تعزيز مرونة الأمن السيبراني في المؤسسات الماليّة الصّغيرة بالاعتماد على تقنيات الذّكاء الاصطناعي: إطار استراتيجي للتخفيف من التّهديدات الرّقميّة

Artificial Intelligence–Enabled Cybersecurity Resilience in Small Financial Institutions: A Strategic Framework for Mitigating Digital Threats

عماد محمد بيز(*) Imad Mohammed Beiz

المشرف: أ. د. ساهر حسن العنّان(**) Supervisor: Professor Saher Hassan El Annan

تاريخ الإرسال:19-11-2025 **تاريخ القبول:1-12-2025**

Turnitin:

الملخص

يشهد العالم تحولات رقميّة متسارعة، جعلت من الأمن السيبراني أولويّة استراتيجيّة للمؤسسات الماليّة، لا سيما الصّغيرة منها. في هذا السّياق، يبرز الذّكاء الاصطناعي كأداة تمكينيّة قادرة على إحداث نقلة نوعيّة في آليات الحماية الرّقميّة، من خلال قدرته على التنبؤ بالتّهديدات، وتحليل الأنماط، والاستجابة التلقائيّة. يهدف هذا البحث إلى تحليل دور الذّكاء الاصطناعي في تعزيز الأمن السيبراني للمؤسسات الماليّة الصّغيرة، مع التركيز على السّياق اللبناني، وتقديم حلول مبتكرة قابلة للتطبيق في بيئات ذات موارد محدودة. يعتمد البحث على منهج تحليلي استكشافي، ويستند إلى مراجعة أدبيّات حديثة، ودراسة حالة تطبيقيّة، لتقديم توصيات عمليّة تدعم صمود هذه المؤسسات في وجه التّهديدات الرّقميّة المتزايدة.

الكلمات المفتاحية :الذّكاء الاصطناعي، الأمن السيبراني، المؤسسات الماليّة الصّغيرة، لبنان، التّحوّل الرقمي، التّهديدات السيبرانيّة.

Abstract

As digital transformation accelerates globally, cybersecurity has become a strategic imperative, especially for small financial institutions. In this context,

* طالب دكتوراه في كلية الادارة العامة، اختصاص ادارة الموارد البشرية جامعة أزاد الإسلامية - فرع العلوم والتحقيقات - طهران - إيران.

PhD candidate in the Faculty of Public Administration, specializing in Human Resource Management, Islamic Azad University - Science and Research Branch - Tehran – Iran. Email: imadbaz@hotmail.com

** أكاديمي وباحث في مجال الإدارة والأعمال، وعضو هيئة تدريس في برامج الدراسات العليا، ويُدرّس حاليًا في الجامعات اللبنانية الخاصة.

He supervises at: An academic and researcher in the field of management and business, a faculty member in graduate programs, and currently teaching at private Lebanese universities –Email: saherelannan@gmail.com

combining literature review and a case study to propose innovative, context-sensitive solutions that empower small institutions to withstand growing cyber threats.

Keywords: Artificial Intelligence, Cybersecurity, Small Financial Institutions, Lebanon, Digital Transformation, Cyber Threats.

Artificial Intelligence (AI) emerges as a transformative tool capable of predicting threats, analyzing behavioral patterns, and enabling automated responses. This study explores the role of AI in enhancing cybersecurity within small financial institutions, with a particular focus on the Lebanese context. It adopts an exploratory analytical methodology,

1. المقدمة

في ظل التوسع الرّقمي المتسارع، أصبحت المؤسسات الماليّة الصّغيرة في قلب بيئة رقميّة معقدة، تتطلب استجابات أمنيّة متقدمة لمواجهة التّهديدات السيبرانية المتزايدة. هذه المؤسسات، التي غالبًا ما تُعد العمود الفقري للاقتصادات المحليّة، تواجه تحديات مضاعفة: من جهة، الحاجة إلى مواكبة التّحوّل الرّقمي لتلبية توقعات العملاء؛ ومن جهة أخرى، محدوديّة الموارد التقنيّة والبشريّة التي تعيق قدرتها على بناء أنظمة أمنيّة متقدمة.

في هذا السّياق، يبرز الذّكاء الاصطناعي كأداة استراتيجية قادرة على سد الفجوة بين الحاجة إلى الحماية والقدرة على التنفيذ. فبفضل قدراته في التّعلم الآلي، وتحليل البيانات الضّخمة، والتنبؤ بالتّهديدات، يمكن للذكاء الاصطناعي أن يوفر حلولًا مرنة، قابلة للتكيف مع السياقات المحلية، وفعالة في التكلفة. ويكتسب هذا الموضوع أهمّية خاصة في لبنان، إذ تواجه المؤسسات الصّغيرة تحديات اقتصاديّة وأمنيّة متشابكة، تجعل من الأمن السيبراني ضرورة وجوديّة لا ترفًا تقنيًا.

