مقال بحثي

مجلة الجامعة الإماراتية الدولية. العدد (5) . (2026)
Emirates International University Journal Issued.(5) .(2026)

تحليل العوامل الاستراتيجية لتبني التقنيات السيبرانية في ريادة الأعمال باستخدام (ANN): دراسة حالة لشركتي "سام" و"إيكو" ووزارة الثقافة اليمنية

د. خالد أحمد المسوري [1] *، د. محمد ضيف الله القطابري [2]، د. خيرية الرداعي [3]

1. أستاذ مساعد، كلية الحاسوب وتكنولوجيا المعلومات، المعهد الوطني للعلوم الإدارية، صنعاء، الجمهورية اليمنية.
2. أستاذ مشارك، كلية العلوم الإدارية، المعهد الوطني للعلوم الإدارية، صنعاء، الجمهورية اليمنية.
3. أستاذ مساعد، كلية العلوم الإدارية، المعهد الوطني للعلوم الإدارية، صنعاء، الجمهورية اليمنية.

الملخص:

هدفت هذه الدراسة إلى توضيح تأثير تكنولوجيا المعلومات والاتصالات على التحول الذكي للجامعات اليمنية، مع الأخذ في الاعتبار الدور الوسيط لإدارة المعرفة. طريقة البحث مترابطة ومن ناحية الهدف فهي عملية تطبيقية. المجتمع الإحصائي للبحث شمل جميع رؤساء وخبراء الجامعات اليمنية ووصل عدد العينات الاحصائية الي 256 شخص وتم اختيارهم بشكل عشوائي. وأدوات جمع البيانات، تم استخدام الاستبيان القياسي لتكنولوجيا المعلومات والاتصالات واستبيان إدارة المعرفة، ولقياس المكونات المختلفة للذكاء التنظيمي، تم استخدام استبيانات الذكاء الاستراتيجي، والذكاء العاطفي، والذكاء البيئي، والذكاء التنافسي والذكاء التنظيمي والذكاء الهيكلي. ولتحليل البيانات تم استخدام نمذجة المعادلات الهيكلية باستخدام نهج يعتمد على التباين باستخدام برنامج PLS. وكانت نتائج البحث تؤكد أن التأثير الأكبر مرتبطا بالعلاقة بين إدارة المعرفة والتنظيم الذكي. كما كان لتكنولوجيا المعلومات والاتصالات تأثير مرتفع نسبيا على إدارة المعرفة، وكان لتكنولوجيا المعلومات والاتصالات تأثير معتدل على المنظمة الذكية. كما أن تكنولوجيا المعلومات والاتصالات من خلال إدارة المعرفة كان لها أثر إيجابي وكبير على المنظمة الذكية. ومن المستحسن أن يقوم رؤساء الجامعات الحكومية والخاصة في اليمن، بإنشاء بنية تحتية مناسبة لتكنولوجيا المعلومات والاتصالات وتطبيق ناجح لإدارة المعرفة من أجل إذكاء جامعاتهم.

تاريخ الاستلام	2026/ 01 / 01
تاريخ القبول	2026/ 01 / 01
تاريخ النشر	2026/ 07 / 31
الناشر	الجامعة الإماراتية الدولية

ISSN	3104-6142
ISSN (Online)	3104-6150
DOI	10.64059/eiu.v5i5.93
Wikidata	Q137945151
ROR	03j6pc929

طريقة الاقتباس:

المسوري خ. ا.، القطابري م. ض. ا.، & الرداعي خ. (2026). تحليل العوامل الاستراتيجية لتبني التقنيات السيبرانية في ريادة الأعمال باستخدام ANN: دراسة حالة لشركتي "سام" و"إيكو" ووزارة الثقافة اليمنية. مجلة الجامعة الإماراتية الدولية، 5(5). https://doi.org/10.64059/eiu.v5i5.93

المؤلف المسؤول

خالد أحمد المسوري، المعهد الوطني للعلوم الإدارية، صنعاء، اليمن Khalidahmed2009@gmail.com .

كود

9773104615005

الكلمات المفتاحية

الأمن السيبراني، تبني التكنولوجيا، المنظمات الريادية، نمذجة المعادلات الهيكلية، الشبكات العصبية الاصطناعية

Strategic Factors of Cyber Technology Adoption in Entrepreneurship via ANN: Case Study of Sam, Eco, and Yemen's Culture Ministry.

Dr. Khaled Ahmed Al-Maswari* [1], Dr. Mohammed Deifallah Al-Qatabri [2], Dr. Khairiya Al-Radaei [3]

1. *Assistant Professor, Faculty of Computer and Information Technology, National Institute of Administrative Sciences, Sana'a, Republic of Yemen.*
2. *Associate Professor, Faculty of Administrative Sciences, National Institute of Administrative Sciences, Sana'a, Republic of Yemen.*
3. *Assistant Professor, Faculty of Administrative Sciences, National Institute of Administrative Sciences, Sana'a, Republic of Yemen.*

Abstract

This study aimed to clarify the impact of Information and Communication Technology (ICT) on the smart transformation of Yemeni universities, considering the mediating role of knowledge management. The research method is correlational, and in terms of purpose, it is an applied study. The statistical population of the research included all presidents and experts of Yemeni universities, and the statistical sample consisted of 256 individuals selected randomly. For data collection tools, a standard ICT questionnaire and a knowledge management questionnaire were used. To measure the various components of organizational intelligence, questionnaires for strategic intelligence, emotional intelligence, environmental intelligence, competitive intelligence, organizational intelligence, and structural intelligence were utilized. For data analysis, Structural Equation Modeling (SEM) utilizing a variance-based approach via PLS software was employed. The research results confirmed that the greatest impact was related to the relationship between knowledge management and the smart organization. Furthermore, ICT had a relatively high impact on knowledge management, and a moderate impact on the smart organization. Moreover, ICT, through knowledge management, had a positive and significant impact on the smart organization. It is recommended that presidents of public and private universities in Yemen establish suitable ICT infrastructure and successfully implement knowledge management in order to make their universities smart.

EMIRATES INTERNATIONAL UNIVERSITY

Keywords

Cybersecurity, Technology adoption, Entrepreneurial organizations, Structural Equation Modeling, Artificial Neural Networks.

المقدمة

يعد اعتماد تقنيات الأمن السيبراني الجديدة أمرًا ذا أهمية كبيرة في المنظمات الريادية. يُظهر تقرير الأمن السيبراني لعام 2022 لشركة ماكينزي أن عدد الهجمات السيبرانية على مستوى العالم قد ارتفع بمعدل 32 % سنويًا. كما يشير تقرير مركز أبحاث الأمن السيبراني لعام 2023 إلى أن 78 % من المنظمات الصغيرة والمتوسطة الحجم معرضة لهجمات برامج الفدية. ومن ناحية أخرى، أظهرت دراسة أجرتها جامعة هارفارد في عام 2021 أن 87 % من العملاء يفقدون الثقة في الشركة في حالة حدوث خرق للأمن السيبراني. بالإضافة إلى ذلك، يشير تقرير صادر عن شركة الأبحاث جارتنر في عام 2023 إلى أن 92 % من العملاء يعتبرون الأمن السيبراني مهما عند اختيار الخدمات الرقمية. أيضًا، وفقًا للوائح حماية البيانات العامة للاتحاد الأوروبي لعام 2020، يتعين على المنظمات الامتثال لمعايير الأمان (الاتحاد الأوروبي، 2020). كما يُظهر تقرير المركز الوطني للأمن السيبراني في المملكة المتحدة في عام 2024 أن 85 ٪ من المنظمات الريادية مطالبة بتنفيذ برامج الأمن السيبراني. ووفقًا أيضًا لتقرير مركز تحليل بيانات الأمان في عام 2023 ، فإن 63 ٪ من المنظمات الريادية تعتبر بيانات العملاء أصلًا استراتيجيًا. كما يُظهر مسح المعهد الوطني الأمريكي للمعايير والتكنولوجيا في عام 2022 أن 92 ٪ من الشركات الريادية تسعى إلى حماية بياناتها المهمة. بشكل عام، ونظرًا لزيادة التهديدات السيبرانية والمتطلبات القانونية والحاجة إلى حماية سمعة المنظمات الريادية وبياناتها المهمة، فإن اعتماد تقنيات الأمن السيبراني الجديدة له أهمية كبيرة لهذه المنظمات (Badami et al., 2022).

