إطار مقترح لتقييم عوامل الخطر المؤثرة على تبنى تقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية

د/ مروه ابراهيم ربيع
أستاذ مساعد بقسم المحاسبة والمراجعة
كلية الأعمال ـ جامعة الإسكندرية

ملخص البحث:

يهدف البحث إلى تحديد المخاطر المحتملة التى تواجه نظام المعلومات المحاسبى عند تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز وكيفية التغلب على تلك المخاطر، مما يساعد على تحسين فرص تبنى الشركات لهذه التقنيات. ولتحقيق ذلك، تم إقتراح إطار يعتمد على إثنين من الأطر المستخدمة بصورة كبيرة فى أدبيات تبنى نظم المعلومات على مستوى الشركة. يعتمد الإطار المقترح على تكامل العوامل التكنولوجية- التنظيمية- البيئية (TOE) ، مع العوامل الخاصة بالتوافق بين البعد البشرى والتنظيمى والتكنولوجى(HOT – fit) . تم جمع البيانات من خلال قوائم إستقصاء وإختبار فروض البحث بالإستناد إلى نمذجة المعادلة البنائية SEM باستخدام برنامج AMOS V. 26.

توصلت النتائج إلى وجود العديد من المخاطر التى يمكن أن تواجه الشركات عند تبنيها تقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية. توصلت النتائج أيضاً إلى أن جميع العوامل التى تضمنها الإطار المقترح تؤثر معنوياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. عرضت الدراسة العديد من التوصيات والمجالات البحثية المستقبلية المرتبطة بموضوع البحث.

الكلمات المفتاحية: نظام المعلومات المحاسبى، الواقع الإفتراضى والمعزز، إطار العوامل التكنولوجية- التنظيمية- البيئية، إطار التوافق بين البعد البشرى والتنظيمى والتكنولوجى.

Abstract:

This research aims not only to identify potential risks facing companies in their accounting information system while adopting virtual and augmented reality technologies, but also how to mitigate these risks. To achieve this a Framework was proposed based on two widely used frameworks in IT adoption literature at corporate level. These two frameworks are (TOE) and (HOT-fit). A questionnaire-based data collection was used. Structural Equation Modeling and AMOS V. 26 were applied for analysis.

Results revealed many risks that companies may face when relying on virtual and augmented reality technologies to automate accounting processes. Results also revealed that all proposed constructs have a significant impact on companies' adoption of these technologies to automate accounting processes. Many recommendations and many future research areas related to the research topic were addressed.

Keywords: accounting information system, virtual and augmented reality, TOE Framework, HOT-fit Framework.

١. مقدمة:

يعتبر نظام المعلومات المحاسبى من أهم نظم المعلومات فى أى شركة؛ لأهميته فى الإمداد بالمعلومات التى تساعد مستخدميه على إتخاذ القرارات بصورة سليمة (Saeidi et al., 2015). ومع تطور التكنولوجيا، ظهرت تقنيات جديدة لتحسين أداء نظام المعلومات المحاسبى مثل تقنيتى الواقع الإفتراضى والمعزز. يمكن إستخدام تقنيتى الواقع الإفتراضى والمعزز فى زيادة كفاءة العمليات التصنيعية وتخفيض الفاقد (Moraes et al., 2023) ، بالإضافة إلى أهميتهما أيضاً فى زيادة كفاءة نظام المعلومات المحاسبى. يتم ذلك من خلال قيام المحاسبين بأداء واجباتهم من بعد (Egiyi, 2022) ، حيث يوفر إستخدام تقنيتى الواقع الإفتراضى والمعزز معالجة وعرض المعلومات المحاسبية فى واجهة رسومية وحوارية تفاعلية. وتتحقق بيئة العمل المحاسبية من خلال تبسيط الإتصالات الإلكترونية بين المشاركين فى وجود بيئة تفاعلية مدمجة تستند على تلك التقنيات إلى مستوى التواصل بين الأشخاص وإستخدام الصور المرئية المختلفة لعرض المعلومات المحاسبية (Zadorozhnyi et al., 2022). كما تُمَكِن مستخدمى نظام المعلومات المحاسبى والمستثمرين من تصور البيانات المالية والحصول على فهم أفضل للموقف المالى للشركة. كما يمكن أن تساعد هذه التقنيات فى تدريب وتعليم المحاسبين، مما يتيح للمستخدمين وبصفة خاصة المحاسبين ممارسة مفاهيم المحاسبة فى بيئة تفاعلية. وأخيراً المساعدة فى إجراء عمليات المراجعة وفحص المخزون عن بعد بطريقة أكثر كفاءة وفعالية، وتحليل البيانات المالية فى الوقت الحقيقى (Chukwuani ,2022).

بينما تسهم هذه التقنيات فى تحقيق العديد من المنافع فى المجال المحاسبى، فإنه يرتبط بها العديد من المخاطر. يرجع ذلك إلى زيادة إستخدام نظارات الواقع الإفتراضى وسماعات الرأس أو أجهزة الواقع المعزز التى يتم فيها تخزين البيانات الحيوية للمستخدمين (وبصفة خاصة المحاسبين)، والتى قد تكون بمثابة نقاط وصول مناسبة للقراصنة. يمكن للأجهزة القابلة للإرتداء، والتى تعد متطلب أساسى لإستخدام تقنيتى الواقع الإفتراضى والمعزز أن تخلق تهديدات جديدة. تتمثل فى التهديدات

المتعلقة بثغرات الأمان مما يؤدى إلى إستغلال القراصنة والمهاجمين لهذه الثغرات للحصول على وصول غير مصرح به للمعلومات المالية الحساسة أو إحداث عطل فى وظائف الأنظمة. كما قد يحتفظ المستخدم (الشركة) بملكية الأصول التابعة له، على الرغم من تشفير القراصنة لملفات بيانات الرموز غير القابلة للإستبدال[١] NFT أو Non Fongable Token فى هجوم بأحد الفيروسات، إلا أنه يمكن حظره من الوصول إلى تلك الأصول إذا لم يدفع المستخدم (الشركة) الفدية المحددة له (Huq et al., 2022; Pooyandeh et al., 2022; Xiao, 2023). وهو ما أكده خبراء شركة Trend Micro للخدمات الإستشارية للأمن السيبرانى، حيث يؤدى وجود عالم إفتراضى رقمى متكامل مثل الميتافيرس[٢] والتقنيات المدعمة له إلى إنتشار ظاهرة الكون المظلم Darkeverse. ففى ظله يمكن للقراصنة إستهداف الرموز غير القابلة للإستبدال NFTs المُستخدمة لتحديد الهوية الرقمية فى ذلك العالم؛ للقيام بعمليات التصيد الإحتيالى ونشر برامج الفدية والإحتيال وغيرها من الهجمات (الكويتى، ٢٠٢٣).

تتمثل مخاطر **سلامة البيانات ومخاوف الخصوصية** المرتبطة بتبنى تقنيتى الواقع الإفتراضى والمعزز فى الوصول غير المصرح به إلى نظم المعلومات المحاسبية مما يؤدى إلى تزوير البيانات وتحقيق أضرار مالية كبيرة للشركات (Pooyandeh et al., 2022; Zadorozhnyi et al., 2022; Xiao,2023).

كما قد يؤدى أتمتة العمليات المحاسبية من خلال تقنيتى الواقع الإفتراضى والمعزز إلى ظهور تحديات جديدة ترتبط **بالإمتثال القانونى والتنظيمى**. حيث يجب على الشركات الالتزام بالعديد من اللوائح والمعايير، مثل اللائحة العامة لحماية البيانات (GDPR) (القمة العالمية للحكومات ، آرثر دى ليتل، ٢٠٢٣).

وأخيراً مع تزايد إعتماد الشركات على تقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية، يزداد خطر **حدوث عطل فى النظام** أو تعطله، بالإضافة إلى تعرض المحاسبين **لمخاطر الصحة والسلامة** من خلال تعرضهم للإصابة الجسدية أو

---

[١] يقصد بالرموز غير القابلة للإستبدال أصول رقمية عبارة عن خط أو مجموعة من الرموز على البلوك تشين ينسب ملكية أحد الأصول إلى شخص ما أو شركة ما (Zadorozhnyi et al., 2022)

[٢] يمثل العالم الإفتراضى الرقمى المتكامل أو الميتافيرس مساحة إفتراضية مشتركة حيث يمكن للمستخدمين، الذين يمثلون الصور الرمزية الرقمية، التواصل والتعاون مع بعضهم البعض والتفاعل مع الأشياء الرقمية فى عوالم إفتراضية يتم إنشاؤها بواسطة الكمبيوتر. ومن خلال ذلك العالم، يظهر الأشخاص فى شكل تجسيدات رقمية مخصصة حيث يمكنهم التواصل مع الآخرين وأداء الأنشطة التى تحاكى الحياة الحقيقية داخل العالم الإفتراضى (Chow et al., 2023). كما يعد العالم الرقمى المتكامل أو الميتافيرس الجيل التالى للإنترنت، ففى حين أن الإنترنت يربط المستخدمين من خلال الأنظمة الأساسية أو مواقع الويب دون التفاعل مع الآخرين على الإنترنت، إلا أن وجود عالم إفتراضى رقمى متكامل يساعد ويُمَكِن المستَخدِم من الإنغماس والتفاعل مع الآخرين من خلال الصور الرمزية أو الهويات الرقمية.

النفسية، وخاصة إذا تم إستخدام هذه التقنيات لفترات طويلة من الزمن (Egiyi , 2022; Soliman et al., 2023).

وفقاً لتقرير إكرونيس يتضح أن مجرمى الإنترنت يستغلون تعقيدات تقنية المعلومات لشن هجمات الكترونية مدمرة. وفى ظل عدم إدراك معظم المستخدمين لحجم التهديدات الإلكترونية؛ نتيجة زيادة تبنى الميتافيرس- وإستخدام تقنيتى الواقع الإفتراضى والمعزز-، فمن المرجح أن تزداد عمليات السرقة للبيانات والهوية وكلمات المرور، وهجمات البرمجيات الخبيثة. يرجع ذلك إلى عدم وجود خطة رئيسية للحماية الإلكترونية (Acronis Cyber Protection Week Global Report, 2022) .

يتضح مما سبق تعرض تقنيتى الواقع الإفتراضى والمعزز للعديد من المخاطر والتى قد تؤدى إلى سرقة المعلومات المالية للشركات وتدميرها أو تغييرها عند إستخدام هذه التقنيات، بالإضافة إلى المخاطر والمشاكل التى يمكن أن يتعرض لها المحاسبين أنفسهم مثل المخاطر الجسدية، والمخاطر المرتبطة بتغيير المعلومات الشخصية للمستخدمين (المحاسبين). وفى هذا الصدد يرى خبراء الأمن السيبرانى أن الاعتماد على التقنيات المُشَكِّلَة للعالم الإفتراضى الرقمى المتكامل "الميتافيرس" - وبصفة خاصة تقنيتى الواقع الإفتراضى والمعزز- يمكن أن يعرض مستخدمى الإنترنت الموجودين فى هذا الفضاء الإفتراضى لعدد كبير من المخاطر. تؤدى تلك المخاطر إلى زيادة حالات إختراق الحسابات، والتلاعب والإحتيال وسرقة الأصول، بالاضافة للمخاطر الصحية والنفسية التى يتعرضون لها عند إستخدام تلك التقنيات لفترات طويلة. وكذلك المخاوف بشأن القوانين المرتبطة بحماية البيانات والمعلومات المحاسبية. لذا يتضح مما سبق أن هناك حاجة لوجود أدوات وآليات أمنية جديدة لحماية البيانات والمعلومات المحاسبية عند تبنى تلك التقنيات.

وفى هذا الصدد يحاول البحث الإجابة على التساؤلات التالية: هل تواجه الشركات مخاطر عند تبنيها لتقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية؟، وهل تؤثر العوامل المتضمنة داخل الإطار المقترح على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية؟

تهدف الدراسة إلى إستنباط القضايا والمخاطر المحتملة عند تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز وكيف يمكن التغلب عليها، مما يساعد على تبنى الشركات لهذه التقنيات. حيث يعد أمن المعلومات المحاسبية وسلامة وصحة المحاسبين أهم جزء فى عمل نظام المعلومات المحاسبى. يرجع ذلك إلى تأثر العمل المحاسبى بمجرد حدوث مشكلة تتعلق بأمن المعلومات وصحة المحاسبين. لذلك يجب

الانتباه دائماً إلى البحث عن الطرق والآليات التى تُمَكِن الشركات من حماية وأمن البيانات والمعلومات المحاسبية. وفى هذا الصدد يهدف البحث إلى إقتراح إطار يتكون من إثنين من الأطر التى تستخدم بصورة كبيرة فى مجال تبنى نظم المعلومات على مستوى الشركة. يتمثل هذين الإطارين فى العوامل التكنولوجية- التنظيمية-البيئية (TOE) ، بالاضافة إلى إطار التوافق بين البعد البشرى والتنظيمى والتكنولوجى (HOT – fit) ، والذى يهتم بمدى توافق الهيكل البشرى والتنظيمى مع البناء التكنولوجى. حيث قد يؤثر الإعتماد على العوامل البشرية الملائمة والمؤهلة على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز وتكامله مع نظام المعلومات المحاسبى.

تتمثل أهمية البحث على **المستوى الأكاديمى** فى ندرة الدراسات المحاسبية -على حد علم الباحثة- المرتبطة بالمخاطر الناتجة من تبنى تقنيتى الواقع الإفتراضى والمعزز على نظام المعلومات المحاسبى. يتم ذلك من خلال تسليط الضوء على المخاوف المتعلقة بالهوية والشبكة وجمع بيانات المستخدمين (المحاسبين) بصورة كبيرة -فى ظل وجود عالم إفتراضى رقمى متكامل- والتى تعذر الوصول إليها سابقاً. كما تتمثل أهمية البحث على **المستوى العملى** فى إبراز أهم المخاطر المترتبة على تبنى تلك التقنيات وكيفية التغلب عليها -باستخدام الإطار المقترح-، وبصفة خاصة بعد إهتمام كل دول العالم بذلك العالم الإفتراضى. ويؤكد على ذلك إطلاق المعهد القومى للحوكمة والتنمية المستدامة فى مصر منتدى الحوكمة الرشيدة فى الميتافيرس، مما يدل على عزم مصر إستكشاف مدى إستعدادها لهذا التحول الثقافى وضمان الحوكمة الرشيدة فى هذا العالم (المعهد القومى للحوكمة الرشيدة والتنمية المستدامة، ٢٠٢٢).

يتبع البحث نهجاً كمياً مع القيام بدراسة تطبيقية لتحديد العوامل الرئيسية المؤثرة على تبنى تقنيتى الواقع الإفتراضى والمعزز من قبل الشركات، من خلال إرسال قوائم إستقصاء للمحاسبين ومديرى الإدارة العليا فى الشركات الصناعية والشركات كثيفة التكنولوجيا وصناعة الإلكترونيات بمحافظة الإسكندرية، وكذلك بعض الشركات التى تعمل فى مجال التجارة الإلكترونية.

وبعد تناول مشكلة البحث وأهميته والهدف منه تتمثل خطة البحث فى تناوله للنقاط التالية:الصعوبات والمخاطر التى تواجه نظام المعلومات المحاسبى عند إستخدام تقنيتى الواقع الإفتراضى و

٢. الصعوبات والمخاطر التى تواجه نظام المعلومات المحاسبى عند إستخدام تقنيتى الواقع الإفتراضى والمعزز:

يعد العالم الإفتراضى الرقمى المتكامل أو الميتافيرس شبكة من العوالم الإفتراضية ثلاثية الأبعاد التى يتم تشغيلها بواسطة الواقع الإفتراضى والمعزز،

ويخلق إقتصاداً رقمياً كاملاً (Al-Gnbri , 2022; Sebastian, 2022; Sebastian, 2023). فمن ناحية يعمل الواقع المعزز على تحسين أو "تعزيز" العالم الحقيقى عن طريق إضافة عناصر رقمية -مرئية أو سمعية أو حسية- إلى منظور العالم الحقيقى. وعلى النقيض من ذلك، وبدلاً من الإضافات الرقمية إلى العالم الحقيقى، يخلق الواقع الإفتراضى بيئته الإلكترونية الخاصة به. عادةً ما تتم تجربة الواقع الإفتراضى من خلال واجهة، مثل سماعة رأس أو نظارات، بدلاً من مشاهدة المحتوى على الشاشة.

وللدخول إلى ذلك العالم الإفتراضى فإنه يمكن إستخدام تقنيتى الواقع الإفتراضى والمعزز من خلال إرتداء أجهزة بما فى ذلك الشاشات المثبتة على الرأس (HMD) ، مع أجهزة إستشعار مدمجة لإلتقاط مدخلات المستخدم وهى تعبر عن الإتصال المادى بين المستخدم النهائى والعالم الإفتراضى. ومن أجل إنشاء إحساس واقعى باللمس عند لمس الأشياء الإفتراضية، يتم وضع قفازات لمسية عند الدخول لذلك العالم؛ (Pooyandeh et al., 2022; Chow et al., 2023; Sebastian, 2023). كما يتطلب إستخدام تقنيتى الواقع الإفتراضى والمعزز وجود شبكات للإتصال ونقل البيانات عبر الإنترنت؛ لتفاعل المستخدمين مع بعضهم البعض (Chow et al., 2023).