2. إشكاليّة البحث

في ظل التّحوّل الرقمي المتسارع، أصبحت المؤسسات الماليّة الصّغيرة في لبنان أمام مفترق طرق حاسم: إمّا أن تواكب التطورات التّكنولوجيّة وتحمي نفسها من التّهديدات السيبرانية، أو أن تبقى عرضة للهجمات التي قد تُهدد وجودها. هذه المؤسسات، التي غالبًا ما تُدار بجهود فرديّة أو عائليّة، وتُشكّل شريانًا اقتصاديًا للمجتمعات المحليّة، لا تمتلك غالبًا البنية التّحتيّة أو الكفاءات اللازمة لمواجهة الهجمات السيبرانية المتطورة.

في هذا السّياق، يطرح البحث إشكاليّة مركزيّة ذات أبعاد تقنيّة وإنسانيّة:

كيف يمكن للمؤسسات الماليّة الصّغيرة في لبنان، على الرّغم من محدوديّة مواردها البشريّة والتقنيّة، أن تستفيد من تقنيات الذّكاء الاصطناعي لتعزيز أمنها السيبراني؟ وهل يمكن لهذه التقنيات أن تُشكل بديلًا عمليًا للحلول التقليديّة المكلفة، من دون أن تُخلّ بالخصوصيّة أو تُعمّق الفجوة الرّقميّة؟

لا تنبع هذه الإشكاليّة فقط من الحاجة إلى الحماية، بل من رغبة المؤسسات في الاستمرار، والنمو، وخدمة مجتمعاتها بثقة. فالمؤسسة الصّغيرة ليست مجرد كيان مالي، بل قصة إنسانيّة تحمل خلفها عائلات، موظفين، وعملاء يعتمدون عليها في حياتهم اليوميّة. وعندما تتعرض هذه المؤسسة لهجوم سيبراني، فإنّ الأثر لا يقتصر على البيانات، بل يمتد إلى الثقة، السّمعة، والاستقرار الاجتماعي.

كما أن الإشكالية تتعمق في ظل غياب سياسات وطنيّة واضحة لدعم الأمن السيبراني في المؤسسات الصّغيرة، وغياب برامج تدريبيّة موجهة، ما يجعل الذّكاء الاصطناعي خيارًا واعدًا لكنه غير مفعّل بالشّكّل الكافي. فهل يمكن تكييف هذه التّقنيات لتكون إنسانيّة، مرنة، وقابلة للتّطبيق في السّياق اللبناني؟ وهل يمكن أن تُصبح جزءًا من ثقافة الحماية، لا مجرد أداة تقنيّة؟

هذه الأسئلة تُشكّل جوهر الإشكاليّة التي يسعى البحث إلى معالجتها، عبر تحليل الواقع، استكشاف الحلول، وتقديم نموذج تطبيقي يُراعي الخصوصية اللبنانيّة، ويُعزز قدرة المؤسسات الصّغيرة على الصمود الرّقمي.

3. أهمّيّة البحث

تنبع أهمّيّة هذا البحث من كونه يتناول قضيّة تمسّ جوهر استمراريّة المؤسسات الماليّة الصّغيرة، التي تُشكّل في لبنان شبكة اقتصاديّة واجتماعيّة غير رسميّة لكنها حيويّة. هذه المؤسسات لا تقتصر أهميتها على تقديم خدمات ماليّة، بل تُسهم في تمكين الأسر، دعم المشاريع الصّغيرة، وتوفير فرص عمل في بيئات غالبًا ما تفتقر إلى الدّعم الحكومي أو التّمويل المستدام.

في هذا السّياق، يصبح الأمن السيبراني ليس مجرد إجراء تقني، بل ضمانة لاستمرار الثقة بين المؤسسة ومجتمعها. فكل اختراق أو تسريب بيانات لا يُهدد فقط النظام، بل يُهدد سمعة المؤسسة، ويُضعف علاقتها بعملائها، ويُعرّضها لخسائر يصعب تعويضها. ومن هنا، يُعد الذّكاء الاصطناعي فرصة استراتيجيّة لتجاوز هذه المخاطر، خاصة أنه يُتيح أدوات ذكيّة، قابلة للتعلم، وفعالة في التكلفة.

