الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

P-ISSN: 2070-898X E-ISSN: 2707-9775

أثر إدارة مخاطر الأمن السيبراني في بناء الثقة الرقمية وانعكاسه على الشمول المالي في ظل التكنولوجيا المالية

م.م. إسراء عبد الحسين عيسى
كلية الإدارة واقتصاد، الجامعه المستنصرية، بغداد، العراق
esraaabdalhussein@uomustansiriyah.edu.iq

مستخلص البحث:
يهدف البحث إلى تحليل أثر إدارة مخاطر الأمن السيبراني في بناء الثقة الرقمية وانعكاسه على الشمول المالي عبر التكنولوجيا المالية في المصارف العراقية. انطلقت الدراسة من مشكلة مفادها أن تصاعد المخاطر السيبرانية قد يضعف ثقة المستخدمين بالخدمات المالية الرقمية، مما يحدّ من انتشارها ويؤثر في مستويات الشمول المالي، وبخاصة عبر أبعاد (الوصول، الاستخدام، الجودة). كشفت النتائج الوصفية أن إدارة مخاطر الأمن السيبراني متوافرة بمستوى مرتفع، مع تميز كبير للوقاية والتحديث، مقابل ضعف في التعلم من الحوادث وتصنيفها وفق المعايير الدولية، كما جاءت الثقة الرقمية بمستوى مرتفع مدفوعة بالأمن وفاعلية الخدمات مع ضعف في الالتزام الأخلاقي، في حين كان الشمول المالي عبر التكنولوجيا المالية بمستوى معتدل، وتحديدًا ضعف جودة الخدمات. وأثبت اختبار الارتباط وجود علاقات موجبة قوية ودالة بين المتغيرات الثلاثة، كما أظهر تحليل التأثير أن الثقة الرقمية تؤدي دور الوسيط الجزئي بين إدارة مخاطر الأمن السيبراني والشمول المالي، أي أن إدارة المخاطر تعزز الشمول المالي بشكل مباشر وبشكل غير مباشر عبر تعزيز الثقة الرقمية. بناءً على ذلك، توصي الدراسة بتعزيز التعلم المؤسسي من الحوادث، وتطوير الشفافية والالتزام الأخلاقي، وتحسين جودة الخدمات الرقمية بما يدعم الشمول المالي في البيئة المصرفية العراقية.

الكلمات المفتاحية: إدارة مخاطر، الأمن السيبراني؛ الثقة الرقمية؛ الشمول المالي؛ التكنولوجيا المالية؛ المصارف العراقية.

تاريخ الاستلام: ٢٠/ ١/ ٢٠٢٦ تاريخ القبول: ٢٠٢٦/٢/٢٢ تاريخ النشر: ١ /٣/ ٢٠٢٦

The impact of cybersecurity risk management on building digital trust and its impact on financial inclusion under financial technology

Researcher:. Israa Abdul Hussein Issa
Faculty of management and economics, Mustansiriya University, Baghdad, Iraq.
esraaabdalhussein@uomustansiriyah.edu.iq

Abstract
This research aims to analyze the impact of cybersecurity risk management on building digital trust and its reflection on financial inclusion through fintech in Iraqi banks. The study stems from the problem that escalating cyber risks may weaken users' trust in digital financial services, thus limiting their spread and affecting levels of financial inclusion, particularly in the dimensions of access, use, and quality. The descriptive results revealed that cybersecurity risk management is available at a high level, with significant improvements in prevention and updates, but weaknesses in learning from incidents and classifying them according to international standards. Digital trust was also found to be at a high level, driven by security and service effectiveness, but with a weakness in ethical commitment. Financial inclusion through fintech was found to be at a moderate level, specifically in terms of weak service quality. Correlation testing demonstrated strong and significant positive relationships between the three variables. The impact analysis showed that digital trust acts as a partial mediator between cybersecurity risk management and financial inclusion, meaning that risk management directly and indirectly enhances financial inclusion by strengthening digital trust. Accordingly, the study recommends enhancing institutional learning from incidents, developing transparency and ethical commitment, and improving the quality of digital services to support financial inclusion in the Iraqi banking environment.

Keywords: cybersecurity risk management; digital trust; financial inclusion; financial technology; Iraqi banks.

Date Received: 20/1/2026 Date Accepted: 22/2 /2026 Date Published:1 /3/2026

DOI: https:// doi. Org/***

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

المبحث الأول: منهجية البحث Research Methodology

المقدمة:

أدى التقدم السريع في مجال التكنولوجيا المالية إلى زيادة الاعتماد على الخدمات المالية الرقمية، الأمر الذي جعل مسألة إدارة مخاطر الأمن السيبراني من القضايا الرئيسة التي تواجه المؤسسات المالية في بيئة التحول الرقمي. إذ إن كفاءة إدارة هذه المخاطر تمثل عاملًا حاسمًا في حماية البيانات وضمان سلامة الأنظمة الرقمية، وهو ما ينعكس بصورة مباشرة على مستوى الثقة الرقمية لدى المستخدمين، والتي تعد بدورها ركيزة أساسية لانتشار الخدمات المالية الرقمية وتعزيز الشمول المالي.

وانطلاقًا من ذلك، تسعى هذه الدراسة إلى توضيح أثر إدارة مخاطر الأمن السيبراني في بناء الثقة الرقمية، وانعكاس ذلك على الشمول المالي في ظل التكنولوجيا المالية، من خلال تحليل واقع الممارسات المعتمدة في المصارف العراقية، وبما يسهم في دعم التحول الرقمي الآمن وتوسيع قاعدة المستفيدين من الخدمات المالية.

- **أهمية البحث**

١-الأهمية العلمية

تتجلى الأهمية العلمية لهذا البحث في إسهامه في تطوير الأدبيات الإدارية المعاصرة من خلال الربط بين إدارة مخاطر الأمن السيبراني والثقة الرقمية والشمول المالي عبر التكنولوجيا المالية ضمن نموذج تحليلي متكامل. كما يقدم البحث إطارًا تفسيريًا يوضح كيف تسهم الممارسات التنظيمية المرتبطة بإدارة المخاطر السيبرانية في بناء الثقة الرقمية، وانعكاس ذلك على تعزيز الشمول المالي، وهو جانب لم يُتناول بصورة كافية في الدراسات السابقة، ولاسيما في بيئة المصارف العراقية التي تشهد تحولات رقمية متسارعة.

٢-الأهمية العملية

تتمثل الأهمية العملية للبحث في الآتي:

أ) مساعدة المصارف والمؤسسات المالية في تطوير وتحسين ممارسات إدارة مخاطر الأمن السيبراني بما يعزز سلامة الأنظمة الرقمية.

ب) دعم صانعي القرار في المصارف العراقية لفهم الدور المحوري للثقة الرقمية في نجاح الخدمات المالية الرقمية.

ت) المساهمة في وضع سياسات وإجراءات عملية تسهم في تعزيز الشمول المالي ضمن بيئة رقمية آمنة.

ث) توفير نتائج تطبيقية يمكن الاستفادة منها في تطوير استراتيجيات التكنولوجيا المالية بما ينسجم مع متطلبات التحول الرقمي الآمن.

- **أهداف البحث**

يسعى البحث إلى تحقيق مجموعة من الأهداف الرئيسة المنسجمة مع نموذج الدراسة القائم على العلاقة بين إدارة مخاطر الأمن السيبراني، والثقة الرقمية، والشمول المالي عبر التكنولوجيا المالية، وذلك على النحو الآتي:

١. تشخيص مستوى تطبيق ممارسات إدارة مخاطر الأمن السيبراني في المصارف العراقية.
٢. قياس مستوى الثقة الرقمية المتحقق لدى مستخدمي الخدمات المالية الرقمية.
٣. تحليل تأثير إدارة مخاطر الأمن السيبراني في بناء الثقة الرقمية.
٤. توضيح تأثير الثقة الرقمية في تعزيز الشمول المالي عبر التكنولوجيا المالية.
٥. اختبار العلاقات والأثر المباشر وغير المباشر بين متغيرات الدراسة، وبيان الدور الوسيط الجزئي للثقة الرقمية في العلاقة بين إدارة مخاطر الأمن السيبراني والشمول المالي.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

- **مشكلة البحث**

في ظل التوسع المتسارع للخدمات المالية الرقمية والاعتماد المتزايد على التكنولوجيا المالية، تواجه المصارف تحديات متعلقة بالمخاطر السيبرانية مثل الهجمات الإلكترونية، وفقدان البيانات، وسرقة الهوية، والتي تؤثر على أمان المعلومات وحماية بيانات العملاء. ويُعد ضعف إدارة هذه المخاطر أحد العوامل التي تؤدي إلى تراجع مستوى الثقة الرقمية لدى المستخدمين، وهو ما ينعكس سلبًا على انتشار الخدمات المالية الرقمية ومستويات الشمول المالي.

ومن هنا، يبرز الدور الوسيط للثقة الرقمية بين إدارة مخاطر الأمن السيبراني ومستوى الشمول المالي، والذي يقاس من خلال أبعاد: الوصول إلى الخدمات المالية، واستخدام الخدمات، وجودة الخدمات. وبالتالي، أصبح من الضروري دراسة أثر إدارة مخاطر الأمن السيبراني في الشمول المالي عبر التكنولوجيا المالية، ودور الثقة الرقمية كمتغير وسيط جزئي يفسر هذه العلاقة، بما يسهم في وضع استراتيجيات فعّالة لتعزيز الشمول المالي في المصارف العراقية. وينبثق عنها التساؤلات البحثية:

١. ما مدى تأثير إدارة مخاطر الأمن السيبراني في بناء الثقة الرقمية داخل المصارف العراقية؟
٢. ما مدى تأثير الثقة الرقمية في تعزيز الشمول المالي عبر التكنولوجيا المالية في المصارف العراقية؟
٣. ما طبيعة تأثير إدارة مخاطر الأمن السيبراني في الشمول المالي عبر التكنولوجيا المالية، وهل تؤدي الثقة الرقمية دورًا وسيطًا في هذه العلاقة؟

- **فرضيات البحث**

اختبار الفرضية الرئيسة الاولى: توجد علاقات ارتباط ذات دلالة احصائية بين المتغيرات (إدارة مخاطر الأمن السيبراني، الثقة الرقمية، الشمول المالي في ظل التكنولوجيا المالية) في المصارف العراقية

اختبار الفرضية الرئيسة الثانية: يسهم متغير الثقة الرقمية بدور الوسيط الجزئي في العلاقة بين إدارة مخاطر الأمن السيبراني والشمول المالي عبر التكنولوجيا المالية في المصارف العراقية.