يؤدى تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز إلى تحقيق العديد من المنافع فى المجال المحاسبى مثل إعداد البيانات المالية والعرض المرئى للبيانات باستخدام تنسيقات ثنائية وثلاثية الأبعاد باستخدام الحركات أو التعليمات الصوتية (Financial Reporting Council, 2021; Chukwuani ,2022;Egiyi, 2022) ، وكذلك تدريب المحاسبين الجدد وإنغماسهم فى بيئة إفتراضية تحاكى بيئة العمل الحقيقية وقيامهم بالمهام الحسابية -والتى تعتبر جزءاً أساسياً من العمل المحاسبى-مثل جرد المخزون ومعرفة قيمته ومتابعة حركة السلع والمنتجات من خلال النقر بالإصبع.

وعلى الرغم من أهمية تبنى الشركات لتلك التقنيات فى أتمتة العمليات المحاسبية، إلا أنه قد يواجه تبنيها لتلك التقنيات العديد من المخاطر. لذا يتطلب من أى شركة تهدف إلى التحول الرقمى لعملياتها توضيح متطلبات التحول الرقمى مثل وجود إستراتيجية رقمية، والمعرفة اللازمة للعنصر الرقمى، والعقبات التى تواجه رقمنة نظم المعلومات المحاسبية (Meraghni et al., 2021; Faizal et al., 2022). وبالنظر للصعوبات والعقبات التى يمكن أن تواجه نظام المعلومات المحاسبى عند إستخدام تقنيتى الواقع الإفتراضى والمعزز يتضح أنها يمكن أن تأتى من أربعة مصادر وهم زيادة التكلفة الإستثمارية، بالإضافة إلى المخاطر المرتبطة بتجربة

المستخدم -التى يمكن أن يتعرض لها المحاسبين عند إستخدام هذه التقنيات-، ومخاطر أمن المعلومات ومن أبرزها الخداع والسرقة والعرقلة، وأخيراً المخاطر المرتبطة بخصوصية البيانات. يرجع ذلك إلى أن فكرة وجود عالم إفتراضى رقمى متكامل لا يزال فى مهده، مما يتطلب النظر والتفكير فى بعض القضايا الهامة المترتبة عليه بدءاً من اليوم، دون الإنتظار للبحث عن حلول عند حدوث تلك المخاطر (Vyas, 2021; Göçen, 2022).

٢-١. التكاليف الإستثمارية المرتبطة بتبنى تقنيتى الواقع الإفتراضى والمعزز:

نظراً لأن الواقع الإفتراضى والمعزز لا يزال فى مراحله الأولى، فإن الأمر يتطلب إستثمارات كبيرة من قبل الشركات لتبنى تلك التقنيات مما يُمَكِنها من تحسين إنتاجية الشركة (Egiyi , 2022) ، بالإضافة إلى أتمتة العمليات المحاسبية الناتجة عن تبنى تلك التقنيات.

وعلى الرغم من إنخفاض أسعار سماعات الرأس بشكل كبير فى السنوات الأخيرة، فإن تكلفة أجهزة الواقع الإفتراضى والمعزز المتطورة، بالإضافة إلى تطوير التطبيقات والبيئات الإفتراضية على العكس من ذلك لا تزال تشكل رادعاً لبعض الشركات. لذا يؤدى زيادة تكلفة هذه الأجهزة إلى إعاقة إستخدام الشركات لهذه التقنيات (PWC, 2019) . كما يرتبط بتبنى تلك التقنيات أيضاً تكاليف صيانة الأجهزة ومراقبتها ومتابعتها وتدريب العاملين (المحاسبين بصفة خاصة) على كيفية التعامل معها (Vargas et al., 2020).

٢-٢. المخاطر المرتبطة بتجربة المستخدم:

يمكن أن يؤدى زيادة المخاطر المرتبطة بتجربة المحاسبين وإستخدامهم لتقنيتى الواقع الإفتراضى والمعزز إلى الحد من إستخدامهم لتلك التقنيات. يرجع ذلك إلى معاناة المحاسبين عند إنغماسهم فى الواقع الإفتراضى وشعورهم بالدوخة والغثيان وحتى النوبات أو فقدان الوعى المكانى عند إستخدام تقنيات الواقع الإفتراضى، عند حجب سماعات الواقع الإفتراضى مجال رؤية المستخدم بالكامل. أى أن إنغماس المستخدمين عند إستخدام تقنية الواقع الإفتراضى يؤدى إلى منع إتصال المستخدم تماماً بصرياً وصوتياً بالعالم الخارجى (Kohnke, 2020). لذا من المهم دائماً تقييم السلامة الجسدية وأمن بيئة المستخدم أولاً (Jaber , 2022) . وينطبق هذا أيضاً على الواقع المعزز، حيث يجب على المستخدمين البقاء على وعى جيد بمحيطهم، لا سيَّما فى البيئات الأكثر إنغماراً فى المحتوى المعروض. كما يجب أن تكون الأجهزة المستخدمة لتقنية الواقع المعزز صغيرة وخفيفة وسهلة الحمل وسريعة بما يكفى

لعرض الرسومات باستخدام هذه التقنية؛ لتعاملها مع كمية هائلة من المعلومات فى الواقع المادى (Chukwuani , 2022) .

لذا قد يستغرق الأمر بعض الوقت حتى تنطلق التكنولوجيا حقاً. كما يجب على المطورين تبسيط العمليات المتضمنة داخل هذه التقنيات حتى يتعامل معها المستخدمين بسهولة ويسر، مما يؤثر على زيادة رضاء المستخدمين (القمة العالمية للحكومات، آرثر دي ليتل، ٢٠٢٣؛ Chukwuani , 2022; Egiyi, 2022).

تتمثل العوامل الأخرى التى قد تعوق تبنى الشركات لتلك التقنيات فى المشاكل الثقافية وعدم الثقة فى التقنيات الجديدة ورفض المحاسبين لإستخدام تلك التقنيات؛ لخوفهم من إختراق حسابات الشركة من خلال سرقة هويتهم وعدم تدريبهم بصورة كافية عند تبنى تلك التقنيات. كما قد يؤدى عدم خبرة المحاسبين بهذه التقنيات -المُشَكَلَة للعالم الإفتراضى- إلى التسجيل الخاطئ للمدفوعات فى ذلك العالم وحدوث خطأ ما مثل الدفع إلى مستفيد أخر أو تحويل مبلغ غير صحيح أو عدم إتمام المعاملات فى الوقت المناسب بسبب وجود خطأ فنى (Narin, 2021).

٢-٣. المخاطر الأمنية المرتبطة بتبنى تقنيتى الواقع الإفتراضى والمعزز:

تتوقع الباحثة أن المخاطر الأمنية المرتبطة بتبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز تنشأ بصفة عامة من قيام المهاجمين والمتسللين بالتلف المادى للأجهزة المرتبطة بالواقع الإفتراضى والمعزز التى يستخدمها المحاسبون عند تشغيل وعرض البيانات والمعلومات المحاسبية، وكذلك المخاطر المرتبطة بفقدان البيانات والمعلومات المحاسبية وذلك كما يلى:

- **المخاطر المرتبطة بأمن أجهزة الواقع الإفتراضى والمعزز (الثغرات الأمنية):**

يعد الواقع الإفتراضى والمعزز، مثل أى نظام آخر قائم على الكمبيوتر، عرضة للهجمات الإلكترونية (Dwivedi et al., 2022). فمن خلال تلك الأجهزة يمكن تعديل وتدمير البيانات المتضمنة بداخلها. ويزداد الأمر سوءاً عند ربط المهاجمين بين الواقع الإفتراضى والواقع المادى؛ للوصول للأنشطة التى يقوم بها الأفراد فى الواقع المادى. لذا ترى الباحثة أنه قد يؤدى إستخدام المحاسب للبيانات المحاسبية وإعدادها وعرضها من خلال تقنيات الواقع الإفتراضى والمعزز إلى مخاطر جمه على نظام المعلومات المحاسبى.

تتمثل المخاطر التى يمكن أن تشوب **الواقع الإفتراضى** فى حجب سماعات الواقع الإفتراضى مجال رؤية المستخدم (المحاسب) بالكامل، مما قد يكون ضاراً إذا تم إختراق الجهاز. لذا يمكن للمهاجمين تعديل المحتوى لجعل المستخدم (المحاسب)

يشعر بالدوار أو الغثيان. كما يعد فقدان الإتصال الطبيعى بالعالم الحقيقى أيضاً أحد المشكلات نتيجة التفاعل فى البيئة الإفتراضية. حيث يعزل الواقع الإفتراضى الأشخاص بعيداً عن عالمهم الفعلى لفترة معينة من الوقت. لذا فإن المستخدمين المنغمسين فى لقاءات الواقع الإفتراضى ليس لديهم إرتباط صوتى ومرئى بالعالم الخارجى (Jaber , 2022) ، مما يساعد المهاجمون على تعديل محتوى البيانات والمعلومات المحاسبية(Dwivedi et al., 2022) .

تتمثل أيضاً المخاطر التى يمكن أن يتعرض لها الواقع الإفتراضى فى تمكن المتسللين والمهاجمين من الوصول إلى بيانات تتبع الحركة الخاصة بسماعات الرأس الخاصة بالواقع الإفتراضى، وإنشائه نسخة رقمية طبق الأصل (تُعرف أيضاً باسم deep fake) . يتم ذلك من خلال إستخدام المهاجم لخوارزميات تعلم الآلة لمعالجة الأصوات، وبالتالى تعرض أمان الواقع الإفتراضى للخطر، من خلال تركيب هذه المعلومات على شخص آخر لتنفيذ هجوم الهندسة الاجتماعية (Chukwuani, 2022; Jaber , 2022; Pooyandeh et al., 2022).

يمكن أن تتعرض **تقنية الواقع المعزز** أيضاً للعديد من الهجمات مثل هجمات الهندسة الإجتماعية، وسرقة الحسابات المالية للمستخدمين (Lee et al., 2021; Pietro and Cresci, 2021; Jaber, 2022). كما يمكن أن يتعرض مستخدمى تقنية الواقع المعزز (المحاسبين) أيضاً لرفض الخدمة الموزعة[٣] distributed denial of service بهدف إعاقة مورد الشبكة من الإستجابة للمهام التى يقوم بها المستخدم، بالإضافة إلى الثغرات الأمنية التى يمكن أن تشوب تقنيات الواقع المعزز (Chukwunonso et al., 2022).

يتضح مما سبق أنه إذا إستولى المهاجمون على حقوق المستخدم من خلال إستغلال نقاط الضعف الأمنية لأجهزة الواقع الإفتراضى والمعزز، يمكنهم التحكم فى الأجهزة المتصلة عن بُعد، وسرقة معلومات الجهاز المحدد (على سبيل المثال، معلومات التحديق) ، كما أنه قد يؤدى عدم توافر الأمن فى أجهزة الواقع الإفتراضى والمعزز والأدوات المرتبطة بهم مثل أجهزة إنترنت الأشياء إلى العديد من التهديدات المتعلقة بالهوية وسرقتها، وهجوم إنتحال الهوية ومشكلة مصادقة الصور الرمزية المستخدمة فى الواقع الإفتراضى (Chukwunonso et al., 2022; Wang et al., 2022) ، بالإضافة إلى برامج الفدية (Jaber, 2022).

[٣] يقصد بهجمات الخدمة الموزعة هجمات تغمر مورد الشبكة بالطلبات بشكل متكرر وبطريقة متسقة بهدف وحيد هو إعاقة مورد الشبكة من الاستجابة للعمليات التى يقوم بها المستخدم.

تخلص الباحثة مما سبق إلى زيادة التهديدات التى يمكن أن تواجه نظام المعلومات المحاسبى عند تبنى تقنيتى الواقع الإفتراضى والمعزز بدرجة كبيرة عن التهديدات التى تهدد أنظمة المعلومات المحاسبية التى تعمل فى الواقع المادى فقط. تتمثل التهديات التى تواجه نظم المعلومات المحاسبية فى الواقع المادى فى الإدخال العرضى والمتعمد لبيانات تالفة، وتدمير البيانات، ومشاركة الموظفين لكلمة المرور، وإدخال الفيروسات في أجهزة الكمبيوتر. بالاضافة إلى التهديدات سالفة الذكر، يزداد الأمر سوءاً عند إختراق أجهزة الواقع الإفتراضى والمعزز، وتحقيق المهاجمون لأهدافهم المنشودة مما يؤثر سلباً على سمعة الشركات المتبنية لتلك التقنيات. كما يؤثر إستخدام تلك التقنيات أيضاً على القرارات التى يتخذها المستثمرون للإستثمار فى الشركة، حيث يمكن للمهاجمون إنشاء محاكاة للواقع الإفتراضى للبيانات المالية للشركة، مما يجعلها تبدو أفضل مما هى عليه فى الواقع.

– **المخاطر المرتبطة بفقدان البيانات والمعلومات المحاسبية:**

كما سبق القول أنه ستنشئ خدمات العالم الإفتراضى المتكامل والأجهزة المرتبطة بها أنواعاً جديدة من البيانات الشخصية (مثل معلومات المقاييس الحيوية والروتين اليومى وعادات المستخدم) ، مما يساعد على تنفيذ هجمات للوصول غير المصرح به إلى البيانات. أى تتمثل التهديدات المرتبطة بالبيانات فى التهديدات المتعلقة بالبيانات التى تم جمعها أو إنشاؤها بواسطة الأجهزة القابلة للإرتداء والمستخدمين / الصور الرمزية. فقد تعانى هذه الأجهزة من تهديدات العبث بالبيانات، وإدخال البيانات الخاطئة، وإنخفاض جودة المحتوى. وقد يقوم المهاجمين بتعديل وتزوير وإستبدال وإزالة البيانات الأولية طوال دورة حياة البيانات للتدخل في الأنشطة العادية للمستخدمين أو الصور الرمزية أو الكيانات المادية مما يؤدى إلى العبث بالبيانات (Wang et al., 2022; Soliman et al., 2023) ، ومن ثم العبث بالبيانات والمعلومات المحاسبية للشركات فى ذلك العالم.

يزداد الوضع سوءاً من خلال إستفادة معظم التطبيقات من مكتبات الطرف الثالث -التى قد يكون لها حق الوصول إلى البيانات التى ينشأها المستخدم- وما يفعله مالكو هذه المكتبات بهذه البيانات وكيف يتم تخزينها مما يمثل مشكلة جوهرية. يؤدى ذلك إلى إستغلال البيانات السرية للمستخدمين. فعلى سبيل المثال، تستفيد تطبيقات الواقع الإفتراضى من تتبع الأصبع للكتابة على لوحات المفاتيح الإفتراضية. ويتم إختراق البيانات من هذه التطبيقات عندما يستخدم المستخدم هذه اللوحات لإدخال كلمة المرور. حيث يمكن للمهاجم إعادة إنشاء كلمات مرور هؤلاء المستخدمين بسهولة (Chukwunonso et al., 2022; Fernandez and Hui,

Techamontrikul, 2022) ، ومن ثم الإستيلاء على البيانات والمعلومات المحاسبية للشركة. يمكن أيضاً فقدان البيانات والمعلومات المحاسبية من خلال حذف المحاسب ملفاً بطريق الخطأ أو إذا تعطل النظام عموماً، مما يؤدى إلى فقدان هذه البيانات إلى الأبد.

٢-٤. مشاكل الخصوصية المرتبطة بتبنى تقنيتى الواقع الإفتراضى والمعزز:

يمكن أن تتعرض خصوصية المستخدم عموماً والمحاسبين بوجه خاص للإنتهاك من خلال قيامهم بالمهام المكلف بها عند إستخدام تقنيتى الواقع الإفتراضى والمعزز. تنشأ تلك المخاطر من العديد من المصادر (Wang et al., 2022) وهى: **إنتشار جمع البيانات**: للتفاعل بشكل غامر مع الصورة الرمزية فى العالم الإفتراضى، يتطلب الأمر جمع المعلومات عن تعابير الوجه، وحركات العين/ اليد، والقياسات الحيوية، وحتى أنماط موجات الدماغ. لذا إذا تم إختراق المستشعرات الخاصة بالحركة من قبل المهاجمين، فيمكن إرتكاب جرائم خطيرة على أساس هذه الكميات الكبيرة من البيانات الحساسة (Lee et al., 2021; Pietro and Cresci, 2021; Fernandez and Hui, 2022; Huq et al., 2022; Pooyandeh et al., 2022; Sebastian, 2022; Smaili and de Rancourt-Raymond ,2022; Wang et al., 2022; Chow et al., 2023; Sebastian, 2023; Soliman et al., 2023). كما يتم **تسرب الخصوصية فى نقل البيانات** من خلال الأجهزة القابلة للإرتداء عبر الإتصالات السلكية واللاسلكية، والتى يجب حظر سريتها على الأفراد غير المصرح لهم. وعلى الرغم من أن الإتصالات يتم تشفيرها ونقل المعلومات بشكل أساسى، إلا أن المهاجمين قد يستطيعون الوصول إلى البيانات الأولية عن طريق التنصت على قناة محددة وحتى تتبع مواقع المستخدمين والهجوم عليهم بإستخدام الهجمات المتقدمة مثل هجمات الإستدلال المتقدم[٤] .