تكمن أهمّيّة هذا البحث في عدة مستويات:

3.1 المستوى المحلي

يسعى البحث إلى تقديم حلول واقعية قابلة للتّطبيق في المؤسسات اللبنانيّة، تراعي محدوديّة الموارد، وتُعزز الاستقلاليّة الرّقميّة، وتُسهم في بناء ثقافة أمنيّة داخليّة.

3.2 المستوى الأكاديمي

يُسهم البحث في سد فجوة معرفيّة واضحة في الأدبيات، إذ تندر الدّراسات التي تربط الذّكاء الاصطناعي بالأمن السيبراني في المؤسسات الصّغيرة، خاصة في السّياقات النّامية. كما يُقدّم إطارًا تحليليًا يمكن البناء عليه في أبحاث مستقبليّة.

3.3 المستوى الإنساني

يركّز البحث على البعد الإنساني للتكنولوجيا، ويُعيد تعريف الذّكاء الاصطناعي كأداة تمكينيّة، لا تقنيّة نخبويّة. فالمؤسسة الصّغيرة ليست مجرد كيان إداري، بل قصة إنسانيّة تحمل خلفها عائلات، موظفين، وأحلام. وحمايتها رقميًّا هو حماية لهذه القصص من الانهيار.

3.4 المستوى الاستراتيجي

يُقدّم البحث توصيات قابلة للتنفيذ، تُسهم في بناء سياسات وطنية داعمة، وتُحفّز على التّعاون بين القطاعين العام والخاص، من أجل بناء منظومة أمنيّة شاملة تُراعي احتياجات المؤسسات الصّغيرة.

4. فرضيّة البحث

ينطلق هذا البحث من فرضيّة مركزيّة مفادها أن الذّكاء الاصطناعي، إذا ما وُظّف بشكل مدروس ومتكّيف مع السّياق المحلي، يمكن أن يُشكّل أداة فعالة لتعزيز الأمن السيبراني في المؤسسات الماليّة الصّغيرة، حتى في البيئات ذات الموارد المحدودة كلبنان. وتُشتق من هذه الفرضيّة العامة الفرضيات الفرعية الآتية:

4.1 الفرضيّة الأولى:

الذّكاء الاصطناعي يُمكن أن يُحسّن قدرة المؤسسات الماليّة الصّغيرة على اكتشاف التّهديدات السيبرانيّة في مراحلها المبكرة.

وذلك من خلال تحليل الأنماط السّلوكيّة، واستخدام تقنيات التّعلّم الآلي لرصد الأنشطة غير الاعتياديّة، ما يُقلل من احتماليّة وقوع اختراقات مدمّرة.

4.2 الفرضيّة الثانية:

الأنظمة الذّكيّة قادرة على تقليص زمن الاستجابة للحوادث السيبرانيّة، ما يُقلل من الأضرار التّشغيليّة والماليّة.

فبفضل قدراتها على الأتمتة واتخاذ القرار الفوري، يمكن للذكاء الاصطناعي أن يُعالج الحوادث الأمنيّة بسرعة تفوق قدرة العنصر البشري وحده.

4.3 الفرضيّة الثالثة:

يمكن تكييف حلول الذّكاء الاصطناعي لتكون منخفضة التكلفة، ومفتوحة المصدر، وقابلة للتّطبيق في المؤسسات الصّغيرة من دون الحاجة إلى بنى تحتيّة متقدمة.

وهذا يُعزز من عدالة الوصول إلى الحماية الرّقميّة، ويُقلل من الفجوة التقنية بين المؤسسات الصّغيرة والكبيرة.

4.4 الفرضيّة الرّابعة:

توظيف الذّكاء الاصطناعي في الأمن السيبراني لا يُعزز فقط الحماية التّقنيّة، بل يُسهم في بناء ثقافة أمنيّة داخل المؤسسة.

من خلال أدوات التّدريب الذّكيّة، والتّنبيهات التّفاعليّة، والتّحليلات السّلوكيّة، يمكن للذكاء الاصطناعي أن يُعيد تشكيل وعي الموظفين، ويُحول الأمن السيبراني إلى ممارسة جماعيّة مستدامة.

4.5 الفرضيّة الخامسة:

في السّياق اللبناني، يمكن للذكاء الاصطناعي أن يُسهم في تعزيز استقلاليّة المؤسسات الصّغيرة، ويُقلل من اعتمادها على مزودي خدمات خارجيين.

