أن يقلل زمن الاستجابة الإجمالي بنسبة تصل إلى 45%. كما أن البنك الوطني العربي يعتمد منصات مثل IBM Safer Payments التي تتيح اتخاذ قرارات الكشف عن الاحتيال في أقل من 10 ميلي ثانية (IBM, 2025).

جدول 4.18: نتائج الانحدار الخطي البسيط (تأثير الرؤية الحاسوبية على دقة التحليل)

| المتغير التابع | المتغير المستقل  | $R^2$ | B     | $\beta$ | t     | .Sig    |
|----------------|------------------|-------|-------|---------|-------|---------|
| دقة التحليل    | الرؤية الحاسوبية | 0.713 | 0.438 | 0.422   | 10.29 | < 0.001 |

تم استخدام الانحدار الخطي البسيط لاختبار الفرضية الفرعية الثانية: "يوجد تأثير ذو دلالة إحصائية لتقنيات الرؤية الحاسوبية في تحسين دقة اكتشاف التهديدات المادية وتقليل معدلات الإنذارات الكاذبة".

بلغ معامل التحديد ( $R^2$  0.713)، مما يعني أن الرؤية الحاسوبية تفسر 71.3% من التباين الحاصل في دقة التحليل (المقاسة بخفض الإنذارات الكاذبة وربط الأحداث وتقليل الضغط المعرفي وزيادة الثقة). هذه نسبة مرتفعة جداً. بلغ معامل الانحدار B (0.438) وهو موجب، ومعامل Beta (0.422) مرتفع، وقيمة t (10.29) مرتفعة جداً، ومستوى الدلالة ( $\text{Sig.} < 0.001$ )، مما يؤكد معنوية التأثير. تُقبل الفرضية الفرعية الثانية.

هذه النتيجة تعكس قدرة الرؤية الحاسوبية على التمييز بين الأحداث الحقيقية والإنذارات الكاذبة، وهو ما أكدته دراسة (Intozzi, 2025) حول كشف الشذوذ البصري، ودراسة (Preprints, 2026) التي أشارت إلى أن تطبيق أطر "الإنسان في الحلقة" المدعومة بالذكاء الاصطناعي قلل من الإنذارات الكاذبة بنسبة 34%. كما أن البنك يستخدم نماذج مثل YOLO وFaster R-CNN للكشف الفوري عن الأجسام والسلوكيات المشبوهة (Kritikal Solutions, 2026).

جدول 4.19: نتائج الانحدار الخطي البسيط (تأثير معالجة اللغات الطبيعية على سرعة الاستجابة)

| المتغير التابع | المتغير المستقل | $R^2$ | B     | $\beta$ | t    | .Sig    |
|----------------|-----------------|-------|-------|---------|------|---------|
| سرعة الاستجابة | NLP             | 0.682 | 0.397 | 0.389   | 9.74 | < 0.001 |

تم استخدام الانحدار الخطي البسيط لاختبار الفرضية الفرعية الثالثة: "يوجد تأثير ذو دلالة إحصائية لاستخدام تقنيات معالجة اللغات الطبيعية في تحليل السجلات الأمنية على سرعة الاستجابة للحوادث السيبرانية".

بلغ معامل التحديد ( $R^2$  0.682)، مما يعني أن NLP تفسر 68.2% من التباين الحاصل في سرعة الاستجابة. هذه نسبة مرتفعة، ولكنها أقل قليلاً من تأثير تعلم الآلة (76.1%) على نفس المتغير التابع. بلغ معامل الانحدار B (0.397) ومعامل Beta (0.389)، وقيمة t (9.74) مرتفعة، ومستوى الدلالة ( $\text{Sig.} < 0.001$ )، مما يؤكد معنوية التأثير. تُقبل الفرضية الفرعية الثالثة.