يمكن أيضاً **تسرب الخصوصية فى معالجة البيانات** من خلال تسريب معلومات المستخدمين الحساسة ومن ثم تسرب المعلومات المحاسبية الحساسة للشركة. فمثلاً، قد يؤدى تجميع البيانات الخاصة والتى تنتمى إلى مستخدمين مختلفين إلى وحدة تخزين مركزية لتدريب نماذج مظهر الأفاتار الشخصية إلى إنتهاك خصوصية المستخدم وإنتهاك لوائح العالم الحقيقى الحالية مثل اللائحة العامة لحماية البيانات (GDPR) (Wang et al., 2022). كما يؤدى **تسرب الخصوصية فى التخزين السحابى / حوسبة الحافة** إلى إثارة مشكلات تتعلق بالكشف عن الخصوصية (Dai and

[٤] يقصد بهجوم الاستدلال المتقدم هو أسلوب لإستخراج البيانات يتم إجراؤه عن طريق تحليل البيانات من أجل اكتساب المعرفة بشكل غير قانوني حول موضوع أو قاعدة بيانات.

(Vasarhelyi , 2016). فمثلاً فى عام ٢٠٠٦، تم إختراق قاعدة بيانات العملاء الخاصة بـ Second Life وتم إختراق بيانات المستخدم بما فى ذلك أسماء المستخدمين والعناوين غير المشفرة، بالإضافة إلى تفاصيل الدفع وكلمات المرور المشفرة (Wang et al., 2022). كما تتمثل مشاكل الخصوصية أيضاً من خلال تعرض **الأجهزة الطرفية لكل من الواقع الإفتراضى والمعزز للإختراق**. فمن ناحية يمكن تعرض أجهزة الواقع الإفتراضى للإختراق من خلال نظارات الواقع الإفتراضى مما يؤدى إلى غزو البرامج الضارة وفقدان الخصوصية إذا تمكن المهاجمون من الوصول إلى تلك الأجهزة. ومن ناحية أخرى يمكن للقراصنة إستخدام الإعلانات لحقن محتوى ضار فى تطبيقات الواقع المعزز، وقد ينقر المستخدمون غير المتشككين Unsuspecting على إعلان يوجههم إلى مواقع ويب رهينة أو خوادم الواقع المعزز المصابة بالبرامج الضارة والتى تحتوى على صور مهتزة، مما يعرض أمان الواقع المعزز للخطر. كما يمكن للقراصنة الوصول إلى جهاز الواقع المعزز للمستخدم وتسجيل أفعالهم وتفاعلاتهم. يؤدى القيام بذلك إلى إحتمالية تهديد المستخدم (المحاسب) لاحقاً بنشر التسجيلات والمعلومات المحاسبية ما لم يدفع المستخدم فدية (Chukwuani , 2022).

يمكن أيضاً تعرض المستخدمين بوجه عام والمحاسبين بوجه خاص **لإساءة إستخدام بياناتهم / صورهم الرمزية.** حيث يمكن الكشف عن البيانات المتعلقة بالمستخدم/ الصورة الرمزية له عن قصد من قبل المهاجمين أو عن غير قصد وينتج عن ذلك صعوبة تتبع أنشطة إساءة إستخدام البيانات فى وجود العوالم الإفتراضية. كما يمكن أن تتعرض **البصمات الرقمية للمحاسبين للتهديدات** من خلال جمع المهاجمين البصمات الرقمية للصور الرمزية وإستغلال التشابه المرتبط بالمستخدمين فى العالم الحقيقى والعالم الرقمى لإستخدام البصمات الرقمية من قبل شخص أخر والقيام بأنشطة غير قانونية (Wang et al., 2022).

تخلص الباحثة مما سبق إلى خضوع كل ما يفعله المستخدمين للمراقبة بدرجة كبيرة جداً، بالإضافة إلى مشاركة بيانات المستخدمين فى مواقع مختلفة، وتتبع حركات قزحية العين مما يساعد على التعرف بدقة على الشخص الحقيقى وراء الصورة الرمزية المخصصة له(Sebastian, 2023) . ويؤثر ذلك بالطبع على تعرف المحتالين على الموقع الحقيقى للشركات التى يعمل بها المستخدمين، مما يتطلب حماية مبانى هذه الشركات وبياناتها من خلال توافر آليات لحماية البيانات فى السحابة والشبكة (Huq et al., 2022; Sebastian, 2023). لذا يتطلب الأمر

إدراك ووعى الشركات والمستخدمين للمخاطر التى يمكن أن يتعرضوا لها عند تبنى تلك التقنيات.

كما يتضح من العرض السابق أيضاً تعرض نظم المعلومات المحاسبية للشركات عند تبنى تقنيتى الواقع الإفتراضى والمعزز للعديد من مخاطر الأمن والخصوصية، والتى قد تُوقِع المحاسبون بتلك الشركات للعديد من المخاطر. تنشأ تلك المخاطر من إستخدام المحاسبين للواقع الإفتراضى والمعزز والأجهزة المرتبطة بهما. يؤكد على ذلك ما توصلت إليه دراسة Vyas (2021) من إتخاذ أحدث تدابير الأمن السيبرانى وخصوصية البيانات التى يتعين تنفيذها من قبل مطورى العوالم الإفتراضية الرقمية المتكاملة. يرجع ذلك إلى أنه قد تكون المراقبة الحديثة لتهديدات الهجمات الإلكترونية المتقدمة وحماية البيانات الخاصة شديدة الحساسية مثل القياسات الحيوية فى صدارة اللعبة مقارنة بتدابير الأمن السيبرانى التقليدية. لذا يجب على السلطات والشركات والأفراد التصدى لتلك المخاطر، مما يتطلب أطراً تنظيمية وإمتثالات جديدة، فضلاً عن ضرورة توافر آليات جديدة للأمن السيبرانى من أجل منع هذه الجرائم (Katterbauer et al., 2022). أى يتضح مما سبق أهمية إدراك الشركات للمخاطر التى تتعرض لها عند تبنيها لتقنيتى الواقع الإفتراضى والمعزز فى هذه العوالم وكيفية التغلب عليها.

٣.الإطار المفاهيمى وصياغة فروض البحث :

بصدد دراسة قرار تبنى الشركات للتكنولوجيا والتقنيات الجديدة، يتضح عدم إعتماد هذه القرارات على العوامل التكنولوجية فقط، بدلاً من ذلك ينبغى دراسة العوامل التنظيمية والبيئية أيضاً(Chandra and Kumar, 2018) . توجد العديد من الأطر التى تدرس العوامل التى تؤثر على تبنى الشركات للتكنولوجيا والتقنيات الجديدة على مستوى الشركة (Xu and Lu ,2022). تتمثل أهم هذه الأطر فى إطار العوامل التكنولوجية- التنظيمية– البيئية- Technology- Organization Environment والمشار إليه بـ TOE ، وإطار التوافق والترابط بين العوامل البشرية والتنظيمية والتكنولوجية -Human, Organization and Technology fit والمشار إليه بـ HOT – fit.

تم تقديم إطار العوامل التكنولوجية-التنظيمية-البيئة (TOE) عام ١٩٩٠على يد Tornatzky and Fleischer. يركز الإطار على أهمية كل من العوامل التكنولوجية والتنظيمية والبيئية والتى يمكن أن تؤثر على تنفيذ أى ابتكار متعلق بتكنولوجيا

المعلومات على مستوى الشركة ككل (Alharbi et al., 2016; Nguyen et al., 2022; Xu and Lu, 2022; Thomas and Yao, 2023).

وعلى الرغم من أهمية إطار عمل TOE فى تبنى التقنيات الجديدة على مستوى الشركة، إلا أنه لا يحتوى على جميع المتغيرات المرتبطة بالشركة مثل العوامل البشرية والتى قد تؤثر على إتخاذ القرارات المتعلقة بتبنى التقنيات الجديدة مثل تقنيتى الواقع الإفتراضى والمعزز. لذا سوف تستند الباحثة بالإضافة إلى إطار العوامل التكنولوجية- التنظيمية- البيئية على إطار التوافق والترابط بين العوامل البشرية والتنظيمية والبيئية HOT- fit (Hapsari et al., 2022). يرجع ذلك إلى أن تبنى تكنولوجيا المعلومات تعد عملية تقنية وإجتماعية. تعتبر الجوانب البشرية والتنظيمية والتقنية كلها شروطاً ضرورية لهذه العملية، ومن هنا يتضح أهمية التوافق بين الأبعاد الثلاثة فى تحقيق الهدف من تبنى أى تكنولوجيا جديدة. حيث يمكن أن يؤدى عدم التوافق بين الموارد البشرية والتنظيمية والتكنولوجية إلى عدم تحقيق الأهداف المطلوبة من تبنى التكنولوجيا، أى عدم تطبيق التكنولوجيا بنجاح. يرجع ذلك إلى أن وجود نقص فى التوافق بين الجوانب البشرية والتنظيمية والتكنولوجية يؤدى إلى الإفتقار إلى الملاءمة وإعاقة إعتماد التكنولوجيا ويحد من إمكاناتها فى الشركات (Xu and Lu, 2022).

وبصدد تقييم عوامل الخطر المؤثرة على تبنى تقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية وكيفية تلافيها، سوف تعتمد الباحثة على العوامل التكنولوجية- التنظيمية- البيئية المتضمنه فى إطار TOE ، مع إضافة العوامل البشرية فقط المتضمنة فى إطار HOT-fit ، ولم يتم دمج العوامل التكنولوجية والتنظيمية الخاصة بإطار HOT-fit ، لتجنب الازدواجية مع العوامل الخاصة بإطار TOE ، وذلك كما يلى:

٣-١. العوامل التكنولوجية:

يشير السياق التكنولوجى إلى كل من التقنيات الداخلية والخارجية ذات الصلة بالشركات. ومن ثم، قد تشمل التكنولوجيا فى هذا السياق الممارسات والمعدات والعمليات الحالية (Baker, 2012; Chandra and Kumar, 2018; Justino et al., 2022; Xu and Lu, 2022). ومن هنا يتضح أهمية البعد التكنولوجى عند تبنى الشركات للتقنيات الجديدة مثل تقنيتى الواقع الإفتراضى والمعزز فى زيادة خصوصية وأمن البيانات عند تبنى هذه التكنولوجى على النحو التالى:

٣-١-١. خصوصية البيانات:

سبق القول أن الخصوصية تعتبر مصدر قلق كبير بشأن تبنى تقنيتى الواقع الإفتراضى والمعزز. تتمثل مشاكل الخصوصية فى الطبيعة الشخصية للغاية للبيانات التى يتم جمعها، أى البيانات الحيوية مثل مسح القزحية أو شبكية العين وبصمات الأصابع واليد وهندسة الوجه وبصمات الصوت. وفى هذا الصدد يمكن إعتبار بيانات تتبع الواقع الإفتراضى والمعزز "معلومات محددة للهوية الشخصية"، إذ يمكن للأطراف الأخرى إستخدامها لتمييز هوية الفرد أو تتبعها، إما بمفردها أو عند دمجها مع معلومات شخصية أو تعريفية أخرى. وهذا يجعل خصوصية معلومات المستخدمين عند تبنى تقنيتى الواقع الإفتراضى والمعزز مصدر قلق كبير. ولحماية خصوصية معلومات المستخدمين (المحاسبين) وكلمات السر للدخول إلى نظام المعلومات المحاسبى يتعين وجود أطراً للتحكم فى خصوصية البيانات عن طريق تأمين والتحكم فى خصوصية بيانات الإدخال (من أجهزة إستشعار مختلفة). يمكن إدارة هذا التحكم الجديد فى البيانات المجمعة من خلال تقنيات تحسين الخصوصية[٥] Privacy-Enhancing Technologies والمشار إليه بـ (PETs) التى تخفى أى بيانات منقولة من المستشعرات قبل مشاركتها مع الخدمات السحابية (Fernandez and Hui, 2022). بالإضافة إلى الإهتمام بأمن البيانات والمعلومات المخزنة فى السحابة، وإستخدام القنوات الآمنة للتنقل مع الكيانات الأخرى (Dai and Vasarhelyi , 2016).

وفى هذا الصدد تقترح الباحثة أهمية إستخدام الشركات للشبكة الإفتراضية الخاصة VPN ، حيث تساعد الشبكة الإفتراضية الخاصة على إنشاء إتصال شبكى محمى عند إستخدام الشبكات العامة. يتم ذلك من خلال تشفير حركة البيانات الخاصة بالمستخدم عبر الإنترنت وإخفاء هويته الإلكترونية، مما يجعل تتبع الأنشطة عبر الإنترنت وسرقة البيانات أمراً فى غاية الصعوبة بالنسبة للغير. لذا فإنه فى ظل التطورات التى يشهدها الواقع الإفتراضى والمعزز، فمن المحتمل أن يتوسع إستخدام الشبكات الإفتراضية الخاصة ليشمل هاتين التقنيتين. ولحماية خصوصية البيانات وهوية المستخدم يمكن أيضاً إستخدام طرق مصادقة ثلاثية الأبعاد فى الواقع الإفتراضى، حيث يتم تزويد المستخدم بمكعب ثلاثى الأبعاد به أرقام وألوان ويمكن

[٥] يقصد بتقنيات تحسين الخصوصية : طرق لحماية البيانات. تسمح تقنيات تحسين وتعزيز الخصوصية لمستخدمي شبكة الإنترنت بحماية خصوصية معلومات التعرف الشخصية (personally identifiable information) التي تُزوّد بها التطبيقات والخدمات أو تعالجها. تُستخدَم هذه التقنيات لتقليل احتكار البيانات الشخصية بدون خسارة الأداء الوظيفي لنظام المعلومات (اى تهدف الى تقليل البيانات الشخصية التي تُجمع وتُستخدم من قبل مزودات الخدمة والشركات)

للمستخدم تدوير المكعب ثلاثى الأبعاد لتغيير إتجاهه. يتم إجراء مصادقة المستخدم عن طريق إختيار مجموعات الألوان والأرقام من المكعب باستخدام إما تحديق العين أو وضع الرأس أو النقر باستخدام وحدة تحكم (Chow et al., 2023).

يتضح مما سبق ضرورة توافر جاهزية أمنية تكنولوجية لخصوصية البيانات فى الشركات مما يساعد على تبنيها لتقنيتى الواقع الإفتراضى والمعزز، كما يتضح من فرض البحث الأول.

H1: تؤثر الجاهزية الأمنية التكنولوجية المتعلقة بخصوصية البيانات إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز.

٣-١-٢. أمن البيانات:

لتحقيق أمن البيانات فى ظل تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز يمكنها القيام بالآتى:

أولاً: إنشاء منصات الأمن الإستباقى:

يتم إجراء المعاملات فى العالم الإفتراضى من خلال تبنى فكرة العقود الذكية على أساس القواعد المشفرة -وهى أكواد رقمية مبرمجة تعمل على البلوكتشين، وتقوم بانجاز العمليات تلقائياً، وتضمن إتمام العمليات التجارية وفقاً لقواعد محددة مسبقاً-، مما قد يساعد ويُمَكِن المحتالين على إنشاء روابط مزيفة، وبمجرد تنشيط هذه الروابط، يتمكن المحتالون من الوصول إلى المحفظة الإفتراضية للمستخدم، ونقل محتوياتها (Huq et al., 2022). لذا أكدت دراسة Dunnett et al., (2023) على تزايد إرتكاب العديد من الهجمات الناجحة القائمة على العقود الذكية فى السنوات الأخيرة مثل هجمات إعادة الدخول. تهدف هجمات إعادة الدخول إلى إستنزاف أموال العقد الذكى. ولكن من خلال مشاركة البيانات الخاصة بالتهديدات السيبرانية بين الشركات، فإن التأثير المحتمل لهذه التهديدات الناشئة يمكن أن يدار بشكل أفضل. على سبيل المثال، إذا عثرت إحدى الشركات على ثغرة أمنية فى عقدها الذكى وقامت بإصلاحها، فإن المشاركة التعاونية للمعلومات المتعلقة بالتهديدات والتى توضح بالتفصيل الثغرة الأمنية المكتشفة، لديها القدرة على السماح للشركات الأخرى بضمان عدم تأثرها بنفس الثغرة الأمنية. فلقد أصبحت أتمتة (برامج) مشاركة معلومات التهديدات السيبرانية (إستخبارات التهديد السيبرانى) (Cyber Threat Intelligence sharing) من خلال التواجد عبر المنصات المخصصة لذلك سلاحاً

جديداً فى يد المدافعين الإلكترونيين للتخفيف بشكل إستباقى من الهجمات الإلكترونية المتزايدة، وهى تعد طريقة جديدة لخلق الوعى بالموقف بين أصحاب المصلحة المشاركين. تساعد تلك البرامج على دعم أنظمة التبادل والتحليل وإتخاذ القرار آلياً، مما يعزز كفاءة المشاركة وبالتالى يحبط الهجمات السيبرانية. لذا يجب أن يكون لدى الشركات برنامج إستخبارات للتهديدات يكون جزءاً من الأمن السيبرانى الإستباقى. ويساعد ذلك على خلق وعى بالوضع الأمنى وأن يتم تنبيههم بالتهديد فى أسرع وقت ممكن (Abu et al., 2018; Wagner et al., 2019).