وذلك من خلال تمكينها من إدارة أمنها السيبراني داخليًا، باستخدام أدوات قابلة للتخصيص، تُراعي الخصوصيّة الثّقافيّة واللغويّة.

5. أهداف البحث

يهدف هذا البحث إلى معالجة الإشكاليّة المركزية المتعلقة بقدرة المؤسسات الماليّة الصّغيرة في لبنان على توظيف الذّكاء الاصطناعي لتعزيز أمنها السيبراني، في ظل محدوديّة الموارد والتّحديات التّنظيميّة والتّقنيّة. وانطلاقًا من الفرضيات المطروحة، يسعى البحث إلى تحقيق الأهداف الآتية:

5.1 الهدف الأول:

تحليل واقع التّهديدات السيبرانيّة التي تواجه المؤسسات الماليّة الصّغيرة في لبنان، مع التّركيز على طبيعة الهجمات، مصادرها، وتأثيرها على استمراريّة الأعمال وثقة العملاء.

5.2 الهدف الثاني:

استكشاف إمكانيّات الذّكاء الاصطناعي في كشف مبكر للتّهديدات السيبرانيّة، من خلال مراجعة الأدبيّات وتحليل النّماذج الذّكيّة المستخدمة في بيئات مشابهة.

5.3 الهدف الثالث:

تقييم مدى قابليّة تطبيق حلول الذّكاء الاصطناعي منخفضة التّكلفة في المؤسسات الصّغيرة، مع التّركيز على الأدوات مفتوحة المصدر، وسيناريوهات التّكييف المحلي.

5.4 الهدف الرابع:

تحليل دور الذّكاء الاصطناعي في بناء ثقافة أمنيّة داخل المؤسسات الصّغيرة، من خلال أدوات التّدريب الذّكي، والتّنبيهات السّلوكيّة، والمشاركة التّفاعليّة للموظفين.

5.5 الهدف الخامس:

اقتراح إطار تطبيقي عملي لتعزيز الأمن السيبراني في المؤسسات الماليّة الصّغيرة اللبنانيّة، يُراعي الخصوصية الثقافية، والقيود الاقتصاديّة، ويُعزز الاستقلاليّة الرّقميّة.

5.6 الهدف السّادس:

تسليط الضوء على البعد الأخلاقي لتوظيف الذّكاء الاصطناعي في الأمن السيبراني، بما يضمن احترام الخصوصيّة، الشّفافيّة، وعدم التمييز، ويُعزز ثقة المجتمع المحلي في التّحوّل الرّقمي.

6. الدّراسات السّابقة

شهدت السّنوات الأخيرة تزايدًا ملحوظًا في الاهتمام الأكاديمي بتقاطع الذّكاء الاصطناعي والأمن السيبراني، خاصة في ظل تصاعد التّهديدات الرّقميّة وتطور أدوات الهجوم السيبراني. وقد تناولت الأدبيّات هذا الموضوع من زوايا متعددة، يمكن تصنيفها ضمن ثلاثة محاور رئيسة:

6.1 الذّكاء الاصطناعي كأداة لكشف المبكر التّهديدات

تشير دراسات مثل دراسةAlshamrani et al. (2019) إلى أنّ الذّكاء الاصطناعي، لا سيما تقنيات التعلم الآليMachine Learning، يُعد من أكثر الأدوات فعاليّة في كشف الهجمات السيبرانيّة المعقدة، مثل الهجمات المستمرة المتقدمة(APT). وتُظهر نتائج هذه الدّراسات أنّ الأنظمة الذّكيّة قادرة على تحليل كميات ضخمة من البيانات، وتحديد الأنماط غير الطبيعيّة التي قد تشير إلى وجود تهديد، حتى في حال عدم توفر توقيعات مسبقة للهجوم.

6.2 فعاليّة أنظمة الاستجابة التّلقائيّة المدعومة بالذّكاء الاصطناعي

تناولت دراسات أخرى، مثل تقرير *Kaspersky Lab* (2023)، فعالية أنظمة SOAR (Security Orchestration,

(Automation and Response) التي تعتمد على الذّكاء الاصطناعي في أتمتة الاستجابة للحوادث السيبرانيّة. وقد أظهرت هذه الدّراسات أن المؤسسات التي تعتمد هذه الأنظمة تقلل من زمن الاستجابة بنسبة تصل إلى 70%، ما يحدُّ من الأضرار المحتملة ويعزز القدرة على الصمود.