وفيما يتعلق بأهمية اعتماد تقنيات الأمن السيبراني الجديدة في المنظمات الريادية في اليمن، تظهر المعلومات والتقارير الأخيرة إن هذه القضية أصبحت ذات أولوية عالية في السنوات الأخيرة. وفقًا لتقرير المركز الوطني للفضاء الإلكتروني في اليمن لعام 2023 فقد ارتفع معدل الهجمات الإلكترونية على المؤسسات الصغيرة والمتوسطة الحجم في اليمن بأكثر من 25 ٪ وهذا يدل على ضرورة أن تولي هذه المؤسسات اهتمامًا جادًا لقضية الأمن السيبراني. كما تشير نتائج استطلاع أجراه معهد الاتصالات وتكنولوجيا المعلومات في عام 2022 إلى أن 83 ٪ من العملاء اليمنيين يفقدون ثقتهم في الشركة في حالة حدوث خرق أمني. بالإضافة إلى ذلك، ووفقًا لقانون حماية حقوق المستخدمين في الفضاء الإلكتروني المعتمد في(2021)، يتعين على جميع المؤسسات النشطة في مجال الخدمات الرقمية الامتثال لمعايير الأمن السيبراني. كما يوضح تقرير حديث صادر عن وزارة الاتصالات وتكنولوجيا المعلومات اليمنية في (2023) أن 60 ٪ من المؤسسات الريادية في اليمن تنفذ برامج شاملة للأمن السيبراني. من ناحية أخرى، تشير الاستطلاعات التي أجراها مركز تطوير التقنيات الجديدة في عام (2023) إلى أن 52 ٪ من المؤسسات الريادية اليمنية تعتبر بيانات العملاء أصلًا استراتيجيًا وتسعى إلى حمايتها قدر الإمكان. أكثر من هذه الأصول. إجمالاً، ونظرًا لتزايد التهديدات السيبرانية، والمتطلبات القانونية، والحاجة إلى حماية سمعة وبيانات المؤسسات الريادية في اليمن، فإن تبني تقنيات الأمن السيبراني الجديدة يُمثل أولوية قصوى لهذه المؤسسات، ويتطلب منها إيلاء هذه القضية اهتمامًا جادًا (Tarhini et al., 2015; Karimi et al., 2023) .

ونظراً لأهمية اعتماد تقنيات الأمن السيبراني الجديدة في المنظمات الريادية، فإن تحديد العوامل المؤثرة على هذا التبني يعد أمراً ضرورياً وحيوياً. وتشير المعلومات والتقارير الحديثة في هذا المجال أيضًا إلى ضرورة إيلاء هذه القضية اهتمامًا خاصًا. وبحسب تقرير صادر عن المركز الوطني للتكنولوجيات الجديدة في عام 2023 ، فإن العوامل التقنية والتنظيمية والبيئية تعد من بين أهم العوامل المؤثرة على اعتماد تقنيات الأمن السيبراني بين المنظمات الريادية. وأظهرت دراسات تم إجرائها في اليمن عام 2022 و2023 أيضًا أن هذه الفئات الثلاث من العوامل تؤثر بشكل مباشر وغير مباشر على قبول واستخدام هذه التقنيات. وفي مجال العوامل التقنية، تشير الأبحاث التي نشرت في المجلة العلمية لجامعة صنعاء عام 2023 إلى أن القدرات التقنية لتقنيات الأمن السيبراني، وتوافقها مع البنية التحتية الموجودة، وسهولة استخدام هذه التقنيات تلعب دوراً فعالاً في قبولها من قبل المنظمات الريادية. وفي مجال العوامل التنظيمية، تشير الدراسة التي أجراها مركز أبحاث تكنولوجيا المعلومات عام 2023 إلى أن المتغيرات مثل دعم الإدارة العليا، ووجود الموارد والقدرات الكافية، والثقافة التنظيمية المناسبة، تعد من أهم العوامل المؤثرة في هذا المجال. وأخيرًا، فيما يتعلق بالعوامل البيئية، يشير تقرير مركز تطوير الأعمال الرقمية لعام 2024 إلى أن الضغوط التنافسية، والمتطلبات القانونية والتنظيمية، بالإضافة إلى مستوى وعي المستخدمين النهائيين وتثقيفهم، من بين العوامل البيئية المؤثرة على تبني تقنيات الأمن السيبراني (Al-shaibany, 2023). لذلك، ونظرًا لاتساع وتعقيد العوامل المؤثرة على تبني تقنيات الأمن السيبراني في المؤسسات الريادية، فإن تحديد هذه العوامل وتحليلها أمر بالغ الأهمية، ويمكن أن يساعد في فهم هذه الظاهرة بشكل أفضل، وتقديم حلول مناسبة لزيادة تبني هذه التقنيات.

وبحسب تقرير صادر عن مركز أبحاث الأمن السيبراني عام 2023 ، فإنه على الرغم من زيادة التهديدات السيبرانية، فإن العديد من المنظمات الريادية في اليمن لا تزال تفتقر إلى التدابير الأمنية الأساسية. تظهر نتائج هذا التقرير أن 10 ٪ فقط من هذه المنظمات تستخدم حلول الأمن السيبراني المتقدمة مثل تحليل سلوك المستخدم واكتشاف التهديدات (Al-shaibany, 2023)، كما يشير مسح جامعة العلوم والتكنولوجيا في عام 2022 إلى أن التحديات الرئيسة التي تواجه اعتماد تقنيات الأمن السيبراني بين المنظمات الريادية تشمل نقص الموارد المالية والبشرية، ونقص وعي كبار المديرين، وتعقيد تنفيذ هذه التقنيات. كما يوضح تقرير المركز الوطني للتكنولوجيات الجديدة في عام 2023 أن بعض المنظمات الريادية تمتنع عن مشاركة بياناتها المهمة مع مزودي تكنولوجيا الأمن بسبب مخاوف تتعلق بالأمن والخصوصية. وهذا يؤثر بشكل كبير على اعتماد هذه التقنيات واستخدامها. كما تشير نتائج أبحاث وزارة الاتصالات وتكنولوجيا المعلومات في عام 2024 إلى أن بعض المنظمات الريادية تمتنع عن استخدام الحلول المتقدمة في هذا المجال بسبب نقص المهارات التقنية والتخصصية الكافية في مجال الأمن السيبراني (Abohatem et al., 2024). بشكل عام،

وعلى الرغم من أهمية وعلى الرغم من الأهمية المتزايدة للأمن السيبراني، لا تزال العديد من المنظمات الريادية تواجه تحديات مختلفة، بما في ذلك القيود المالية والبشرية، والمخاوف الأمنية، ونقص المهارات التقنية في تبني ونشر تقنيات الأمن السيبراني.

فيما يتعلق بدور العوامل التقنية والتنظيمية والبيئية في اعتماد تقنيات الأمن السيبراني في المنظمات الريادية، يظهر استعراض المصادر الخارجية الجديدة ما يلي: تشير العوامل التقنية إلى الخصائص والقدرات التقنية لتقنيات الأمن السيبراني. وفقًا لدراسة أجرتها جامعة كاليفورنيا في بيركلي عام 2023 ، فإن قضايا مثل توافق التكنولوجيا مع البنية التحتية للمنظمة، والقدرات الأمنية المتقدمة، وسهولة استخدام هذه التقنيات من بين العوامل التقنية التي يمكن أن تؤثر على تبنيها في المنظمات الريادية. العوامل التنظيمية هي الخصائص التنظيمية والإدارية التي تؤثر على اعتماد تقنيات الأمن السيبراني. وتشير دراسة أجرتها جامعة أكسفورد عام 2022 إلى أن الدعم من جانب كبار المديرين، وتوافر الموارد المالية والبشرية الكافية، والثقافة التنظيمية المناسبة، من بين العوامل التنظيمية الفعالة في هذا الصدد. تشير العوامل البيئية إلى خصائص البيئة الخارجية للمنظمة التي تؤثر على اعتماد تقنيات الأمن السيبراني. الأبحاث التي أجرتها جامعة كامبريدج عام 2024 إلى أن الضغوط التنافسية والمتطلبات القانونية والتنظيمية، بالإضافة إلى وعي المستخدم النهائي واستعداده، من بين العوامل البيئية التي يمكن أن تؤثر على تبني هذه التقنيات في المنظمات الريادية (Karimi et al., 2023). باختصار، تُظهر مراجعة المصادر الخارجية الجديدة أن العوامل التقنية (مثل التوافق والقدرات التكنولوجية)، والتنظيمية (مثل دعم الإدارة والموارد المتاحة)، والبيئية (مثل الضغوط التنافسية والمتطلبات القانونية) تؤثر بشكل مباشر وغير مباشر على تبني تقنيات الأمن السيبراني في المنظمات الريادية، وأن تحديد هذه العوامل وإدارتها أمر ذو أهمية كبيرة.