أى أن الإستثمار فى إستخبارات التهديدات السيبرانية يمكن أن يوفر للشركات قدرة أكبر على الدفاع ضد الهجمات السيبرانية الحالية أو المحتملة. يرجع ذلك إلى أن مشاركة البيانات الخاصة بالهجمات السيبرانية يحقق العديد من المنافع للشركات عند تبنيها لتقنيتى الواقع الإفتراضى والمعزز. على سبيل المثال، فى حالة تعرض إحدى الشركات للهجوم، فإن مشاركة البيانات الخاصة بالهجمات السيبرانية مع الشركات الأخرى يساعد تلك الشركات على زيادة قدرتها على التنفيذ الاستباقى للاستراتيجيات الوقائية، والاستقصائية، و / أو التصحيحية للتخفيف من حدة التهديدات. وبذلك يسمح وجود منصة لمشاركة معلومات التهديد السيبرانى للشركات بمشاركة معلومات التهديدات الإلكترونية والتهديدات فى الوقت الفعلى والوصول إليها دون الكشف عن تفاصيل حساسة حول شبكاتهم وأنظمتهم .

ثانياً: الإهتمام بأمن الأجهزة والبرامج المتضمنة فى الواقع الإفتراضى والمعزز:

تعد كل من الأجهزة والبرامج المرتبطة بنظام المعلومات المحاسبى مكونات مهمة يجب أخذها فى الإعتبار لحماية البيانات والمعلومات المحاسبية. لذا تعتقد الباحثة لحماية البيانات والمعلومات المحاسبية، من الضرورى تحديث البرامج الثابتة الخاصة بسماعات رأس الواقع الافتراضى والمعزز والأجهزة القابلة للارتداء الخاصة بهاتين التقنيتين مما يساعد على تصحيح الثغرات الأمنية، بالإضافة إلى إستخدام البرامج التى يمكن أن توفر حماية قوية ضد التهديدات المختلفة عبر الإنترنت، مثل الفيروسات والبرمجيات الضارة وبرامج طلب الفدية وبرامج التجسس والتصيُّد وغيرها من تهديدات أمن الإنترنت الناشئة. أى يتضح مما سبق أهمية وجود جاهزية أمنية تكنولوجية للشركات بغرض حماية البيانات والمعلومات المحاسبية مما يساعد على تبنيها لتقنيتى الواقع الإفتراضى والمعزز، كما يتضح من فرض البحث الثانى.

H2: تؤثر الجاهزية الأمنية التكنولوجية المتعلقة بأمن البيانات والمعلومات المحاسبية إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز.

٣-٢. العوامل التنظيمية:

تشير العوامل التنظيمية إلى الخصائص والموارد، بما فى ذلك عمليات الإتصال داخل الشركة، وحجم الشركة (Baker, 2012; Chandra and Kumar, 2018; Justino et al., 2022) ، والتى يمكن أن تؤثر على تبنى التقنيات والتكنولوجيا الجديدة. وفى هذا الصدد تعد الموارد المالية العنصر الأساسى فى تعزيز الإبتكار. وذلك لأن تنفيذ التقنيات والتكنولوجيا الجديدة قد يتطلب إستثمارات كبيرة. أى يتأثر تبنى التكنولوجيا الجديدة بشكل إيجابى بالحجم التنظيمى ومقدار الموارد المملوكة له.

تعد قدرة الشركة على دفع تلك التكاليف عاملاً مؤثراً على إتخاذ القرار بتبنى التكنولوجيا الجديدة. نظراً لأن تنفيذ التكنولوجيا الجديدة يحتاج إلى إستثمارات طويلة الأجل وتكلفة عالية لإعداد تكنولوجيا المعلومات. لذا فإن الشركات التى لديها موارد مالية كافية ستفضل إعتماد التقنيات الجديدة وتبنيها. ومن ثم، فإن الشركات التى لديها إمكانية الوصول إلى التمويل الكافى هى وحدها القادرة حقاً على تبنى التكنولوجيا. وفى سياق تبنى تقنيتى الواقع الإفتراضى والمعزز، تحتاج الشركات إلى الإستثمار بكثافة فى خوادم الويب لإستضافة البيانات وقواعد البيانات (Chandra and Kumar, 2018). أى تعد تكلفة الأدوات والأجهزة المرتبطة بتقنيتى الواقع الإفتراضى والمعزز، بالإضافة إلى التعلم والتدريب من خلال تقنيتى الواقع الإفتراضى والمعزز، والتدريب على حماية البيانات والمعلومات المحاسبية عوامل هامة يجب أخذها فى الإعتبار عند إتخاذ القرار بتبنى هذه التقنيات، كما يجب أن يكون هناك حاجة إلى خطة مناسبة للإستثمار.

كما يمكن أن تقوم الشركات بالعديد من الإجراءات التنظيمية لحماية خصوصية وأمن البيانات والمعلومات المحاسبة عند تبنيها لتقنيتى الواقع الإفتراضى والمعزز. تتمثل تلك الإجراءات فى الإجراءات الداخلية وتبنى فكرة الثقة المعدومة، بالإضافة إلى الإجراءات الخارجية.

تتمثل **الإجراءات الداخلية** فى إهتمام الشركات بحوكمة الأمن السيبرانى وإدارة المخاطر من خلال تحديد التهديدات التى تتعرض لها الشركة ووضع سياسات وإجراءات وتدريبات ومواد تعليمية للأمن السيبرانى، وتثقيف العاملين لديها، حول حماية البيانات الحساسة من أجل منع الوصول غير المرغوب فيه إلى الأنظمة والشبكات. لذلك، فمن المتوقع إستثمار المحاسبين وشركات المحاسبة فى المستقبل فى الأمن السيبرانى لحماية مصالحهم ومصالح عملائهم (Imene and Imhanzenobe, 2020). كما يتطلب الأمر وضع الشركات لتدابير الأمان الأساسية مثل وضع كلمات المرور القوية، والمصادقة متعددة العوامل، وإدارة الهوية

القوية(Chukwunonso et al., 2022; Wang et al., 2022) ، والتحديثات البرمجية. وكذلك وضع الإجراءات الخاصة بعناصر التحكم والرقابة المتمثلة فى معيار الأيزو ISO / IEC 27002 لإدارة أنظمة المعلومات مثل التحكم في الوصول وإدارة الهوية، والإهتمام بضوابط الخصوصية فى معيار الأزو ISO / IEC 27701 وهو نظام لإدارة معلومات الخصوصية، بالاضافة إلى التعامل مع منصات تعمل بجدية على حماية مستخدميها.

كما تعد بنية شبكة الثقة المعدومة/الصفرية Zero Trust من قبل الشركات فلسفة يمكن أن تتبناها الشركات لحمايتها من الهجمات الإلكترونية. يتمثل المبدأ الأساسى لها فى "لا تثق أبداً، تحقَّق دائماً". مما يحافظ على أمن الشركات من الهجمات الإلكترونية من خلال إدارة الهوية والوصول، وحماية نقاط النهاية فى الشبكة، وتأمين الشبكة من خلال إجراء التجزئة الدقيقة، وتطبيق الحماية من التهديدات للمساعدة فى منع التهديدات والهجمات الأمنية (الكويتى، ٢٠٢٣).

وأخيراً تتمثل **الإجراءات الخارجية** فى تعزيز التعاون العالمى بين أصحاب المصلحة من القطاعين العام والخاص، من خلال تعزيز الإستجابة الجماعية للجرائم الإلكترونية، والتصدى المشترك للتحديات الأمنية الرئيسية (الكويتى، ٢٠٢٣).

يتضح مما سبق أهمية القدرة المالية للشركة والإستعدادات والجاهزية التنظيمية لأمن البيانات والمعلومات المحاسبية على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية، كما يتضح من فرضى البحث الثالث والرابع.

H3: تؤثر القدرة المالية للشركة والإستثمار فى أمن البيانات والمعلومات المحاسبية إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز.

H4: تؤثر الإجراءات التنظيمية (الداخلية والخارجية) المتعلقة بأمن البيانات والمعلومات المحاسبية إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز.

٣-٣. العوامل البيئية:

تشير العوامل البيئية إلى ساحة عمل الشركة، وهى تشمل خصائص الصناعة وهيكلها، ووجود أو عدم وجود بنية تحتية لدعم التكنولوجيا، بالإضافة إلى البيئة التنظيمية والقوانين والتشريعات (Baker, 2012; Chandra and Kumar, 2018; Justino et al., 2022; Nguyen et al., 2022) ، والدعم الحكومى. تؤكد العوامل البيئية على فكرة أن البيئة ستحدد قرار تبنى التكنولوجيا. أى أن تبنى

التكنولوجيا مرتبط بمجموعات معينة من الخصائص البيئية التى من شأنها تلعب دوراً هاماً فى عملية تكامل التكنولوجيا (Justino et al., 2022).

وفى هذا الصدد يمكن أن تؤثر العوامل الخارجية والبيئية على قرار تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. حيث يؤدى إندماج الأفراد (البشر) فى البيئات الإفتراضية وشبه الإفتراضية فى ظل إستخدام تقنيتى الواقع الإفتراضى والمعزز إلى تكثيف المشاكل القانونية المرتبطة بعلاقة الفرد بالتكنولوجيا (Dwivedi et al., 2022). لذا يتطلب الأمر من الحكومات الإستعداد للتحول للعالم الإفتراضى الرقمى المتكامل أو للميتافيرس، وكيف ستضمن الحكومات أمن البيانات فى ذلك العالم الموازى(Johan, 2022; Sia, 2023). كما يتطلب الأمر إهتمام الحكومات بإنشاء وزارات للتعامل مع ذلك العالم بصفة عامة وبناء إستراتيجية للتوائم الرقمية. وضرورة وجود إجراءات تساعد على وجود حوكمة أمن البيانات والمعلومات للعالم الإفتراضى (القمة العالمية للحكومات، آرثر دى ليتل، ٢٠٢٣) ، حيث يعد إصدار القوانين والأنظمة المناسبة ضرورياً لتشجيع المشاركة والإستثمار فى العالم الإفتراضى والأدوات المبنية عليه. كما يتطلب الأمر وضع لوائح وتشريعات جديدة ومعايير لتحقيق متطلبات الأمن السيبرانى عند إستخدام تقنيتى الواقع الإفتراضى والمعزز، وكذلك وضع القواعد واللوائح لحماية البيانات مثل قانون حماية البيانات والذى يهدف إلى تنظيم إستخدام المعلومات الشخصية التعريفية للأفراد من قبل الشركات، بالإضافة إلى اللوائح والقوانين المرتبطة بصحة وأمان المستخدمين عند إستخدام تلك التقنيات.

كما يؤثر الدعم الحكومى وإهتمام الحكومات بأمن البيانات والمعلومات المحاسبية على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. يمكن للحكومة أن تدعم الإبتكار من خلال تعزيز الإطار المفاهيمى الرقمى لإعتماد تلك التقنيات، ودعم حاضنات التكنولوجيا، وتمويل البحث والتطوير للشركات (Chiu et al., 2017; Khwaji et al., 2022; Nguyen et al., 2022). وقد وضعت مصر الإستراتيجية الوطنية للأمن السيبرانى (٢٠١٧- ٢٠٢١) لتنفيذ برامج تدعم الأهداف الإستراتيجية للأمن السيبرانى من خلال توزيع الأدوار بين الحكومة والقطاع الخاص، فضلاً على التأكيد على أهمية الشراكة المجتمعية بهدف تنفيذ الإجراءات ذات الصلة، والإهتمام بتبنى برامج لإعداد الكوادر البشرية والخبرات لتفعيل منظومة الأمن السيبرانى فى مختلف المجالات (الإستراتيجية الوطنية للأمن السيبرانى، ٢٠١٧). وفى هذا الصدد يؤكد المعهد القومى للحوكمة الرشيدة والتنمية المستدامة على إهتمام مصر بالدخول فى الميتافيرس وإستعداها لهذا التحول الثقافى، ومن ثم تبنى التقنيات

التى تعتمد عليها وضمان إستيعاب المحتوى التجريبى والتواصل فى العوالم الافتراضية، وبالتالى ضمان الحوكمة الرشيدة فى هذا العالم (المعهد القومى للحوكمة الرشيدة والتنمية المستدامة، ٢٠٢٢).

يتضح مما سبق أهمية الجاهزية البيئية المتمثلة فى الإمتثال القانونى والدعم الحكومى لأمن البيانات والمعلومات المحاسبية على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية، كما يتضح من فرضى البحث الخامس والسادس.

H5: يؤثر وجود إطار قانونى وسياسات ولوائح حكومية إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز.

H6: يؤثر الدعم الحكومى والإمداد ببرامج الأمن السيبرانى إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز.

٣-٤. البعد البشرى (أمن المحاسبين):

سبق التطرق إلى العديد من المخاطر المترتبة على إستخدام تقنيتى الواقع الإفتراضى والمعزز على صحة المستخدمين (المحاسبين) أنفسهم. تشمل هذه المخاطر المخاطر الجسدية، مثل خطر الوقوع أو السقوط أثناء إستخدام معدات الواقع الإفتراضى والمعزز والإنغماس فيه، بالإضافة إلى المخاطر النفسية، مثل خطر الإدمان أو الإصابة بأمراض صحية وعقلية. وفى سبيل التغلب على تلك المخاطر، يتطلب الأمر تدريب المحاسبين على تقنيتى الواقع الإفتراضى والمعزز جيداً. يرجع ذلك إلى أن الأخلاق الفكرية والقدرة المهنية للمحاسب تعتبر ذات أهمية كبيرة للتطوير الآمن لنظام المعلومات المحاسبى، وبصفة خاصة عند تبنى تقنيتى الواقع الإفتراضى والمعزز. لذلك، يجب الإهتمام بتطوير قدرات ومهارات المحاسبين والإهتمام بالتعليم المستمر على كيفية قيامهم بالمهام عبر العالم الإفتراضى. وبصفة خاصة أن تقنيات تعلم الآلة تسمح بالتلاعب بالأصوات ومقاطع الفيديو إلى الحد الذى تبدو عنده كأنها لقطات حقيقية أصيلة. حيث أنه إذا تمكن المتسلل أو المهاجم من الوصول إلى بيانات تتبع الحركة من سماعة رأس المستخدم (المحاسب) للواقع الإفتراضى، فمن المحتمل أن يستخدمها لإنشاء نسخة رقمية مماثلة ومن ثم تنفيذ هجوم الهندسة الاجتماعية.

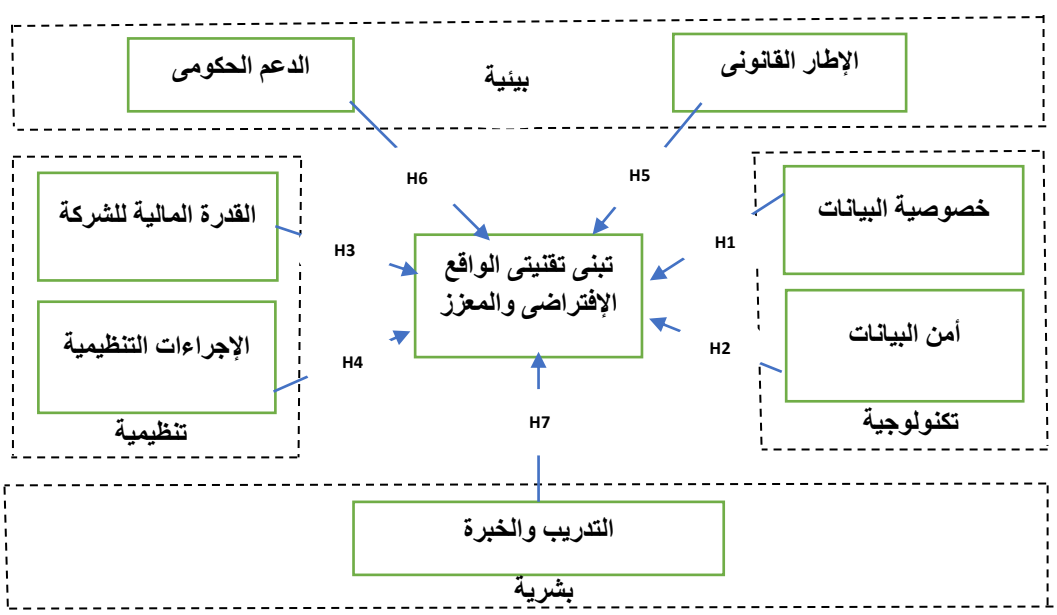
لذا يعد تدريب وتعليم المحاسبين فى كافة فروع المحاسبة من خلال هذه التقنيات أمراً هاماً (Hornik and Thornburg , 2010; Moscato and Moscato ,2011; Anastacio , 2019; PWC, 2019; Financial Reporting

Council, 2021; Göçen, 2022; Smaili and de Rancourt-Raymond ,2022; Tlili et al., 2022) يرجع ذلك إلى أن التدريب على إستخدام تقنيتى الواقع الإفتراضى والمعزز يساعد فى صقل مهارات المحاسبين والمراجعين وخاصة مهارات التفكير النقدى والحكم المهنى والعمل الجماعى (Buck, and McDonnell, 2022; Chukwuani, 2022; Egiyi, 2022). كما قد يؤدى تدريب المحاسبون من خلال هذه التقنيات على تلافى المخاطر المترتبة عليها، وزيادة رضائهم عند إستخدامها.