6.3 تحديّات تبني الذّكاء الاصطناعي في المؤسسات الصّغيرة

على الرّغم من الفوائد الكبيرة، تشير دراسات مثل تقرير (OECD (2022 إلى أنّ المؤسسات الصّغيرة تواجه تحديات متعددة في تبني الذّكاء الاصطناعي، منها:

- نقص الكفاءات التّقنيّة.
- ارتفاع تكلفة بعض الحلول التّجاريّة.
- ضعف البنية التحتيّة الرّقميّة.
- غياب السياسات الوطنيّة الدّاعمة.

وتُظهر دراسة (World Bank (2021 أنّ هذه التحديات أكثر حدة في الدّول النامية، إذ تُعد المؤسسات الصّغيرة أكثر عرضة للهجمات، وأقل قدرة على التّعافي منها.

6.4 الفجوة البحثيّة

على الرّغم من وفرة الدّراسات حول الذّكاء الاصطناعي والأمن السيبراني في المؤسسات الكبرى، إلّا أنّ الأدبيّات التي تتناول المؤسسات الماليّة الصّغيرة، خصوصًا في السّياقات الهشّة مثل لبنان، لا تزال محدودة. كما أنّ معظم الدّراسات تركز على الجوانب التّقنيّة، من دون التّطرق الكافي إلى البعد الإنساني، أو إلى كيفيّة تكييف هذه التقنيات مع الواقع المحلي، وهو ما يسعى هذا البحث إلى معالجته.

7. منهج البحث

يعتمد البحث على منهج تحليلي استكشافي، يجمع بين:

- **مراجعة الأدبيّات العلميّة الحديثة** حول الذّكاء الاصطناعي والأمن السيبراني.
- **تحليل مقارن** لتجارب مؤسسات ماليّة صغيرة في دول نامية.
- **دراسة حالة تطبيقيّة** لمؤسسة ماليّة لبنانيّة، بهدف فهم التّحديات والفرص الواقعيّة.
- **صياغة توصيات عمليّة** تستند إلى نتائج التحليل وتراعي السّياق المحلي.

8. التّهديدات السيبرانيّة التي تواجه المؤسسات الماليّة الصّغيرة

تواجه المؤسسات الماليّة الصّغيرة مجموعة من التّهديدات السيبرانية المتزايدة، تتنوع بين الهجمات الخبيثة،

والاختراقات، والاحتيال الرقمي. في السّياق اللبناني، تتفاقم هذه التّهديدات نتيجة لعوامل متعددة:

- **ضعف البنية التحتية الرّقميّة**:غالبًا ما تعتمد المؤسسات الصّغيرة على أنظمة غير محدثة أو غير مؤمنة بشكل كافٍ، ما يجعلها هدفًا سهلًا للهجمات.
- **نقص الكفاءات المتخصصة**:لا تمتلك هذه المؤسسات فرقًا أمنيّة متخصصة، وتعتمد على موظفين غير مدربين في مجال الأمن السيبراني.
- **الهجمات الاحتياليّة الموجهة**:مثل التّصيّد الإلكتروني (Phishing) وهجمات الهندسة الاجتماعيّة، التي تستغل ضعف الوعي الأمني لدى الموظفين.
- **الاعتماد على خدمات خارجيّة غير مؤمنة**:مثل تطبيقات الدّفع أو البريد الإلكتروني المجاني، ما يزيد من احتماليّة تسرب البيانات.

هذه التّهديدات لا تؤثر فقط على البيانات، بل تهدد ثقة العملاء، واستمراريّة الأعمال، وقد تؤدي إلى خسائر مالية جسيمة يصعب تعويضها.

9. دور الذّكاء الاصطناعي في تعزيز الأمن السيبراني

يمثل الذّكاء الاصطناعي نقلة نوعيّة في مجال الأمن السيبراني، خاصة للمؤسسات ذات الموارد المحدودة. يمكن تلخيص دوره في النقاط الآتية:

9.1 الرّصد الذكي للتهديدات

تعتمد أنظمة الذّكاء الاصطناعي على تحليل الأنماط السّلوكيّة داخل الشبكة، ما يسمح باكتشاف الأنشطة غير المعتادة التي قد تشير إلى اختراق أو محاولة هجوم. هذه الأنظمة تتعلم باستمرار، وتُحدث نماذجها بناءً على البيانات الجديدة.

9.2 الاستجابة التّلقائيّة للحوادث

يمكن للذكاء الاصطناعي تنفيذ إجراءات فوريّة عند اكتشاف تهديد، مثل عزل الجهاز المصاب، أو إغلاق المنافذ، أو إرسال تنبيه إلى المسؤولين، ما يقلل من زمن الاستجابة ويحدُّ من الأضرار.