- **منهجية البحث**

اعتمدت الدراسة على الاستبانة بوصفها الأداة الرئيسة لجمع البيانات، نظرًا لملاءمتها لطبيعة البحث الذي يهدف إلى قياس آراء وتقديرات العاملين في المصارف العراقية بشأن مستوى تطبيق ممارسات إدارة مخاطر الأمن السيبراني، ومستوى الثقة الرقمية، وانعكاس ذلك على الشمول المالي عبر التكنولوجيا المالية. وقد وُزّعت الاستبانة على عينة من العاملين في المصارف التي تتبنى استخدام التقنيات المصرفية الرقمية والتكنولوجيا المالية، ولاسيما تلك التي تعتمد أنظمة الدفع الإلكتروني، والخدمات المصرفية الرقمية، وإجراءات الأمن السيبراني. وتم اختيار العينة بأسلوب العينة القصدية لكون أفرادها الأكثر ارتباطًا بموضوع الدراسة والأقدر على تقديم بيانات دقيقة تعكس واقع الممارسات داخل المصارف. وبلغ حجم عينة البحث (٩٦) مفردة من العاملين في هذه المصارف، ممن تتطلب طبيعة عملهم التعامل المباشر مع الأنظمة الرقمية أو الإشراف عليها أو إدارتها، مما يعزز موثوقية البيانات ودقتها. وتندرج هذه الدراسة ضمن إطار المنهج الوصفي–التحليلي، إذ تم وصف متغيرات الدراسة وتشخيص مستواها، ومن ثم تحليل العلاقات والأثر بينها. وبعد استكمال جمع الاستبانات، جرى تحويل الإجابات إلى قيم رقمية وفق مقياس ليكرت الخماسي، ثم إدخال البيانات وتحليلها باستخدام برنامج (SPSS) لاستخلاص المؤشرات الإحصائية اللازمة واختبار فرضيات البحث وتحقيق أهدافه.

- **الدراسات السابقة**

١-المشهداني، واخرون ، ٢٠٢٥، لتكنلوجيا المالية في ظل تحديات الأمن السيبراني ودورها في القطاع المصرفي، يهدف البحث إلى بيان مفهوم التكنولوجيا المالية وأهميته في تطوير الأعمال

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

المصرفية في ظل تحديات الأمن السيبراني، توصل البحث إلى أن هناك دوراً للتكنولوجيا المالية في الحسين جودة وكفاءة الخدمات المصرفية من خلال تسريع العمليات وتقليل التكاليف، مما أسهم في تحسين التجربة الرياضي، رغم التحديات التي تمثلت في الأمن السيبراني فضلاً عن كسب ثقة الزبائي والامتثال التنظيمي ، كما أكد البحث على وجود فرض كبيرة لتحسين الشمول المالي وتعزيز إدارة المخاطر من خلال التعاون بين المصارف وشركات التكنولوجيا المالية، الذي يعزز الابتكار ويساهم في التحول الرقمي، وأوصى البحث بضرورة التركيز على تعزيز الأمن السيبراني.

٢-عطاء الله، وآخرون، ٢٠٢٥، استخدام التكنولوجيا المالية كالية لتحديث نظام الاعتماد المستندي لتطوير التجارة الخارجية الجزائرية، تهدف الدراسة إلى استكشاف دور التكنولوجيا المالية في تحديث نظام الاعتماد المستندي لدعم وتطوير التجارة الخارجية في الجزائر في ظل التطورات المتسارعة في مجال التكنولوجيا، وتقترح حلولا لتعزيز تكاملها في النظام المالي الجزائري من خلال هذه الدراسة، يتوقع أن يساهم تحديث نظام الاعتماد المستندي في زيادة فعالية التجارة الخارجية وتقليل التكاليف والمخاطر المرتبطة بالمعاملات التجارية، مما يعزز من قدرة الجزائر على التنافس في السوق العالمية، وختاما، تقدم الدراسة توصيات عملية لدعم عملية التحديث وضمان تطبيق التكنولوجيا المالية بشكل فعال ومستدام.

3- Hassan. El. At., 2025, *Decentralized Fintech Platforms Adoption Intention in Cyber Risk Environment among Gen Z: A Dual-Method Approach Using PLS-SEM and Necessary Condition Analysis,*

هدفت الدراسة إلى استكشاف العوامل التي تؤثر في نية جيل Z المولودين بين ١٩٩٦–٢٠١٠) في تبنّي منصات التكنولوجيا المالية اللامركزية (Decentralized Fintech Platforms) في ظل وجود مخاطر سيبرانية .وقد توصلت الدراسة الى ان **الثقة في التكنولوجيا** لعبت **دورًا وسيطًا جزئيًا** بين قدرة تحمل المخاطر ونية التبنّي، أي أن الثقة في التكنولوجيا تساهم في **تعزيز تأثير تحمل المخاطر على نية الاستخدام**، الدراسة قدمت توصيات مهمة لتعزيز تبنّي التكنولوجيا المالية في بيئات عالية المخاطر السيبرانية ينبغي على مزوّدي الخدمات الرقمية ومطوّري المنصات تعزيز ميزات الأمان وإظهارها بوضوح للمستخدمين لزيادة الثقة.

المبحث الثاني: الجانب النظري Theoretical Framework

اولاً: المخاطر السيبرانية

تُعد الأسواق المالية من أكثر القطاعات استهدافًا من قبل الهجمات السيبرانية، نتيجة التوسع المتزايد في الخدمات المالية الرقمية وتشابك الأنظمة المالية. وتمثل هذه الهجمات تهديدًا مباشرًا لاستقرار الأسواق والثقة الرقمية، الأمر الذي قد يحد من جهود الشمول المالي، ولا سيما في الاقتصادات النامية . (Welbum& Strong, 2022)

وتعتبر المخاطر الإلكترونية شكلاً من أشكال المخاطر التشغيلية وتعرف على أنها مخاطر الخسارة الناتجة عن الحوادث الرقمية الناجمة عن الحوادث الداخلية والخارجية أو أطراف ثالثة، بما في ذلك السرقة أو النزاهة المعرضة للخطر أو تلف المعلومات أو أصول التكنولوجيا، والاحتيال الداخلي والخارجي، وتعطيل الأعمال. وهذا التعريف يتوافق إلى حد كبير مع جهود القطاع الخاص المتزامنة المعروفة لتحديد المخاطر السيبرانية على سبيل المثال، مبادرة مخاطر الأمن السيبراني والمعلوماتية الخاصة بشركة ORX. وقد تؤدي حوادث المخاطر السيبرانية إلى إضعاف سرية وسلامة وتوافر البيانات (Curti .et.al. ,2019) والمعلومات، والتشغيل السليم للبنية التحتية لتكنولوجيا المعلومات حيث أن أنظمة الأمن السيبراني هي أنظمة مدعومة بالذكاء الاصطناعي للحماية من الانتهاكات الأمنية المحتملة ومنعها، ويستخدم الذكاء الاصطناعي لتطبيق الخدمات المصرفية عبر الهاتف المحمول

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

وتطوير حلول الذكاء الاصطناعي لدعم العملاء واتمتة العمليات والموارد البشرية والأمن واكتشاف الاحتيال (Saon& Miglanic, 2019)

عُرِّفَت مخاطر الأمن السيبراني على أنها المخاطر التشغيلية التي تتعرض لها أصول المعلومات والتقنية، والتي قد تؤثر في سرية المعلومات أو سلامتها أو توافرها، وكذلك في كفاءة وموثوقية أنظمة المعلومات (Kumar & Thomas, 2022). وتتمثل التهديدات السيبرانية الرئيسة في سرقة بيانات وهوية المستهلكين، والتلاعب بالبيانات، والهجمات التي تستهدف البنية التحتية المالية، فضلًا عن المخاطر الناجمة عن البرامج الضارة المدمرة، والتي تؤثر بصورة مباشرة في أعمال البنوك واستقرارها المالي والتشغيلي.(Piotrowski, 2022) وفي هذا السياق، يُسهم تصنيف مخاطر الأمن السيبراني وتحديد المحفزات الكامنة وراءها في بناء فهم مشترك لطبيعة هذه المخاطر بين المصارف، بما يشمل السلطات الرقابية والجهات الفاعلة في القطاع الخاص، الأمر الذي يسهم في تسهيل تبادل المعلومات وتعزيز التعاون في مجال إدارة المخاطر السيبرانية. ووفقًا لـ(Curti et al. ,2019) ، يتم تنظيم تصنيف مخاطر الأمن السيبراني ضمن إطار منهجي يضم فئات رئيسة تهدف إلى توحيد المفاهيم وتحسين كفاءة إدارة هذه المخاطر داخل المؤسسات المالية .منها:

مسببات المخاطر السيبرانية : تشير مسببات المخاطر السيبرانية إلى الطرق أو الآليات التي يتم من خلالها تنفيذ الهجوم الإلكتروني الضار، وتشمل ما يأتي:

(Piotrowski, 2022)& &. (OWASP, 2021) & (Curti et al., 2019)