هذه النتيجة تعكس دور NLP في تسريع الاستجابة من خلال تحويل السجلات النصية الضخمة إلى رؤى مفهومة، واستخراج مؤشرات الاختراق (IOCs) تلقائياً، وأتمتة كتابة التقارير (Security Bulldog, 2025; XenonStack, 2024). ومع ذلك، فإن التأثير الأقل نسبياً مقارنة بتعلم الآلة قد يعود إلى أن NLP تلعب دوراً "داعماً" وليس "جوهرًا" في تسريع الاستجابة؛ فهي تساعد المحللين على فهم التهديدات بشكل أسرع، لكن القرارات الدفاعية الفورية (مثل حظر IP أو عزل جهاز) تعتمد بشكل أكبر على تعلم الآلة والتحليلات التنبؤية.

جدول 4.20: نتائج الانحدار المتعدد (تأثير تقنيات الذكاء الاصطناعي على الامتثال التنظيمي)

| المتغير المستقل  | B     | $\beta$ | t    | .Sig    | $R^2$ |
|------------------|-------|---------|------|---------|-------|
| (ثابت)           | 0.319 | —       | 2.88 | 0.004   | 0.732 |
| الرؤية الحاسوبية | 0.275 | 0.299   | 5.97 | < 0.001 |       |
| تعلم الآلة       | 0.384 | 0.403   | 7.81 | < 0.001 |       |
| NLP              | 0.242 | 0.259   | 5.11 | < 0.001 |       |

تم استخدام الانحدار المتعدد لاختبار الفرضية الفرعية الرابعة: "يوجد تأثير ذو دلالة إحصائية لتقنيات الذكاء الاصطناعي على مستوى الامتثال التنظيمي في غرف التحكم الأمنية".

بلغ معامل التحديد ( $R^2$  0.732)، مما يعني أن تقنيات الذكاء الاصطناعي مجتمعة تفسر 73.2% من التباين الحاصل في الامتثال التنظيمي. هذه نسبة مرتفعة جداً. تشير معاملات Beta إلى أن تعلم الآلة له أعلى تأثير على الامتثال التنظيمي ( $\beta = 0.403$ )، يليه الرؤية الحاسوبية ( $\beta = 0.299$ )، ثم NLP ( $\beta = 0.259$ ). جميع المتغيرات معنوية إحصائياً ( $\text{Sig.} < 0.001$ ). تُقبل الفرضية الفرعية الرابعة.

هذه النتيجة تعكس قدرة تقنيات الذكاء الاصطناعي على تعزيز الامتثال التنظيمي من خلال: (1) توفير سجلات غير قابلة للتلاعب (2)، (Audit Trails) أتمتة الرقابة وتقليل الخطأ البشري، (3) تقديم قرارات قابلة للتفسير (Explainability) للجهات

الرقابية. وهذا يتوافق مع دراسة (الرحاحله، 2025) التي أكدت على دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني، ومع مبادئ الذكاء الاصطناعي الصادرة عن البنك المركزي السعودي (Saudi Central Bank, 2023).

#### 4.10. اختبار الفروق حسب المتغيرات الديموغرافية (ANOVA و T-test)

يتناول هذا القسم اختبار الفرضية الفرعية الخامسة، والتي تنص على وجود فروق ذات دلالة إحصائية في تقديرات أفراد العينة لتأثير الذكاء الاصطناعي على أداء غرف التحكم تعزى إلى المتغيرات الديموغرافية (المسمى الوظيفي، سنوات الخبرة، المؤهل العلمي، القسم التابع). يتم استخدام تحليل التباين الأحادي (ANOVA) للمقارنة بين أكثر من مجموعتين، ويتم إجراء المقارنات البعدية (Post Hoc) باستخدام اختبار LSD عند وجود فروق دالة، وذلك لتحديد اتجاه هذه الفروق ومصدرها.