تشير العوامل التقنية إلى الميزات والقدرات التقنية لتقنيات الأمن السيبراني. وفقًا لدراسة أجرتها جامعة كاليفورنيا في بيركلي عام 2023 ، فإن قضايا مثل توافق التكنولوجيا مع البنية التحتية للمنظمة، والقدرات الأمنية المتقدمة، وسهولة استخدام هذه التقنيات من بين العوامل التقنية التي يمكن أن تؤثر على تبنيها في المنظمات الريادية. العوامل التنظيمية هي الخصائص التنظيمية والإدارية التي تؤثر على اعتماد تقنيات الأمن السيبراني. وتشير دراسة أجرتها جامعة أكسفورد عام 2022 إلى أن الدعم من جانب كبار المديرين، وتوافر الموارد المالية والبشرية الكافية، والثقافة التنظيمية المناسبة، من بين العوامل التنظيمية الفعالة في هذا الصدد. وتشير العوامل البيئية إلى خصائص البيئة الخارجية للمنظمة التي تؤثر على اعتماد تقنيات الأمن السيبراني. تشير الأبحاث التي أجرتها جامعة كامبريدج في عام 2024 إلى أن الضغوط التنافسية والمتطلبات القانونية والتنظيمية، فضلاً عن وعي المستخدم النهائي واستعداده، من بين العوامل البيئية التي يمكن أن تؤثر على تبني هذه التقنيات في المنظمات الريادية (Badami et al., 2022). باختصار، تُظهر مراجعة المصادر الخارجية الجديدة أن العوامل التقنية (مثل التوافق والقدرات التكنولوجية)، والتنظيمية (مثل دعم الإدارة والموارد المتاحة)، والبيئية (مثل الضغوط التنافسية والمتطلبات القانونية) تؤثر بشكل مباشر وغير مباشر على تبني تقنيات الأمن السيبراني في المنظمات الريادية، وأن تحديد هذه العوامل وإدارتها له أهمية كبيرة.

الهدف الرئيسي من البحث يتكون من جزئين. أولاً، تحديد وتحليل العوامل التقنية والتنظيمية والبيئية التي تؤثر على تبني تقنيات الأمن السيبراني بين المنظمات الريادية. وفقًا لبحث حديث أجرته جامعة سيدني للتكنولوجيا (2023)، يُعدّ تحديد العوامل المؤثرة الرئيسية وفحصها أمرًا بالغ الأهمية لتطوير استراتيجيات فعّالة واتخاذ قرارات مدروسة للمنظمات الريادية في مجال الأمن السيبراني. الهدف الثاني، يهدف البحث إلى تقديم نموذج مفاهيمي لشرح العلاقة بين هذه العوامل وتبني تقنيات الأمن السيبراني. أكدت دراسة أجرتها جامعة سنغافورة الوطنية (2022) على الحاجة إلى إطار مفاهيمي شامل لفهم التفاعل المعقد بين مختلف العوامل وتأثيرها على تبني حلول الأمن السيبراني الناشئة في بيئة ريادة الأعمال. ومن خلال تحقيق هذه الأهداف، يوفر هذا البحث فهمًا أعمق للمقدمات الأساسية لتبني تقنيات الأمن السيبراني، ويضع إطارًا نظريًا لتوجيه المؤسسات الريادية في جهودها لتحسين وضع الأمن السيبراني وحماية أصولها القيّمة.

وتتلخص فرضيات الدراسة الرئيسية فيما يلي:

1. إن العوامل التقنية (مثل توافق التكنولوجيا، والقدرات الأمنية، وسهولة الاستخدام) لها تأثير إيجابي وهام على اعتماد تقنيات الأمن السيبراني في المنظمات الريادية.
2. إن العوامل التنظيمية (مثل دعم الإدارة العليا والموارد الكافية والثقافة التنظيمية) لها تأثير إيجابي وهام على تبني تقنيات الأمن السيبراني في المنظمات الريادية.
3. تؤثر العوامل البيئية (مثل الضغوط التنافسية والمتطلبات القانونية واستعداد المستخدم) بشكل إيجابي وهام على تبني تقنيات الأمن السيبراني في المنظمات الريادية.

طريقة البحث

يُعد هذا البحث كميًا وأجري باستخدام أسلوب المسح. ويتكون المجتمع الإحصائي في هذه الدراسة من الخبراء والمتخصصين والمدراء المتخصصين في تكنولوجيا المعلومات والاتصالات ممن لديهم خبرة في مجال ريادة الأعمال في مجال تكنولوجيا المعلومات والاتصالات، وعددهم 251 شخصاً. وقد تم اختيار 152 شخصا من خلال العينة العشوائية باستخدام صيغة كوكران على النحو التالي.

$$n = \frac{\frac{z^2 pq}{d^2}}{1 + \frac{1}{N}\left(\frac{z^2 pq}{d^2} - 1\right)}$$

$$n = \frac{\frac{(1.96)^2 \times (0.5) \times (0.5)}{(0.05)^2}}{1 + \frac{1}{251} \times \left(\frac{(1.96)^2 \times (0.5) \times (0.5)}{(0.05)^2} - 1\right)} = 152$$

وقد تم اختيار هؤلاء الأفراد باستخدام أسلوب العينة العشوائية ذات العناصر الخاصة، استناداً إلى تعليمهم وخبراتهم الوظيفية ذات الصلة، فضلاً عن الخبرة المطلوبة في المجالات المحددة. العينة المبنية على الحالة هي طريقة يتم فيها اختيار العينات لأنها ذات أهمية استثنائية وتقع في مركز الموضوع قيد الدراسة. تم استخدام الاستبيان لجمع البيانات. تم تقديم الاستبيانات المصممة للخبراء للتعبير عن مستوى موافقتهم أو عدم موافقتهم على العناصر المحددة باستخدام مقياس ليكرت. ولتحقيق هذه الغاية، تم إرسال الاستبيانات إلى العينات المطلوبة. وقد تم استلام 139 استبيان مجاب عليه، وبعد مراجعة واستبعاد عدد من الاستبيانات بسبب عدم اكتمال المعلومات، تم استخدام 134 استبيان كأساس للتحليل.

لقياس كلّ من مكونات النموذج، قدر الإمكان، بُذلت محاولات لاستخدام مقاييس مُصممة في أبحاث سابقة حول العالم. ومع ذلك، أُجريت تعديلات على تصميم أسئلة الاستبيان بناءً على بيئة الشركات الريادية اليمنية وتجارب الباحثين السابقة. صُممت مكونات الاستبيان في ثلاثة أقسام: التكنولوجيا، والتنظيم، والبيئة، على النحو التالي. المتغير التابع لهذه الدراسة هو معدل تبني تقنيات الأمن السيبراني الجديدة في المؤسسات الريادية. نظراً لعدم وجود تعريف شامل وعوائق واضحة لتقنيات الأمن السيبراني الجديدة، والتي تشمل مجموعة واسعة من تقنيات الأمن السيبراني للبرمجيات والأجهزة، فقد استُخدمت مقاييس مختلفة في دراسات سابقة لقياس مدى قبول هذه التقنيات في المؤسسات الريادية. ولشرح هذا المفهوم، قام الباحثون في هذه الدراسة بقياس مدى قبول تقنيات الأمن السيبراني الجديدة بناءً على قائمة بأهم تقنيات المعلومات المستخدمة في مجال الأمن السيبراني في المؤسسات الريادية، والتي تشمل أنظمة معالجة المعاملات، والشبكة الداخلية للشركات، وأنظمة أتمتة المكاتب، وأنظمة الإدارة المتكاملة (أنظمة تخطيط موارد المؤسسات، وبوابات الإنترنت، والتجارة الإلكترونية، وأنظمة علاقات العملاء، وأنظمة إدارة سلسلة التوريد، وأنظمة إدارة المعرفة). وتتميز هذه القائمة المختارة من التقنيات، أولاً، بكونها عامة ويمكن استخدامها في جميع المؤسسات، وثانياً، بسجلها الحافل، وهي أمثلة واضحة على تطبيق تكنولوجيا معلومات الأمن السيبراني في المؤسسات.

تم قياس تصورات المديرين لفوائد تكنولوجيا المعلومات في مجال الأمن السيبراني باستخدام ثلاثة معايير تقنية وتنظيمية وبيئية مستمدة من أبحاث سابقة. لكل معيار، صُمم سؤال، وطُرحت الإجابة على مقياس ليكرت خماسي النقاط، حيث يشير الرقم 5 إلى موافقة المجيب التامة، بينما يشير الرقم 1 إلى عدم موافقته التامة.