- هجمات رفض الخدمة وهجمات رفض الخدمة الموزعة: وهي هجمات تستهدف إغراق الأنظمة أو الخوادم أو الشبكات بحركة مرور كثيفة تؤدي إلى استنزاف الموارد وعرض النطاق الترددي، مما يمنع النظام من تلبية الطلبات المشروعة.
- هجمات التنصت: يقوم المهاجمون بإدخال أنفسهم في الاتصال بين طرفين، مما يتيح لهم اعتراض حركة البيانات وتصفيتها وسرقتها.
- هجمات التصيد الاحتيالي:تتمثل في إرسال اتصالات احتيالية تبدو وكأنها واردة من مصادر موثوقة، غالبًا عبر البريد الإلكتروني، بهدف سرقة البيانات الحساسة أو تثبيت برامج ضارة
- هجمات كلمات المرور: تحدث عندما يحصل أطراف غير مصرح لهم على كلمات المرور من خلال الهندسة الاجتماعية، أو هجمات القوة الغاشمة، أو هجمات القاموس، أو اعتراض الاتصالات غير المشفرة؛
- هجمات حقن أوامر:يقوم المهاجم بإدخال تعليمات برمجية ضارة في خادم يستخدم قواعد بيانات SQLلإجبار النظام على الكشف عن بياناته أو تعديلها.
- هجمات البرمجة النصية عبر المواقع :تستغل موارد ويب تابعة لجهات خارجية لتشغيل شيفرات ضارة داخل متصفح المستخدم أو التطبيق.
- البرامج الضارة :برامج مصممة بقصد ضار لإحداث أضرار مباشرة أو غير مباشرة لأنظمة المعلومات أو سرقة البيانات.
- استغلال ثغرات اليوم الصفري: استغلال ثغرات أمنية غير معروفة سابقًا في الأجهزة أو البرمجيات قبل إصدار تصحيحات لها .
- هجمات أخرى / غير معروفة:تشير إلى الهجمات التي لا يمكن تصنيفها ضمن الفئات السابقة أو التي لا تكون طبيعتها معروفة للمؤسسة .

١. نتائج الحادث السيبراني: حيث يتمثل بما يلي (Curti et al., 2019)& (BCBS, 2021)

- اضطراب الأعمال وفشل الأنظمة: حوادث داخلية أو خارجية تؤدي إلى تعطل العمليات أو فشل أنظمة تكنولوجيا المعلومات.

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

P-ISSN: 2070-898X E-ISSN: 2707-9775

- خرق البيانات: فقدان أو كشف بيانات تتضمن معلومات التعريف الشخصية.
- سرقة أو فقدان معلومات غير شخصية: تشمل فقدان الملكية الفكرية أو المعلومات التجارية أو التقنية.
- سرقة الأموال: خسائر مالية مباشرة ناتجة عن حوادث رقمية عبر القنوات الإلكترونية.

٢. النية: تتمثل بمايلي: (Curti et al., 2019)

- حوادث متعمدة:عندما يكون الحادث السيبراني ناتجًا عن فعل مقصود أو إجرامي.
- حوادث غير مقصودة: عندما يحدث الحادث نتيجة خطأ بشري أو خلل غير متعمد.

٣. منشأ الحادث السيبراني: حيث يمكن تقسيمها الى: (Curti et al., 2019) & (BCBS, 2021)

- طرف خارجي: عندما ينشأ الحادث لدى طرف ثالث مثل الموردين أو مزودي الخدمات.
- طرف داخلي:عندما يبدأ الحادث داخل المؤسسة أو إحدى شركاتها التابعة.

٤. تصنيف الحوادث وفق فئات بازل: (BCBS, 2006)؛(BCBS, 2011)

- الاحتيال الداخلي: خسائر ناتجة عن أفعال احتيالية أو اختلاس من قبل أطراف داخلية.
- الاحتيال الخارجي: خسائر ناتجة عن أفعال احتيالية أو إجرامية من قبل أطراف خارجية.

ثانياً: الثقة الرقمية

ثانيا: الثقة الرقمية

الثقة الرقمية هي إيمان العملاء بأن الأنظمة الرقمية والخدمات المالية الإلكترونية التي تقدمها المؤسسات المالية آمنة وموثوقة، وأن البيانات والمعاملات التي يقومون بها محمية من المخاطر السيبرانية. وهي سمة مكتسبة تنشأ نتيجة سلوك المؤسسة والتزامها بالشفافية والأمن والامتثال للأخلاقيات المهنية، وتنعكس في استعداد العملاء للتفاعل واعتماد الخدمات الرقمية .(Launer et al., 2020)

تعد الثقة الرقمية عنصرًا أساسيًا لتحقيق الشمول المالي، إذ أنها تعزز اعتماد العملاء على المنتجات والخدمات المالية الرقمية، وتحفزهم على المشاركة الفعالة في الاقتصاد الرقمي (Levine, 2022)

١. **أبعاد الثقة الرقمية**

أ الشفافية الرقمية: تعني وضوح المعلومات المالية المتاحة للعملاء حول الخدمات الرقمية، بما يتيح لهم فهم كيفية إدارة بياناتهم واتخاذ القرارات المالية بثقة.(Guo, 2022)

ب **الأمن الرقمي :** يتعلق بحماية بيانات العملاء والمعلومات المالية من التهديدات السيبرانية الخارجية، وهو عامل أساسي في بناء الثقة الرقمية لدى العملاء (.Kluiters et al., 2023)

ج **الالتزام بالمعايير الأخلاقية :** يشير إلى تطبيق السياسات والمعايير الأخلاقية والمهنية في التعاملات الرقمية، بما يحمي حقوق العملاء ويضمن النزاهة في تقديم الخدمات، ويعزز الثقة الرقمية (Sharpe, 2022).

د **فاعلية الخدمات الرقمية:** يقصد بها قدرة المؤسسة على تقديم أدوات وخدمات مالية رقمية موثوقة وفعالة، تمكن العملاء من إتمام معاملاتهم بسرعة وكفاءة، مما يدعم الثقة الرقمية ويحفز الشمول المالي (Launer et al., 2022).

٢. **متطلبات بناء الثقة الرقمية**

يتطلب بناء الثقة الرقمية تحديد مواصفات خاصة للخدمات الإلكترونية تحظى بثقة المستخدم وتشعره بالأمان. إضافة إلى توفير بيئة قانونية. وفيما يأتي أهم متطلبات بناء الثقة الرقمية (بوميديان، ٢٠٢٠)

أ **ثقة المستخدم بالبيئة الرقمية**

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

يشكل انعدام ثقة المستخدمين بالعالم الرقمي أحد أهم الاسباب التي تحول دون استثمار الامكانيات الكامنة للإنترنت، وتطوير تطبيقات وخدمات الكترونية جديدة. حيث يعد عنصر الثقة والأمن أبرز العناصر اللازمة لتوفير بيئة مواتية لبناء مجتمع المعلومات إذ يرتبط استخدام الأفراد للخدمات الإلكترونية على شعورهم بالراحة والطمأنينة والأمان عند استخدامها.

ب البنية الأساسية والنظم المعلوماتية

في ظل اتساع نطاق شبكة الانترنت، أصبح المجرمون قادرين على إيجاد فرص جديدة في البيئة الرقمية القابلة للخرق، وذلك للقيام بأعمال إجرامية ضدها أو ضد البنية الأساسية الوطنية، وأصبحت البرمجيات الخبيثة والاعتداءات على الشبكات والنظم عن بعد معروفة بالنسبة لمستخدمي شبكة الانترنت، ولا ينجو منها إلا المستخدمون المحصنون.

ج الإطار القانوني للتحول الرقمي

يستغل المجرمون غياب نظم المساءلة، والثغرات في بنى تكنولوجيا المعلومات والاتصالات وأنظمتها وفي التشريعات الوطنية لارتكاب الجرائم المعلوماتية وخاصة في البلاد التي لم تسن قوانين تجرم الاعتداءات المعلوماتية أو التي لا تطبق هذه القوانين وقد وضعت بعض البلدان قوانين المكافحة الجرائم المعلوماتية وسوء استخدام تكنولوجيا المعلومات والاتصالات، ولكن تطبيقها مازال يواجه عددا من الصعوبات، لاسيما في المنطقة العربية، في غياب آليات للتطبيق ومحامين وقضاة مدربين على تطبيقها.

د ضعف البنية الأساسية

يشكل غياب البنية التنظيمية إحدى الاشكاليات التي تعيق حماية القضاء السيبراني فالمؤسسات والشركات التي تستخدم تكنولوجيا المعلومات والاتصالات لا تعتبر عنصري الحماية والأمن أساسين في حالات عديدة، ولا تستحدث في هيكلتها المؤسسي أية إدارة وحدة تختص بمراقبة أمن تكنولوجيا المعلومات والاتصالات وتطبيقاتها وبحمايته وهماله، كما انها لا تخضع أية سياسات أو خطط عمل لمواجهة التهديدات المعلوماتية الخارجية.

ثالثاً: الشمول المالي

١. تعريف الشمول المالي

يعرفه تقرير للبنك الدولي بأنه: نسبة الأفراد والشركات التي تستخدم الخدمات المالية باختلافها، حيث يتم استخدام الخدمات المصرفية على نطاق أوسع من قبل السكان كلما زادت سهولة الوصول توافر أجهزة الصراف الآلي أو الفروع - وانخفضت التكلفة، وزادت جودة الخدمات (Barajas et al, 2020) و الشمول المالي يعني أن الأفراد والشركات لديهم إمكانية الوصول إلى منتجات وخدمات مالية مفيدة وبأسعار معقولة تلبي احتياجاتهم - معاملات ومدفوعات ومنتجات ادخار وتسهيلات ائتمانية وقروض وخدمات تأمين - ويتم تقديمها على نحو مسؤول ومستدام (البنك الدولي، ٢٠٢٢) كما أن صندوق النقد الدولي واللجنة الاستشارية لمساعدة الفقراء عرفا الشمول المالي بأنه تمكن الأفراد وصغار السن من الوصول والاستفادة من مصفوفة متكاملة من الخدمات المالية ذات الجودة العالية المدفوعات التحويلات المدخرات الائتمان والتأمين والمقدمة من قبل مجموعة متنوعة من مقدمي تلك الخدمات بطريقة سهلة ومستدامة في ظل بيئة قانونية وتنظيمية مناسبة " (أنور ، ٢٠٢١).