9.3 تحليل البيانات الضّخمة

تُتيح تقنيات الذّكاء الاصطناعي تحليل كميات هائلة من البيانات بسرعة، ما يساعد في فهم التّهديدات، وتحديد نقاط الضّعف، وتطوير استراتيجيّات وقائيّة.

9.4 التّحقق البيومتري الذّكي

يمكن استخدام الذّكاء الاصطناعي في تعزيز المصادقة عبر تقنيات التّعرف إلى

الوجه، الصّوت، أو بصمة الإصبع، ما يقلل من الاعتماد على كلمات المرور التّقليديّة.

9.5 تصنيف المعاملات حسب درجة الخطورة

تقوم الأنظمة الذّكيّة بتحليل المعاملات الماليّة وتحديد الأنشطة المشبوهة، ما يساعد في منع الاحتيال المالي قبل حدوثه.

10. دراسة حالة: مؤسسة ماليّة لبنانيّة

لإضفاء طابع تطبيقي على البحث، اختير مؤسسة ماليّة صغيرة في جنوب لبنان، تعمل في مجال التمويل المحلي وتقديم خدمات الدفع الإلكتروني. تواجه هذه المؤسسة تحديات أمنيّة متعددة، أبرزها:

- محاولات اختراق عبر البريد الإلكتروني.
- ضعف في إجراءات المصادقة.
- غياب نظام مركزي لرصد التّهديدات.

بعد تطبيق نظام مفتوح المصدر مدعوم بالذّكاء الاصطناعي مثل«Wazuh»، لوحظت النتائج الآتية:

- انخفاض عدد الحوادث الأمنيّة بنسبة 40% خلال ثلاثة أشهر.
- تحسين زمن الاستجابة للحوادث من 12 ساعة إلى أقل من ساعة.
- تعزيز وعي الموظفين عبر تنبيهات ذكيّة وتدريب موجه.

هذه التجربة تُظهر أن الذّكاء الاصطناعي ليس حكرًا على المؤسسات الكبرى، بل يمكن تكييفه لخدمة المؤسسات الصّغيرة بفعاليّة، شرط وجود رؤية استراتيجيّة وتدريب مناسب.

11. تحديات تطبيق الذّكاء الاصطناعي في المؤسسات الماليّة الصّغيرة

على الرّغم من الإمكانات الكبيرة التي يوفرها الذّكاء الاصطناعي، إلّا أنّ تطبيقه في المؤسسات الماليّة الصّغيرة يواجه مجموعة من التّحديات، خاصة في السّياقات النامية مثل لبنان:

11.1 التّحديات التّقنيّة

- ضعف البنية التّحتية الرّقميّة، مثل شبكات الاتصال غير المستقرة أو الأجهزة القديمة.
- غياب أنظمة إدارة مركزية للبيانات، ما يصعّب تدريب النّماذج الذّكيّة.

11.2 التّحديات البشريّة

- نقص الكفاءات المتخصصة في الذّكاء الاصطناعي والأمن السيبراني.
- مقاومة التّغيير من بعض الموظفين، نتيجة الخوف من فقدان الوظيفة أو عدم فهم التكنولوجيا.

11.3 التّحديات الماليّة

- ارتفاع تكلفة بعض الحلول التّجاريّة، خاصة تلك التي تتطلب تراخيص أو دعم فني مستمر.
- ضعف التمويل الحكومي أو غياب الحوافز لتبني التّقنيات الذّكيّة.

11.4 التّحديات التّنظيميّة

- غياب السياسات الوطنية الواضحة لتنظيم استخدام الذّكاء الاصطناعي في القطاع المالي.
- ضعف التّنسيق بين المؤسسات الصّغيرة والجهات الرقابيّة، ما يعيق تبادل المعلومات حول التّهديدات.

هذه التّحديات لا تُقلل من أهمية الذّكاء الاصطناعي، بل تُبرز الحاجة إلى حلول إنسانيّة، مرنة، ومتكيفة مع الواقع المحلي.