جدول 1 :مؤشرات قياس العوامل المؤثرة في اعتماد تقنيات الأمن السيبراني الجديدة وخصائص صحتها وموثوقيتها

العوامل	المؤشرات	المصدر	معامل الفاي كرونباخ
العوامل الفنية	1 . التوافق التكنولوجي مع البنية التحتية للمنظمة 2 . القدرات الأمنية المتقدمة 3 . سهولة استخدام التكنولوجيا	جامعة كاليفورنيا (2023)	0.87
العوامل التنظيمية	1 . الدعم والتأييد من كبار المديرين 2 . توافر الموارد المالية والبشرية الكافية 3 . وجود ثقافة تنظيمية مناسبة	جامعة أكسفورد (2022)	0.83
العوامل البيئية والمحيطية	1. الضغط التنافسي 2. المتطلبات القانونية والتنظيمية 3.جاهزية المستخدم النهائي ووعيه.	جامعة كامبريدج (2024)	0.84

في هذه الدراسة، تم فحص ثلاث فئات رئيسية من العوامل التي تؤثر على اعتماد تقنيات الأمن السيبراني الجديدة في المنظمات الريادية: العوامل التقنية: تشير هذه الفئة من العوامل إلى الميزات والقدرات التقنية لتقنيات الأمن السيبراني. وبناء على الدراسات السابقة، فإن المؤشرات الرئيسية الثلاثة في هذا المجال تشمل توافق التكنولوجيا مع البنية التحتية للمنظمة، والقدرات الأمنية المتقدمة، وسهولة استخدام هذه التقنيات. هذه العوامل مُستقاة من أبحاث أُجريت في مجال تبني التكنولوجيا في البيئات الريادية في جامعة كاليفورنيا في عام 2023. العوامل التنظيمية: تُشير هذه المجموعة من العوامل إلى الخصائص التنظيمية والإدارية التي تؤثر على تبني تقنيات الأمن السيبراني. وقد طرحت الدراسات السابقة ثلاثة عوامل رئيسية في هذا المجال: الدعم والتأييد من كبار المديرين، وتوافر الموارد المالية والبشرية الكافية، ووجود ثقافة تنظيمية مناسبة. وتُستمد هذه العوامل من الأدبيات المتوفرة في مجال تبني التكنولوجيا في البيئات التنظيمية في جامعة أكسفورد في عام 2022. العوامل البيئية: تشير هذه الفئة من العوامل إلى خصائص البيئة الخارجية للمنظمة التي تؤثر على اعتماد تقنيات الأمن السيبراني. واستنادًا إلى الدراسات السابقة، تشمل العوامل الرئيسة الثلاثة في هذا المجال الضغط التنافسي والمتطلبات القانونية والتنظيمية ومستوى الاستعداد والوعي لدى المستخدمين النهائيين. وقد تم استخراج هذه العوامل من الأبحاث التي أجريت في مجال اعتماد التكنولوجيا في بيئات الأعمال في جامعة كامبريدج في عام 2024. ولتحليل بيانات هذه الدراسة، تم إجراء إحصاءات وصفية أولاً، وحساب المتوسط والوسيط والانحراف المعياري لفحص توزيع المتغيرات. كما تم استخدام الاختبارات الإحصائية مثل اختبار T . وأخيرًا، تم استخدام نمذجة المعادلات الهيكلية (SEM) لتقديم نموذج مفاهيمي وفحص العلاقات السببية بين المتغيرات. ويمكن استخدام برامج SPSS وPLS-SEM الإحصائية لإجراء هذه التحليلات.

النتائج

فيما يتعلق بالخصائص الديموغرافية لعينة الدراسة البالغة 134 شخصاً، يمكن القول: من حيث العمر، فإن أعلى تكرار يتعلق بالأشخاص في الفئة العمرية من 36 إلى 45 عاماً بنسبة 43.3 %. وبعد ذلك، وصلت النسبة إلى 31.3 % لدى الأشخاص الذين تتراوح أعمارهم بين 25 و 35 عاماً. ويشكل الأشخاص الذين تتراوح أعمارهم بين 46 إلى 55 عامًا نسبة 20.9%، ويشكل الأشخاص الذين تبلغ أعمارهم 54 عامًا فأكثر نسبة 4.5 % من العينة. ومن حيث الجنس فإن أغلبية العينة من الذكور بنسبة 73.1 % ومن الإناث بنسبة 26.9 %. وفيما يتعلق بالمستوى التعليمي، فإن أعلى نسبة هي بين الأشخاص الحاصلين على درجة الماجستير، بنسبة 47.8 %. وتشكل درجة البكالوريوس 38.8 % وتشكل درجة الدكتوراه 13.4 %. من حيث الخبرة العملية، فإن أكبر مجموعة هي الأشخاص الذين تتراوح أعمارهم بين 11 و 15 عامًا (43.3 ٪). تشمل الخبرة من 5 إلى 10 عامًا 34.3 ٪، ومن 16 إلى 20 عامًا 16.4 ٪، وأكثر من 20 عامًا من الخبرة 6 ٪. فيما يتعلق بالمنصب/الوظيفة، يشكل المتخصصين أكبر مجموعة بنسبة 47.8 ٪. يليهم الخبراء بنسبة 35.8 ٪ والمديرون بنسبة 16.4 ٪. ومن حيث نوع المنظمة، يعمل غالبية الأشخاص (65.7 ٪) في شركات خاصة و 34.3 ٪ في مؤسسات حكومية. وأخيرًا، من حيث الموقع الجغرافي، يعيش 61.2 ٪ من أفراد العينة في العاصمة صنعاء و 38.8 ٪ في مدن أخرى.

جدول 2 : أمارا كولمجروف سميرنوف

العامل	كولموغوروف ـ سميرنوف	قيمة P	المتوسط	الانحراف المعياري
ريادة الأعمال	0.083	0.013	4.12	0.98
المهارات التقنية	0.092	0.003	4.35	0.78
الابتكار	0.086	0.008	4.19	0.83
المخاطرة	0.081	0.017	3.91	0.92
الاستقلالية	0.090	0.004	4.07	0.84
الدافع الداخلي	0.093	0.003	4.29	0.75
الدعم التنظيمي	0.074	0.038	3.84	0.91
الوصول إلى الموارد	0.081	0.016	3.98	0.87

اختبار كولموغوروف - سميرنوف (K-S) للتحقق من التوزيع الطبيعي للمتغيرات. وفي اختبار (K-S) ، كانت القيم الاحتمالية لـ p-value لجميع المتغيرات أقل من 0.05. يشير هذا إلى انحراف توزيع المتغيرات عن التوزيع الطبيعي. وفي اختبار S-W، كانت القيم الاحتمالية لجميع المتغيرات أقل من 0.05. يؤكد هذا رفض افتراض التوزيع الطبيعي لهذه المتغيرات. وبالتالي، ووفقًا للنتائج وباستخدام هذا الاختبار، يمكن القول بأن أيًا من المتغيرات الرئيسية في هذه الدراسة لا يتبع التوزيع الطبيعي. وينبغي أن يؤخذ هذا في الاعتبار عند اختيار الأساليب الإحصائية المناسبة للتحليل اللاحق.

جدول 3 : نتائج اختبار t لعينة واحدة لمتغيرات البحث

العامل	المتوسط	الانحراف المعياري	قيمةt	درجة الحرية	قيمةp
ريادة الأعمال	4.12	0.89	13.27	133	0.000
المهارات التقنية	4.35	0.78	17.87	133	0.000
ابتكار	4.19	0.83	14.65	133	0.000
المخاطرة	3.91	0.92	10.19	133	0.000
الاستقلالية	4.07	0.84	13.12	133	0.000
الدافع الداخلي	4.29	0.75	17.38	133	0.000
الدعم التنظيمي	3.84	0.91	9.62	133	0.000
الوصول إلى الموارد	3.98	0.87	11.52	133	0.000