لذا يتضح مما سبق أهمية تطبيق تقنيتى الواقع الإفتراضى والمعزز فى التدريب المحاسبى وإتمام العمليات المحاسبية؛ لزيادة ثقة المتدربين فى أنفسهم ومن ثم زيادة رضائهم عند إجراء العمليات المحاسبية. كما يساعد التدريب على إستخدام هذه التقنيات على تلافى المخاطر الجسدية التى يمكن التعرض لها نتيجة لعدم خبرتهم فى إستخدام تلك التقنيات. لذا ترى الباحثة أهمية تعيين المحاسبين ذوى الكفاءة فى التعامل مع تقنيتى الواقع الإفتراضى والمعزز؛ لخبرتهم فى التعامل مع تلك التقنيات ومن ثم تخفيض المخاطر الجسدية التى قد يتعرضوا لها. ويؤثر ذلك فى نهاية الأمر على تبنى الشركات لتلك التقنيات لأتمتة العمليات المحاسبية. لذا ينص فرض البحث السابع على:

H7: يؤثر تعليم وتدريب المحاسبين من خلال تقنيتى الواقع الإفتراضى والمعزز إيجابياً على تبنى الشركات لتلك التقنيات.

يلخص الشكل (١) فروض البحث المرتبطة بالعوامل المؤثرة على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز.



شكل١: الإطار المقترح للعوامل المؤثرة على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز

٤. منهجية الدراسة :

يمكن عرض منهجية الدراسة التطبيقية من خلال الخطوات التالية:

٤-١. وصف عينة الدراسة :

تتألف عينة الدراسة من مديرى الإدارة العليا -لأهميتهم فى إتخاذ القرارات الخاصة بتبنى التقنيات الجديدة-، وكذلك المحاسبين فى الإدارة المالية فى الشركات الصناعية والشركات كثيفة التكنولوجيا وصناعة الإلكترونيات بمحافظة الإسكندرية، بالإضافة إلى بعض الشركات التى تعمل فى مجال التجارة الإلكترونية؛ لأهمية تلك التقنيات فى مجال عملهم. تم تسليم بعض قوائم الإستقصاء يدوياً مع إجراء بعض المقابلات الشخصية لتوضيح الهدف من الدراسة، كما تم تسليم البعض الأخر قوائم إستقصاء عبر البريد الإلكترونى الشخصى للمستقصى منهم. يوضح جدول رقم١ بيان بعدد قوائم الإستقصاء الموزعة على عينة الدراسة ونسبة الإستجابة.

جدول١: عدد القوائم الموزعة ونسبة الإستجابة

	الموزع	المستلم	نسبة الإستجابة	المستبعد	المستخدم
عبر الإيميل	٦٠	٤٧	٠.٧٨	١٣	٣٤
نسخة ورقية	٢٤٠	١٩٥	٠.٨١	٢٥	١٧٠
الإجمالى	٣٠٠	٢٤٢	٠.٨١	٣٨	٢٠٤

يوضح الجدول السابق عدد قوائم الإستقصاء الموزعة على المستقصى منهم[٦]، حيث بلغت ٣٠٠ قائمة إستقصاء منها ٢٤٠ قائمة تم تسليمها يدوياً. إستلمت الباحثة ٢٤٢ قائمة بمعدل إستجابة ٨١% وهى نسبة جيدة. كما تم استبعاد ٣٨ قائمة لعدم إكتمال الإجابة على تساؤلات البحث أو لعدم إنتماء المستقصى منهم لعينة الدراسة. وبالتالى يصبح عدد القوائم الصالحة للتحليل الإحصائى وإختبار فروض البحث ٢٠٤ قائمة. إستخدمت الباحثة برنامج الحزم الإحصائية SPSS V.26 لإجراء التحليل الوصفى وإختبار فروض البحث، بالإضافة إلى إستخدام برنامج AMOS V.26 لنمذجة المعادلة البنائية.

[٦] بالنسبة لقوائم الإستقصاء المرسلة عبر البريد الإلكترونى تم وضع لينك يوضح كيفية عرض القوائم المالية من خلال تقنية الواقع المعزز https://www.youtube.com/watch?v=ff-n0Rol-xw&feature=youtu.be ، وكذلك لينك محاكاة البيانات والمعلومات المحاسبية من خلال تقنية الواقع الإفتراضى https://www.youtube.com/watch?v=m28bwv_ydbo

يتضح من تحليل الخصائص الديمغرافية لعينة الدراسة أن ٤٩ مفردة (بنسبة ٢٤%) مديرى إدارة عليا، وأن ١١٤ مفردة (بنسبة ٥٦%) من عينة الدراسة تتراوح أعمارهم من ٣٠ إلى أقل من ٤٥ سنة. إتضح أيضاً من نتائج التحليل الوصفى أن ١٤٣ مفردة (بنسبة ٧٠%) لديهم خبرة أقل من ١٠ سنوات فى مجال العمل. وقد تبين أيضاً أن ١٠٠% من عينة الدراسة حاصلون على مؤهل جامعى عالى، وأن ٣١ مفردة (بنسبة ١٥%) حاصلون على دراسات عليا. لذا يتضح من نتائج التحليل الوصفى للخصائص الديمغرافية للمستقصى أنهم على دراية وعلم بالمستجدات الحديثة فى بيئة العمل، مما يتناسب مع موضوع البحث.

٤-٢. أداة جمع البيانات والمقاييس المستخدمة:

إعتمدت الباحثة على جمع البيانات من خلال توزيع قوائم الإستقصاء لإختبار فروض البحث والإجابة على تساؤلاته. أعدت قائمة الإستقصاء وفقاً لمقياس ليكرت الخماسى. تضمنت قائمة الإستقصاء -الموضحة فى ملحق البحث- ثلاثة محاور رئيسية. خصص المحور الأول لقياس الخصائص الديمغرافية للمستقصى منهم (السن، والمؤهل، والخبرة). فى حين تناول المحور الثانى التحديات والمخاطر المرتبطة بتبنى تقنيتى الواقع الإفتراضى والمعزز (بواقع ٢٣ سؤال)، وأخيراً تناول المحور الثالث المقاييس الأساسة لمتغيرات البحث المتضمنة فى الإطار المقترح (بواقع ٢٥ سؤال). إعتمدت الباحثة فى قياس المتغيرات على الدراسات السابقة التى تناولت إطار العوامل التكنولوجية- التنظيمية- البيئية TOE ، وكذلك العوامل البشرية المتضمنة فى إطار HOT-fit، كما يتضح من الجدول التالى:

جدول٢: متغيرات وأبعاد الإطار المقترح

المتغيرات	الأبعاد	الدراسات
العوامل التكنولوجية	**خصوصية البيانات**	Senarathna et al., 2018; Nagahawatta et al., 2021
	أمن البيانات	Gangwar et al., 2015; Senarathna et al., 2018; Nagahawatta et al., 2021; Justino et al., 2022; Lutfi et al., 2022
العوامل التنظيمية	**القدرة المالية**	Alharbi et al., 2016; Chandra and Kumar, 2018; Jere and Ngidi, 2020; Li, 2020
	الإجراءات التنظيمية	Salleh et al., 2015; Alharbi et al., 2016

العوامل البيئية	الإطار القانونى	Alharbi et al., 2016; Nagahawatta et al., 2021; Justino et al., 2022; Lutfi et al., 2022; Nguyen et al., 2022; Thomas and Yao, 2023
	الدعم الحكومى	Koduah et al., 2014; Alharbi et al., 2016; Chiu et al., 2017; Jere and Ngidi, 2020; Li, 2020; Nguyen et al., 2022
العوامل البشرية	التعليم والتدريب	Salleh et al., 2015; Alharbi et al., 2016; Chiu et al., 2017; Ateş and Gunes, 2018; Chandra and Kumar, 2018; Nagahawatta et al., 2021; Meunier et al., 2023
تبنى التكنولوجى		Gangwar et al., 2015; Alharbi et al., 2016; Li, 2020; Nagahawatta et al., 2021; Justino et al., 2022; Nguyen et al., 2022

يوضح الجدول السابق إستناد الباحثة على سبعة أبعاد تؤثر على تبنى تقنيتى الواقع الإفتراضى والمعزز. تتمثل الأبعاد فى أمن البيانات، وخصوصية البيانات، والقدرة المالية، والإجراءات التنظيمية، والدعم حكومى، والإطار القانونى، وأخيراً تعليم وتدريب المحاسبين من خلال تقنيتى الواقع الإفتراضى والمعزز.

٤-٣. إختبار ثبات وصدق العبارات والمقاييس المستخدمة فى الدراسة:

للتحقق من مستوى الثبات إستخدمت الباحثة إختبار معامل كرونباخ ألفا لمعرفة ثبات أداة القياس أو الإعتمادية على إجابات المستقصى منهم على قائمة الإستقصاء على عينة مبدئية (٢٧ مفردة). توصلت الدراسة عند تطبيق كرونباخ الفا على العينة المبدئية إلى أن قيمة كرونباخ ألفا للإختبار الكلى يساوى٠.٩٧٣ وهى قيمة عالية وأكبر من ٠.٧٠ القيمة المتعارف عليها فى الدراسات السابقة (Jere and Ngidi, 2020; Li , 2020; Lutfi et al., 2022). لذا أوضحت نتائج الإختبار أن قائمة الاستقصاء تتمتع بدرجة ثبات مرتفعة، مما يدل على الإطمئنان عند تطبيق قائمة الاستقصاء على عينة الدراسة. كما يتضح من الجدول التالى

جدول ٣: نتائج إختبار الثبات لمتغيرات الدراسة (معامل كرونباخ الفا)

العوامل/ العناصر	المتغيرات	عدد العبارات لكل متغير		قيمة معامل الثبات (كرونباخ ألفا)
التحديات والمخاطر المرتبطة بتبنى تقنيتى الواقع الإفتراضى والمعزز				
	تكلفة الإستثمار	٢		٠.٧٥
	المخاطر المرتبطة بتجربة المستخدم	٣		٠.٧٣
المخاطر الأمنية	أمن الأجهزة	١٠	١٤	٠.٩٣

	فقدان البيانات	٤			٠.٩٠
مشاكل الخصوصية		٤			٠.٩١
إجمالى		٢٣			٠.٩٧
الإطار المقترح					
تكنولوجية	خصوصية البيانات	٣	٦	٠.٧٢	٠.٨٠
	أمن البيانات	٣		٠.٧٤	
تنظيمية	الإجراءات التنظيمية	٣	٦	٠.٨٨	٠.٨٩
	القدرة المالية	٣		٠.٨٥	
بيئية	الإطار القانونى	٣	٦	٠.٧٣	٠.٨٠
	الدعم الحكومى	٣		٠.٧٤	
بشرية	التدريب والخبرة	٤			٠.٨١
تبنى الواقع الإفتراضى والمعزز		٣			٠.٨٢
إجمالى متغيرات الإطار		٢٥			٠.٩٢
إجمالى قائمة الإستقصاء		٤٨			٠.٩٧٣

يتضح من الجدول السابق تراوح قيمة كرونباخ ألفا للتحديات التى تواجه نظام المعلومات المحاسبى عند تبنى تقنيتى الواقع الإفتراضى والمعزز ما بين ٠.٧٣- ٠.٩٣ ، وبالنسبة للإطار المقترح فهى تتراوح ما بين ٠.٨٠- ٠.٨٩ وجميعها أكبر من ٠.٧ . يؤكد ذلك على أن هذه المقاييس الواردة فى قائمة الإستقصاء تتمتع بدرجة ثبات مرتفعة.

للتحقق من مستوى الصدق: تم التحقق من مستوى الصدق من خلال:

- **صدق المحتوى**: قامت الباحثة بعرض القائمة فى صورتها الأولية للتحكيم من بعض المحكين الأكاديميين وبعض المتخصصين من مفردات عينة الدراسة، وقد أبدى هؤلاء المحكمون مجموعة من الملاحظات على العبارات الواردة بقائمة الاستقصاء. لذا تم تعديل بعض الفقرات العديد من المرات فى ضوء مقترحاتهم.
- **الإعتماد على أسلوب التحليل العاملى التوكيدى:** Confirmatory Factor Analysis (CFA)

يعد أسلوب التحليل العاملى التوكيدى أحد تطبيقات نمذجة المعادلة البنائية. تم الإعتماد على برنامج AMOS V.26 بهدف التأكد من الصدق التقاربى للمقاييس الواردة فى البحث، والتى يوضحها الجدول التالى.

جدول ٤ : نتائج التحليل العاملى التوكيدى لقياس الصدق التقاربى لمتغيرات الدراسة

المتغيرات	المؤشرات	معاملات تحميل (التشبع) للعبارات	الموثوقية المركبة	متوسط التباين المفسر
خصوصية البيانات	priv_1	٠.٩٠	٠.٧٧٦	٠.٥٤١

المتغيرات	المؤشرات	معاملات تحميل (التشبع) للعبارات	الموثوقية المركبة	متوسط التباين المفسر
	priv_2	٠.٨٧		
	priv_3	٠.٨٦		
أمن البيانات	sec_1	٠.٨٩	٠.٧٩٢	٠.٥٦٢
	sec_2	٠.٨٤		
	sec_3	٠.٨٩		
الإجراءات التنظيمية	proced_1	٠.٨٩	٠.٨٣٣	٠.٦٢٧
	proced_2	٠.٨٥		
	proced_3	٠.٨٤		
القدرة المالية	fina_1	٠.٩٠	٠.٨٢١٢	٠.٥٥٨
	fina_2	٠.٩٢		
	fina_3	٠.٨٩		
الإطار القانونى	leg_1	٠.٨٦	٠.٨٧٨	٠.٦٤١
	leg_2	٠.٨٧		
	leg_3	٠.٨٦		
الدعم الحكومى	gov_1	٠.٨٦	٠.٩١٥	٠.٧٨
	gov_2	٠.٩٣		
	gov_3	٠.٩٢		
التدريب والخبرة	hum_1	٠.٩٣	٠.٨٧٣	٠.٧٠
	hum_2	٠.٩٠		
	hum_3	٠.٩٠		
	hum_4	٠.٩٢		
التبنى	adop_1	٠.٩٣	٠.٨٧١	٠.٧١
	adop_2	٠.٩١		
	adop_3	٠.٩٢		

توضح نتائج التحليل العاملى التوكيدى أن نموذج القياس يتمتع بمؤشرات جودة مطابقة عالية، حيث جاءت جميعها فى النطاق المقبول. كما يتضح أيضاً أن جميع قيم معاملات التحميل (التشبع)Loading Factors والتى تقيس مدى إرتباط العبارات بالبعد الذى تنتمى إليه تتراوح بين ٠.٨٤ – ٠.٩٣ وهى أكبر من القيمة المعيارية ٠.٥ (Chiu et al., 2017; Chandra and Kumar, 2018; Justino et al., 2022).

أوضحت النتائج أيضاً إرتفاع مستوى الإتساق الداخلى للعبارات المتضمنة داخل كل بعد من أبعاد متغيرات الدراسة، حيث إتضح أن قيمة الموثوقية المركبة Composite Reliability(CR) تتراوح بين ٠.٧٧٦ – ٠.٩١٥ وهى أكبر من ٠.٧(Chandra and Kumar , 2018; Nguyen et al., 2022) .

إتضح أيضاً إرتفاع الصدق البنائى للمقاييس الواردة فى الدراسة، حيث تراوحت قيم متوسط التباين المفسر بين ٠.٥٤١ – ٠.٧٨. وهى بذلك تجاوزت القيمة المعيارية ٠.٥ ويؤكد ذلك على تجاوز قيم متوسط التباين المفسر الدال على وجود إرتباط بين الأبعاد المختلفة داخل كل متغير القيمة المعيارية ٠.٥ (Chandra and Kumar , 2018).

كما أوضحت النتائج أيضاً تمتع نموذج القياس بصدق تمييزى جيد. يقيس الصدق التمييزى الإرتباط بين المتغيرات الكامنة Latent Constructs والجذر التربيعى لمتوسط التباين المفسر Square root of average variance extracted. يرجع ذلك إلى أن قيم الجذر التربيعى لمتوسط التباين المفسر لجميع المتغيرات تراوحت بين ٠.٧٣٢ – ٠.٨٩٣ وهى أكبر من معاملات الإرتباط فيما بينها (Justino et al., 2022)، كما يتضح من الجدول التالى.

جدول ٥: نتائج التحليل العاملى التوكيدى لقياس الصدق التمييزى لمتغيرات الدراسة

	المتوسط الحسابى	الإنحراف المعيارى	الخصوصية	الأمن	القدرة المالية	الإجراءات التنظيمية	الإطار القانونى	الدعم الحكومى	التدريب	التبنى
الخصوصية	٣.٩٤	٠.٥٤	**٠.٧٣٢**							
الأمن	٤.٠٣	٠.٥٨	٠.٢٢ **	**٠.٧٥٢**						
القدرة المالية	٤.١٦	٠.٥٢	**٠.٠١	**٠.١٤	**٠.٧٩٢**					
الإجراءات التنظيمية	٣.٨٤	٠.٥٤	٠.٠٤ **	٠.٠٣ **	**٠.٠٥	**٠.٧٤٧**				
الإطار القانونى	٣.٨١	٠.٤٨	**٠.٠٣	**٠.٠٤	**٠.٠٢	**٠.٠٢	**٠.٨٠٢**			
الدعم الحكومى	٣.٨٠	٠.٤١	**٠.٠٣	٠.٠٤ **	**٠.٠٤	**٠.٠٥	**٠.١٨	**٠.٨٩٣**		
التدريب	٤.١١	٠.٣	٠.١١ **	٠.٠١ **	**٠.٠١	٠.٠٣ **	**٠.٠٤	٠.٠٢ **	**٠.٨٣٥**	
التبنى	٤.٠٤	٠.٥٢	٠.٥١٥ **	**٠.٠٣٥	**٠.٠٤	٠.٠٣ **	**٠.٠٢	٠.٠١ **	**٠.٠٢	**٠.٨٣٤**

** **جميع معاملات الإرتباط معنوية عند مستوى معنوية ٠.٠٥ ، كما يظهر الجذر التربيعى لمتوسط التباين المفسر (المستخرج) AVE فى القطر الرئيسى للمصفوفة**

يتضح من جدول ٥ أن قيم الجذر التربيعى لمتوسط التباين المفسر لجميع المتغيرات أكبر من معاملات الإرتباط فيما بينها المتغيرات مما يؤكد على تمتع نموذج القياس بصدق تمييزى جيد.