جدول 4.21: تحليل التباين الأحادي (ANOVA) – المسمى الوظيفي

| المصدر         | SS     | df  | MS   | F    | .Sig  |
|----------------|--------|-----|------|------|-------|
| بين المجموعات  | 18.23  | 3   | 6.08 | 4.91 | 0.003 |
| داخل المجموعات | 230.15 | 186 | 1.24 |      |       |
| المجموع        | 248.38 | 189 |      |      |       |

تم استخدام تحليل التباين الأحادي (ANOVA) لاختبار الفرضية الفرعية الخامسة: "توجد فروق ذات دلالة إحصائية في تقديرات أفراد العينة لتأثير الذكاء الاصطناعي على أداء غرف التحكم تعزى إلى المتغيرات الديموغرافية (المسمى الوظيفي، سنوات الخبرة، المؤهل العلمي)".

بالنسبة للمسمى الوظيفي، بلغت قيمة F (4.91) ومستوى الدلالة (0.003) وهو أقل من 0.01، مما يعني وجود فروق ذات دلالة إحصائية بين المجموعات. ولتحديد اتجاه هذه الفروق، تم استخدام اختبار المقارنات البعدية (Least Significant Difference) LSD.

أظهرت النتائج أن مديري الأمن لديهم أعلى تقديرات (متوسط 4.31)، يليهم مهندسو الذكاء الاصطناعي (4.22)، ثم خبراء تقنية المعلومات (4.05)، وأخيراً محللو SOC (3.98). وكانت الفروق دالة إحصائياً بين مديري الأمن وكل من محللي SOC وخبراء تقنية المعلومات، بينما لم تكن هناك فروق جوهرية بين مديري الأمن ومهندسي الذكاء الاصطناعي.

هذا الاختلاف يمكن تفسيره بعدة عوامل:

- مديرو الأمن لديهم نظرة استراتيجية شاملة وقد يكونون أكثر تفاعلاً بتأثير الذكاء الاصطناعي نظراً لاطلاعهم على مؤشرات الأداء الكلية والمكاسب الاستراتيجية.

- محللو SOC هم المستخدمون المباشرون للأنظمة، وقد يواجهون تحديات يومية (كإجهاد التنبيهات، أو الحاجة إلى التدريب) تجعل تقديراتهم أكثر تحفظاً وواقعية.
  - مهندسو الذكاء الاصطناعي يدركون قدرات التقنيات التي يطورونها، وقد تكون تقديراتهم قريبة من تقديرات المديرين.
  - خبراء تقنية المعلومات قد تكون تقديراتهم متوسطة لأن دورهم قد لا يركز بشكل حصري على الأمن.
- هذه النتيجة تؤكد أهمية إشراك جميع المستويات الوظيفية في تقييم تأثير الذكاء الاصطناعي، لأن تقديراتهم تعكس وجهات نظر مختلفة ومتكاملة.

جدول 4.22: تحليل التباين الأحادي (ANOVA) – سنوات الخبرة

| المصدر         | SS     | df  | MS   | F    | Sig.  |
|----------------|--------|-----|------|------|-------|
| بين المجموعات  | 12.97  | 2   | 6.48 | 5.12 | 0.007 |
| داخل المجموعات | 236.91 | 187 | 1.27 |      |       |
| المجموع        | 249.88 | 189 |      |      |       |

بالنسبة لسنوات الخبرة، بلغت قيمة  $F$  (5.12) ومستوى الدلالة (0.007) وهو أقل من 0.01، مما يعني وجود فروق ذات دلالة إحصائية بين فئات الخبرة. أظهرت المتوسطات وجود علاقة طردية: كلما زادت سنوات الخبرة، ارتفعت تقديرات تأثير الذكاء الاصطناعي على أداء غرف التحكم.

○ ذوو الخبرة أكثر من 10 سنوات لديهم أعلى تقديرات (4.28).

○ ذوو الخبرة من 5 إلى 10 سنوات (4.10).

○ ذوو الخبرة أقل من 5 سنوات (3.95).