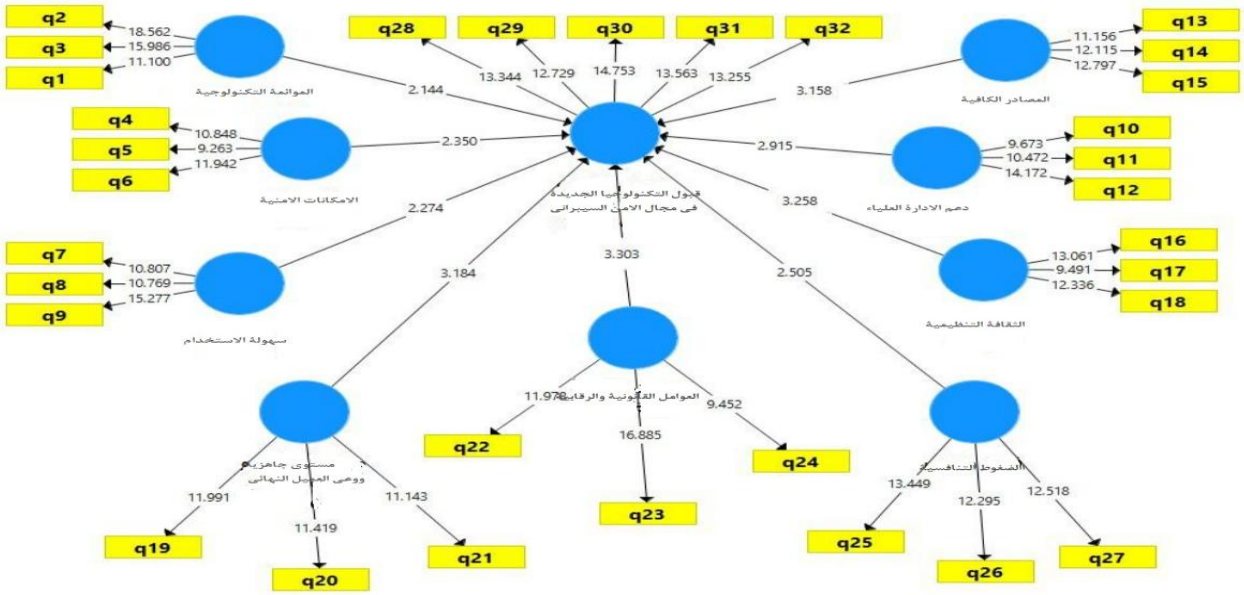
نتائج اختبار (T) لعينة واحدة على المتغيرات الرئيسة لهذه الدراسة إلى الوضع المطلوب لهذه المتغيرات في العينة قيد الدراسة. وفي مجال ريادة الأعمال، فإن متوسط الدرجة 4.12 أعلى بشكل ملحوظ من الحد المتوسط 4 وهذا يدل على أن مستوى ريادة الأعمال في المجتمع المدروس مرتفع نسبيا. كما أن المتغيرات المتعلقة بريادة الأعمال هي الأخرى في حالة إيجابية. المهارات التقنية بمتوسط 4.35 ، والابتكار بمتوسط 4.19، والمخاطرة بمتوسط 3.91، والاستقلالية بمتوسط 4.07 أعلى بشكل ملحوظ من المتوسط 4 . وهذا يعني أن الأشخاص في المجتمع الإحصائي يتمتعون بمستوى مرتفع من هذه الخصائص. كما أن العوامل التحفيزية والبيئية في حالة مواتية أيضًا. الدافع الداخلي بمتوسط 4.29، والدعم التنظيمي بمتوسط 3.84، والوصول إلى الموارد بمتوسط 3.98 أعلى بشكل ملحوظ من المتوسط 4 . وهذا يدل على أن هذه العوامل موجودة أيضًا بمستوى مقبول في المجتمع المدروس. وبشكل عام، تظهر نتائج اختبار T أن جميع المتغيرات المتعلقة بريادة الأعمال في مجال تكنولوجيا المعلومات تأتي بمستوى مرتفع، وهذا من شأنه أن يساهم في نجاح وتقدم ريادة الأعمال في هذا المجال .

جدول 4 : تقييم صحة وموثوقية وملاءمة نموذج المعادلة الهيكلية

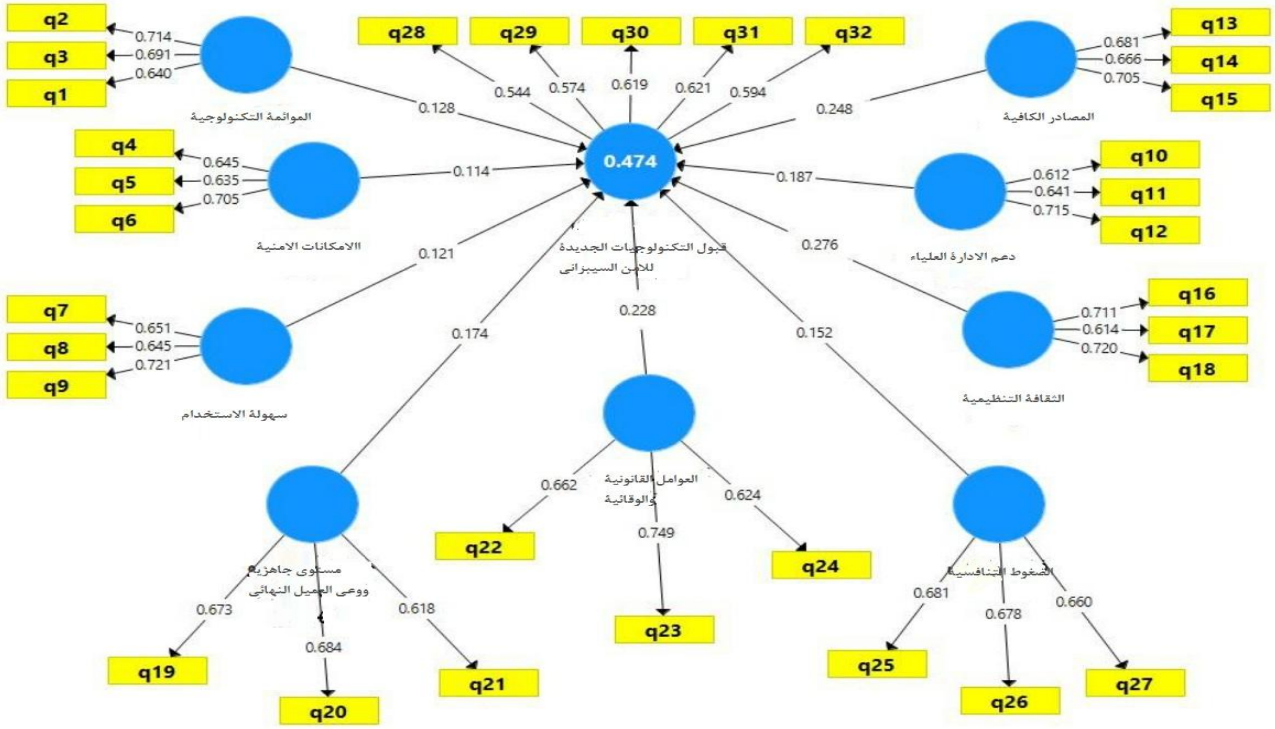
المعايير	كرونباخ ألفا	مركب المصداقية	متوسط التباين المستخرجAVE	مربع R
ريادة الأعمال	**0.88**	**0.92**	**0.71**	**0.47**
المهارات التقنية	**0.84**	**0.89**	**0.67**	-
ابتكار	**0.86**	**0.90**	**0.69**	-
المخاطرة	**0.82**	**0.87**	**0.63**	-
حركة الاستقلالية	**0.85**	**0.90**	**0.68**	-
الدافع الداخلي	**0.87**	**0.91**	**0.72**	-
الدعم التنظيمي	**0.83**	**0.88**	**0.65**	-
الوصول إلى الموارد	**0.84**	**0.89**	**0.66**	-

الجدول رقم 4 نتائج تقييم صحة وموثوقية وملاءمة نموذج المعادلة الهيكلية في هذه الدراسة. ومن حيث الموثوقية الداخلية فإن جميع المتغيرات لها قيم ألفا كرونباخ أعلى من 0.7 مما يدل على أنها تتمتع بموثوقية داخلية جيدة. كما أن الموثوقية المركبة لجميع المتغيرات أعلى من 0.7 ، مما يدل على اتساق داخلي جيد للمتغيرات. ومن حيث الصلاحية المتقاربة، فإن قيم متوسط التباين المستخرج (AVE) لجميع المتغيرات أعلى من 0.5.

وهذا يعني أن كل معيار أكثر من 50 ٪ فإن تباين مؤشراته صلاحيته متقاربة جيدا. ومن منظور ملاءمة النموذج الهيكلي، فإن معامل التحديد (R - Square) لمتغير ريادة الأعمال هو 0.47. وهذا يعني أن 47 ٪ من تباين ريادة الأعمال يفسره المتغيرات المستقلة في النموذج.



شكل 1 : نموذج المعادلة الهيكلية، إحصاءات t



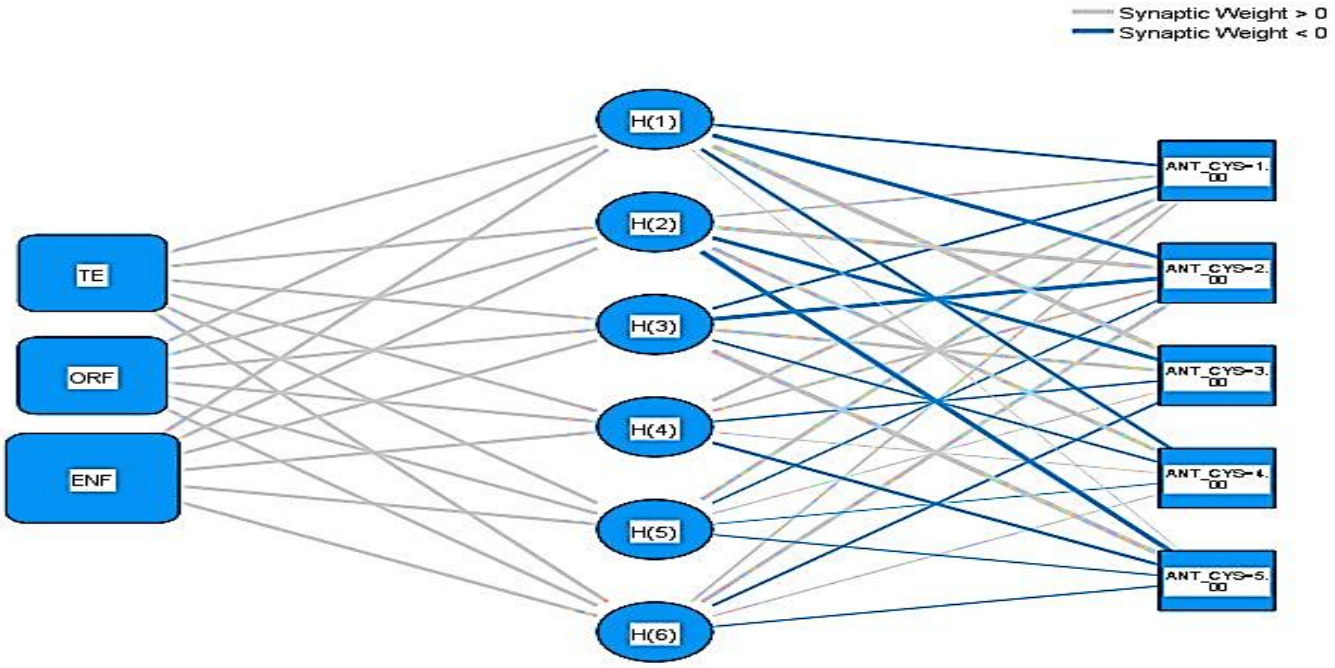
شكل 2 : نموذج المعادلة الهيكلية القياسية