٤-٤. إختبار إعتدالية التوزيع الإحتمالى للبيانات:

إعتمدت الباحثة على إختبار كولمجروف– سمرنوف؛ لمعرفة مدى تبعية البيانات للتوزيع الطبيعى ولإختبار فرض العدم الذى ينص على أن المشاهدات المتعلقة بمتغيرات الدراسة تتبع التوزيع الطبيعى. لذا تم إجراء هذا الإختبار على عينة الدراسة وإتضح أن قيمة p.value لجميع مفردات عينة الدراسة أكبر من مستوى المعنوية ٥% ، يعنى ذلك أن البيانات تتبع التوزيع الطبيعى. كما يتضح من الجدول التالى.

جدول ٦ : نتائج إختبار إعتدالية التوزيع الاحتمالى باستخدام اختبار كولمجروف– سمرنوف

المتغيرات	إحصائية الإختبار	مستوى الدلالة P.VALUE	القرار
المخاطر	٠.١٤٩	٠.٢	توزيع طبيعى
الإطار المقترح	٠.١٣٥	٠.٢	توزيع طبيعى

يتضح من نتائج التحليل الإحصائى لإختبار كولمجروف– سمرنوف أن قيمة p. value لأبعاد الدراسة أكبر من مستوى المعنوية ٥%. وبالتالى يتم قبول فرض العدم الذى ينص على أن بيانات العينة مسحوبة من مجتمع تتبع بياناته التوزيع الطبيعى. ومن ثم يتم الإعتماد على الأساليب الإحصائية الخاصة بالإختبارات المعلمية.

٥. نتائج التحليل الوصفى للإجابة على التساؤل البحثى الأول:

يتعلق السؤال البحثى الأول بمعرفة التحديات والمخاطر التى يمكن أن تواجه نظام المعلومات المحاسبى عند تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. يتضح من التحليل الوصفى موافقة المستقصى منهم على وجود العديد من التحديات والمخاطر التى يمكن أن تواجه الشركات عند تبنيها لتقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية، كما يتضح من الجدول التالى:

جدول٧: الإحصاء الوصفى للتساؤل البحثى الأول

		الموافقة	المتوسط الحسابى	الإنحراف المعيارى	الترتيب
تكلفة الاستثمار	التكرار	١٧٢	٣.٧٥	٠.٦٠٤	٥
	نسبة الموافقة	٠.٨٤			
المخاطر المرتبطة بتجربة المستخدم	التكرار	١٧٥	٣.٨١	٠.٥٤٢	٤
	نسبة الموافقة	٠.٨٦			
أمن الأجهزة	التكرار	١٧٧	٤	٠.٤١	٢
	نسبة الموافقة	٠.٨٧			
فقدان البيانات	التكرار	١٧٣	٣.٩١	٠.٤٦٦	٣
	نسبة الموافقة	٠.٨٥			
مشاكل الخصوصية	التكرار	١٨١	٤.١	٠.٣٨٧	١
	نسبة الموافقة	٠.٨٩			

يتضح من جدول ٧ إرتفاع عدد الموافقين ونسبة الموافقة والمتوسط الحسابى المرتبط بالعبارات المتعلقة بالتحديات والمخاطر الناتجة عند تبنى هذه التقنيات على نظام المعلومات المحاسبى. تتمثل هذه التحديات والمخاطر فى إرتفاع التكاليف المرتبطة بتبنى تلك التقنيات والأجهزة المرتبطة بها، بالإضافة إلى خطر فقدان البيانات وتعطل تلك التقنيات مما يؤثر على نظام المعلومات المحاسبى بالسلب، وعدم وصول المحاسبين للبيانات المالية. علاوة على المخاطر الصحية والجسمانية والنفسية التى يمكن أن يتعرض لها المحاسبين نتيجة إستخدام تلك التقنيات. بالإضافة إلى إمكانية إستخدام المهاجمين لتقنيتى الواقع الإفتراضى والمعزز لإنشاء وتزييف وسرقة المعلومات المالية الحساسة للشركات. وأخيراً مخاطر الخصوصية المرتبطة بإستخدام تلك التقنيات. لذا تؤكد إجابات المستقصى منهم على وجود تحديات ومخاطر ترتبط بتلك التقنيات على نظام المعلومات المحاسبى، مما يتطلب الأمر الأخذ فى الإعتبار العديد من المتغيرات التى تؤثر على تبنى هذه التقنيات، وهو ما أكده أيضاً إختبار ت وفقاً للجدول رقم ٨ :

جدول٨: نتائج إختبار One Sample t-test

المتغير	المتوسط الحسابى	متوسط الفرق	إختبار ت (t-test)	p.value
التحديات والمخاطر	٣.٧٤١٣	٠.٧٤١٣	٤٨.٣٣٨	٠.٠٠١ **

يشير متوسط الفرق إلى الفرق بين المتوسط الحسابى والقيمة المحايدة (٣)
إختبار ت (t-test) يوضح مستوى المعنوية لإجابات المستقصى منهم عند مستوى معنوية ٥ %

يتضح من الجدول السابق إتفاق نتائج إختبار ت مع نتائج التحليل الوصفى. يوضح الجدول أن هناك إرتفاع فى إدراك المستقصى منهم للتحديات والمخاطر المترتبة على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز، حيث يزداد متوسط ذلك المتغير عن القيمة المحايدة (٣) بمقدار ٠.٧٤١٣ وذلك عند مستوى معنوية ٥ %. ويدل ذلك على وجود مخاطر تتعلق بتبنى هاتين التقنيتين، مما يتطلب الأمر ضرورة البحث عن حلول للتغلب على تلك المخاطر قبل تبنى هذه التقنيات.

٦. نتائج الإطار المقترح وإختبار فروض البحث:

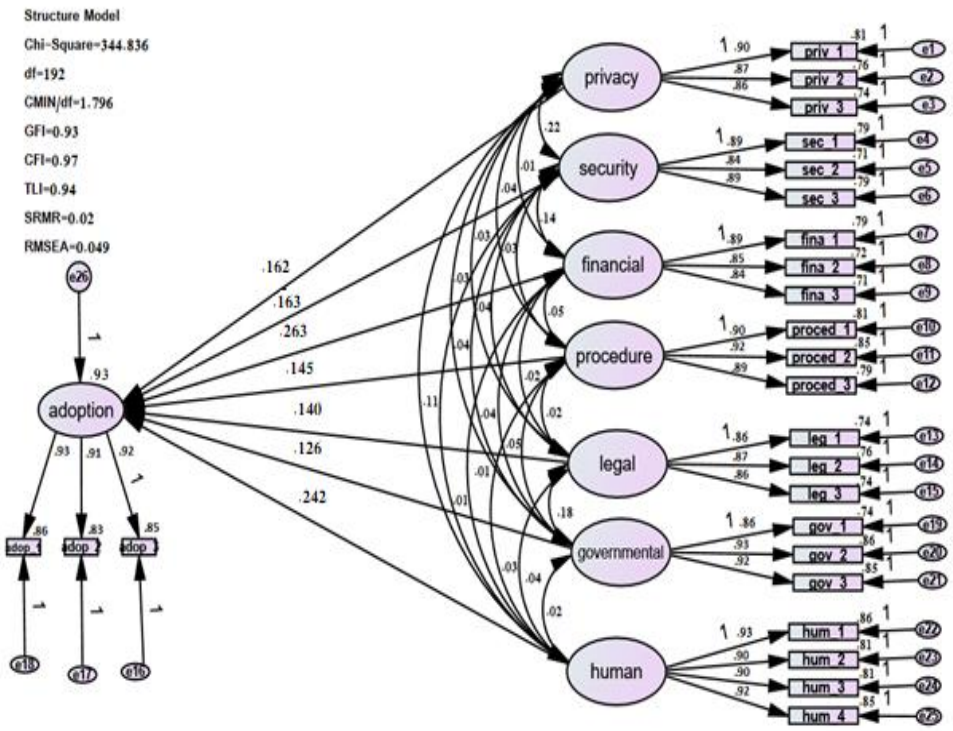
إعتمدت الباحثة فى سبيل إختبار فروض البحث على حزمتى SPSS.V.26 ، AMOS V.26 وهما من أشهر الحزم المستخدمة فى العلوم الإجتماعية. وفى سبيل ذلك إعتمدت الباحثة على نمذجة المعادلة البنائية لإستكشاف العلاقات بين المتغيرات المستقلة والمتغير التابع فى ضوء مؤشرات جودة التوافق للنموذج البنائى للدراسة وذلك كما يلى:

٦-١. تقييم نموذج المعادلة البنائية:

يوضح جدول رقم ٩ والشكل رقم ٢ مؤشرات جودة توافق نموذج الدراسة مقارنة بالقيم الموصى بها من قبل الدراسات السابقة (Chiu et al., 2017; Jere and Ngidi, 2020; Justino et al., 2022; Nguyen et al., 2022) ، وذلك كما يلى:

جدول٩: مؤشرات جودة الملاءمة والمطابقة لنموذج الدراسة

مؤشر جودة التوافق	القيمة المعيارية	TOE-HOT fit
CMIN/df	≤ ٣	١.٧٩٦
GFI	≤ ٠.٩	٠.٩٣٤
CFI	≤ ٠.٩٥	٠.٩٧١
TLI	≤ ٠.٩٠	٠.٩٤٣
SRMR	≤ ٠.٠٨	٠.٠٢٢
RMSEA	≤ ٠.٠٨ – ٠.٠٥	٠.٠٤٩



شكل ٢ : النموذج البنائى لمتغيرات الدراسة

يتضح من الجدول والشكل السابق زيادة جودة توافق نموذج الدراسة وفقاً للقيم المعيارية الموصى بها من قبل الدراسات السابقة، حيث تخطت القيم المعيارية الموصى بها. توضح النتائج أن نسبة كا^{2} إلى درجة الحرية CMIN/df تساوى ١.٧٩٦ وهى أقل من ٣ ، كما أن مؤشر التوافق المقارن CFI يساوى ٠.٩٧ ، ومؤشر جودة التوافق GFI يساوى ٠.٩٣ ، وكذلك مؤشر تاكر لويس TLI يساوى ٠.٩٤ ، بالإضافة إلى جذر متوسط مربعات البواقى SRMR يساوى ٠.٠٢ ، وكذلك جذر متوسط مربعات الخطأ التقريبى RMSEA يساوى ٠.٠٤٩ .

٦-٢. نتائج إختبار فروض البحث:

فى ضوء ما أسفرت عنه نمذجة المعادلة البنائية فى الشكل رقم ٢ ، والجدول رقم ١٠، يمكن عرض نتائج إختبار فروض البحث.

على مستوى العوامل التكنولوجية: أوضحت النتائج ثبوت صحة الفرض الأول، حيث إتضح أن الجاهزية الأمنية التكنولوجية لخصوصية البيانات تؤثر إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. يرجع ذلك إلى أن قيمة الوزن الإنحدارى (H1: B= 0.162, t= 4.81, P= 0.00) وهى دالة معنوياً عند مستوى

٠.٠٥ . وقد أتفقت نتائج الدراسة مع الدراسات التى أكدت على ضرورة الإهتمام بخصوصية البيانات عند تبنى التقنيات والتكنولوجيا الجديدة (Senarathna et al., 2018; Nagahawatta et al., 2021). يرجع ذلك إلى ضرورة الإهتمام بالمصادقة ثلاثية الأبعاد عند تبنى هذه التقنيات، وتشفير البيانات، وإستخدام تقنيات تحسين الخصوصية.

كما إتضح من النتائج أيضاً ثبوت صحة الفرض الثانى، حيث أن الجاهزية الأمنية التكنولوجية لأمن البيانات والمعلومات المحاسبية يؤثر إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. يرجع ذلك إلى أن قيمة الوزن الإنحدارى (H2: B= 0.163, t= 5.52, P= 0.00) وهى دالة معنوياً عند مستوى ٠.٠٥ . وقد أتفقت نتائج الدراسة مع الدراسات التى أكدت على ضرورة الإهتمام بأمن البيانات عند تبنى التقنيات والتكنولوجيا الجديدة (Gangwar et al., 2015; Senarathna et al., 2018; Nagahawatta et al., 2021; Justino et al., 2022; Lutfi et al., 2022). يرجع ذلك إلى أهمية تشفير البيانات والإستثمار فى المنصات الذكية لمشاركة البيانات الخاصة بالتهديدات السيبرانية، والإهتمام بأمن الأجهزة والبرامج المتضمنة فى تقنيتى الواقع الإفتراضى والمعزز.

على مستوى العوامل التنظيمية: أوضحت النتائج ثبوت صحة الفرض الثالث، حيث إتضح أن القدرة المالية للشركة والإستثمار فى أمن البيانات والمعلومات المحاسبية تؤثر إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. يرجع ذلك إلى أن قيمة الوزن الإنحدارى (H3: B= 0.263, t= 8.49, P= 0.00) وهى دالة معنوياً عند مستوى ٠.٠٥. وقد أتفقت نتائج الدراسة مع الدراسات التى أكدت على ضرورة الإهتمام بالقدرة المالية للشركة عند تبنيها للتقنيات والتكنولوجيا الجديدة (Alharbi et al., 2016; Chandra and Kumar, 2018; Jere and Ngidi, 2020; Li, 2020). يرجع ذلك إلى أهمية القدرة والموارد المالية التى تمتلكها الشركات فى إستيعاب التكاليف المرتبطة بهذه التقنيات. مما يؤكد على أهمية القدرة المالية للشركة والإستثمار فى أمن البيانات والمعلومات المحاسبية على تبنى تقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية. يرجع ذلك إلى ضرورة إستيعاب الشركات لتكلفة تنفيذ التكنولوجيا والتدريب على الحد من المخاطر المترتبة على تلك التقنيات، والإهتمام بتنفيذ وصيانة وإنشاء المنصات لمشاركة البيانات الخاصة بالتهديدات السيبرانية.

إتضح من النتائج أيضاً ثبوت صحة الفرض الرابع، حيث أن الإجراءات التنظيمية المتعلقة بأمن البيانات والمعلومات المحاسبية تؤثر إيجابياً على تبنى

الشركات لتقنيتى الواقع الإفتراضى والمعزز. يرجع ذلك إلى أن قيمة الوزن الإنحدارى (H4: B= 0.145, t= 4.79, P= 0.00) وهى دالة معنوياً عند مستوى ٠.٠٥ . وقد أتفقت نتائج الدراسة مع الدراسات التى أكدت على ضرورة الإهتمام بالإجراءات التنظيمية للشركة عند تبنى التقنيات والتكنولوجيا الجديدة (Salleh et al., 2015; Alharbi et al., 2016). يرجع ذلك إلى أهمية الإجراءات التى تقوم بها الشركة لحوكمة تكنولوجيا الأمن السيبرانى ووضع سياسات وإجراءات ومواد تعليمية للأمن السيبرانى وتثقيف المحاسبين لديها حول حماية البيانات والمعلومات المالية وغير المالية. مما يؤكد على أهمية الإجراءات التنظيمية -الداخلية والخارجية- المتعلقة بأمن البيانات والمعلومات المحاسبية على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية.

على مستوى العوامل البيئية: أوضحت النتائج ثبوت صحة الفرض الخامس، حيث إتضح أن وجود إطار قانونى وسياسات ولوائح حكومية يؤثر إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. يرجع ذلك إلى أن قيمة الوزن الإنحدارى (H5: B= 0.140, t= 4.079, P= 0.00) وهى دالة معنوياً عند مستوى ٠.٠٥. وقد أتفقت نتائج الدراسة مع الدراسات التى أكدت على ضرورة الإهتمام بوجود إطار قانونى يحدد جميع الإجراءات القانونية عند تبنى الشركات للتقنيات والتكنولوجيا الجديدة (Alharbi et al., 2016; Nagahawatta et al., 2021; Justino et al., 2022; Lutfi et al., 2022; Nguyen et al., 2022; Thomas and Yao, 2023). يرجع ذلك إلى أهمية وضع اللوائح الحكومية لحماية المستخدمين من المخاطر المرتبطة بهذه التقنيات، بالإضافة إلى القوانين الخاصة بحماية الخصوصية وسرية المعلومات عبر الإنترنت.