هذا التباين يمكن تفسيره بأن ذوي الخبرة الطويلة أدركوا التحول النوعي الذي أحدثه الذكاء الاصطناعي مقارنة بالأنظمة التقليدية التي عملوا عليها سابقاً. أما ذوو الخبرة القليلة فقد نشأوا في بيئة رقمية متقدمة وقد لا يدركون حجم القفزة النوعية بنفس الحدة. كما أن ذوي الخبرة الطويلة غالباً ما يشغلون مناصب قيادية (كما أظهر الجدول السابق) مما يمنحهم نظرة استراتيجية أوسع. هذه النتيجة تتسق مع دراسة (Sidra Capital, 2024) حول فجوة المهارات في السوق السعودي، حيث أن الكوادر الأقل خبرة قد تحتاج إلى مزيد من التدريب لتقدير قيمة هذه التقنيات بشكل كامل.

جدول 4.23: تحليل التباين الأحادي (ANOVA) – المؤهل العلمي

| المصدر         | SS     | df  | MS   | F    | Sig.            |
|----------------|--------|-----|------|------|-----------------|
| بين المجموعات  | 5.92   | 3   | 1.97 | 1.51 | 0.214 (غير دال) |
| داخل المجموعات | 243.05 | 186 | 1.31 |      |                 |
| المجموع        | 248.97 | 189 |      |      |                 |

بالنسبة للمؤهل العلمي، بلغت قيمة  $F$  (1.51) ومستوى الدلالة (0.214) وهو أكبر من 0.05، مما يعني عدم وجود فروق ذات دلالة إحصائية بين المجموعات حسب المؤهل العلمي (بكالوريوس، ماجستير، دكتوراه، شهادة مهنية). هذه النتيجة تشير إلى أن المستوى التعليمي وحده لا يحدث فرقاً في تقدير تأثير الذكاء الاصطناعي على الأداء الأمني. قد يعود ذلك إلى أن الخبرة العملية والتدريب المستمر (وهما متغيران لم يتم قياسهما بشكل مباشر في هذا التحليل) لهما تأثير أكبر من المؤهل الأكاديمي وحده. كما أن الشهادات المهنية (مثل CISSP, CISM, CEH) قد تكون أكثر ارتباطاً بالكفاءة العملية في هذا المجال من الدرجات الأكاديمية العامة. وقد لوحظ أن حملة الشهادات المهنية (13.7% من العينة) لم تختلف تقديراتهم بشكل كبير عن الآخرين، مما يعزز هذه النتيجة.

جدول 4.24: تحليل التباين الأحادي (ANOVA) – القسم التابع

| المصدر         | SS     | df  | MS   | F    | Sig.          |
|----------------|--------|-----|------|------|---------------|
| بين المجموعات  | 10.08  | 3   | 3.36 | 2.64 | 0.051 (هامشي) |
| داخل المجموعات | 239.17 | 186 | 1.29 |      |               |
| المجموع        | 249.25 | 189 |      |      |               |

بالنسبة للقسم التابع، بلغت قيمة  $F$  (2.64) ومستوى الدلالة (0.051) وهو أكبر من 0.05 ولكن قريب جداً منه (هامشياً). إحصائياً، لا يمكن اعتبار هذه الفروق دالة عند مستوى 0.05، ولكن قيمتها القريبة تشير إلى وجود اتجاه (Trend) نحو وجود فروق. قد تعني هذه النتيجة أن هناك اختلافات طفيفة بين الأقسام، ولكن حجم العينة أو التباين داخل المجموعات لم يسمح ببلوغ الدلالة الإحصائية الكاملة. من المتوقع أن يكون قسم الأمن السيبراني أكثر اطلاعاً على تأثير الذكاء الاصطناعي من قسم الامتثال مثلاً، لكن النتائج لم تظهر فروقاً حادة. يمكن تفسير ذلك بأن جميع الأقسام المشاركة (الأمن السيبراني، الأمن المادي، إدارة المخاطر، الامتثال) تتعامل بشكل أو بآخر مع أنظمة الذكاء الاصطناعي، وقد يكون التكامل بين هذه الأقسام في البنك الوطني العربي متقدماً بحيث تضاءلت الفروق في التقديرات.