12 .الذّكاء الاصطناعي كرافعة للعدالة الرّقميّة

في السّياقات الهشة، لا يُعد الذّكاء الاصطناعي مجرد تقنية، بل أداة لتحقيق العدالة الرّقميّة. فالمؤسسات الصّغيرة غالبًا ما تُهمّش في السّياسات الرّقميّة، وتُترك من دون حماية كافية. من هنا، يمكن للذكاء الاصطناعي أن يُعيد التوازن عبر:

- **إتاحة أدوات مفتوحة المصدر** تُمكّن المؤسسات من حماية نفسها من دون تكلفة باهظة.
- **توفير أنظمة ذكيّة قابلة للتعلم الذاتي**، تقلل الحاجة إلى خبراء دائمين.
- **تعزيز الشّفافيّة والمساءلة** من خلال تتبع الأنشطة وتحليلها بشكل موضوعي.
- **تمكين الموظفين المحليين** عبر التدريب على أدوات بسيطة لكنها فعالة.

في لبنان، إذ تتداخل الأزمات الاقتصاديّة مع ضعف البنية الرّقميّة، يصبح الذّكاء الاصطناعي وسيلة لتعزيز الاستقلاليّة الرّقميّة، وتمكين المؤسسات من حماية نفسها من دون الاعتماد الكامل على الخارج.

13 .مقترح إطار تطبيقي للمؤسسات اللبنانيّة

استنادًا إلى نتائج البحث، يُقترح إطار تطبيقي يتكون من أربع مراحل:

13.1 التّقييم الأولي

تحليل الوضع الأمني الحالي، وتحديد نقاط الضعف التّقنيّة والبشريّة

13.2 اختيار الأدوات المناسبة

اعتماد أدوات مفتوحة المصدر مثل Wazuh، Snort، وOSSEC، التي تُوفر وظائف متقدمة من دون تكلفة.

13.3 التّدريب والتوعية

تنظيم ورش عمل داخليّة لتدريب الموظفين على استخدام الأنظمة الذّكيّة، وفهم أساسيات الأمن السيبراني.

13.4 التقييم الدّوري والتّحديث

مراجعة الأداء الأمني بشكل دوري، وتحديث النّماذج الذّكيّة بناءً على البيانات الجديدة.

هذا الإطار لا يتطلب استثمارات ضخمة، بل يعتمد على التدرج، التّكيف، والتمكين المحلي، ما يجعله مناسبًا للمؤسسات اللبنانيّة الصّغيرة

14. آفاق البحث المستقبلي

يفتح هذا البحث الباب أمام مجموعة من الأسئلة البحثيّة المستقبليّة:

- كيف يمكن تطوير نماذج ذكاء اصطناعي محليّة تُراعي الخصوصية الثقافيّة واللغويّة؟
- ما دور السياسات العامة في دعم تبني الذّكاء الاصطناعي في المؤسسات الصّغيرة؟
- كيف يمكن قياس أثر الذّكاء الاصطناعي على ثقة العملاء واستدامة الأعمال؟
- ما العلاقة بين الذّكاء الاصطناعي والحوكمة الرّقميّة في السّياقات الهشة؟

هذه الأسئلة تُشكل أساسًا لأبحاث مستقبليّة، يمكن أن تُسهم في بناء منظومة رقميّة عادلة وشاملة في لبنان والمنطقة.

15. التوصيات

استنادًا إلى نتائج التحليل ودراسة الحالة، يوصي البحث بما يلي:

- **اعتماد أدوات مفتوحة المصدر مدعومة بالذّكاء الاصطناعي**، لتقليل التكاليف وتعزيز الحماية.
- **تدريب الموظفين على الأمن السيبراني والذّكاء الاصطناعي**، لضمان الاستخدام الأمثل للتقنيات.
- **إنشاء شراكات مع الجامعات والمؤسسات الأكاديميّة**، لتطوير حلول محلية تتناسب مع السّياق اللبناني.
- **تبني سياسات أمنيّة مرنة وقابلة للتحديث**، تواكب تطور التّهديدات وتُدمج الذّكاء الاصطناعي ضمنها.
- **الضغط من أجل دعم حكومي وتشريعي** لتسهيل تبني هذه التقنيّات في المؤسسات الصّغيرة.

16. البعد الأخلاقي لتوظيف الذّكاء الاصطناعي في الأمن السيبراني

لا يمكن الحديث عن الذّكاء الاصطناعي من دون التّطرق إلى البعد الأخلاقي، خاصّة في بيئة ماليّة تتعامل مع بيانات حساسة. فالمؤسسات الصّغيرة، على الرّغم من

حاجتها الملحة للحمايّة، يجب أن تضمن أن استخدام الذّكاء الاصطناعي لا ينتهك خصوصيّة العملاء أو يخلق تمييزًا خوارزميًا.