إتضح من النتائج أيضاً ثبوت صحة الفرض السادس، حيث أن الدعم الحكومى والإمداد ببرامج الأمن السيبرانى يؤثر إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. يرجع ذلك إلى أن قيمة الوزن الإنحدارى (H6: B= 0.126, t= 3.95, P= 0.00) وهى دالة معنوياً عند مستوى ٠.٠٥. وقد أتفقت نتائج الدراسة مع الدراسات التى أكدت على ضرورة الإهتمام بوجود دعم حكومى يساعد على تبنى الشركات للتقنيات والتكنولوجيا الجديدة (Koduah et al., 2014; Alharbi et al., 2016; Chiu et al., 2017; Jere and Ngidi, 2020; Li, 2020; Nguyen et al., 2022). ويتطلب ذلك قيام الحكومات بالدعم من خلال القيام بمبادرات تدريبية وتوفير جهات إستشارية لتقديم النصح والإرشاد بصدد المنافع والمخاطر الناتجة من الدخول فى عالم إفتراضى رقمى متكامل من خلال التقنيات المدعمة له. أى يؤكد ذلك

على أهمية الدعم الحكومى لبرامج الأمن السيبرانى على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية.

على مستوى العوامل البشرية: أوضحت النتائج ثبوت صحة الفرض السابع، حيث يتضح أن تعليم وتدريب المحاسبين من خلال تقنيتى الواقع الإفتراضى والمعزز يؤثر إيجابياً على تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز. يرجع ذلك إلى أن قيمة الوزن الإنحدارى (H7: B= 0.242, t= 7.437, P= 0.00) وهى دالة معنوياً عند مستوى ٠.٠٥ . وقد أتفقت نتائج الدراسة مع الدراسات التى أكدت على ضرورة الإهتمام بالإستثمار فى الأفراد بصفة عامة والمحاسبين بصفة خاصة مما يساعد على تبنى الشركات للتقنيات والتكنولوجيا الجديدة (Salleh et al., 2015; Alharbi et al., 2016; Chiu et al., 2017; Chandra and Kumar, 2018; Nagahawatta et al., 2021; Meunier et al., 2023). لذا تؤكد نتائج الدراسة على أهمية تعليم وتدريب المحاسبين من خلال تقنيتى الواقع الإفتراضى والمعزز على تبنى الشركات لتلك التقنيات لأتمتة العمليات المحاسبية.

إتضح من النتائج أيضاً أن القدرة المالية للشركة تحتل المرتبة الأولى من بين تلك العوامل، والتى قد ترجع إلى أهمية إمتلاك الشركات للموارد المالية للإستثمار فى تلك التقنيات والأجهزة المرتبطة بحمايتها. كما جاءت العوامل البشرية لتحتل المرتبة الثانية والتى قد ترجع إلى ضرورة الإهتمام بالأمن البشرى من خلال تدريب وتعليم المحاسبين من خلال تقنيتى الواقع الإفتراضى والمعزز. ثم يحتل عاملى أمن البيانات والمعلومات وخصوصية البيانات المرتبة الثالثة والرابعة على التوالى؛ يرجع ذلك إلى ضرورة حماية البيانات والمعلومات المحاسبية وخصوصية البيانات عند تبنى تقنيتى الواقع الإفتراضى والمعزز. كما يحتل عامل الإجراءات التنظيمية (الداخلية والخارجية) المرتبة الخامسة ويرجع ذلك لأهمية تحديد الشركات للسياسات والإجراءات التنظيمية وكذلك السياسات الخاصة بالأمن السيبرانى لحماية البيانات والمعلومات المحاسبية. وأخيراً يحتل وجود إطار قانونى وسياسات ولوائح حكومية وكذلك الدعم الحكومى المرتبة السادسة والسابعة على التوالى؛ مما يؤكد على أهمية العوامل البيئية عند إتخاذ القرار بتبنى الشركات للتكنولوجيا الجديدة.

وأخيراً يتضح من تحليل الإنحدار أن قيمة معامل التحديد R^2 يبلغ ٨٩.٥ % فى ظل إطار TOE. أى أن العوامل التكنولوجية – التنظيمية- البيئية تفسر ٨٩.٥ % من التباين فى تبنى تقنيتى الواقع الإفتراضى والمعزز ، بينما ترجع ١٠.٥% منها إلى عوامل أخرى لم يتناولها الإطار المقترح. كما تبين أيضاً زيادة قيمة R^2 لتصل إلى ٩٣% عند إضافة العامل البشرى المتواجد فى إطار HOT-fit ، وبذلك يتضح تحسن

قيمة معامل التحديد بنسبة ٣.٥ %. يدل ذلك على زيادة القدرة التفسيرية للإطار المقترح فى تفسير تبنى تقنيتى الواقع الإفتراضى والمعزز بالمقارنة باستخدام إطار TOE فقط . وفيما يلى يلخص الجدول رقم ١٠ نتائج فروض الدراسة.

جدول ١٠ : نتائج إختبار فروض الدراسة

الفرض	المسار	قيمة معامل المسار B	قيمة T	المعنوية	نتيجة إختبار الفرض
العوامل التكنولوجية					
H1	adop ← priv	٠.١٦٢	٤.٨١	٠.٠٠	قبول
H2	adop ← sec	٠.١٦٣	٥.٥٢	٠.٠٠	قبول
العوامل التنظيمية					
H3	adop ← fina	٠.٢٦٣	٨.٤٩	٠.٠٠	قبول
H4	adop ← Proced	٠.١٤٥	٤.٧٩	٠.٠٠	قبول
العوامل البيئية					
H5	adop ← leg	٠.١٤٠	٤.٠٧٩	٠.٠٠	قبول
H6	adop ← gov	٠.١٢٦	٣.٩٥	٠.٠٠	قبول
العوامل البشرية					
H7	adop ← hum	٠.٢٤٢	٧.٤٣٧	٠.٠٠	قبول

٧. خلاصة البحث والنتائج والتوصيات:

خلصت الباحثة من الدراسات النظرية والدراسة التطبيقية إلى أن تقنيتى الواقع الإفتراضى والمعزز تعتبر تقنيتان ناشئتان لهما القدرة على إحداث ثورة فى الطريقة التي يتم التفاعل بها مع العالم الخارجى، مما يؤثر أيضاً على المهام التى تقوم بها الشركات. ومع ذلك، تشكل هذه التقنيات أيضاً بعض المخاطر على نظم المعلومات المحاسبية. فمن أبرز هذه المخاطر هى المخاطر الصحية والجسمانية والنفسية التى يمكن أن يتعرض لها المحاسبين؛ عند إستخدام تلك التقنيات. بالإضافة إلى إمكانية إستخدام المتسللين والمهاجمين لتقنيتى الواقع الإفتراضى والمعزز لإنشاء وتزييف البيانات المالية للشركات وسرقة المعلومات المالية الحساسة. وأخيراً، من الممكن إستخدام المهاجمين للواقع الإفتراضى والمعزز لعرقلة العمل الطبيعى لأنظمة المعلومات المحاسبية فى الشركات ومنع المحاسبين من القيام بوظائفهم، ومن ثم تحقيق خسائر مالية للشركة. لذا يتطلب الأمر إتخاذ الشركات العديد من الخطوات لحماية المعلومات المالية من هجمات الواقع الإفتراضى والمعزز عند تبنيهم تلك التقنيات.

وحتى يمكن تخفيض المخاطر المترتبة على تبنى هذه التقنيات، إقترحت الباحثة إطاراً مبنى على إطار كلٍ من TOE، HOT-fit. توصلت الباحثة إلى زيادة جودة توافق نموذج الدراسة وفقاً للقيم المعيارية الموصى بها وفقاً لنمذجة المعادلة البنائية. كما توصلت الدراسة إلى أهمية الجاهزية الأمنية التكنولوجية لخصوصية البيانات وأمنها، والجاهزية التنظيمية لأمن البيانات والمعلومات المحاسبية، بالإضافة إلى أهمية الإمتثال القانونى والدعم الحكومى، وإهتمام الشركات بالأمن البشرى عند تبنى تقنيتى الواقع الإفتراضى والمعزز لأتمتة العمليات المحاسبية.

توصى الباحثة بضرورة إهتمام الشركات بوضع الضوابط التى تساعدها على حماية نظام المعلومات المحاسبى المرتبط بتبنى تلك التقنيات المستحدثة. كما توصى الباحثة بضرورة إهتمام أقسام المحاسبة بكليات التجارة والأعمال فى الجامعات المصرية بدراسة المنافع والمخاطر المترتبة على تبنى تقنيتى الواقع الإفتراضى والمعزز على نظام المعلومات المحاسبى.

فى ضوء ما توصل اليه البحث من نتائج وتوصيات، ظهرت بعض المجالات البحثية المرتبطة بموضوع البحث والتى يمكن تناولها فى البحوث المستقبلية ومنها: إستخدام إطار قبول التكنولوجى لدراسة تبنى تقنيتى الواقع الإفتراضى والمعزز فى المجال المحاسبى، وكذلك دراسة أثر تطبيق تقنيتى الواقع الإفتراضى والمعزز على التعليم المحاسبى وزيادة كفاءة المحاسبين، بالإضافة إلى دراسة تأثير تبنى تقنية الواقع الإفتراضى على إجراءات المراجعة، وكذلك دراسة ملامح التقارير المالية فى ظل وجود عالم إفتراضى رقمى متكامل مثل الميتافيرس، ودراسة تأثير الواقع الإفتراضى على المراجعة الداخلية، بالإضافة إلى دراسة دور القوانين والتشريعات وأهمية إصدار المعايير المالية المرتبطة بالمعاملات المالية فى الميتافيرس. يمكن أيضاً دراسة أثر إستخدام الشركات لتقنية الواقع الإفتراضى على مستقبل التقارير المالية وزيادة كفاءة التحليل المالى للقوائم المالية، وكذلك دراسة أثر إستخدام تقنية الواقع الإفتراضى فى تعزيز وترشيد القرارات المالية. كما يمكن دراسة أثر إستخدام تقنية الواقع المعزز على زيادة كفاءة العمليات المحاسبية. يمكن أن تتعرض البحوث المستقبلية أيضاً لدراسة أفاق وتحديات إستخدام تقنيتى الواقع الإفتراضى والمعزز على نظام المعلومات المحاسبى، وأخيراً دراسة المخاطر الأخرى- بخلاف المذكورة فى البحث- التى يمكن أن تواجه نظام المعلومات المحاسبى عند دخول الشركات للعالم الإفتراضى وكيفية تجنب هذه المخاطر.

تعارض المصالح: تقر الباحثة أنه لا يوجد أى تعارض مصالح جراء نشر هذا البحث.

التمويل: لم تتلق الباحثة أى منحة أو تمويل من أى جهة.

قائمة المراجع

المراجع باللغة العربية:

- الاستراتيجية الوطنية للأمن السيبرانى ،٢٠١٧ ، المجلس الأعلى للأمن السيبرانى، رئاسة مجلس الوزراء، جمهورية مصر العربية.
- القمة العالمية للحكومات ، آرثر دي ليتل، ٢٠٢٣ ، " تنظيم عالم الميتافيرس الافتراضى: الحوكمة ودورها الأساسى فى دخول عالم الميتافيرس الافتراضى وتطويره" ، ١-٣٨.
- الكويتى ، محمد ، ٢٠٢٣ ، الأمن السيبراني في ٢٠٢٣: تحولات وتحديات عصر الذكاء الاصطناعي، ١-١٨ . https://trendsresearch.org/ar/insight
- المعهد القومى للحوكمة الرشيدة والتنمية المستدامة، ٢٠٢٢، الحوكمة والعاصمة الإدارية الجديدة، مجلة الحوكمة والتمية المستدامة، ١-٩٦.

المراجع باللغة الإنجليزية:

- Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence – Issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371–379.
- *Acronis Cyber Protection Week Global Report. (2022). Introduction and survey methodology*, 1-29. www.acronis.com.
- Al-Gnbri, M.K., (2022). *Accounting and Auditing in the Metaverse World from a Virtual Reality Perspective: A Future Research*. Journal of Metaverse, 29-41.
- Alharbi, F., Atkins, A., & Stanier, C. (2016). Understanding the determinants of Cloud Computing adoption in Saudi healthcare organisations. *Complex & Intelligent Systems*, *2*(3), 155–171.
- Anastacio, S. (2019). Use of Virtual Reality in Auditing. AGIA Annual National Convention 2019 | October 9, 2019, 1-10.
- Ateş, V. & Gunes, B. (2018). The Factors Affecting Information Technologies Risk Management at Turkey's State Universities. *International Journal of E-business and E-government Studies*, *10*(2), 46-62.

- Baker, J. (2012). *The Technology–Organization–Environment Framework. in Information System Theory: Explaining and Predicting Our Digital Society, Springer Science Business Media, LLC, vol. I, no. 28, 2012.*
- Buck, L., & McDonnell, R. (2022). Security and Privacy in the Metaverse: The Threat of the Digital Human, CHI EA '22, Proceedings of the 1st Workshop on Novel Challenges of Safety, Security and Privacy in Extended Reality, April 29 - May 5, 2022, New Orleans, LA, USA, 1-4.
- Chandra, S. S., & Kumar, K.N. (2018). Exploring Factors Influencing Organizational Adoption of Augmented Reality in E-Commerce: Empirical Analysis Using Technology-Organization-Environment Model. International Journal of E. Business and E. Government Studies Vol 10, No 2, 46-62. ISSN: 2146-0744.
- Chiu, C. Y., Chen, S., & Chen, C. L. (2017). An integrated perspective of TOE framework and innovation diffusion in broadband mobile applications adoption by enterprises. International Journal of Management, Economics and Social Sciences (IJMESS) (Vol. 6, Issue 1), 14- 36. ISSN 2304 – 1366.
- Chow, Y. W., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2023). Visualization and Cybersecurity in the Metaverse: A Survey. *Journal of Imaging* (Vol. 9, Issue 1), 1-15.
- Chukwuani, V. (2022). Virtual Reality and Augmented Reality: Its Impact in the Field of Accounting. Contemporary Journal of Management, 35-40, ISSN 2766-1431, Published by Air Journals https://airjournal.org/cjm.
- Chukwunonso, A., Njoku, J. N., Lee, & Kim, D.-S. (2022). Security in Metaverse: A Closer Look, Working Paper, 1-2, https://www.researchgate.net/publication/358948229.
- Dai, J., & Vasarhelyi, M. A. (2016). Imagineering audit 4.0. Journal of Emerging Technologies in Accounting 13(1), 1–15. https://doi.org/10.2308/jeta-10494.
- Dunnett, K., Pal, S., Jadidi, Z., & Jurdak, R. (2023). The Role of Cyber Threat Intelligence Sharing in the Metaverse. *IEEE Internet of Things Magazine, 6*(1), 154–160.
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D.,

Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 66, 1-25, https://doi.org/10.1016/j.ijinfomgt.2022.102542.

- Egiyi, M. (2022). *The Benefits of Augmented and Virtual Reality In The Accounting Field.* Contemporary Journal of Management (CJM Vol. 4, No. 1), 15-21.
- Faizal, S., Jaffar, N., & Mohd nor, A. S. (2022). Integrate the adoption and readiness of digital technologies amongst accounting professionals towards the fourth industrial revolution. *Cogent Business and Management*, *9* (1), 1-14.
- Fernandez, C. & Hui, P. (2022). Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse, 1-7. https://doi.org/10.13140/RG.2.2.35094.63042.
- Financial Reporting Council (FRC). (2021). Virtual And Augmented Reality in Corporate Reporting Digital Future of Corporate Reporting, 1-28. https://www.frc.org.uk/Lab.
- Gangwar, H., Date, H., & 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.
- Göçen, A. (2022). Metaverse In the Context of Education. Uluslararası Batı Karadeniz Sosyal ve Beşeri Bilimler Dergisi, 1-26. https://doi.org/10.46452/baksoder.1124844.
- Hapsari, W. P., Labib, U. A., Haryanto, H., & Safitri, W. (2021). *A Literature Review of Human, Organization, Technology (*HOT)-Fit Evaluation Model. Advances in Social Science, Education and Humanities Research, volume 541 Proceedings of the 6th International Seminar on Science Education (ISSE 2020), 876-833.
- Huq, N., Reyes, R., Lin, P., & Swimmer, M. (2022). Metaverse Or Metaworse? Cybersecurity Threats Against the Internet of Experiences. Published by Trend Micro Research, 1-24. www.trendmicro.com.