٢. أبعاد الشمول المالي

يُعرف الشمول المالي بأنه قدرة الأفراد على الوصول إلى الخدمات المالية واستخدامها والاستفادة من جودتها بطريقة مستدامة، ويشمل عدة أبعاد رئيسية تهدف إلى تعزيز المشاركة الفعالة للأفراد والشركات في النظام المالي. ولقياس مستوى الشمول المالي، قامت عدة منظمات دولية، وعلى رأسها

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

Financial Inclusion Global Working Group (FIDWG)، بتحديد أبعاد ومؤشرات للشمول المالي، كما أضافت الشراكة العالمية من أجل الشمول المالي التابعة لمجموعة العشرين بعدًا ثالثًا يركز على جودة الخدمات المالية

(FIDWG, 2011)&(Global Partnership for Financial Inclusion, 2013).

أ. الوصول إلى الخدمات المالية: يشير هذا البعد إلى قدرة الأفراد على الوصول الفعلي إلى الخدمات المالية، إذ يشكل أي قصور في نقاط الخدمة عائقًا مباشرًا أمام الشمول المالي. يتم قياس الوصول باستخدام مؤشرات كمية تشمل: عدد نقاط تقديم الخدمات المالية لكل ١٠,٠٠٠ مواطن، عدد أجهزة الصراف الآلي وفروع المؤسسات المالية لكل ١,٠٠٠ كلم، قرب وترابط نقاط تقديم الخدمات المالية، النسبة المئوية للسكان مقارنة بعدد نقاط الخدمة، وحسابات النقود الإلكترونية

(عطية، ٢٠٢١) &(بوتبينة، ٢٠١٨).

ب.استخدام الخدمات المالية: يقيس هذا البعد مدى قدرة الأفراد على استخدام الخدمات المالية بعد الوصول إليها، مع مراعاة العوامل الاجتماعية والثقافية والدينية والتكلفة الإدارية. تشمل مؤشرات الاستخدام: نسبة البالغين الذين يملكون حسابات بنكية أو ودائع، عدد المعاملات المنجزة عبر الإنترنت أو تطبيقات الهاتف، مدى استمرارية استخدام الحسابات البنكية، عدد التحويلات المالية المحلية والدولية، ونسبة الشركات الصغيرة والمتوسطة ومتناهية الصغر التي تملك حسابات بنكية أو استفادت من القروض (محمد علي، ٢٠٢٠)&(شنبي وبن لخضر، ٢٠١٩)

ج. جودة الخدمات المالية: بعد الوصول والاستخدام، تعتبر جودة الخدمات المالية العامل الأساسي الذي يدفع الأفراد للاستمرار في استخدامها والاعتماد عليها. تشمل مؤشرات الجودة: تغطية تكاليف الحصول على الخدمات المالية (الرسوم وتكاليف الاحتفاظ بالحسابات)، مؤشرات الشفافية والمصداقية في عرض المعلومات، سهولة الوصول والاستخدام، توفر أدوات حماية العملاء، ونسبة الوعي والثقافة المالية لدى العملاء. تلعب جودة الخدمات المالية دورًا مهمًا في كسب ثقة العملاء وزيادة رضاهم وولائهم (شنبي وبن لخضر، ٢٠١٩)& (بوتبينة، ٢٠١٨).

رابعاً: دور التكنولوجيا المالية في تحقيق الشمول المالي وجذب العملاء

لم تعد الخدمات المالية التقليدية عاملا جانبا للأفراد، فقد سهلت التكنولوجيا الأمر كثيرا، خاصة في تطوير الخدمات المصرفية وتعزيز اليات جذب العملاء للمؤسسات المالية.

شمول الخدمات المالية المصرفية الحديثة تعتبر الخدمات المالية منتجات مالية غير مادية تقوم البنوك والمؤسسات المالية بتقديمها للعملاء حسب الطلب، وعادة ترتبط هذه المنتجات المالية بالوظائف الرئيسية للبنوك المتمثلة في الإيداع والائتمان وخدمات الاستثمار (نيس، ٢٠٢٢) وللاستفادة من هذه الخدمات على العميل التنقل إلى المؤسسة المالية وتقديم ملف كامل، إلا أن دمج التكنولوجيا الحديثة في المعاملات المالية حولتها إلى خدمات مالية رقمية ، حيث يعرفها البنك الدولي على أنها تلك الخدمات المالية التي تعتمد على التقنيات الرقمية لتسليمها واستخدامها من قبل المستهلكين (Pazarbasioglu et al, 2020) وتسهم التكنولوجيا المالية بأدواتها في تسهيل تقديم الخدمات المالية وايصالها للعملاء من خلال إدخال الابتكارات خاصة في وسائل الدفع الالكتروني مثل أنظمة تحويل الأموال وأنظمة الدفع عن طريق بطاقات الائتمان وأجهزة الصرف والموزعات الآلية (نيس ، ٢٠٢٢).

ترى الباحثة انه في ظل التوسع السريع في استخدام الخدمات المالية الرقمية والاعتماد المتزايد على التكنولوجيا المالية، تواجه المؤسسات تحديات كبيرة نتيجة المخاطر السيبرانية، مثل الهجمات الإلكترونية وفقدان البيانات وسرقة الهوية، والتي تؤثر بشكل مباشر على أمان المعلومات وحماية بيانات العملاء. هذه المخاطر قد تقلل من ثقة العملاء الرقمية في الأنظمة والخدمات المقدمة، وهو ما يعد عاملاً حاسمًا لضمان قبولهم للخدمات المالية الرقمية والمشاركة الفعالة في النظام المالي. ومن هنا

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

يظهر الدور المركزي للثقة الرقمية كعامل وسيط بين إدارة المخاطر السيبرانية ومستوى الشمول المالي، الذي يقاس من خلال أبعاد متعددة تشمل الوصول إلى الخدمات المالية، واستخدامها، وجودة هذه الخدمات. وبالتالي، فإن فهم العلاقة بين المخاطر السيبرانية والثقة الرقمية وتأثيرها على الشمول المالي أصبح ضرورة للسيطرة على المخاطر وتعزيز مشاركة الأفراد في الخدمات المالية الرقمية بشكل آمن وفعّال، مما يتيح وضع سياسات واستراتيجيات قادرة على تعزيز الشمول المالي في البيئة الرقمية.

المبحث الثالث: الجانب العملي Practical Framework

التمهيد

يتناول هذا المحور تحليل البيانات التي جرى جمعها من خلال الاستبانة الموزعة على عينة البحث، بهدف تشخيص مستوى توفر متغيرات الدراسة والمتمثلة في: إدارة مخاطر الأمن السيبراني، والثقة الرقمية، والشمول المالي عبر التكنولوجيا المالية، واختبار العلاقات والأثر فيما بينها. وبلغ حجم عينة البحث (٩٦) مفردة من العاملين في المصارف محل الدراسة.

أولاً: السمات الشخصية لعينة البحث

يهدف هذا الجزء إلى عرض الخصائص الديموغرافية لأفراد العينة، لما لها من دور في إعطاء صورة واضحة عن خلفية المبحوثين، والتي تسهم في تفسير نتائج الدراسة لاحقًا. ويعرض الجدول (١) توزيع أفراد العينة وفق (النوع الاجتماعي، العمر، التحصيل الدراسي).

جدول (١) السمات الشخصية لعينة البحث (ن = ٩٦)

السمة	الفئة	التكرار	النسبة المئوية
النوع الاجتماعي	ذكر	94	97.9%
	أنثى	2	2.1%
	المجموع	96	100%
العمر	25سنة فأقل	13	13.5%
	26–35سنة	35	36.5%
	36–45سنة	30	31.3%
	46–55سنة	10	10.4%
	56سنة فأكثر	8	8.3%
	المجموع	96	100%
التحصيل الدراسي	دكتوراه	1	1.0%
	ماجستير	1	1.0%
	دبلوم عالي	1	1.0%
	بكالوريوس	70	72.9%
	أخرى	23	24.1%
	المجموع	96	100%

المصدر: من عمل الباحثة بالاعتماد على نتائج البرنامج SPSS

فيما يتعلق بالجدول (١) يمكن توضيح ما يأتي:

- النوع الاجتماعي :يتضح أن الذكور يشكلون الغالبية العظمى من أفراد العينة بنسبة (٩٧,٩٪) ممثلة بـ (٩٤) فردًا، في حين بلغت نسبة الإناث (٢,١٪) ممثلة بفردين فقط من إجمالي العينة. ويعكس هذا التوزيع التفوق العددي للذكور في بيئة العمل المصرفي محل الدراسة، والذي قد يرتبط بطبيعة الهيكل

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧ - ٢٢٦

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

P-ISSN: 2070-898X E-ISSN: 2707-9775

الوظيفي في المصارف أو طبيعة الأعمال التقنية والإدارية المرتبطة بمجال الأمن السيبراني والخدمات الرقمية.

- العمر :تشير البيانات إلى أن الفئة العمرية (٢٦–٣٥ سنة) تمثل النسبة الأعلى من العينة بنسبة (٣٦,٥٪) وبواقع (٣٥) فردًا، تليها الفئة (٣٦–٤٥ سنة) بنسبة (٣١,٣٪) وبعدد (٣٠) فردًا، ثم الفئة (٢٥ سنة فأقل) بنسبة (١٣,٥٪). بينما جاءت الفئات الأكبر سنًا (٤٦–٥٥ سنة) و(٥٦ سنة فأكثر) بنسب أقل بلغت (١٠,٤٪) و(٨,٣٪) على التوالي. ويعكس هذا التوزيع أن غالبية أفراد العينة ينتمون إلى الفئات العمرية النشطة مهنيًا، والتي غالبًا ما تكون أكثر تفاعلًا مع التقنيات الرقمية وأكثر قدرة على التعامل مع متطلبات التكنولوجيا المالية والأمن السيبراني.
- التحصيل الدراسي :يتضح أن حملة شهادة البكالوريوس يمثلون النسبة الأكبر من أفراد العينة بنسبة (٧٢,٩٪) وبعدد (٧٠) فردًا، تليهم فئة (أخرى) بنسبة (٢٤,١٪) وبواقع (٢٣) فردًا، في حين جاءت شهادات الدراسات العليا (دكتوراه، ماجستير، دبلوم عالي) بنسب محدودة جدًا بلغت (١٪) لكل منها. ويشير هذا التوزيع إلى أن معظم أفراد العينة يمتلكون تأهيلًا علميًا مناسبًا يمكّنهم من فهم طبيعة الأسئلة المتعلقة بمحاور الدراسة، مما يعزز من دقة الإجابات وموثوقية النتائج.