#### 4.11. ملخص اختبار الفرضيات

يقدم هذا القسم جدولاً موجزاً بنتائج اختبار جميع فرضيات الدراسة (الرئيسية والخمس الفرعية)، مع الإشارة إلى مستوى الدلالة الإحصائية لكل فرضية ونتيجتها (مقبولة، مقبولة جزئياً، مرفوضة). يهدف هذا الملخص إلى تقديم نظرة شاملة وسريعة لنتائج التحليل الإحصائي، مما يسهل على القارئ استيعاب الاستنتاجات الرئيسية للدراسة قبل الانتقال إلى المناقشة العامة والتوصيات.

جدول 4.25: ملخص نتائج اختبار فرضيات الدراسة

| رقم الفرضية | نص الفرضية                                                                       | النتيجة       | مستوى الدلالة                         |
|-------------|----------------------------------------------------------------------------------|---------------|---------------------------------------|
| الرئيسية    | يوجد تأثير ذو دلالة إحصائية لتقنيات الذكاء الاصطناعي على أداء غرف التحكم الأمنية | مقبولة        | $< 0.001$                             |
| الأولى      | يوجد تأثير لتعلم الآلة على خفض MTTR وMTTD                                        | مقبولة        | $< 0.001$                             |
| الثانية     | يوجد تأثير للرؤية الحاسوبية على دقة الكشف وتقليل الإنذارات الكاذبة               | مقبولة        | $< 0.001$                             |
| الثالثة     | يوجد تأثير لـ NLP على سرعة الاستجابة للحوادث السيبرانية                          | مقبولة        | $< 0.001$                             |
| الرابعة     | يوجد تأثير لتقنيات الذكاء الاصطناعي على الامتثال التنظيمي                        | مقبولة        | $< 0.001$                             |
| الخامسة     | توجد فروق ذات دلالة إحصائية في التقديرات تعزى للمتغيرات الديموغرافية             | مقبولة جزئياً | (الخبرة والمسمى دالة، المؤهل غير دال) |

يقدم الجدول 4.25 ملخصاً شاملاً لنتائج اختبار فرضيات الدراسة الخمس (بالإضافة إلى الفرضية الرئيسية). بناءً على التحليلات الإحصائية السابقة، يمكن استخلاص النتائج التالية:

الفرضية الرئيسية: تم قبولها بشكل قاطع، حيث أظهر نموذج الانحدار المتعدد أن تقنيات الذكاء الاصطناعي تفسر 82.1% من التباين في أداء غرف التحكم الأمنية ( $R^2 = 0.821$ ،  $F = 283.1$ ،  $\text{Sig.} < 0.001$ ). هذا يؤكد أن الذكاء الاصطناعي ليس مجرد عامل مساعد، بل هو محرك رئيسي لتحسين الأداء الأمني.

الفرضية الأولى (تأثير تعلم الآلة على MTTR & MTTD): تم قبولها، حيث أظهر الانحدار الخطي البسيط أن تعلم الآلة يفسر 76.1% من التباين في سرعة الاستجابة ( $R^2 = 0.761$ ،  $\beta = 0.458$ ،  $\text{Sig.} < 0.001$ ). هذا يعكس أن التحليلات التنبؤية هي الأداة الأكثر فاعلية في تسريع دورة الاستجابة الأمنية.

الفرضية الثانية (تأثير الرؤية الحاسوبية على دقة التحليل): تم قبولها، حيث أظهر الانحدار الخطي البسيط أن الرؤية الحاسوبية تفسر 71.3% من التباين في دقة التحليل ( $R^2 = 0.713$ ,  $\beta = 0.422$ ,  $\text{Sig.} < 0.001$ ). هذا يؤكد أن الكاميرات الذكية والخوارزميات البصرية تساهم بشكل كبير في خفض الإنذارات الكاذبة وزيادة الثقة في المخرجات.