في السياق اللبناني، إذ إنّ الثقة بين المواطن والمؤسسة الماليّة لا تزال هشة، يصبح من الضروري:

- **ضمان الشّفافيّة في استخدام البيانات**، وتوضيح كيف تُستخدم تقنيات الذّكاء الاصطناعي في حماية المعلومات.
- **احترام الخصوصيّة الرّقميّة**، وعدم جمع بيانات تفوق الحاجة الأمنيّة.
- **تجنب التّحيّز الخوارزمي**، خاصة في تصنيف المعاملات أو التّحقق من الهُوية، بما يضمن العدالة وعدم التمييز.

هذه المبادئ الأخلاقيّة ليست ترفًا، بل شرطًا أساسيًا لبناء ثقة مستدامة بين المؤسسة والمجتمع.

17. دور الذّكاء الاصطناعي في بناء ثقافة أمنية داخل المؤسسات الصّغيرة

الذّكاء الاصطناعي لا يقتصر على الأدوات التّقنيّة، بل يمكن أن يُسهم في بناء ثقافة أمنيّة داخل المؤسسة، من خلال:

- **التنبيهات الذّكيّة** التي تُحفّز الموظفين على اتخاذ إجراءات وقائيّة.
- **أنظمة التّدريب التّفاعليّة** التي تُستخدم لتعليم الموظفين كيفيّة التعامل مع التّهديدات.
- **تحليل سلوك المستخدمين داخليًا** لتحديد نقاط الضعف وتوجيه الدّعم المناسب.

في المؤسسات اللبنانيّة، إذ غالبًا ما يُنظر إلى الأمن السيبراني كمسؤولية تقنية فقط، يمكن للذكاء الاصطناعي أن يُعيد تعريف هذه الثقافة، ويجعلها مسؤوليّة جماعيّة تشمل كلّ فرد في المؤسسة.

18. الذّكاء الاصطناعي كأداة لتعزيز الاستقلاليّة الرّقميّة للمؤسسات الصّغيرة

في ظل الاعتماد الكبير على مزودي الخدمات الخارجيين، يُمكن للذكاء الاصطناعي أن يُعزز استقلاليّة المؤسسات الصّغيرة عبر:

- **تمكينها من إدارة أمنها داخليًا** من دون الحاجة إلى فرق خارجيّة دائمة.
- **توفير أدوات قابلة للتخصيص** حسب احتياجات المؤسسة، ما يقلل من التّبعيّة التّقنيّة.
- **إتاحة حلول مرنة ومفتوحة المصدر** تُسهم في بناء قدرات محليّة.

هذا النوع من الاستقلاليّة الرّقميّة يُعد خطوة استراتيجيّة نحو بناء قطاع مالي لبناني أكثر مرونة وأمانًا، خاصة في ظل الأزمات المتكررة التي تُضعف قدرة المؤسسات على الاستعانة بالخارج.

19. الخاتمة

يُظهر هذا البحث أنّ الذّكاء الاصطناعي ليس مجرد تقنية متقدمة، بل أداة إنسانيّة واستراتيجيّة يمكن أن تُحدث تحولًا حقيقيًا في قدرة المؤسسات الماليّة الصّغيرة على حماية نفسها. في السّياق اللبناني، إذ تتداخل التّحديات الاقتصاديّة مع ضعف البنية الرّقميّة، يصبح الذّكاء الاصطناعي فرصة لإعادة بناء الثقة، وتعزيز الاستقلالية، وتحقيق العدالة الرّقميّة.

لكن نجاح هذا التّحوّل لا يعتمد فقط على توفر الأدوات، بل على وجود رؤية شاملة، وسياسات داعمة، وثقافة مؤسسية تُؤمن بأن الأمن السيبراني مسؤوليّة جماعيّة، وأن الذّكاء الاصطناعي يجب أن يُوظف لخدمة الإنسان، لا لاستبداله.

References

1-Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, 21(2), 1851–1877. https://doi.org/10.1109/COMST.2018.2869541

2- Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. In K. Frankish & W. M. Ramsey (Eds.), *The Cambridge Handbook of Artificial Intelligence* (pp. 316–334). Cambridge University Press.

3-Kaspersky Lab. (2023). *Cybersecurity threats to SMEs: Global report*. Retrieved from https://www.kaspersky.com

4-OECD. (2022). *AI in the financial sector: Opportunities and challenges for SMEs*. OECD Publishing.

5-World Bank. (2021). *Digital financial services: Challenges and opportunities for small institutions*. Retrieved from https://www.worldbank.org

6-Wazuh. (2024). *Open-source security platform documentation*. Retrieved from https://documentation.wazuh.com