ثانياً: اختبار الثبات

لغرض التحقق من اتساق فقرات الاستبانة واستقرارها الداخلي، تم استخدام معامل كرونباخ ألفا (Cronbach's Alpha)بوصفه أحد أكثر المقاييس شيوعًا في تقييم ثبات أدوات القياس التي تتضمن عدة فقرات تقيس المتغير نفسه. وتعكس قيمة هذا المعامل درجة التجانس بين الفقرات؛ إذ تتراوح بين (٠–١)، وكلما اقتربت من (١) دلّ ذلك على مستوى أعلى من الثبات. ويُعدّ الحد الأدنى المقبول عادةً (٠,٧٠) للحكم على جودة الثبات. وقد طُبّق اختبار كرونباخ ألفا على فقرات الاستبانة الخاصة بكل متغير من متغيرات الدراسة، وكذلك على المقياس الكلي، وذلك بالاعتماد على بيانات عينة البحث البالغة (٩٦) مفردة.

جدول (٢) قيم معامل الثبات(Cronbach's Alpha)

المتغير	عدد الفقرات	قيمة الثبات
إدارة مخاطر الأمن السيبراني	8	0.811
الثقة الرقمية	8	0.756
الشمول المالي في ظل التكنولوجيا المالية	8	0.923
المقياس الكلي	24	0.901

المصدر: من عمل الباحثة بالاعتماد على نتائج البرنامج SPSS

يتضح من الجدول أعلاه أن جميع قيم معاملات الثبات الخاصة بمتغيرات الدراسة، وكذلك للمقياس الكلي، قد تجاوزت الحد الأدنى المقبول (٠,٧٠)، مما يدل على وجود اتساق داخلي مرتفع بين فقرات كل متغير، ويؤكد أن الاستبانة تتمتع بدرجة عالية من الثبات، الأمر الذي يعزز من موثوقية النتائج المستخلصة منها في التحليل الإحصائي اللاحق.

ثالثاً: اختبار التوزيع الطبيعي

تعتمد طبيعة الأساليب الإحصائية المستخدمة في التحليل على خصائص توزيع البيانات. فإذا كانت البيانات تتبع التوزيع الطبيعي، يمكن استخدام الاختبارات الإحصائية المعلمية(Parametric Tests) ، أما إذا لم تتبع هذا التوزيع فيُصار إلى استخدام الاختبارات اللامعلمية. ولغرض التحقق من طبيعة توزيع بيانات متغيرات الدراسة، تم استخدام اختبار كولموغوروف–سميرنوف(Kolmogorov–

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧ - ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

Smirnov). وقد أُجري هذا الاختبار على بيانات عينة البحث البالغة (٩٦) مفردة لكل من متغيرات الدراسة: إدارة مخاطر الأمن السيبراني، والثقة الرقمية، والشمول المالي عبر التكنولوجيا المالية.

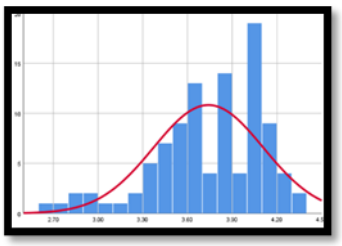
جدول (٣) اختبار التوزيع الطبيعي لمتغيرات الدراسة

المتغير	إحصاءة الاختبار (K-S)	عدد المفردات	معنوية الاختبار (Sig.)
إدارة مخاطر الأمن السيبراني	0.082	96	0.097
الثقة الرقمية	0.079	96	0.071
الشمول المالي في ظل التكنولوجيا المالية	0.087	96	0.108

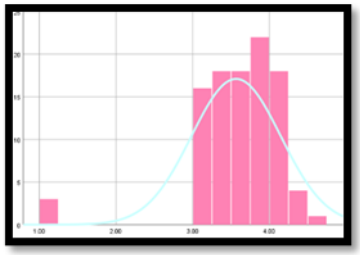
المصدر: من عمل الباحثة بالاعتماد على نتائج البرنامج SPSS

يتضح من الجدول أعلاه أن قيم معنوية الاختبار (Sig.) لجميع متغيرات الدراسة كانت أكبر من مستوى الدلالة الإحصائية (٠,٠٥)، مما يدل على أن بيانات هذه المتغيرات تتبع التوزيع الطبيعي.

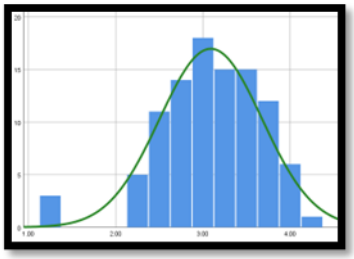
وعليه، يمكن الاعتماد على الاختبارات الإحصائية المعلمية في تحليل البيانات واختبار فرضيات الدراسة بثقة إحصائية مناسبة .وتؤكد الأشكال البيانية اللاحقة (المدرجات التكرارية) هذا الاستنتاج، إذ تُظهر أن تدرج البيانات لمتغيرات الدراسة يقترب من المنحنى الطبيعي.



الشكل (١) التدرج لبيانات المتغير إدارة مخاطر الأمن السيبراني



الشكل (٢) التدرج لبيانات المتغير الثقة الرقمية



الشكل (٣) التدرج لبيانات المتغير الشمول المالي في ظل التكنولوجيا المالية

رابعاً: التحليل الوصفي لأبعاد ومتغيرات الدراسة

لأغراض تشخيص مستوى توفر متغيرات الدراسة لدى عينة البحث، تم الاعتماد على أدوات الإحصاء الوصفي والمتمثلة في الوسط الحسابي والانحراف المعياري، لما لهما من أهمية في توضيح الاتجاه العام لإجابات أفراد العينة وقياس درجة تشتت القيم حول هذا الاتجاه.

من الجدول (٤) يتضح إن المتغير إدارة مخاطر الأمن السيبراني له وسط حسابي بلغ (٣,٦٧) أي بمستوى توافر مرتفع، في حين بلغ الانحراف المعياري (٠,٧١) مما يشير إلى وجود تشتت قليل في آراء أفراد العينة، أما معامل الاختلاف فقد بلغ (١٩,٣٤٪)، وهو ما يدل على وجود تجانس واضح في الآراء. وقد احتل هذا المتغير الترتيب الأول بين متغيرات البحث. أما تحليل أبعاد متغير إدارة مخاطر الأمن السيبراني فقد أظهر ما يأتي:

- الوقاية والتحديث المستمر :يتميز هذا البعد بوسط حسابي قدره (٤,٣٢)، مما يدل على توافر مرتفع جدًا، مع انحراف معياري بلغ (٠,٦٨) مشيرًا إلى تشتت قليل في الآراء، في حين بلغ معامل الاختلاف (١٥,٧٤٪)، مما يدل على تجانس عالٍ بين آراء العينة، ليحتل هذا البعد الترتيب الأول.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226
P-ISSN: 2070-898X E-ISSN: 2707-9775
الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

- نتائج الحادث السيبراني :بلغ الوسط الحسابي لهذا البعد (٣,٨٨)، وهو ما يشير إلى توافر مرتفع، بينما بلغ الانحراف المعياري (٠,٧٣) دالًا على تشتت قليل، وسجل معامل الاختلاف (١٨,٨١٪) مما يعكس وجود تجانس في الآراء، ليأتي هذا البعد في الترتيب الثاني.
- مسببات المخاطر السيبرانية :حقق هذا البعد وسطًا حسابيًا قدره (٣,٦٤)، مما يدل على توافر مرتفع، مع انحراف معياري بلغ (٠,٧٩) يشير إلى تشتت محدود، وبلغ معامل الاختلاف (٢١,٧٠٪) مما يدل على تجانس نسبي في الآراء، ليحتل الترتيب الثالث.
- نية الحادث السيبراني (البعد البشري/التدريب) :بلغ الوسط الحسابي (٣,١٢)، وهو ما يدل على توافر معتدل، بينما بلغ الانحراف المعياري (٠,٨٦) مشيرًا إلى تشتت متوسط في الآراء، وسجل معامل الاختلاف (٢٧,٥٦٪) مما يدل على وجود تباين نسبي بين إجابات العينة، ليأتي هذا البعد في الترتيب الرابع.
- التعلم من الحوادث وتصنيفها وفق المعايير الدولية :جاء هذا البعد بوسط حسابي بلغ (٢,٤١)، مما يدل على توافر ضعيف، مع انحراف معياري بلغ (٠,٩١) يشير إلى وجود تشتت واضح في الآراء، وبلغ معامل الاختلاف (٣٧,٧٦٪) مما يعكس وجود تباين ملحوظ بين إجابات أفراد العينة، ليحتل هذا البعد الترتيب الخامس والأخير.

ويُلاحظ من ذلك أن المصارف تركز بصورة كبيرة على الجوانب الوقائية والتقنية المباشرة للأمن السيبراني، في حين يظهر ضعف نسبي في الجوانب المرتبطة بالتعلم المؤسسي من الحوادث وتصنيفها وفق الأطر والمعايير الدولية، وهو ما يعكس واقع الممارسات المؤسسية في البيئة المصرفية العراقية.