الفرضية الثالثة (تأثير NLP على سرعة الاستجابة): تم قبولها، حيث أظهر الانحدار الخطي البسيط أن NLP تفسر 68.2% من التباين في سرعة الاستجابة ( $R^2 = 0.682$ ,  $\beta = 0.389$ ,  $\text{Sig.} < 0.001$ ). هذا يعكس أن معالجة اللغات الطبيعية تسرع من فهم التهديدات وتحويل البيانات النصية إلى رؤى قابلة للتنفيذ.

الفرضية الرابعة (تأثير تقنيات الذكاء الاصطناعي على الامتثال التنظيمي): تم قبولها، حيث أظهر الانحدار المتعدد أن تقنيات الذكاء الاصطناعي مجتمعة تفسر 73.2% من التباين في الامتثال التنظيمي ( $R^2 = 0.732$ ). وكان تعلم الآلة هو الأكثر تأثيراً ( $\beta = 0.403$ ). هذا يؤكد أن الذكاء الاصطناعي لا يحسن الكفاءة فحسب، بل يعزز أيضاً الالتزام بالمعايير الرقابية.

الفرضية الخامسة (الفروق حسب المتغيرات الديموغرافية): تم قبولها جزئياً. تبين وجود فروق دالة إحصائية حسب المسمى الوظيفي ( $F = 4.91$ ,  $\text{Sig.} = 0.003$ ) وسنوات الخبرة ( $F = 5.12$ ,  $\text{Sig.} = 0.007$ )، بينما لم تظهر فروق حسب المؤهل العلمي ( $F = 1.51$ ,  $\text{Sig.} = 0.214$ ). كما كانت الفروق حسب القسم التابع هامشية ( $F = 2.64$ ,  $\text{Sig.} = 0.051$ ). هذا يعني أن موقع الفرد في التنظيم وخبرته المتراكمة يؤثران على طريقة تقديره لتأثير الذكاء الاصطناعي، بينما المؤهل الأكاديمي وحده ليس عاملاً حاسماً.

## 4.12. مناقشة عامة للنتائج في ضوء الإطار النظري والدراسات السابقة

### 4.12.1. التأثير القوي للذكاء الاصطناعي على الأداء الأمني

تؤكد نتائج هذه الدراسة، وبشكل قاطع، أن تبني تقنيات الذكاء الاصطناعي (الرؤية الحاسوبية، تعلم الآلة، معالجة اللغات الطبيعية) يؤدي إلى تحسين كبير في أداء غرف التحكم الأمنية في البنك الوطني العربي. هذا يتسق مع النتائج التي توصلت إليها دراسة (Khayat et al., 2025) والتي أكدت أن دمج تعلم الآلة في مراكز العمليات الأمنية يقلل من MTTD بشكل كبير، ومع دراسة (Kovačević et al., 2024) حول الفرص والمخاطر المرتبطة بالذكاء الاصطناعي في القطاع المصرفي، ومع دراسة (كامل، 2024) حول استخدام الذكاء الاصطناعي في الأمن والمراقبة.

كما أن النتائج تدعم توجهات رؤية المملكة 2030 في التحول الرقمي والأمن السيبراني، حيث أظهرت أن المؤسسات السعودية (مثل البنك الوطني العربي) قادرة على تبني هذه التقنيات بنجاح وتحقيق عائد استثماري آمي ملموس. هذا يتوافق مع تقارير (Cisco, 2025) التي أشارت إلى أن 97% من الشركات السعودية تشعر بضرورة ملحة لتبني الذكاء الاصطناعي.