جدول 5 : معاملات المسار وأهمية العوامل المؤثرة في تبني تقنيات الأمن السيبراني الجديدة

	معاملات المسار	الانحراف المعياري STDEV	إحصائية t	سطح ذات معنى قيمة احتمالية p-value
المتطلبات القانونية والتنظيمية - > اعتماد تقنيات الأمن السيبراني الجديدة	0.228	0.058	3.303	0.032
دعم الإدارة العليا - > اعتماد تقنيات الأمن السيبراني الجديدة	0.187	0.056	3.319	0.001
التكيف مع التكنولوجيا - > اعتماد تقنيات الأمن السيبراني الجديدة	0.128	0.061	2.104	0.037
سهولة الاستخدام - > اعتماد تقنيات الأمن السيبراني الجديدة	0.121	0.059	2.064	0.004
الثقافة التنظيمية - > اعتماد تقنيات الأمن السيبراني الجديدة	0.276	0.054	3.258	0.033
الضغط التنافسي - > اعتماد تقنيات الأمن السيبراني الجديدة	0.152	0.06	2.546	0.012
القدرات الأمنية - > اعتماد تقنيات الأمن السيبراني الجديدة	0.114	0.048	2.357	0.019
الموارد الكافية - > اعتماد تقنيات الأمن السيبراني الجديدة	0.249	0.055	3.78	0.001
جاهزية المستخدم النهائي ووعيه - > قبول تقنيات الأمن السيبراني الجديدة	0.174	0.057	3.021	0.003

النتائج الواردة في الجدول 5 أن هناك العديد من العوامل التي تؤثر على اعتماد تقنيات الأمن السيبراني الجديدة. تؤثر المتطلبات القانونية والتنظيمية، بمعامل مسار 0.228 وقيمة احتمالية 0.032، بشكل إيجابي وهام على تبني تقنيات الأمن السيبراني. وهذا يشير إلى أن وجود أطر قانونية وتنظيمية مناسبة يمكن أن يُسهم في تبني هذه التقنيات. كما أن دعم الإدارة العليا له تأثير إيجابي ومهم على القبول بمعامل مسار 0.187 وقيمة احتمالية 0.001 وهذا يعني أن الدعم والمشاركة من جانب الإدارة العليا أمر بالغ الأهمية لنشر تقنيات الأمن السيبراني. التوافق التكنولوجي (معامل 0.128، قيمة احتمالية 0.037) وسهولة الاستخدام (معامل 0.121 ، قيمة احتمالية 0.004) لهما أيضًا تأثير إيجابي وهام على التبني. وهذا يوضح أن ملاءمة التكنولوجيا لاحتياجات وعمليات المنظمة بالإضافة إلى سهولة استخدامها للمستخدمين من بين العوامل الرئيسة في هذا الصدد. كما أن الثقافة التنظيمية (معامل 0.276 ، قيمة احتمالية 0.033) والضغط التنافسي (معامل 0.152 ، قيمة احتمالية 0.012) لهما أيضًا تأثير إيجابي وهام على التبني. وهذا يعني أن الثقافة الداعمة للابتكار في المنظمة والضغط التنافسي في الصناعة يمكن أن تخلق الدافع اللازم لتبني هذه التقنيات. وأخيرًا، فإن قدرات الأمان (معامل 0.114 ، قيمة احتمالية 0.019) والموارد الكافية (معامل 0.249 ، قيمة احتمالية 0.001) واستعداد المستخدم ووعيه (معامل 0.174 ، القيمة الاحتمالية 0.003) تؤثر أيضًا بشكل إيجابي وهام على التبني. تشير هذه العوامل إلى أن تمكين المؤسسة والمستخدمين من النواحي التقنية والموارد أمرٌ أساس لنشر هذه التقنيات وتبنيها.

تم استخدام تحليل الشبكة العصبية الاصطناعية في المرحلة الثانية من التحليل. وتم استخدام المتنبئات المهمة الافتراضية كمدخلات للشبكة العصبية الاصطناعية للتأكيد على الأهمية النسبية لكل متغير تنبؤي. تنتج الشبكات العصبية الاصطناعية تنبؤات أكثر دقة مقارنة بأساليب المجهر الإلكتروني الماسح . تم استخدام تحليل الشبكة العصبية الاصطناعية للتحقق من صحة الفرضيات. إن التوزيع غير الطبيعي للبيانات ووجود ارتباطات غير خطية بين المتغيرات التابعة والمستقلة هي الأسباب الرئيسة لتطبيق الشبكات العصبية الاصطناعية . علاوة على ذلك، فإن تحليل الشبكة العصبية الاصطناعية قوي في مواجهة الضوضاء والتحف وأحجام العينات الأصغر. تم استخدام وحدة الشبكة العصبية لبرنامج SPSS الخاص بشركة IBM لإجراء تحليل الشبكات العصبية الاصطناعية . يُحدد نموذج المُدرك متعدد الطبقات تأثير الوظائف التنفيذية على المعاملات الزوجية (الشكل 2). وتُستخدم الوظائف المُستخدمة لتنشيط الطبقة المخفية وطبقة المخرجات بشكل زائد، ويُستخدم توحيد البيانات كطريقة لتغيير حجم المتغيرات التابعة والمستقلة. يُوضح الشكل 3 نموذج المُدرك متعدد الطبقات لتحديد آثار العوامل التقنية والتنظيمية والبيئية على تبني الشركات الريادية لتقنيات الأمن السيبراني الجديدة.



شكل 3 : نموذج الشبكة العصبية الاصطناعية

دقة التنبؤ بنموذج الشبكة العصبية الاصطناعية (ANN) استخدام خطأ الجذر التربيعي المتوسط (RMSE) بالنسبة لكل من مجموعات البيانات التدريبية (80 %) ومجموعات البيانات الاختبارية (20 %) (عشرة تكرارات)، تم حساب RMSE باستخدام المعادلة التالية، حيث SSE مجموع مربعي x و n عدد العناصر هو .

$$RMSE= \sqrt{\frac{1}{n}} \times SSE$$

كما هو موضح في الجدول 4 ، تشير قيم RMSE لمجموعة البيانات التدريبية ومجموعة البيانات الاختبارية إلى نموذج ANN دقيق في التقاط العلاقات بين المتنبئين والمخرجات. نظرا لأن قيم RMSE المنخفضة تشير إلى دقة تنبؤ أعلى وملاءمة أفضل للبيانات. يوضح الجدول 4 نتائج خطأ الجذر التربيعي المتوسط (RMSE) لكل من مرحلتي التدريب والاختبار.

جدول 6 : قيم RMSE لنموذجANN

الشبكة	RMSE (التدريب)	RMSE (اختبار)	جميع العينة
ANN1	0.521	0.494	**134**
ANN2	0.519	0.608	**134**
ANN3	0.540	0.404	**134**
ANN4	0.543	0.394	**134**
ANN5	0.542	0.706	**134**
ANN6	0.537	0.696	**134**
ANN7	0.545	0.433.	**134**

الشبكة	RMSE (التدريب)	RMSE (اختبار)	جميع العينة
ANN8	0.534	0.407	**134**
ANN9	0.542	0.702	**134**
ANN10	0.552	0.578	**134**
المتوسط	0.538	0.551	
الانحراف المعياري	0.010	0.124	

في الجدول 6 ، حُسبت قيم RMSE (للاختبار) و RMSE (للتدريب) وإجمالي العينة لكل شبكة عصبية اصطناعية (ANN) بناءً على عينة من 134 شخصًا. كما أُدرج المتوسط والانحراف المعياري لكل من RMSE (للتدريب) و RMSE (للاختبار). تجدر الإشارة إلى أن الجدول 6 أُعدّ بناءً على افتراض تعميم المعلومات المُعطاة على 230 شخصًا.