جدول (٤) تحليل أبعاد المتغير المستقل إدارة مخاطر الأمن السيبراني

ت	البُعد	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	الترتيب
1	الوقاية والتحديث المستمر	4.32	0.68	15.74%	1
2	نتائج الحادث السيبراني	3.88	0.73	18.81%	2
3	مسببات المخاطر السيبرانية	3.64	0.79	21.70%	3
4	نية الحادث السيبراني (البعد البشري/التدريب)	3.12	0.86	27.56%	4
5	التعلم من الحوادث وتصنيفها وفق المعايير الدولية	2.41	0.91	37.76%	5
	المتغير: إدارة مخاطر الأمن السيبراني	3.67	0.71	19.34%	الأول

المصدر: من عمل الباحثة بالاعتماد على نتائج البرنامج SPSS

من الجدول (٤) يتضح إن المتغير الثقة الرقمية له وسط حسابي بلغ (٣,٥٣) أي بمستوى توافر مرتفع، في حين بلغ الانحراف المعياري (٠,٧٣) مما يشير إلى وجود تشتت قليل في آراء أفراد العينة، أما معامل الاختلاف فقد بلغ (٢٠,٦٧٪)، وهو ما يدل على وجود تجانس واضح في الآراء. وقد احتل هذا المتغير الترتيب الثاني بين متغيرات البحث. أما تحليل أبعاد متغير الثقة الرقمية فقد أظهر ما يأتي:

- الأمن الرقمي :يتميز هذا البعد بوسط حسابي قدره (٤,٢٨)، مما يدل على توافر مرتفع جدًا، مع انحراف معياري بلغ (٠,٦٩) مشيرًا إلى تشتت قليل في الآراء، في حين بلغ معامل الاختلاف (١٦,١٢٪) مما يدل على تجانس عالٍ بين آراء العينة، ليحتل هذا البعد الترتيب الأول.

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧ - ٢٢٦

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

P-ISSN: 2070-898X E-ISSN: 2707-9775

- فاعلية الخدمات الرقمية :بلغ الوسط الحسابي لهذا البعد (٣,٨٢)، وهو ما يشير إلى توافر مرتفع، بينما بلغ الانحراف المعياري (٠,٧٥) دالًا على تشتت محدود، وسجل معامل الاختلاف (١٩,٦٣٪) مما يعكس وجود تجانس في الآراء، ليأتي هذا البعد في الترتيب الثاني.
- الشفافية الرقمية :حقق هذا البعد وسطًا حسابيًا قدره (٣,٤٧)، مما يدل على توافر مرتفع، مع انحراف معياري بلغ (٠,٨١) يشير إلى تشتت نسبي في الآراء، وبلغ معامل الاختلاف (٢٣,٣٤٪) مما يدل على تجانس نسبي بين الإجابات، ليحتل الترتيب الثالث.
- الالتزام بالمعايير الأخلاقية :جاء هذا البعد بوسط حسابي بلغ (٢,٥٤)، مما يدل على توافر ضعيف، مع انحراف معياري بلغ (٠,٨٨) يشير إلى وجود تشتت واضح في الآراء، وبلغ معامل الاختلاف (٣٤,٦٤٪) مما يعكس وجود تباين ملحوظ بين إجابات أفراد العينة، ليحتل هذا البعد الترتيب الرابع والأخير.

ويُلاحظ من ذلك أن الثقة الرقمية لدى العملاء ترتكز بصورة أساسية على الجوانب الأمنية والتقنية للخدمات الرقمية، في حين يظهر ضعف واضح في الجوانب المرتبطة بالالتزام بالمعايير الأخلاقية والشفافية التنظيمية، وهو ما يعكس واقع الممارسات المؤسسية في البيئة المصرفية العراقية.

جدول (٥) تحليل أبعاد المتغير الوسيط (الثقة الرقمية)

ت	البُعد	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	الترتيب
1	الأمن الرقمي	4.28	0.69	16.12%	1
2	فاعلية الخدمات الرقمية	3.82	0.75	19.63%	2
3	الشفافية الرقمية	3.47	0.81	23.34%	3
4	الالتزام بالمعايير الأخلاقية	2.54	0.88	34.64%	4
	المتغير: الثقة الرقمية	3.53	0.73	20.67%	الثاني

المصدر: من عمل الباحثة بالاعتماد على نتائج البرنامج SPSS

من الجدول (٦) يتضح إن المتغير الشمول المالي عبر التكنولوجيا المالية له وسط حسابي بلغ (٢,٨٤) أي بمستوى توافر معتدل، في حين بلغ الانحراف المعياري (٠,٨٦) مما يشير إلى وجود تشتت متوسط في آراء أفراد العينة، أما معامل الاختلاف فقد بلغ (٣٠,٢٨٪)، وهو ما يدل على وجود تباين نسبي في الآراء. وقد احتل هذا المتغير الترتيب الثالث بين متغيرات البحث. أما تحليل أبعاد متغير الشمول المالي عبر التكنولوجيا المالية فقد أظهر ما يأتي:

- ✓ الوصول إلى الخدمات المالية :يتميز هذا البعد بوسط حسابي قدره (٣,٢٨)، مما يدل على توافر معتدل، مع انحراف معياري بلغ (٠,٨٢) مشيرًا إلى تشتت متوسط في الآراء، في حين بلغ معامل الاختلاف (٢٥,٠٠٪) مما يدل على تجانس نسبي بين آراء العينة، ليحتل هذا البعد الترتيب الأول.
- ✓ استخدام الخدمات المالية :بلغ الوسط الحسابي لهذا البعد (٢,٩٤)، وهو ما يشير إلى توافر معتدل يميل إلى الضعف، بينما بلغ الانحراف المعياري (٠,٨٦) دالًا على تشتت متوسط، وسجل معامل الاختلاف (٢٩,٢٥٪) مما يعكس وجود تباين نسبي في الآراء، ليأتي هذا البعد في الترتيب الثاني.
- ✓ جودة الخدمات المالية :جاء هذا البعد بوسط حسابي بلغ (٢,٣١)، مما يدل على توافر ضعيف، مع انحراف معياري بلغ (٠,٩١) يشير إلى وجود تشتت واضح في الآراء، وبلغ معامل الاختلاف (٣٩,٣٩٪) مما يعكس وجود تباين ملحوظ بين إجابات أفراد العينة، ليحتل هذا البعد الترتيب الثالث والأخير.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

ويُلاحظ من ذلك أن المصارف تمكنت إلى حدٍ ما من توفير قنوات الوصول إلى الخدمات المالية الرقمية، إلا أن الاستخدام الفعلي لهذه الخدمات لا يزال دون المستوى المطلوب، في حين تمثل جودة الخدمات المالية الحلقة الأضعف في تحقيق الشمول المالي، وهو ما يعكس الواقع الفعلي لبيئة التكنولوجيا المالية في المصارف العراقية، ويبرر المشكلة البحثية التي انطلقت منها الدراسة.

جدول (٦) تحليل أبعاد المتغير التابع الشمول المالي عبر التكنولوجيا المالية

ت	البُعد	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	الترتيب
1	الوصول إلى الخدمات المالية	3.28	0.82	25.00%	1
2	استخدام الخدمات المالية	2.94	0.86	29.25%	2
3	جودة الخدمات المالية	2.31	0.91	39.39%	3
	المتغير: الشمول المالي عبر التكنولوجيا المالية	2.84	0.86	30.28%	الثالث

المصدر: من عمل الباحثة بالاعتماد على نتائج البرنامج SPSS

خامسا: اختبار الفرضيات

اختبار الفرضية الرئيسة الاولى: توجد علاقات ارتباط ذات دلالة احصائية بين المتغيرات (إدارة مخاطر الأمن السيبراني، الثقة الرقمية، الشمول المالي في ظل التكنولوجيا المالية) في المصارف العراقية

بلغت قيمة الارتباط بين إدارة مخاطر الأمن السيبراني والثقة الرقمية (0.742)، وهي قيمة مرتفعة تشير إلى وجود ارتباط قوي وموجب بين المتغيرين، مما يدل على أن تحسن ممارسات إدارة مخاطر الأمن السيبراني داخل المصارف يسهم بصورة واضحة في تعزيز مستوى الثقة الرقمية لدى المستخدمين. كما بلغت قيمة الارتباط بين إدارة مخاطر الأمن السيبراني والشمول المالي عبر التكنولوجيا المالية (0.681)، وهي قيمة مرتفعة تعكس وجود علاقة موجبة ذات دلالة إحصائية، مما يشير إلى أن فعالية إدارة المخاطر السيبرانية تمثل عاملًا مهمًا في دعم انتشار الخدمات المالية الرقمية وتعزيز الشمول المالي. في حين بلغت قيمة الارتباط بين الثقة الرقمية والشمول المالي (0.703)، وهي قيمة مرتفعة تدل على علاقة موجبة قوية، بما يؤكد أن زيادة مستوى الثقة الرقمية لدى العملاء تنعكس بشكل مباشر على زيادة اعتمادهم على الخدمات المالية الرقمية. وبما أن جميع قيم معنوية الاختبار (Sig.)كانت أقل من (٠,٠٥)، فإن هذه العلاقات تُعد ذات دلالة إحصائية عالية، مما يتيح قبول الفرضية الرئيسة الأولى، والتي تنص على وجود علاقات ارتباط ذات دلالة إحصائية بين متغيرات الدراسة في المصارف العراقية.

جدول (٧) معاملات الارتباط بين متغيرات الدراسة (Pearson Correlation)

المتغيرات	إدارة مخاطر الأمن السيبراني	الثقة الرقمية	الشمول المالي
إدارة مخاطر الأمن السيبراني	1	.742**	.681**
Sig. (2-tailed)	—	.000	.000
N	96	96	96
الثقة الرقمية	.742**	1	.703**
Sig. (2-tailed)	.000	—	.000
N	96	96	96

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

الشمول المالي	.681**	.703**	1
Sig. (2-tailed)	.000	.000	—
N	96	96	96
**دالة عند مستوى(0.01)			

المصدر: من عمل الباحثة بالاعتماد على نتائج البرنامج SPSS

اختبار الفرضية الرئيسة الثانية: يسهم متغير الثقة الرقمية بدور الوسيط الجزئي في العلاقة بين إدارة مخاطر الأمن السيبراني والشمول المالي عبر التكنولوجيا المالية في المصارف العراقية.