#### 4.12.2. تفوق تعلم الآلة والتحليلات التنبؤية كأكثر التقنيات تأثيراً

أظهرت النتائج أن تعلم الآلة والتحليلات التنبؤية هو الأكثر تأثيراً بين تقنيات الذكاء الاصطناعي الثلاث على الأداء الأمني الكلي (،  $\beta = 0.371$ ) يليه الرؤية الحاسوبية (،  $\beta = 0.328$ ) ثم NLP ( $\beta = 0.301$ ) هذا الترتيب منطقي من الناحية النظرية والتطبيقية، لأن تعلم الآلة يشكل "عقل" المنظومة الأمنية الاستباقية، حيث يقوم بتحليل الأنماط والتنبؤ بالتهديدات قبل وقوعها. وقد أشارت دراسة (Olaoye & Egon, 2024) إلى أن التحليلات التنبؤية تمثل جوهر التحول من الدفاع التفاعلي إلى الأمن الاستباقي. كما أن البنك الوطني العربي يعتمد على منصات مثل IBM Safer Payments التي تستخدم نماذج تعلم الآلة لاتخاذ قرارات الكشف عن الاحتيال في أقل من 10 ميلي ثانية (IBM, 2025).

#### 4.12.3. معالجة تحديات إرهاق التنبيهات (Alert Fatigue)

أظهرت النتائج أن الذكاء الاصطناعي ساهم بشكل كبير في تقليل الإنذارات الكاذبة وتقليل الضغط المعرفي على المحللين (متوسط 4.04 لهذه الفقرة). هذه النتيجة تعالج واحدة من أكثر المشكلات إزعاجاً في غرف التحكم التقليدية، حيث تفقد الأنظمة التقليدية المحللين بسبب "إرهاق التنبيهات" الذي ينتج عن نسب إنذارات كاذبة تتجاوز 50% (Mandadi, 2025; CyberDefenders, 2026). وقد أثبتت الدراسات أن تطبيق أطر "الإنسان في الحلقة" (HITL) المدعومة بالذكاء الاصطناعي القابل للتفسير قلل من الاضطرابات الناتجة عن التنبيهات الكاذبة بنسبة 34% (Preprints, 2026).

#### 4.12.4. الامتثال التنظيمي كأحد مكاسب الذكاء الاصطناعي

أظهرت النتائج أن تقنيات الذكاء الاصطناعي تساهم بشكل كبير في تعزيز الامتثال التنظيمي ( $R^2 = 0.732$ )، وهو ما يتسق مع دراسة (الرحاحله، 2025) حول دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني. وقد أظهر البنك الوطني العربي التزاماً واضحاً بإطار الأمن السيبراني للبنك المركزي السعودي (SAMA CSF) من خلال توحيد عملياته الأمنية على منصة Trellix وتوفير سجلات غير قابلة للتلاعب (Trellix, 2024). كما أن قابلية تفسير القرارات (Explainability) حصلت على متوسط 4.03، وهو جيد لكنه يشير إلى وجود مجال للتحسين، وهو ما يتوافق مع متطلبات البنك المركزي السعودي (Saudi Central Bank, 2023) التي تؤكد على ضرورة بقاء "الإنسان في الحلقة" لاتخاذ القرارات المصيرية.

#### 4.12.5. التحديات كعقبات تحتاج إلى معالجة استراتيجية

أظهرت النتائج أن أبرز التحديات التي تواجه البنك هي: نقص الكوادر البشرية المؤهلة (متوسط 3.99)، وارتفاع التكاليف التشغيلية (4.02)، وتحديات الخصوصية والأخلاقيات (3.94). هذه النتائج تتسق مع الأدبيات المحلية والعالمية. فقد أشارت دراسة (Sidra Capital, 2024) إلى أن 82% من المؤسسات السعودية ترى وجود فجوة مهارية في التعامل مع أدوات الذكاء الاصطناعي. وقد أطلقت المملكة مبادرات وطنية مثل "سماي" لتدريب مليون مواطن على علوم البيانات (Sharikat, 2025)، لكن النتائج تشير إلى أن الفجوة لا تزال قائمة. كما أن التكاليف التشغيلية المرتفعة تمثل تحدياً عالمياً، لكن الدراسات الاقتصادية تشير إلى أن العائد على الاستثمار (ROI) يتحقق على المدى المتوسط والطويل من خلال خفض تكاليف الحوادث الأمنية (IBM, 2024).