– Imene, F., Imhanzenobe, J. (2020). Information technology and the accountant today: What has really changed? Journal of Accounting and Taxation, 12(1), 48–60. https:// doi.org/ 10.5897/jat2019.0358.
– Jaber, T. A. (2022). Security Risks of the Metaverse World. International Journal of Interactive Mobile Technologies, 16(13), 4–14. https://doi.org/10.3991/ijim.v16i13.33187.
– Jere, J. N., & Ngidi, N. (2020). A technology, organisation and environment framework analysis of information and communication technology adoption by small and medium enterprises in Pietermaritzburg. South African Journal of Information Management, 22(1), 1-9. https://doi.org/10.4102/sajim.v22i1.1166.
– Johan, S. (2022). "Metaverse And Its Implication in Law and Business," Jurnal Hukum Progresif, vol. 10, no. 2, 153-166, Oct. 2022. https://doi.org/10.14710/jhp.10.2.153-166.
Hornik, S., & Thornburg, S. (2010). Really engaging accounting: Second LifeTM as a learning platform. Issues in Accounting Education, 25(3), 361–378. https:// doi.org/10.2308/ iace .2010.25.3.361
– Justino, M. V., Tengeh, R. K., & Twum-Darko, M. (2022). A Revised Technology–Organisation–Environment Framework for Brick-and-Mortar Retailers Adopting M-Commerce. *Journal of Risk and Financial Management*, *15*(7), 1-18. https://doi.org/10.3390/jrfm15070289.
– Katterbauer, K., Syed, H., & Cleenewerck, L. (2022). *Financial cybercrime in the Islamic Finance Metaverse*. Journal of Metaverse, 56-61.
– Khwaji, A., Alsahaf, Y., & Hussain, F. (2022). Conceptual Framework of Blockchain Technology Adoption in Saudi Public Hospitals Using TOE Framework. IN Advances in Network-Based Information Systems, *Springer* Nature Switzerland AG 2022.
– Koduah, S., Popovsky, B., & Tsetse, A. (2014). Barriers to government cloud adoption. International Journal of Managing Information Technology, 1-15. https:// www.researchgate.net/ publication/ 268746006.
– Kohnke, A. (2020). The Risk and Rewards of Enterprise Use of Augmented Reality and Virtual Reality. ISACA Journal Vol 1, 16- 23.
– Lee, L.-H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A., Bermejo, C., & Hui, P. (2021). All One Needs to Know about Metaverse:

A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda. Journal Of L At Ex Class Files, 14 (8), 1-66. Https://Www.Roblox.Com/

- Li, J. (2020). Roles of individual perception in technology adoption at organization level: Behavioral model versus toe framework. *Journal of System and Management Sciences*, *10*(3), 97–118. https://doi.org/10.33168/JSMS.2020.0308.
- Lutfi, A., Alsyouf, A., Almaiah, M. A., Alrawad, M., Abdo, A. A. K., Al-Khasawneh, A. L., Ibrahim, N., & Saad, M. (2022). Factors Influencing the Adoption of Big Data Analytics in the Digital Transformation Era: Case Study of Jordanian SMEs. Sustainability (Switzerland), 14(3), 1-17. https://doi.org/10.3390/su14031802.
- Meraghni, O., Bekkouche, L., & Demdoum, Z. (2021). Impact Of Digital Transformation on Accounting Information Systems-Evidence from Algerian Firms. Economics and Business 35, 249–264. https://doi.org/10.2478/eb-2021-017.
- Meunier, P. Y., Raynaud, C., Guimaraes, E., Gueyffier, F., & Letrilliart, L. (2023). Barriers and Facilitators to the Use of Clinical Decision Support Systems in Primary Care: A Mixed-Methods Systematic Review. Annals of Family Medicine.Vol. 21, Issue 1, 57–69. Annals of Family Medicine, Inc. https://doi.org/10.1370/afm.2908.
- Moraes, A., Carvalho, A. M., & Sampaio, P. (2023). Lean and Industry 4.0: A Review of the Relationship, Its Limitations, and the Path Ahead with Industry 5.0. *Machines*, Vol. 11, Issue 4, 1-25. MDPI. https://doi.org/10.3390/machines11040443.
- Moscato, D. & Moscato, E. (2011). An Evaluation of the Use of a Virtual World Experiential Case Study to Teach Information Systems Auditing Skills. Communications of the IIMA (Vol. 11), 1-17. http://scholarworks.lib.csusb. edu /ciima Availableat: http: //scholarworks.lib.csusb.edu /ciima/vol11/iss1/1
- Nagahawatta, R., Warren, M., Lokuge, S., & Salzman. S. (2021). Security and Privacy Factors Influencing the Adoption of Cloud Computing in Australian SMEs, 1-9, Twenty-fifth Pacific Asia Conference on Information Systems, Dubai, UAE. https://www.researchgate.net/publication/352968387_Security_and_Priva

cy_Factors_Influencing_the_Adoption_of_Cloud_Computing_in_Australian_SMEs

- Narin, N. (2021). A Content Analysis of the Metaverse. Journal of Metaverse 1 (1), 17-24. www.secondlife.com.
- Nguyen, T. H., Le, X. C., & Vu, T. H. L. (2022). An Extended Technology-Organization-Environment (TOE) Framework for Online Retailing Utilization in Digital Transformation: Empirical Evidence from Vietnam. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(4), 1-22. https://doi.org/10.3390/joitmc8040200.
- Pietro, R., & Cresci, S. (2021). Metaverse: Security and Privacy Issues. Proceedings - 2021 3rd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2021, 281–288. https: //doi.org/10.1109/ TPSISA52974. 2021 .00032.
- Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences (Switzerland)* (Vol. 12, Issue 24). MDPI, 2-23, https://doi.org/10.3390/app122412993.
- PWC. (2019). Seeing Is Believing How virtual reality and augmented reality are transforming business and the economy. 1-20, pwc.com/SeeingIsBelieving.
- Saeidi, H., Prasad, B., & Saremi.H. (2015). The Role of Accountants in Relation to Accounting Information Systems and Difference between Users of AIS and Users of Accounting. Bulletin of Environment, Pharmacology and Life Sciences. Vol 4 [11], 115-123.
- Salleh, K., Janczewski, L., & Beltran, F. (2015). SEC-TOE Framework: Exploring Security Determinants in Big Data Solutions Adoption. PACIS 2015 Proceedings. 203, 1-11. http://aisel.aisnet.org/pacis2015/203.
- Sebastian, G. (2022). A Study on Metaverse Awareness, Cyber Risks, and Steps for Increased Adoption. *International Journal of Security and Privacy in Pervasive Computing*, *14* (1), 1–11. https://doi.org/10.4018/ijsppc.308785.
- Sebastian, G. (2023). A Descriptive Study on Metaverse. *International Journal of Security and Privacy in Pervasive Computing*, *15*(1), 1–14. https://doi.org/10.4018/ijsppc.315591.
- Senarathna, I., Wilkin, C., Warren, M., Yeoh, W., & Salzman, S. (2018). Factors That Influence Adoption of Cloud Computing: An Empirical

Study of Australian SMEs. Australasian Journal of Information Systems Senarathna (Vol. 22), 1-31.

- Sia, C. (2023). The Role of Legal Governance Framework in the Metaverse World, in title: Strategies and Opportunities for Technology in the Metaverse World, 321–330. https://doi.org/10.4018/978-1-6684-5732-0.ch017.
- Smaili, N., & de Rancourt-Raymond, A. (2022). Metaverse: welcome to the new fraud marketplace. Journal of Financial Crime, 1-13. https://doi.org/10.1108/JFC-06-2022-0124.
- Soliman, M., Darwish, A & Hassanien, A. (2023). The Threat of the Digital Human in the Metaverse: Security and Privacy. IN The Future of Metaverse in the Virtual Era and Physical World, *Springer*.
- Techamontrikul, S. (2022). Metaverse On The Board,s Agenda, Deloitte , 1-3. https://www2.deloitte .com/content/dam/ Deloitte/th/Documents /audit/th-metaverse-on-the-board-agenda-EN.pdf.
- Thomas, D., & Yao. Y. (2023). Technology-Organization-Environment Meta-Review and Construct Analysis: Insights for Future Research. Proceedings of the 56th Hawaii International Conference on System Sciences, 5811-5821, URI: https://hdl.handle.net/10125/103341.
- Tlili, A., Huang, R., Shehata, B., Liu, D., Zhao, J., Metwally, A. H. S., Wang, H., Denden, M., Bozkurt, A., Lee, L. H., Beyoglu, D., Altinay, F., Sharma, R. C., Altinay, Z., Li, Z., Liu, J., Ahmad, F., Hu, Y., Salha, S., & Burgos, D. (2022). Is Metaverse in education a blessing or a curse: a combined content and bibliometric analysis. Smart Learning Environments 9 (1), 1-31. Springer. https://doi.org/10.1186/s40561-022-00205-x
- Vargas, D. G. M., Vijayan, K. K., & Mork, O. J. (2020). Augmented reality for future research opportunities and challenges in the shipbuilding industry: A literature review. Procedia Manufacturing, 45, 497–503. https://doi.org/10.1016/j.promfg.2020.04.063.
- Vyas, K. (2021). What Is the Metaverses and How Do Enterprises Stand to Benefit? 1-4, https:// www.itbusinessedge .com/ networking/ metaverse - enterprises-benefits/.

- Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers and Security*, *87*, 1-13. https://doi.org/10.1016/j.cose.2019.101589.
- Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy, 1-31. https:// doi.org/ 10.1109/COMST.2022.3202047.
- Xiao, X. (2023). Metaverse and Its Efforts on Auditing. Frontiers in Business, Economics and Management. Vol. 7, No. 1, 85-87, ISSN: 2766-824X.
- Xu, J., & Lu, W. (2022). Developing a human-organization-technology fit model for information technology adoption in organizations. *Technology in Society*, *70*, 1-11, https://doi.org/10.1016/j.techsoc.2022.102010.
- Zadorozhnyi, Z.-M., Muravskyi, V., Humenna-Derij, M., & Zarudna, N. (2022). Innovative Accounting and Audit of Metaverse Resources. *Marketing and Management of Innovations*, *13*(4), 10–19. https://doi.org/10.21272/mmi.2022.4-02.

ملحق البحث: قائمة الإستقصاء

	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
المحور الثانى: التحديات والمخاطر التى يمكن أن تواجه نظام المعلومات المحاسبى عند تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز					

١. تكلفة الاستثمار والعوامل البشرية والثقافية						
١. زيادة تكلفة الإستثمارات لإنشاء تقنيات واقع إفتراضى ومُعزز.						
٢. زيادة تكاليف تطوير التطبيقات والبيئات الإفتراضية.						
٢. المخاطر المرتبطة بتجربة المستخدم						
٣. معاناة المحاسبين من الدوار والغثيان جراء الدخول للعالم الإفتراضى.						
٤. وجود أخطاء فنية قد تؤدى إلى عدم إتمام المعاملات فى الوقت المناسب.						
٥. عدم ثقة المحاسبين فى التقنيات الجديدة.						
٣. المخاطر الأمنية المرتبطة بتبنى تقنيتى الواقع الإفتراضى والمعزز						
المخاطر المرتبطة بأمن أجهزة الواقع الإفتراضى والمعزز (الثغرات الأمنية):						
٦. إحتمالية تعرض أمن أجهزة الواقع الإفتراضى والمعزز للهجمات الإلكترونية.						
٧. إحتمالية حجب المهاجمين لسماعات الواقع الإفتراضى مجال رؤية المحاسب.						
٨. تمكن المهاجمين من الوصول إلى بيانات تتبع الحركة الخاصة بسماعات الرأس الخاصة بالواقع الإفتراضى للمحاسبين.						
٩. إحتمالية تعرض المحاسبين عند إستخدام تقنية الواقع المعزز لرفض الخدمة الموزعة.						
١٠. إحتمالية تحكم المهاجمين للأجهزة المتصلة عن بُعد، وسرقة المعلومات المالية الخاصة بالشركة من خلال الهجوم على الأجهزة المستخدمة من قبل المحاسب.						
١١. إحتمالية التعرض لهجوم إنتحال الهوية والتعرض لمشكلة مصادقة الصور الرمزية						
١٢. إمكانية حدوث إنتهاجات للحوسبة السحابية.						
١٣. إحتمالية تلاعب المهاجمين بالهويات المزيفة والمسروقة.						
١٤. يمكن للبرامج الضارة "تعمية" المحاسب مؤقتاً للحصول على بيانات ومعلومات الشركة.						
١٥. إمكانية إستخدام المحاسبين للبرامج الضارة.						
المخاطر المرتبطة بفقدان البيانات والمعلومات المحاسبية						
١٦. قد تتعرض البيانات التى يتم جمعها أو إنشاؤها بواسطة الأجهزة القابلة للإرتداء والمستخدمين / الصور الرمزية للعديد من التهديدات.						
١٧. قد تتعرض الأجهزة القابلة للإرتداء- والتى يرتديها المحاسبين- لتهديدات العبث بالبيانات، وإدخال البيانات الخاطئة من المهاجمين.						
١٨. يمكن العبث بالبيانات والمعلومات المحاسبية للشركات من خلال الأجهزة التى يرتديها المحاسبين للدخول فى عالم إفتراضى رقمى متكامل .						
١٩. يمكن للمهاجم إعادة إنشاء كلمات مرور المستخدمين بسهولة عند تتبعه حركة الأصبع للكتابة على لوحات المفاتيح الإفتراضية.						
٤. مشاكل الخصوصية المرتبطة بتبنى تقنيتى الواقع الإفتراضى والمعزز						
٢٠. قد يستطيع المهاجمون الوصول إلى البيانات الأولية للمستخدمين والهجوم عليهم بإستخدام الهجمات المتقدمة.						
٢١. يمكن تسرب خصوصية المستخدمين فى طبقة معالجة البيانات وطبقة التخزين السحابى						
٢٢. يمكن إختراق الأجهزة الطرفية لكل من الواقع الإفتراضى والمعزز						
٢٣. قد تتعرض البصمات الرقمية للتهديدات فى العالم الإفتراضى						
المحور الثالث: العوامل المؤثرة على تبنى تقنيتى الواقع الإفتراضى والمعزز						
العوامل التكنولوجية						
خصوصية البيانات						
٢٤. أتوقع أن تستخدم تقنيتى الواقع الإفتراضى والمعزز نظام المصادقة						
٢٥. أتوقع إهتمام الشركة باخفاء البيانات المنقولة من المستشعرات قبل مشاركتها مع الخدمات السحابية.						
٢٦. أتوقع إهتمام الشركة بطرق مصادقة ثلاثية الأبعاد عند تبنى تقنيتى الواقع الإفتراضى والمعزز.						
أمن البيانات						
٢٧. أتوقع أن تعمل تقنيتى الواقع الإفتراضى والمعزز بطريقة مشفرة						

٢٨.أتوقع أن تنضم الشركة وتستثمر فى منصات مشاركة البيانات الخاصة بالتهديدات السيبرانية عند تبنيها تقنيتى الواقع الإفتراضى والمعزز					
٢٩.أتوقع أن يتم فرض رقابة صارمة على الشركة فى الوصول إلى معلومات عن شركاء الأعمال					
العوامل التنظيمية					
القدرة المالية للشركة					
٣٠.أعتقد أن الشركة لديها القدرة على استيعاب تكلفة تنفيذ التكنولوجيا والتدريب على الحد من المخاطر المترتبة تلك التقنيات					
٣١.اعتقد أن الشركة لديها المقدرة على دفع التكاليف الخاصة بتنفيذ وصيانة وإنشاء المنصات لمشاركة البيانات الخاصة بالتهديدات السيبرانية الخاصة بتقنية الواقع الإفتراضى والواقع					
٣٢.يعد الوصول إلى التمويل الكافى محدداً هاماً لتبنى التكنولوجيا الجديدة					
الإجراءات التنظيمية					
٣٣.أعتقد أن الشركة تهتم بترسيخ ثقافة التعليم المستمر					
٣٤.أعتقد أن الشركة تهتم بتوطيد ثقافة الأمن السيبرانى لدى العاملين					
٣٥.أعتقد أن الشركة سوف تهتم بوضع الإجراءات الداخلية والخارجية المرتبطة بإستخدام تقنيتى الواقع الإفتراضى والمعزز					
العوامل البيئية:					
الإطار القانونى					
٣٦.أتوقع وضع اللوائح الحكومية بدرجة كافية لحماية المستخدمين من المخاطر المرتبطة بتبنى تقنيتى الواقع الإفتراضى والمعزز					
٣٧.أتوقع الإهتمام بوضع قوانين حماية الخصوصية وسرية المعلومات عبر الإنترنت.					
٣٨.أتوقع وضع التشريعات التى تحمى مستخدمى تقنيتى الواقع الإفتراضى والمعزز.					
الدعم الحكومى					
٣٩.أتوقع وضع الحكومات لسبل الدعم للتكنولوجيا الجديدة					
٤٠.أتوقع وضع الحكومات لمبادرات تدريبية للأفراد على إستخدام تقنيتى الواقع الإفتراضى والمعزز					
٤١.أتوقع توفير الحكومات لجهات إستشارية تساعد على توفير النصح والإرشاد بصدد المنافع والمخاطر الناتجة من الدخول فى العوالم الإفتراضية والتقنيات المدعمة لها مثل تقنيتى الواقع الإفتراضى والمعزز					
البعد البشرى					
تدريب وخبرة المحاسبين					
٤٢.ترحب الشركة دائما بتدريب المحاسبين على التقنيات الجديدة قبل إستخدامها					
٤٣.أعتقد أن الشركة ستهتم بتدريب المحاسبين من خلال تقنيتى الواقع الإفتراضى والمعزز.					
٤٤.أعتقد أن الشركة تمتلك موارد بشرية كافية بالمهارات اللازمة لاستخدام التقنيات الجديدة.					
٤٥.سوف يلقى تبنى تقنيتى الواقع الإفتراضى والمعزز قبول المحاسبين فى الشركة					
تبنى الشركات لتقنيتى الواقع الإفتراضى والمعزز					
٤٦.أعتقد أن الشركة تنوي إعتماد تقنية الواقع الإفتراضى والمعزز فى المستقبل					
٤٧.من المفيد للشركة إستخدام تقنيتى الواقع الإفتراضى والمعزز					
٤٨.من المتوقع أن إعتماد الواقع الإفتراضى والمعزز سيفيد الشركة إلى حد كبير					