يتضح من الجدول (٨) وجود تأثيرات مباشرة موجبة ذات دلالة إحصائية بين متغيرات الدراسة. إذ بلغ تأثير إدارة مخاطر الأمن السيبراني في الثقة الرقمية (Beta = 0.742) وهو تأثير قوي ودال إحصائيًا، مما يدل على أن تحسن إدارة المخاطر يسهم في بناء الثقة الرقمية. كما بلغ تأثير الثقة الرقمية في الشمول المالي (Beta = 0.703) وهو تأثير قوي ودال، مما يشير إلى أن ارتفاع مستوى الثقة الرقمية يؤدي إلى زيادة الاعتماد على الخدمات المالية الرقمية. في حين بلغ التأثير المباشر لإدارة مخاطر الأمن السيبراني في الشمول المالي(Beta = 0.681) ، وهو تأثير مرتفع ودال إحصائيًا. أما التأثير غير المباشر لإدارة مخاطر الأمن السيبراني في الشمول المالي عبر الثقة الرقمية فقد بلغ (٠,٥٢١)، تشير النتائج إلى أن الثقة الرقمية تؤدي دور الوسيط الجزئي في العلاقة بين إدارة مخاطر الأمن السيبراني والشمول المالي، إذ بقي التأثير المباشر دالًا إحصائيًا بعد إدخال المتغير الوسيط، بالتزامن مع وجود تأثير غير مباشر معنوي، مما يدل على أن إدارة مخاطر الأمن السيبراني تؤثر في الشمول المالي بشكل مباشر، وكذلك بشكل غير مباشر عبر تعزيز الثقة الرقمية.

جدول (٨) تحليل تأثير متغيرات الدراسة (التأثيرات المباشرة وغير المباشرة)

ت	مسار التأثير	Beta	T	Sig.	R^2	نوع التأثير
1	إدارة مخاطر الأمن السيبراني ← الثقة الرقمية	0.742	10.88	0.000	0.551	مباشر
2	الثقة الرقمية ← الشمول المالي	0.703	9.96	0.000	0.494	مباشر
3	إدارة مخاطر الأمن السيبراني ← الشمول المالي	0.681	9.21	0.000	0.463	مباشر
4	إدارة مخاطر الأمن السيبراني ← الثقة الرقمية ← الشمول المالي	0.521		0.000		غير مباشر (وسيط)

المصدر: من عمل الباحثة بالاعتماد على نتائج البرنامج AMOS

المبحث الرابع: استنتاجات وتوصيات Conclusions and Recommendations

اولاً: الاستنتاجات

١. تُظهر العينة تمركزًا لدى فئات عمرية نشطة مهنيًا وبمستوى تعليمي مناسب، ما يعزز موثوقية الإجابات وقدرتها على تمثيل واقع العمل المصرفي الرقمي.

٢. تركّز المصارف بدرجة عالية على الجوانب الوقائية والتقنية المباشرة، مقابل ضعف نسبي في التعلم من الحوادث والالتزام بالمعايير الدولية، مع مستوى متوسط للبعد البشري والتدريب. يعكس ذلك اهتمامًا بالحماية أكثر من إدارة المعرفة السيبرانية المؤسسية.

٣. تقوم الثقة الرقمية أساسًا على قوة الأمن الرقمي وفاعلية الخدمات، مع ضعف واضح في الشفافية والالتزام بالمعايير الأخلاقية. يدل هذا على أن بناء الثقة يتم من منظور تقني أكثر من كونه تنظيميًا.

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

P-ISSN: 2070-898X E-ISSN: 2707-9775

٤. تحقق المصارف مستوى معتدلًا في الوصول للخدمات، لكن الاستخدام الفعلي وجودة الخدمات ما زالا دون المطلوب. تمثل جودة الخدمة الحلقة الأضعف في تحقيق الشمول المالي الفعّال.
٥. توجد علاقات ارتباط موجبة قوية ودالة إحصائيًا بين إدارة مخاطر الأمن السيبراني، والثقة الرقمية، والشمول المالي، بما يؤكد ترابط هذه المتغيرات وتأثيرها المتبادل داخل المصارف العراقية.
٦. تلعب الثقة الرقمية دور الوسيط الجزئي في العلاقة بين إدارة مخاطر الأمن السيبراني والشمول المالي، إذ يستمر التأثير المباشر مع وجود تأثير غير مباشر معنوي عبر الثقة الرقمية.

ثانياً: التوصيات

١. بتوسيع مشاركة الكوادر النسوية وتعزيز التدريب التقني للفئات المختلفة لدعم متطلبات الأمن السيبراني والتكنولوجيا المالية.
٢. تعزيز التدريب، وتوثيق الحوادث، والالتزام بالمعايير الدولية لتحويل الأمن السيبراني إلى ثقافة مؤسسية متكاملة.
٣. تقوية الشفافية وسياسات حماية البيانات والإفصاح الأخلاقي لتعزيز الثقة من جانبها التنظيمي.
٤. تحسين جودة الخدمات الرقمية عبر تطوير البنية التقنية، وتسريع الأنظمة، وتبسيط الإجراءات، وتعزيز الدعم الفني.
٥. تطوير ممارسات إدارة مخاطر الأمن السيبراني بوصفها أساسًا لتعزيز الثقة الرقمية ودعم الشمول المالي.
٦. تعزيز سياسات بناء الثقة الرقمية بالتوازي مع تحسين إدارة المخاطر لضمان تعظيم أثرهما في تحقيق الشمول المالي.

التمويل

لم يتلق هذا البحث أي تمويل محدد من أي جهة مانحة في القطاعات العامة أو التجارية أو غير الربحية.

تضارب المصالح

يُعلن المؤلفون عدم وجود أي تضارب في المصالح فيما يتعلق بنشر هذه الورقة البحثية .

شكر وتقدير

يتقدم المؤلفون بجزيل الشكر للمؤسسة على دعمها المعنوي طوال فترة هذا البحث. لقد كان لتشجيعها وتوجيهها دورٌ بالغ الأهمية في إنجاز هذا البحث.

المصادر العربية

- أنور، إيمان إسماعيل (٢٠٢١). دور الشمول المالي في تعزيز المدخرات، مجلة الدراسات المالية.ص٦
- باراخاس وآخرون (٢٠٢٠). الشمول المالي: ماذا تعلمنا حتى الآن؟ وماذا علينا أن نتعلم؟
- صندوق النقد الدولي. تم الاطلاع عليه بتاريخ ٢٠٢٣/٠٦/٢٣، من الرابط التالي:
https://www.imf.org/en/Publications/WP/Issues/2020/08/07/Financial-Inclusion-What-Have-We-Learned-So-Far-What-Do-We-Haveto-Learn-49660.
- بوتبينا، دام (٢٠١٨). الشمول المالي في تحقيق البحث: دراسة لوجهات نظر الشمول الداعمة للمؤسسة التجارية الجزائرية، مجلة المحاسبة والدراسات المفاهيمية، الصفحات ١-٢٤.
- بومديان، محمد (٢٠٢٠). آليات بناء الثقة الرقمية في المغرب، مجلة المنارة للدراسات القانونية والإدارية، عدد خاص عن القانون الرقمي، يوليو.٩١-٩٢

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

P-ISSN: 2070-898X E-ISSN: 2707-9775

- تحالف الشمول المالي .(2011) (FIDWG). قياس الشمول المالي: المؤشرات الأساسية للشمول المالي. تمت مراجعة هذا المصدر بتاريخ ٤ أكتوبر ٢٠٢٣ من الرابط التالي : https://www.afiglobal.org/wpcontent/uploads/publications/fidwg_core%20set%20of%20indicators-fr.pdf
- الحكومة الرقمية: البحث والممارسة، ٣(٤)، ١-١٩. 28. حسن، شريف، نغوين هونغ ماي، نور شاياه عبد الوهاب، محمد بن أمين، محمد معروف حسن، جوديت أولاه، ٢٠٢٥، نية تبني منصات التكنولوجيا المالية اللامركزية في بيئة المخاطر السيبرانية لدى جيل زد: منهجية مزدوجة باستخدام نمذجة المعادلات الهيكلية الجزئية (PLS-SEM) وتحليل الشروط الضرورية.https://www.albankaldawli.org/ar/topic/financialinclusion/overview
- الشراكة العالمية للشمول المالي .(2013). (Global PFI) إطلاق مجموعة مؤشرات الشمول المالي الأساسية لمجموعة العشرين. تم الاطلاع عليه بتاريخ ٤ نوفمبر ٢٠٢٣ من موقع الشراكة العالمية للشمول المالي: https://www.gpfi.org/featured/launch-g20-basic-set-financial-inclusion-indicators
- شنبي، سوريا وبن لخضر، سعيد (٢٠١٩). فخر الفخر في تحقيق التنمية، مجلة الفخر في العلوم المالية والمحاسبية، ٤.(1) ١١٠:١٠٩
- عطا الله، سابرينا وبورغبة، كويدر (2025). استخدام التكنولوجيا المالية كآلية لتحديث نظام الاعتمادات المستندية لتطوير التجارة الخارجية الجزائرية.
- عطية، أشرف إبراهيم (2021). تعزيز الشمول المالي بين الثقة والتحديات: عرض تقديمي حول تحقيق الشمول المالي في مصر، الرابطة الدولية للشمول المالي وتعزيزه.
- غو ي. (٢٠٢٢). الثقة الرقمية وإعادة بناء الثقة في المجتمع الرقمي: نموذج متكامل قائم على نظرية الثقة ونظرية تأكيد التوقعات. الحكومة الرقمية: البحث والممارسة، ٣(٤)، ١-١٩.
- كلوترز، ل.، سريفاستافا، م.، وتيل، ل. (2023). أثر الثقة الرقمية على قيمة الشركة وحوكمتها: دراسة تجريبية للشركات الأمريكية. مجلة المجتمع والأعمال، 18(1)، 71-١٠٣.
- كورتي، ف.، جيرلاش، ج.، كازينيك، س.، لي، م. ج.، وميهوف، أ. (٢٠١٩). تعريف وتصنيف المخاطر السيبرانية لإدارة المخاطر المالية. بنك الاحتياطي الفيدرالي في سانت لويس، أغسطس، نسخة غير منشورة.
- كورتي، ف.، جيرلاش، ج.، كازينيك، س.، لي، م. ج.، وميهوف، أ. (٢٠١٩). تعريف وتصنيف المخاطر السيبرانية لإدارة المخاطر المالية. بنك الاحتياطي الفيدرالي في سانت لويس. الصفحات ٣-٢٣.
- كومار، أ.، وتوماس، ر. (٢٠٢٢). إدارة المخاطر السيبرانية في المؤسسات المالية: الآثار التشغيلية واستراتيجيات التخفيف. مجلة إدارة المخاطر المالية، ١١(٣)، ١٠٠-١١٣.
- لاونر، م.، وجيتين، ف.، وباليسكيفيتش، ج. (مارس ٢٠٢٢). الثقة الرقمية في مكان العمل: اختبار أداة جديدة على عينة متعددة الثقافات. في منتدى العلوم الاقتصادية، ١٠(١)، ٣٠-٤٧.
- لجنة بازل للرقابة المصرفية .(2006). (BCBS) التقارب الدولي لقياس رأس المال ومعاييره: بازل ٢. بنك التسويات الدولية. الصفحات ١٠-١٢.
- لجنة بازل للرقابة المصرفية .(2011). (BCBS) المخاطر التشغيلية - مراجعات لإطار عمل بازل ٢. بنك التسويات الدولية. الصفحات ٦-٩.
- لجنة بازل للرقابة المصرفية .(2021). (BCBS) مبادئ المرونة التشغيلية. بنك التسويات الدولية. الصفحات ٦-١٢.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