#### 4.12.6. الفروق الديموغرافية ودلالاتها الإدارية

أظهرت النتائج أن المسمى الوظيفي وسنوات الخبرة يؤثران على تقدير تأثير الذكاء الاصطناعي، بينما لا يؤثر المؤهل العلمي. هذه النتيجة لها دلالات إدارية مهمة: يجب على البنك أن يولي اهتماماً خاصاً لتدريب المحللين الجدد (ذوي الخبرة الأقل) ومساعدتهم على تقدير قيمة الذكاء الاصطناعي، كما يجب أن يستفيد من خبرات المديرين وكبار المحللين في تصميم استراتيجيات التحول الرقمي. أما بالنسبة للمؤهل العلمي، فتشير النتيجة إلى أن الخبرة العملية والتدريب المستمر قد يكونان أكثر أهمية من الدرجة الأكاديمية وحدها، مما يدعو إلى الاستثمار في برامج التطوير المهني المستمر.

### خلاصة الفصل

قدم هذا الفصل تحليلاً إحصائياً شاملاً للبيانات التي تم جمعها من 190 مشاركاً في البنك الوطني العربي. وقد أظهرت النتائج ما يلي:

1. تميزت عينة الدراسة بتنوعها الوظيفي (مديرو أمن، محللو SOC، مهندسو ذكاء اصطناعي، خبراء تقنية معلومات) وتباين خبراتهم (من أقل من 5 سنوات إلى أكثر من 10 سنوات)، مما يعكس حرص الباحث على الحصول على رؤية شاملة ومتكاملة.
2. أظهرت المتوسطات الحسابية أن مستوى تبني تقنيات الذكاء الاصطناعي (المتوسط العام 4.11) ومستوى أداء غرف التحكم الأمنية (المتوسط العام 4.08) كلاهما مرتفع، مما يعكس نجاح البنك في التحول الرقمي.
3. تم التحقق من ثبات وصدق الأداة، حيث بلغ معامل ألفا كرونباخ للأداة الكاملة 0.967 (ممتاز جداً)، وكانت جميع معاملات ارتباط بيرسون دالة إحصائياً عند مستوى 0.01، مما يؤكد جودة الاستبانة.

4. تم قبول الفرضية الرئيسية، حيث أظهر تحليل الانحدار المتعدد أن تقنيات الذكاء الاصطناعي تفسر 82.1% من التباين في أداء غرف التحكم الأمنية ( $R^2 = 0.821, F = 283.1, \text{Sig.} < 0.001$ ).

5. تم قبول جميع الفرضيات الفرعية، حيث تبين أن:

○ تعلم الآلة يفسر 76.1% من التباين في سرعة الاستجابة (MTTD & MTTR).

○ الرؤية الحاسوبية تفسر 71.3% من التباين في دقة التحليل.

○ NLP تفسر 68.2% من التباين في سرعة الاستجابة.

○ تقنيات الذكاء الاصطناعي مجتمعة تفسر 73.2% من التباين في الامتثال التنظيمي.

6. تم قبول الفرضية الخامسة جزئياً، حيث تبين وجود فروق دالة حسب المسمى الوظيفي وسنوات الخبرة، وعدم وجود فروق حسب المؤهل العلمي.

7. تم تحديد أبرز التحديات التي تواجه البنك، وأبرزها نقص الكوادر المؤهلة (متوسط 3.99) وارتفاع التكاليف التشغيلية (4.02).

هذه النتائج تؤكد أن الذكاء الاصطناعي يمثل نقلة نوعية في أداء غرف التحكم الأمنية بالبنك الوطني العربي، وتضع الأساس للتوصيات التي سيتم تقديمها في الفصل الخامس.