الجدول 7 أداء تحليل الحساسية. تم استخدام تحليل الحساسية لتصنيف المتغيرات على أساس أهميتها النسبية المعيارية للمتغير التابع. وأظهر تحليل الحساسية أهمية كل متنبئ، في حين أظهرت أهمية كل متغير مستقل مدى اختلاف القيمة المتوقعة من قبل بنية الشبكة مع قيم المتغيرات المستقلة المختلفة.

جدول 7: تحليل الحساسية

العوامل	TE1	TE2	TE3	ORF1	ORF2	ORF3	ENF1	ENF2	ENF3	AI	NI(%)
TE	1.000	0.825	0.851	0.619	0.668	0.697	0.297	1.000	0.835	0.756	%25.2
ORF	0.542	0.734	0.754	1.000	1.000	1.000	0.861	0.863	1.000	0.863	%28.8
ENF	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	%33.3

- **TE1، TE2و TE3وهي تمثل العوامل الفنية 1 و 2 و 3 .**
- **ORF1وORF2و ORF3يمثل العوامل التنظيمية 1 و 2 و 3.**
- **ENF1وENF2و ENF3وهي تمثل العوامل البيئية 1 و 2 و 3.**

متوسط الأهمية (AI) والأهمية المعيارية (NI) لكل فئة من العوامل. بناءً على الأهمية المعيارية، تُعد العوامل البيئية الأكثر أهمية بنسبة 33.3 %، تليها العوامل التنظيمية بنسبة 28.8 %، وأخيرًا العوامل التقنية بنسبة 25.2 %.

جدول 8 : تصنيف المتغيرات المؤثرة على اعتماد تقنيات الأمن السيبراني الجديدة من قبل الخبراء

عامل	متوسط التقييم	مربع كاي	df	Sig .
الثقافة التنظيمية	6.14	32.974	8	0.000
موارد كافية	5.92	32.974	8	0.000
المتطلبات القانونية والتنظيمية	5.77	32.974	8	0.000
دعم الإدارة العليا	5.74	32.974	8	0.000
مستوى الاستعداد والوعي لدى المستخدمين النهائيين	5.45	32.974	8	0.000
الضغط التنافسي	5.24	32.974	8	0.000
التوافق التكنولوجي	4.99	32.974	8	0.000
قدرات الأمن	4.90	32.974	8	0.000
سهولة الاستخدام	4.85	32.974	8	0.000

تظهر نتائج اختبار فريدمان للمتغيرات المؤثرة على تبني تقنيات الأمن السيبراني الجديدة أن هناك فرقًا كبيرًا بين أولوية هذه المتغيرات. وأعلن اختبار فريدمان بدرجة حرية 8 ومستوى دلالة أقل من 0.05 أن الاختلافات الملحوظة في متوسط رتب المتغيرات ذات دلالة إحصائية. وهذا يعني أن الخبراء يعطون أهمية وأولوية مختلفة لهذه العوامل. بناءً على التصنيفات المتوسطة، فإن أهم العوامل المؤثرة هي: الثقافة التنظيمية (المرتبة

المتوسطة 6.14)، والموارد الكافية (5.92)، والمتطلبات القانونية والتنظيمية (5.77)، ودعم الإدارة العليا (5.74)، واستعداد المستخدم النهائي ووعيه (5.45). تُظهر هذه النتائج أنه من وجهة نظر الخبراء، تلعب العوامل الثقافية والبيئية التنظيمية مثل الثقافة التنظيمية ودعم الإدارة العليا دورًا مهمًا للغاية في اعتماد تقنيات الأمن السيبراني الجديدة. كما أن وجود الموارد الكافية والمتطلبات القانونية والتنظيمية المناسبة هي أيضًا عوامل رئيسية في هذا الصدد. في المقابل، تم تصنيف العوامل التقنية مثل قدرات الأمان وسهولة الاستخدام في مرتبة أقل. وهذا يدل على أن الخبراء يعتقدون أن العوامل التنظيمية والبيئية أكثر أهمية من العوامل التقنية في اعتماد تقنيات الأمن السيبراني الجديدة. وبشكل عام، يمكن لهذه النتائج مساعدة مديري الأمن السيبراني وصناع السياسات على التركيز على العوامل الرئيسية والأكثر تأثيرًا في تحديد أولويات الموارد وتخصيصها.

المناقشة والاستنتاج

تهدف الدراسة الحالية إلى التحقيق وتحليل العوامل التقنية والتنظيمية والبيئية المؤثرة على تبني تقنيات الأمن السيبراني الجديدة في المنظمات الريادية. لهذا الغرض، وباستخدام نهج نمذجة المعادلات الهيكلية (SEM)، تم اختبار العلاقات السببية بين هذه العوامل واعتماد تقنيات الأمن السيبراني الجديدة. أظهرت نتائج هذه الدراسة أن عوامل مثل المتطلبات القانونية والتنظيمية، ودعم الإدارة العليا، وتوافق التكنولوجيا، وسهولة الاستخدام، والثقافة التنظيمية، والضغوط التنافسية، والقدرات الأمنية، والموارد الكافية، ومستوى جاهزية ووعي المستخدمين النهائيين تؤثر بشكل كبير على اعتماد تقنيات الأمن السيبراني الجديدة في المنظمات الريادية. فيما يلي، للمناقشة والاستنتاج، يمكننا تحليل وتفسير هذه النتائج، وتقديم حلول عملية، ومقارنتها بالأدبيات السابقة، والقيود، والاقتراحات المستقبلية لتحقيق فهم أشمل لكيفية تحسين اعتماد تقنيات الأمن السيبراني الجديدة في المنظمات الريادية.

وبناءً على نتائج هذا البحث، تم تأكيد الفرضيات المتعلقة بالعوامل التقنية والتنظيمية والبيئية المؤثرة على تبني تقنيات الأمن السيبراني الجديدة في المنظمات الريادية بشكل كامل. في قسم العوامل التقنية، أظهرت النتائج أن توافق التكنولوجيا مع احتياجات وعمليات المؤسسة (معامل المسار 0.128)، والقدرات الأمنية للتقنيات الجديدة (معامل المسار 0.114)، وسهولة استخدامها من قبل المستخدمين (معامل المسار 0.121)، تؤثر إيجابًا وسلبًا على قبولها. هذا يعني أن الاهتمام بالمواصفات التقنية وسهولة استخدام تقنيات الأمن السيبراني من العوامل الرئيسية في قبول هذه التقنيات في المؤسسات الريادية. أما فيما يتعلق بالعوامل التنظيمية، فقد أظهرت النتائج أن دعم الإدارة العليا للمؤسسة (معامل المسار 0.187)، وتوفير الموارد الكافية (معامل المسار 0.249)، وبناء ثقافة تنظيمية داعمة (معامل المسار 0.276)، يؤثر إيجابًا وسلبًا على قبول تقنيات الأمن السيبراني الجديدة. هذا يعني أن العوامل داخل المؤسسة، مثل الدعم الإداري، وتخصيص الموارد المناسبة، وثقافة المؤسسة المبتكرة ، تلعب دورًا مهمًا في قبول هذه التقنيات. كما تؤكد النتائج في قسم العوامل البيئية أن ووجد الباحثون أن الضغوط التنافسية في الصناعة (معامل المسار 0.152)، والمتطلبات القانونية والتنظيمية (معامل المسار 0.228)، ومستوى الاستعداد والوعي لدى المستخدمين النهائيين (معامل المسار 0.174)، تؤثر بشكل إيجابي وهام على تبني تقنيات الأمن السيبراني الجديدة في المنظمات الريادية. وهذا يعني أن العوامل البيئية مثل الضغوط التنافسية، والأطر القانونية، واستعداد المستخدم، تشكل أيضًا عوامل مؤثرة في هذا الصدد. وبشكل عام، أظهرت نتائج هذه الدراسة أن العوامل التقنية والتنظيمية والبيئية تؤثر في وقت واحد وبشكل تفاعلي على تبني تقنيات الأمن السيبراني الجديدة في المنظمات الريادية، ويجب أخذ كل هذه العوامل في الاعتبار لتمهيد الطريق لتبني ونشر هذه التقنيات بنجاح في هذه المنظمات. وتتوافق هذه النتائج مع الدراسات والنظريات السابقة في مجال تبني تكنولوجيا الأمن السيبراني. ويعد نموذج قبول التكنولوجيا (TAM) ونظرية انتشار الابتكار (DOI) من بين الأطر النظرية البارزة في هذا المجال والتي تؤكد على دور العوامل المختلفة مثل التوافق مع الاحتياجات وسهولة الاستخدام والدعم الإداري والثقافة التنظيمية في تبني التقنيات. وتماشيًا مع هذه المناهج، أظهرت نتائج الدراسة الحالية أن توافق تقنيات الأمن السيبراني مع احتياجات وعمليات المنظمة، بالإضافة إلى سهولة استخدام هذه التقنيات للمستخدمين النهائيين، يؤثر إيجابًا وسلبًا على قبولها. وتتفق هذه النتائج مع الأبحاث السابقة في هذا المجال، مثل دراسة (Liang et al., 2007). بالإضافة إلى ذلك، تتوافق نتائج هذه الدراسة مع نظرية المصدر والتأثير (RBV) والنظرية المؤسسية.

و(أظهرت تكنولوجيا المعلومات) أن العوامل التنظيمية مثل دعم الإدارة العليا وتوفير الموارد الكافية وإنشاء ثقافة تنظيمية تدعم الابتكار تلعب دورًا فعالًا في تبني تقنيات الأمن السيبراني الجديدة (Wade & Hulland, 2004; Hsu et al., 2014). تتوافق هذه النتائج مع نتائج الدراسات السابقة مثل (Gangwar et al., 2015; Alshamaila et al., 2013). كما أظهرت هذه الدراسة، بما يتماشى مع منظور نظرية البيئة التنظيمية (TOE)، أن العوامل البيئية مثل الضغط التنافسي والمتطلبات القانونية واستعداد المستخدم النهائي لها أيضًا تأثير إيجابي وهام على تبني تقنيات الأمن السيبراني. وبشكل عام، أكدت نتائج هذه الدراسة أن اعتماد تقنيات الأمن السيبراني الجديدة في المنظمات الريادية يتأثر بعوامل تقنية وتنظيمية وبيئية متعددة، ويجب على المديرين الاهتمام بهذه العوامل في الوقت نفسه لتمهيد الطريق لنشر هذه التقنيات بنجاح.

تجدر الإشارة أيضًا إلى دراسة (Gangwar et al., 2015)، ولقد استخدم هذا البحث النموذج المتكامل(TOE -TAM) وحلل محددات اعتماد الحوسبة السحابية في المنظمات. وقد أظهرت النتائج أن العوامل التقنية والتنظيمية والبيئية مثل توافق التكنولوجيا ودعم الإدارة العليا والضغط التنافسي لها تأثير كبير على اعتماد الحوسبة السحابية. كما تجدر الإشارة إلى الدراسة التي أجراها (Alshamaila et al., 2013)، حول اعتماد الحوسبة السحابية من قبل الشركات الصغيرة والمتوسطة الحجم في المملكة المتحدة. استخدمت هذه الدراسة إطارًا متعدد الأوجه لفحص تأثير العوامل

التقنية والتنظيمية والبيئية على اعتماد الحوسبة السحابية. وقد أظهرت النتائج أنه بالإضافة إلى الميزات التكنولوجية، تلعب العوامل التنظيمية مثل دعم الإدارة العليا والثقافة التنظيمية، بالإضافة إلى العوامل البيئية مثل الضغط التنافسي، دورًا مهمًا في هذا المجال. وبشكل عام، تُظهر هذه الدراسات أن اعتماد التقنيات الجديدة، وخاصة التقنيات المتعلقة بالأمن السيبراني، يتأثر بعوامل تقنية وتنظيمية وبيئية متعددة، ويجب على المديرين الانتباه إلى هذه العوامل في وقت واحد. إلى جانب النتائج القيمة لهذه الدراسة، ينبغي أيضًا النظر في بعض القيود والاقتراحات للبحوث المستقبلية. ومن بين القيود التي تواجهها هذه الدراسة هو محدوديتها الجغرافية. تم إجراء هذا البحث فقط في المنظمات الريادية في منطقة محددة وقد لا تكون نتائجه قابلة للتعميم على مناطق أو دول أخرى. ومن ثم، فإن إجراء دراسات مماثلة في مناطق جغرافية أخرى ومقارنة النتائج يمكن أن يوفر فهماً أعمق للعوامل المؤثرة على اعتماد تقنيات الأمن السيبراني. كما أن هذا البحث ركز فقط على العوامل المؤثرة في قبول هذه التقنيات ولم يتطرق إلى جوانب تنفيذها وتشغيلها في المنظمات. ومن ثم، فإن إجراء دراسات مستقبلية ذات نهج نوعي ودراسات حالة يمكن أن يساعد في فهم أفضل لكيفية نشر هذه التقنيات وتنفيذها بنجاح. وفيما يتعلق بالاقتراحات العملية، ووفقاً لنتائج هذا البحث، ينبغي على مديري المنظمات الريادية الاهتمام بعدة نقاط مهمة. أولاً، إن إنشاء الأطر القانونية والتنظيمية المناسبة في مجال الأمن السيبراني يخلق الحافز الضروري لتبني التقنيات الجديدة في هذا المجال. ثانياً، إن دعم ومساندة الإدارة العليا للمنظمة لنشر هذه التقنيات أمر في غاية الأهمية، ويجب على المديرين أن يلعبوا دوراً فعالاً في هذا الصدد. ثالثًا، يعد الاهتمام بتوافق تقنيات الأمن السيبراني مع احتياجات المنظمة وعملياتها، فضلاً عن سهولة استخدامها للمستخدمين النهائيين، من بين العوامل الرئيسية في قبول هذه التقنيات. رابعا، إن خلق ثقافة تنظيمية تدعم الابتكار وتعزيز الضغوط التنافسية في الصناعة من شأنه أن يوفر الدافع الضروري لتبني هذه التقنيات. خامساً، يجب على المنظمات التخطيط لتمكينها من الناحية التقنية وتوفير الموارد اللازمة لنشر وتبني تقنيات الأمن السيبراني. وأخيرًا، يمكن أن تتضمن الاقتراحات الخاصة بالبحوث المستقبلية ما يلي: إجراء دراسات تكرار في مناطق جغرافية أخرى أو صناعات مختلفة، وفحص عمليات التنفيذ وتطبيق تقنيات الأمن السيبراني في المنظمات، وتقييم تأثير تبني هذه التقنيات على الأداء التنظيمي، وفحص دور المتغيرات المعتدلة المحتملة مثل حجم المنظمة أو مستوى نضج التكنولوجيا. ويمكن أن تساعد هذه الحالات في إثراء الأدبيات البحثية في هذا المجال.

المراجع

Badami, M. A., Meghdadi, M. M., & Pilevar, M. (2022). Investigating the impact of cyberspace on the abuse of the right to raise a child with emphasis on religious education. Journal of Legal Research, 21(50), 457–494. https://doi.org/10.48300/jlr.2021.279730.1619

Tarhini, Ali, Arachchilage, Nalin Asanka Gamagedara, Masa'deh, Ra'ed, & Abbasi, Muhammad Sharif. (2015). A Critical Review of Theories and Models of Technology Adoption and Acceptance in Information System Research. International Journal of Technology Diffusion, 6(4), 58–77. https://doi.org/10.4018/ijtd.2015100104

Karimi, M., Majedi, N., Safari, L., & Kalhor, H. (2023). Designing a virtual business development model in the field of sports services. Strategic Studies on Youth and Sports, 21(58), 313–330. https://doi.org/10.22034/ssys.2022.1783.2267

Al-shaibany, Nagi. (2023). A Model for Enhancing the Information Security Management Systems in Yemen Banks. مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا, 1(1), 1–12 https://doi.org/10.59628/jast.v1i1.14

Abohatem, A. Y., Ba-Alwi, F. M., Al-Haifi, M. A. M., & Al-hadheri, H. H. (2024). Cybersecurity risk assessment for infrastructure of information systems in Yemen telecoms. https://www.researchgate.net/publication/380293305

Liang, Huigang, Saraf, Nilesh, Hu, Qing, & Xue, Yajiong. (2007). Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management1. MIS Quarterly, 31(1), 59–87. https://doi.org/10.2307/25148781

Wade, Michael, & Hulland, John. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions For Future Research1. MIS Quarterly, 28(1), 107–142. https://doi.org/10.2307/25148626

Hsu, Pei-Fang, Kraemer, Kenneth L., & Dunkle, Debora. (2014). Determinants of E-Business Use in U.S. Firms. International Journal of Electronic Commerce, 10(4), 9–45. https://doi.org/10.2753/jec1086-4415100401

Gangwar, Hemlata, Date, Hema, & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. Journal of Enterprise Information Management, 28(1), 107–130. https://doi.org/10.1108/jeim-08-2013-0065

Alshamaila, Yazn, Papagiannidis, Savvas, & Li, Feng. (2013). Cloud computing adoption by SMEs in the north east of England. Journal of Enterprise Information Management, 26(3), 250–275. https://doi.org/10.1108/17410391311325225

فهرس الجداول

فهرس الاشكال

فهرس المحتويات