- ليفين، ل. (٢٠٢٢). الثقة الرقمية والتعاون في ظل عقد اجتماعي رقمي تكاملي. في الأعمال التجارية والآثار الأخلاقية للتكنولوجيا (ص ٨٧-١٠١). تشام: سبرينغر نيتشر سويسرا.
- محمد علي، صلاح الدين سيد (يوليو ٢٠٢٠). الاجتهاد الرياضي وأهميته في التدريب في ضوء التدريب التطبيقي: دراسة حالة عن الاجتهاد الرياضي في مصر، مجلة كلية التربية البدنية، طنطا – مصر ص٢٥١
- المشهداني، بشرى نجم عبد الله وكاظم، عمر علي حسين (٢٠٢٥). التكنولوجيا المالية في ظل تحديات الأمن السيبراني ودورها في القطاع المصرفي.
- المعهد الوطني للمعايير والتكنولوجيا (NIST). ٢٠٢٠. الأمن
- نيس، سعيدة (٢٠٢٢). دور التكنولوجيا المالية في تطوير الخدمات المالية، مجلة البحوث الاقتصادية المتقدمة، ٧(٢). ٢٣٥:٢٣٤
- وكالة الأمن السيبراني للاتحاد الأوروبي. (ENISA). (2023). مشهد التهديدات ٢٠٢٣: مخاطر الأمن السيبراني للخدمات المالية. وكالة الأمن السيبراني للاتحاد الأوروبي.

Sources

- Al-Mashhadani, Bushra Najm Abdullah & Kadhim, Omar Ali Hussein (2025). Financial Technology under Cybersecurity Challenges and Its Role in the Banking Sector.
- Anwar, Iman Ismail (2021). The Role of Financial Inclusion in Enhancing Savings, Journal of Financial Studies.
- Atta Allah, Sabrina & Bouragba, Kouider (2025). Using Financial Technology as a Mechanism to Modernize the Documentary Credit System to Develop Algerian Foreign Trade.
- Attia, Ashraf Ibrahim (2021). Enhancing Financial Inclusion between Trust and Challenges: A Presentation on Achieving Financial Inclusion in Egypt, International Association for Financial Inclusion and Its Promotion.
- Barajas et al A. (2020). Financial Inclusion: What Have We Learned So Far? What Do We Have to Learn? International Monetary Fund. Retrieved 23/06/2023, from https://www.imf.org/en/Publications/WP/Issues/2020/08/07/Financial-Inclusion-What-Have-We-Learned-So-Far-What-Do-We-Haveto-Learn-49660. 1-51
- Basel Committee on Banking Supervision (BCBS). (2006). International convergence of capital measurement and capital standards: Basel II. Bank for International Settlements. pp. 10–12.
- Basel Committee on Banking Supervision (BCBS). (2011). Operational risk – Revisions to the Basel II framework. Bank for International Settlements. pp. 6–9.
- Basel Committee on Banking Supervision (BCBS). (2021). Principles for operational resilience. Bank for International Settlements. pp. 6–12.

- Boumdiane, Mohamed (2020). Mechanisms for Building Digital Trust in Morocco, Al-Manara Journal for Legal and Administrative Studies, Special Issue on Digital Law, July.
- Boutbina, Daam (2018). Financial Inclusion in Achieving Research Financial Inclusion: A Study of Inclusion Views Supporting the Algerian Commercial Enterprise, Journal of Accounting and Conceptual Studies, pp. 1–24.
- Chenbi, Souria & Ben Lakhdar, Said (2019). Pride of Pride in Achieving Development, Journal of Pride in Financial and Accounting Sciences, 04(01).
- Curti, F., Gerlach, J., Kazinnik, S., Lee, M. J., & Mihov, A. (2019). Cyber risk definition and classification for financial risk management. Federal Reserve Bank of St. Louis. pp. 3–23.
- ENISA – European Union Agency for Cybersecurity. (2023). Threat Landscape 2023: Cybersecurity risks for financial services. European Union Agency for Cybersecurity.
- FIDWG. (2011). Mesurer l'Inclusion Financière : Les Indicateurs Fondamentaux de l'Inclusion Financière. Alliance for Financial Inclusion. Consulté le 04 10, 2023 from: https://www.afiglobal.org/wpcontent/uploads/publications/fidwg_core%20set%20of%20indicato rs-fr.pdf. 1-4
- Global PFI. (2013). Launch of the G20 Basic Set of Financial Inclusion Indicators. Retrieved 11/04/2023, from Global Partnership for Financial Inclusion: https://www.gpfi.org/featured/launch-g20- basic-set-financial-inclusion-indicators1-19
- Guo, Y. (2022). Digital trust and the reconstruction of trust in the digital society: An integrated model based on trust theory and expectation confirmation theory. Digital Government: Research and Practice, 3(4), 1 -19 .
- Hassan, Sharif ،Nguyen Hong Mai ،Nor Shaipah Abdul Wahab ، Mohammad Bin Amin ،Md Maruf Hassan ،Judit Oláh, 2025, *Decentralized Fintech Platforms Adoption Intention in Cyber Risk Environment among Gen Z: A Dual-Method Approach Using PLS-SEM and Necessary Condition Analysis*.
https://www.albankaldawli.org/ar/topic/financialinclusion/overview
- Kluiters, L., Srivastava, M., & Tyll, L. (2023). The impact of digital trust on firm value and governance: an empirical investigation of US firms. Society and Business Review, 18(1), 71-103.
- Kumar, R., & Thomas, B. (2022). BRICS in Global Governance: A Gradual but Steady Expansion. Governance and Politics, 1(1), 100-113.

Mustansiriya University
Al-Mustansiriya Journal of Arab and International Studies
2026 Vol .23 No. 93 pp:207-226

الجامعة المستنصرية
مجلة المستنصرية للدراسات العربية والدولية
٢٠٢٦ المجلد: ٢٣ العدد: ٩٣ ص: ٢٠٧- ٢٢٦

P-ISSN: 2070-898X E-ISSN: 2707-9775

- Launer, M., Çetin, F., & Paliszkiewicz, J. (2022, March). Digital trust in the
- workplace: Testing a new instrument on a multicultural sample. In Forum Scientiae Oeconomia, 10(1), 30-47 .
- Levine, L. (2022). Digital trust and cooperation with an integrative digital social contract. In Business and the Ethical Implications of Technology (pp. 87-101). Cham: Springer Nature Switzerland .
- Mohamed Ali, Salah Al-Din Sayed (July, 2020). Sports Diligence and Its Importance in Training in Light of Applied Training: A Case Study of Sports Diligence in Egypt, Journal of the Faculty of Physical Education, Tanta – Egypt.
- Niss, Saida (2022). The Role of Financial Technology in Developing Financial Services, Journal of Advanced Economic Research, 07(02).
- NIST – National Institute of Standards and Technology. (2020). Security and privacy controls for federal information systems and organizations (NIST Special Publication 800-53, Rev. 5). U.S. Department of Commerce.
- OWASP – Open Web Application Security Project. (2021). OWASP Top Ten Web Application Security Risks. Retrieved from https://owasp.org
- Pazarbasioglu et al, C. (2020). DIGITAL FINANCIAL SERVICES. Washington, USA: World Bank Group. Retrieved from https://pubdocs.worldbank.org/en/230281588169110691/DigitalFinancial-Services.pdf,
- Piotrowski, D. (2022). Consumer perceived ethicality of banks in the era of digitalisation: The case of Poland. Economics and Business Review, 8(1), 90-114.
- Saon Raya, S. P., & Miglanic, S., (2019), Use of Blockchain and Aritificial Intelligence to promote financial inclusion in India. TECH MONITOR • Jan-Mar 2019. : 39-43)
- SHARPE, A. (2024). What Is Resilience and How Does It Promote Digital Trust?. ISACA Journal, (3). Sayed, E., & Mansour, K. (2023). Impact of Digital Transformation on Banks' Profitability and Liquidity in Emerging Markets: Evidence from Egypt. IUP Journal of Bank Management, 22(1).
- Welburn, J. W., & Strong, A. M. (2022). Systemic cyber risk and aggregate impacts. Risk Analysis, 42(8) p: 1606-1622,
- World Bank (2022). Financial Inclusion. Retrieved April 4, 2023, from the World Bank: