مجلة الاسكندرية للبحوث المحاسبية
قسم المحاسبة والمراجعة
العدد الثالث – سبتمبر 2022 – المجلد السادس

مدخل مقترح لمواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى

د/ مروة إبراهيم ربيع
أستاذ مساعد بقسم المحاسبة والمراجعة
كلية التجارة – جامعة الإسكندرية

ملخص البحث

يهدف البحث إلى إقتراح مدخل لمواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. يتكون المدخل المقترح من ثلاثة أبعاد وهم المورد البشرى، والعملية، والتكنولوجى؛ لما لهم من أهمية فى مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء. قامت الباحثة باختبار فروض البحث من خلال القيام بدراسة تجريبية وتوزيع قائمة استقصاء على عينة الدراسة فى العديد من القطاعات ذات العلاقة بموضوع البحث. تم ارسال قائمة الإستقصاء لكل المهندسين المختصين بالنظم وتكنولوجيا المعلومات والمحاسبين (تم استقبال عدد 78 مفردة صالحة للتحليل الإحصائى)؛ وذلك لغرض الاجابة على تساؤلات البحث واختبار فروضه. استخدمت الباحثة برنامج SPSS الاصدار 26 لاستكشاف البيانات من خلال إستخدام التحليل الوصفى للعبارات المتضمنه فى قائمة الاستقصاء ، واستخدام الإختبارات الإحصائية اللامعلمية لإختبار فروض البحث. توصلت نتائج الدراسة إلى أهمية المدخل المقترح فى مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. أوصت الدراسة بالعديد من التوصيات ولعل من أهمها ضرورة إهتمام أقسام المحاسبة بكليات التجارة فى الجامعات المصرية بدراسة المقررات البينية فى المجالات المختلفة لتوضيح منافع ومخاطر تبنى أدوات الثورة الصناعية الرابعة على نظام المعلومات المحاسبى. عرضت الدراسة أيضاً العديد من المجالات البحثية المرتبطة بموضوع البحث.

الكلمات المفتاحية: تكنولوجيا إنترنت الأشياء، نظام المعلومات المحاسبى، الأمن السيبرانى، تقنية البلوك تشين.

E.mail: marwa.rabie2@gmail.com

A proposed Approach for Facing IOT Adoption Risks on AIS

Abstract

This paper aims to propose an approach to mitigate IoT adoption risks on AIS. This proposed approach is based on three main dimensions: people, process, and technology. These dimensions are significant on IoT adoption risks mitigation. An experimental study was conducted to test research hypotheses. Participants from different related economic sectors are asked to respond to a questionnaire conducted in experimental settings for the purpose of hypotheses testing. They include IS and IT professionals, and accountants. Questionnaires are sent to these participants, however only 78 valid responds are received. SPSS 26 was used for data analysis. First, research questions were explored through descriptive analysis. Then, non-parametric tests were performed. Results revealed the importance of proposed approach for IoT-based accounting information systems adoption risk mitigation. Finally, Numerous recommendations arises. Mainly, raising awareness of accounting academic departments in Egyptian universities of studying interdisciplinary courses that clarify prospects and risks of Industry 4.0 tools adoption for accounting information systems. This paper refers to numerous research fields related to research problem.

Keywords: internet of things, AIS, cyber security, blockchain.

1- مقدمة

ساهم التطور السريع لتكنولوجيا المعلومات وإستخدام الإنترنت في أواخر القرن العشرين وأوائل القرن الحادى والعشرون، وإدخاله فعلياً في جميع مجالات الحياة البشرية إلى العديد من المميزات. تتمثل تلك المميزات فى توفير الوقت والتكاليف والحصول على الموارد فى الوقت المناسب. كما أدى إنتشار الإنترنت إلى اهتمام الشركات أيضاً بإستخدام إنترنت الأشياء وبصفة خاصة إنترنت الأشياء فى الصناعة. يستخدم إنترنت الأشياء شبكة من الأجهزة تتضمن أجهزة إستشعار ومشغلات وأجهزة كمبيوتر، بالإضافة إلى مجموعة من البرامج وأجهزة إتصال تسمح لهذه الأشياء بالتفاعل والإتصال والتواصل مع بعضها البعض. أى يتضمن إنترنت الأشياء مجموعة متنوعة من الكائنات (الأشياء) التى يمكن توصيلها بإستخدام شبكات لاسلكية أو سلكية بحيث تحتوى هذه الكائنات على عنوان فريد يسمح لها بالتفاعل مع بعضها البعض لإنشاء تطبيقات وخدمات جديدة، مما يساعد على توفير المعلومات فى الوقت المناسب (Payne,2019 ; Atlam and wills, 2020).

وفقاً لتقرير ماكينزى حول التأثير الإقتصادى لإنترنت الأشياء على مستوى العالم، بحلول عام 2025 سيتراوح قيمة ما يتم إستخدامه من إنترنت الأشياء فى مجال التصنيع من 2,7 إلى 6,2 تريليون دولار (Tavana et al.,2020, P.1). يرجع ذلك إلى أن تبنى تكنولوجيا إنترنت الأشياء فى الصناعة يؤدى إلى توفير التكاليف وزيادة المراقبة والتتبع، ومراعاة إجراءات السلامة والأمن فى الشركات (جودة الهواء، ودرجة الحرارة، والرطوبة) وسلامة أنشطة الشركة عن بعد، وإدارة كفاءة الطاقة، وإدارة المخزون.

لذا يمكن القول أن إنترنت الأشياء يمكن أن يلعب دوراً كبيراً فى القريب العاجل فى جميع العمليات وبصفة خاصة العمليات المحاسبية وسيكون جزءاً لا يتجزأ من العمل المحاسبى. يتم ذلك من خلال الإمداد بالبيانات فور حدوثها وتقليص الوقت المستغرق بين حدوث الحدث وتسجيله وإدارة الأصول وتتبعها، وإدارة المخزون. أى يساعد إستخدام إنترنت الأشياء على تجميع المحاسبين للبيانات اللازمة تلقائياً وفى الوقت الفعلى مما يؤدى إلى تحسين الإجراءات المحاسبية. كما يؤدى تبنى تكنولوجيا إنترنت الأشياء إلى تحقيق وفورات فى التكلفة وزيادة الجودة والمراقبة وتحسين عملية التنبؤ وإدارة المخاطر (Moll and Yigitbasioglu,2019; Yilmaz and Hazar,2019) .

وعلى الرغم من المنافع المترتبة على إستخدام إنترنت الأشياء، إلا أنه قد يظهر العديد من المشاكل فى حالة عدم وجود ضوابط أمنية كافية. لأن عدم وجود تلك الضوابط سوف يؤدى إلى إنتهاك الشبكات من قبل القراصنة، مما يؤدى إلى حدوث خلل فى نظام المعلومات المحاسبى

المرتبط بإنترنت الأشياء. لذا يتطلب الأمر ضرورة إهتمام الشركات بقضايا إدارة المخاطر والرقابة الداخلية فى تلك البيئة (Chang et al.,2020). أي يجب الإهتمام بالأمن السيبرانى في بيئة إنترنت الأشياء لحماية البيانات والمعلومات المتولدة منها. يرجع ذلك إلى أن إختراق البيانات المتولدة من إنترنت الأشياء سوف يؤثر على المدخلات والمخرجات المحاسبية، حيث أنه في حالة وجود مدخلات منخفضة الجودة أو عدم وجود بيانات جيدة، فإن المخرجات المترتبة عليها تؤدى إلى إتخاذ قرارات خاطئة(Bhol et al.,2021, Sarwar et al., 2021).

بلغ متوسط الخسارة من إنتهاكات سلامة البيانات على مستوى العالم بأكمله فى عام 2017 ما قيمته 3.62 مليون دولار أمريكى، كما إتضح أن المعلومات المحاسبية والمالية تأتى في المرتبة الثانية لجذب قراصنة الإنترنت (القرصنة الإلكترونية) بعد المعلومات المتعلقة بالعملاء (Ernst and Young,2018). أجرت أيضاً مجموعة Cyber Edge عام 2019 دراسة لتحديد التهديدات الإلكترونية، توصلت الدراسة إلى أن 63% من الشركات الخاصة بعينة الدراسة تعرضت للتهديدات الإلكترونية وكانت من الدول الرائدة هى أسبانيا والمملكة العربية السعودية وكولومبيا. وأوضحت الدراسة أن المصادر الرئيسية للخطر هى البرامج الضارة وهجمات التصيد الإحتيالى، وبرامج الفدية ورفض الخدمة والتلاعب المادى والتلف والسرقة وفقدان البيانات.

وبخصوص الهجمات السيبرانية على مصر، إتضح أن هناك أكثر من 1.5 مليون عملية إكتشاف لبرامج الفدية فى عام 2020، وفى الربع الأول من عام 2021 واجهت مصر وجنوب أفريقيا وتونس أعلى معدلات الإكتشاف فى جميع أنحاء أفريقيا، وتمثل مصر بمفردها ما يقرب من 35% من جميع عمليات إكتشاف برامج الفدية فى أفريقيا (Interpol African Cyber Threat, 2021). لذا فإنه يجب الإهتمام بتطبيق برامج الأمن السيبرانى فى الشركات؛ لتجنب التهديدات السيبرانية (Ponemon Institute ,2019; Haapamäki and Sihavonen,2019)، وبصفة خاصة بعد تطبيق إنترنت الأشياء وربطه بنظام المعلومات المحاسبى. ولن يقتصر الأمر على الشركات فقط، بل يجب أن يتم ذلك على مستوى الدولة بأكملها. وهذا ما قامت به مصر حيث قام المجلس الأعلى للأمن السيبرانى التابع لرئاسة مجلس الوزراء بوضع إستراتيجية وطنية للأمن السيبرانى إستعداداً للأضرار التى يمكن أن تلحق بالدولة ككل نتيجة للتحول الرقمى (الاستراتيجية الوطنية للأمن السيبرانى،2017، المجلس الأعلى للأمن السيبرانى ، رئاسة مجلس الوزراء ، جمهورية مصر العربية).

سوف يؤدى وجود الإستراتيجية الوطنية للأمن السيبرانى إلى تقليل المخاطر التى يمكن أن تتعرض لها الشركات والجهات الحكومية عند تبنى تكنولوجيا إنترنت الأشياء، وبصفة خاصة بعد إعلان مصر فى شهر أكتوبر عام 2021 بإنشاء أول منصة لتكنولوجيا إنترنت الأشياء وبالفعل تم توقيع إتفاقية تعاون بين الشركة المصرية للإتصالات وشركة نوكيا العالمية لبناء تلك المنصة لتقديم خدمات إنترنت الأشياء.

وبالنظر إلى الدراسات يتضح جلياً الإهتمام بتطبيق الأمن السيبرانى وإستخدام إنترنت الأشياء بصورة منفرده، ولكن يتضح فى الوقت الحالي ضرورة نظر كل من الأكاديميين والممارسين إلى كلاهما بصورة متكاملة (Suraj,2021). لذا يتعين ضرورة التفكير والتدبر لوجود حلول فى حالة قيام واحد من آلاف أو ملايين الأجهزة المتصلة بنظام المعلومات المحاسبى بإرسال بيانات ومعلومات غير سليمة، مما يترتب عليه أيضاً إتخاذ قرارات غير صحيحة. لذا تكثر مخاوف الأمن والخصوصية بشأن إنترنت الأشياء، وبالتالي فإن الأمن والخصوصية لهما أهمية قصوى فى عصر إنترنت الأشياء والذى ينطبق على المحاسبة أيضاً .

قد تعتقد الشركات أن فقد أو التلاعب فى البيانات عند تبنى تكنولوجيا إنترنت الأشياء هى مشكلة تقنية فقط يمكن للحلول التكنولوجية معالجتها، ولسوء الحظ فإن التكنولوجيا لا تعد الحل السحرى لحل هذه المشكلة. وقد يكون السبب فى ذلك هو عدم تدريب المورد البشرى بصورة كافية على تلك التكنولوجيا، بالإضافة إلى عدم وجود إجراءات مناسبة لحماية هذه البيانات (Ernst and Young, 2011; Janes 2012) . يؤكد ذلك على أهمية وجود مدخل لمواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى.

1-1 مشكلة البحث

تسعى الشركات فى الوقت الراهن إلى الاستفادة من الإنترنت كمورد عالمى لتخفيض التكلفة وزيادة رضاء الموظفين والعملاء، مما يؤدى إلى تحقيق مزايا تنافسية للشركات وتحسين انتاجيتهم فى أعقاب إستخدام إنترنت الأشياء. وعلى الرغم من المزايا المتحققة من إستخدام إنترنت الأشياء فى الشركات، إلا أن الأمر يتطلب حماية خصوصية وأمن البيانات والمعلومات المحاسبية المرتبطة بتطبيق إنترنت الأشياء. يرجع ذلك إلى أنه يمكن فقدان أو إتلاف أو الإستخدام غير المصرح به للبيانات والمعلومات المحاسبية فى ظل تلك البيئة. وبصفة خاصة أن عدم وجود إهتمام كافى بالأمن السيبرانى لإنترنت الأشياء يرجع إلى العديد من الأسباب. تتمثل تلك الأسباب فى صعوبة معرفة المنتجات المتصلة بالإنترنت، ومن الذى قام بجمع البيانات، كما قد يكون من غير المجدى

الإستثمار فى الأمن السيبرانى لأجهزة إنترنت الأشياء؛ لإنخفاض قيمة تلك الأجهزة. لذا يتطلب الأمر وجود مدخل لمواجهة مخاطر تبنى تكنولوجيا إنترنت الاشياء على نظام المعلومات المحاسبى. لذا تحاول الدراسة الاجابة على التساؤلات التالية:

- هل يؤدى إهتمام الشركات بوضع الضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبط بالمورد البشرى عند تبنى تكنولوجيا إنترنت الأشياء إلى حماية نظام المعلومات المحاسبى المرتبط به؟
- هل يؤدى إهتمام الشركات بوضع الضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبط بالعملية عند تبنى تكنولوجيا إنترنت الأشياء إلى حماية نظام المعلومات المحاسبى المرتبط به؟
- هل يؤدى إهتمام الشركات بوضع الضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبط بالحلول التكنولوجية عند تبنى تكنولوجيا إنترنت الأشياء إلى حماية نظام المعلومات المحاسبى المرتبط به؟
- هل يؤدى تطبيق المدخل المقترح إلى تحسين أداء الشركات المتبنية لتلك التكنولوجيا فى المستقبل؟

1-2 أهداف البحث

تهدف الدراسة إلى إقتراح مدخل ثلاثى الأبعاد لحماية أمن وخصوصية البيانات والمعلومات المحاسبية المتولدة من تبنى تكنولوجيا إنترنت الأشياء. يتمثل المدخل المقترح فى أهمية المورد البشرى وبصفة خاصة المحاسبين والعمليات الخاصة بالشركة، وكذلك التكنولوجى المستخدم لحماية المعلومات المحاسبية من الفقدان والتلاعب. كما يهدف البحث إلى توضيح تأثير الضوابط المقترحة عند تبنى الشركات لتكنولوجيا إنترنت الأشياء على تحسين أداء الشركات وتحسين الإجراءات المحاسبية.

1-3 أهمية البحث

تتمثل أهمية البحث من **الناحية العملية** فى أن البيانات المحاسبية تعد جزءاً لا يتجزأ من نظام المعلومات المحاسبى. وبالتالي فهى تتطلب إعتبارات خاصة عندما يتم التعامل مع تخزين البيانات ونقلها بطريقة آمنه ومأمونه وبصفة خاصة عندما تنتج هذه البيانات من أجهزة الإستشعار، مما يؤثر على نظام المعلومات المحاسبى بأكمله والقرارات المترتبه عليه. لذا يتضح أن تسريب هذه المعلومات أو البيانات المحاسبية وحدوث هجمات عليها من المتسللين من خلال إختراق شبكات المعلومات، يتطلب الإنتباه لمزيد من الأمن السيبرانى لحماية تلك البيانات والمعلومات داخل نظام المعلومات المحاسبى المرتبط بإنترنت الأشياء. كما تنبع أهمية البحث أيضاً من تناوله للمخاطر

المتعلقة بإنترنت الأشياء والتى تزداد كثيراً عن المخاطر المرتبطة بتطبيق التكنولوجيا الحديثة مثل تكنولوجيا الحوسبة السحابية؛ لأن مخاطر إنترنت الأشياء متضمنه بداخلها مخاطر الحوسبة السحابية لارتباطها بها عند تخزين البيانات والمعلومات المتولدة من إنترنت الأشياء. كما أن إدارة أمن المعلومات فى بيئة إنترنت الأشياء لا تزال فى مهدها، مما يتطلب الأمر ضرورة تطوير آليات الحماية الممكنة فى تلك البيئة.

تتمثل أهمية البحث من **الناحية الأكاديمية** فى أن هذا الموضوع –على حد علم الباحثة– لم يلقى الإهتمام من الدراسات سواء باللغة الأجنبية أو العربية فى المجال المحاسبى وتم تناوله فقط من الناحية التكنولوجية. أى يتطلب الأمر الإهتمام بالضوابط الوقائية لحماية أمن البيانات والمعلومات المحاسبية فى بيئة إنترنت الأشياء، وبصفة خاصة قيام الشركات بممارسة الأعمال فى الوقت الراهن عن بُعد نتيجة إنتشار جائحة فيروس كورونا المستجد والسلالات (المتحورات) المرتبطه به. يتضح أيضاُ أهمية البحث فى توضيح دور المحاسب فى حماية البيانات والمعلومات المحاسبية المتولدة من تكنولوجيا إنترنت الأشياء.

1-4 منهج البحث

يتكون منهج البحث بصفة عامة من ثلاثة عناصر أساسية هى مدخل البحث وأدوات البحث وطريقة البحث. يقوم مدخل البحث على دراسة وتحليل الدراسات السابقة الخاصة المرتبطة بكلٍ من المورد البشرى– العملية– التكنولوجى فى مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. أما أدوات البحث فهى تنقسم إلى مجموعتين، تتمثل المجموعة الأولى فى أدوات البناء النظرى اللازمة لتأصيل واشتقاق فروض البحث. فى حين تتمثل المجموعة الثانية فى أدوات جمع البيانات والتحليل الاحصائى، وفيها اعتمدت الباحثة على توزيع حالتين افتراضيتين على عينة الدراسة وذلك لإختبار فروض البحث. قامت الباحثة أيضاً باستخدام الإختبارات المناسبة لإختبار فروض البحث. أما طريقة البحث فهى تعتمد على إجراء دراسة تجريبية ويتم ذلك من خلال تقديم حالتين افتراضيتين كل حالة مكونة من عدة أسئلة لإختبار فروض البحث وعلى المستقصى منهم الإجابة على الأسئلة التى تلى كل حالة.

1-5 حدود البحث

سوف تعتمد الباحثة على توزيع الحالات التجريبية الخاصة بالدراسة على بعض الشركات المطبقة لأحدث تكنولوجيا التصنيع، بالإضافة إلى بعض المهندسين بوزارة الاتصالات والأمن السيبرانى ذوى الدراية بأهمية تطبيق تكنولوجيا إنترنت الأشياء ؛ لعدم إدراك الكثيرون لتكنولوجيا

إنترنت الأشياء وأهميته التى يمكن تحقيقها منه والمخاطر التى يمكن أن تعوق تطبيقها، لذا يخرج عن نطاق البحث الشركات غير المطبقة لتكنولوجيا المعلومات الحديثة. كما يخرج عن نطاق البحث قطاع الخدمات.

1-6 خطة البحث

فى ضوء مشكلة البحث والهدف منه سوف ينقسم البحث الى الفرعيات التالية: الدراسات السابقة وصياغة فروض البحث، والدراسة التجريبية، وأخيراً خلاصة البحث ونتائجه وتوصياته.

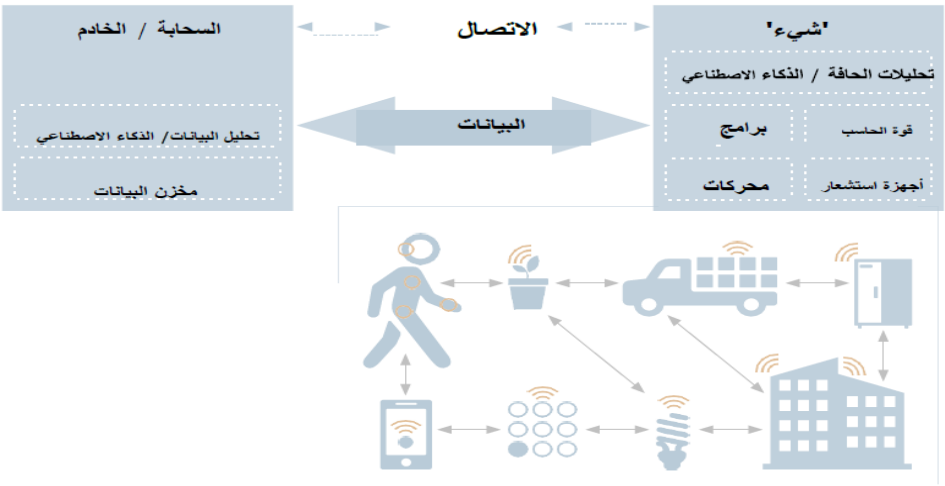
1-7 الدراسات السابقة

تنقسم الدراسات السابقة المتعلقة بموضوع البحث إلى دراسات تهتم بالأطر المفاهيمية والبنية الهندسية (معمارية) إنترنت الأشياء، والمنافع المحاسبية الناتجة عن تطبيق تلك التكنولوجيا، والدراسات التى تناولت المخاطر المرتبطة بتبنى تلك التكنولوجيا من الناحية الفنية (الهندسية) .

1-2 البنية الهندسية (المعمارية) لتكنولوجيا إنترنت الأشياء وأثرها على الإجراءات والعمليات المحاسبية

تم التعرف على مصطلح إنترنت الأشياء فى عام 1999 من قبل كيفين أشتون Kevin Ashton المدير التنفيذى لمركز التعرف التلقائى فى معهد ساتشوستسى للتكنولوجيا. تدور الفكرة الأصلية حول قدرة أجهزة الكمبيوتر على إدارة الأشياء الفردية من خلال تقنية تحديد التردد اللاسلكى (Atlam et al.,2018; Atlam and Wills,2020 ; Valentinetti and Munoz,2021) . أى أنه يمكن القول أن إنترنت الأشياء عبارة عن شبكة شاملة من الأشياء[1] الذكية التى لديها القدرة على التنظيم التلقائى ومشاركة المعلومات والبيانات والموارد والتفاعل والتصرف في مواجهة المواقف والتغيرات فى البيئة. أى أنه يتم التواصل فى ظل تبنى تكنولوجيا إنترنت الأشياء بين الأجهزة وبعضها البعض عن طريق الإنترنت دون تدخل الإنسان. لذا يوضح الشكل التالى بيئة إنترنت الأشياء.

[1] يقصد بالأشياء : أى جهاز يمكن تعريفه على الإنترنت من خلال الصاق عنوان الإنترنت IP (مثل السيارات ، الأدوات المنزلية ، الآلآت ، والسلع والمنتجات،....إلخ)



شكل 1: بيئة إنترنت الأشياء

المصدر: Payne (2019, p.5)

يتضح من الشكل السابق أن النظام البيئى لإنترنت الأشياء يتكون من الأجهزة الذكية التى تدعم الويب والتى تستخدم أنظمة مدمجة، مثل المعالجات وأجهزة الإستشعار وأجهزة الإتصال؛ لجمع البيانات التى يتم الحصول عليها من البيئة المرتبطة بها وإرسالها وإتخاذ القرار بناءً عليها. تشارك أجهزة إنترنت الأشياء بيانات أجهزة الاستشعار التى تجمعها عن طريق الإتصال ببوابة إنترنت الأشياء حيث يتم إرسال البيانات إلى السحابة لتحليلها. فى بعض الأحيان ، تتواصل هذه الأجهزة مع الأجهزة الأخرى ذات الصلة ويتخذ القرار بناءً على المعلومات المتبادلة بين الأجهزة. كما تعمل الأجهزة دون تدخل بشري، إلا فى حالة تفاعل الأشخاص عند إعدادها أو إعطائها تعليمات أو الوصول إلى البيانات من خلال واجهة المستخدم.

زادت قيمة وعدد الأشياء المتصلة بالشبكات على مستوى العالم (Yilmaz and Hazar, 2019; Popescu et al.,2019; Bagay,2020)، حيث بلغ فى عام 2016 6.4 مليار دولار وهو ما يمثل زيادة بنسبة 30% عن عام 2015 ، وفى عام 2020 إزداد إلى 20.8 مليار دولار (Chang et al.,2020). كما أنه من المتوقع فى نهاية عام 2025 وصول عدد الأجهزة المرتبطة بإنترنت الأشياء إلى أكثر من 60 مليار جهاز (Khadam et al.,2020). يهدف إستخدام تكنولوجيا إنترنت الأشياء إلى تقديم البيانات وقت حدوثها عبر الشبكات السلكية واللاسلكية (بلوتوث، تحديد الهوية بموجات الراديو RFID ، ونظام تحديد المواقع العالمى GPS أو الحوسبة السحابية)؛ بهدف الفهم والتواصل ومراقبة العمليات التجارية (Chang et al.,2020). أى تتكون تكنولوجيا

إنترنت الأشياء من إتصال الأشياء بآليات تعريف فريدة مثل أجهزة الأستشعار والأشياء المدمجة مع الإنترنت (Payne,2019; Martens et al.,2021).

تتسم إنترنت الأشياء بالعديد من الخصائص والتى تتمثل فى زيادة عدد أجهزة إنترنت الأشياء وتوليدها لكمية هائلة من البيانات والمعلومات، مما يمكن من إتخاذ قرارات ذكية فى مختلف المواقف. كما تتسم بأنها نظام معقد يتكون من مليارات الأشياء غير المتجانسة والتى تعمل فى بيئة ديناميكية. تتصف أيضاً بوجود طاقة محدودة لأنها مصممة للعمل مع الحد الأدنى من إستهلاك الطاقة، وأخيراً تتميز بالهوية الفريدة من خلال عنوان IP الخاص بها (Atlam andWills,2020).

وللتعرف على أثر تطبيق تكنولوجيا إنترنت الأشياء على العمل المحاسبى، يتطلب الأمر أولاً التطرق إلى الطبقات التى تتكون منها تلك التكنولوجيا. لذا يتم فى الجزء التالى من البحث التطرق إلى الطبقات التى تتكون منها إنترنت الأشياء وأثر تطبيق تلك التكنولوجيا على العمل المحاسبى ومهنة المحاسبة والمراجعة.

2-1-1. الطبقات المكونة لتكنولوجيا إنترنت الأشياء

تعددت الدراسات التى تناولت عدد الطبقات التى تتكون منها تكنولوجيا إنترنت الأشياء فمنها من حددها بثلاث طبقات (Wang, 2016; Change et al.,2020; Haddadpajouh et al., 2021) ، ومنها من حددها بأربع طبقات (Leloglu, 2017) ، ومنها من حددها بخمس طبقات (Lee,2020; Valentinetti and Munoz, 2021) ، ومنها من حددها بسبع طبقات (Atlam and Wills,2020). يمكن القول أن هذه الدراسات تتناول معمارية أو البيئة الهندسية لإنترنت الأشياء، ولكن قد تقوم بعض الدراسات بدمج طبقة أو طبقتين معاً. لذا يتضح وجود خمس طبقات أساسية لإنترنت الأشياء والتى تتمثل فى: **طبقة الإدراك:** وهى الطبقة التى يتم فيها إنتاج البيانات وجمعها من خلال الأجهزة وهى تتكون من تقنية تحدد التردد اللاسلكى التى يمكن توصيلها مباشرة. وتتمثل **طبقة الشبكة** فى طبقة الإتصال وهى الطبقة المسئولة عن نقل البيانات التى تجمعها الطبقة المادية إلى السحابة ووحدات التخزين من خلال إحدى وسائل الاتصال، مثل البلوتوث، الواي فاي، والهاتف المحمول، وغيرها، بحيث يتمكن مستخدم تكنولوجيا إنترنت الأشياء من التواصل مع أجهزتهم. تتسم **طبقة المعالجة** بالتخزين والمعالجة وإمكانيات إتخاذ الإجراءات، وفى هذه الطبقة تقوم البرمجيات بمعالجة البيانات التى يتم جمعها من خلال أجهزة إنترنت الأشياء للحصول على بيانات مُعالجة (معلومات) ذات قيمة للمستخدم. تشمل **طبقة واجهة المستخدم** كافة التطبيقات، حيث تقوم واجهة المستخدم بتزويد البيانات الهامة للمستخدم على هيئة رسائل وإشعارات، بحيث تُمَكِن

المستخدم من عرض جميع البيانات النهائية فى مكان واحد والتفاعل معها. لذا من أمثلة طبقة المستخدم (طبقة التطبيق) إرسال رسائل البريد الإلكتروني، ووجود إشارات التنبيه، ونظام الأمان، وتشغيل أو إيقاف تشغيل الجهاز. وأخيراً تساعد **طبقة إدارة الخدمة والأعمال** على تحليل البيانات وإتخاذ القرارات بناء عليها (Lee,2020; Valentinetti and Munoz, 2021).

أى أن البنية المادية لتكنولوجيا إنترنت الأشياء تتكون من الأشياء وتقنية تحديد التردد اللاسلكى، والشبكات اللاسلكية، والحوسبة السحابية لتخزين البيانات المتولدة من أجهزة الاستشعار والوصول إليها عند الحاجة، بالإضافة إلى البرامج الوسيطة والتى تقوم بربط أجهزة الإستشعار بالسحابة، كما يتطلب الأمر وجود برنامج لتطبيقات إنترنت الأشياء والذى يمكن من التفاعل من جهاز إلى جهاز، ومن جهاز إلى إنسان بطريقة موثوقة.

2-1-2. أثر تطبيق تكنولوجيا إنترنت الأشياء على المحاسبة والمراجعة

تعزز تكنولوجيا إنترنت الأشياء الإقتصاد العالمى وتحدث ثورة فى الكثير من جوانب الأعمال، بما فى ذلك المحاسبة. فمن المتوقع أن يلعب إنترنت الأشياء دوراً كبيراً في القريب العاجل فى المجال المحاسبى وسيكون جزءاً لا يتجزأ من العمل المحاسبى من خلال الإمداد بالبيانات فور حدوثها وإدارة الأصول وإدارة المخزون وتحسين جودة البيانات والمعلومات، بالإضافة إلى تحسين عمليات التخطيط والمراقبة المستمرة للبيانات المحاسبية وإعداد الموازنات التقديرية وتحسين إدارة المخاطر (O'leary,2013; Dai and Ge,2015; Lee and Lee,2015; Leloglu,2017 ; Payne,2019; Yilmaz and Hazar , 2019; Martens et al., 2021).

يتضح تأثير تبنى تكنولوجيا إنترنت الأشياء على المحاسبة المالية والإدارية والتكاليف من خلال القيام بمعالجة الأصول والمخزون بصورة سهلة. يتم ذلك من خلال إمكانية تتبع المخزون آلياً دون وجود جرد دورى من قبل الأشخاص، من خلال إستخدام الأرفف الذكية التى تساعد على وجود سجلات محدثة لحالة المخزون، يمكن من خلالها معرفة رصيد المخزون فى كل الأوقات وبكل سهولة (خميس، 2021). تساعد أيضاً تكنولوجيا إنترنت الأشياء على تتبع ومراقبة مواقع الأصول –والتعرف على اللصوص حال سرقة الأصول– مما يساعد على إنخفاض فرص توقف الإنتاج وإعداد القوائم المالية بسرعة. تلعب تكنولوجيا إنترنت الأشياء أيضاً دوراً هاماً فى إدارة التكلفة والتنبؤ بها من خلال توفير المعلومات فى الوقت الفعلى لحدوث الحدث مما يساعد على تخطيط موارد الشركة بكفاءة (Qiu, 2016; CPA,2019; Payne , 2019; Zhang,2019). يمكن أن يساعد تبنى تكنولوجيا إنترنت الأشياء فى تحليل التكاليف من خلال تتبع أجهزة الإستشعار المسار

الأصلى للمنتج وتسجيل أى إنحرافات عن المسار المحدد له تلقائياً. كما يمكن أن تساعد تكنولوجيا إنترنت الأشياء أيضاً فى تخفيض تكاليف الطاقة من خلال إستخدام أجهزة الإستشعار لقياس الإستخدام الفعلى لطاقة الآلات.

لذا تخلص الباحثة إلى أن المنافع المتولدة من تبنى تكنولوجيا إنترنت الأشياء فى مجال المحاسبة تتمثل فى تحقيق مزايا اقتصادية وتنافسية متمثلة فى تحسين إنتاجية الشركات وتخفيض التكاليف وتخفيض زمن تسليم المنتجات، والمحافظة على المستوى الأمثل للمخزون، وإدارة المخزون، وزيادة جودة المنتجات مما يساعد على ترشيد عملية إتخاذ القرارات، بالإضافة إلى إنشاء المستندات المحاسبية تلقائياً فى الوقت الفعلى، وإصدار التقارير المالية تلقائياً وبجودة عالية (Cao and Zhu,2012; Saif et al.,2015; Qiu, 2016; Wang ,2016; Thangiah et al., 2018; Van Niekerk and Rudman,2019; Yilmaz and Hazar,2019; Tavana et al.,2020; Valentinetti and Munoz,2021; Onyshchenko et al., 2022).

كما يمكن أن يؤثر إستخدام تكنولوجيا إنترنت الأشياء أيضاً بشكل إيجابى على مراجعة حسابات الشركات، حيث تؤدى إلى تغيير الطريقة التى تتم بها عمليات المراجعة لكل جوانب نشاط الشركة. يتم ذلك من خلال إستخدام الطائرات بدون طيار drones [2] لمساعدة مراجع الحسابات فى فحصه للمخزون وبصفة خاصة فى حالة توزيع المخزون فى مناطق عديدة –حيث يتم تحويل الصور الملتقطة عبر الطائرة بدون طيار إلى بيانات قابلة للتحليل– مما يساعد على زيادة جودة عملية المراجعة الخارجية (The Association of Chartered Certified Accountants,2019) .

وبإستطلاع رأى طلاب المحاسبة فى عدة جامعات بأندونيسيا حول مقدرتهم على إجادة إستخدام تكنولوجيا إنترنت الأشياء ومدى إمتلاكهم المهارات المطلوبة لإستخدام إنترنت الأشياء (مثل المهارات الاجتماعية، والتنقل بين المعلومات من خلال القدرة على البحث فى الإنترنت، والمهارات الإبداعية[3]). تم التوصل إلى أهمية متابعة المحاسبين والمراجعين للتطورات الحديثة فى مجال الأعمال وإتقان مهارات إنترنت الأشياء وتحقيق الإبتكار فيما يتعلق بربط إنترنت الأشياء بالعمليات المحاسبية. يؤكد ذلك على ضرورة إدراك طلاب المحاسبة لأهمية إنترنت الأشياء في الأعمال المحاسبية وتحديث مهاراتهم ليتمكنوا من المنافسة فى عالم الأعمال(Hatane et al., 2019) .

[2] تعد الطائرات بدون طيار أحد أمثلة إنترنت الأشياء التى يمكن أن يستخدمها المراجع لحصر المخزون لدى عميل المراجعة.

[3] هى المهارات اللازمة لإنشاء محتوى مناسب ليتم عرضه على الإنترنت مثل انشاء نصوص ومقاطع فيديو.

لذا يجب على المحاسبين فهم الأسس والفرص الناتجة عن إستخدام إنترنت الأشياء والتقنيات والمفاهيم ذات الصلة (Busulwa and Evans,2021).

يتضح مما سبق أهمية تطبيق تكنولوجيا إنترنت الأشياء وربطه بنظام المعلومات المحاسبى؛ لما له من أهمية فى تحسين العمليات والإجراءات المحاسبية وإدارة الأصول وإدارة المخزون وزيادة جودة التقارير المالية وترشيد عملية اتخاذ القرارات. مما يتطلب الأمر إلمام المحاسب بالعديد من المهارات والكفاءات عند ربط تكنولوجيا إنترنت الأشياء بنظام المعلومات المحاسبى. ولكن يجب توخى الحذر أيضاً عند تطبيقه لوجود العديد من العقد ونقاط الإتصال بالإنترنت بدءاً من التقاط البيانات بأجهزة الإستشعار وتخزينها عبر الحوسبة السحابية ومعالجتها وصولاً لنظام المعلومات المحاسبى، مما يؤدى إلى إحتمالية تعرض نظام المعلومات المحاسبى للإختراق وهو ما سوف يتم التعرض له بالمناقشة فى الجزء التالى من البحث.

2-2 المخاطر والتحديات الناتجة عن تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى

تعد تكنولوجيا المعلومات من أهم الأصول قيمة للشركة. يتطلب الأمر عندما تتأثر هذه الأصول بالقرصنة والجرائم الإلكترونية الإهتمام بإدارة المخاطر وأمن المعلومات فى تلك البيئة. لأن تطبيق تلك التكنولوجيا قد تؤثر بشكل كبير على الأداء التشغيلى للشركات (Solms and Sloms,2018; Van Niekerk and Rudman,2019). يرجع تزايد خرق البيانات الناتجة عن تطبيقات الويب إلى أن تطبيقات الويب فى العديد من الشركات ليست مكشوفة فقط، ولكنها تكون حساسة للغاية مقارنة بنقاط الهجوم الأخرى (Sangani and Zarger,2017). لذا قد يؤدى إنشاء البيانات ونقلها فى بيئة إنترنت الأشياء إلى تعرض هذه البيانات والمعلومات للخطر من قبل المهاجمين؛ نتيجة لإنتقال البيانات والمعلومات عبر الشبكات (Saif et al., 2015). ويرجع ذلك إلى أن أجهزة إنترنت الأشياء تصنع بموارد قليلة وبدون إجراءات أمنية كافية (Ghumro et al., 2020; HaddadPajouh et al., 2021). كما يؤدى إختراق بيانات الشركات إلى العديد من الأضرار والتى تتمثل فى فقدان ثقة العملاء وشركاء الأعمال وإنخفاض قيمة الشركة، بالإضافة إلى خروجها من السوق (WatchGuard,2010). لذا سوف يتم فى الجزء التالى من البحث التعرض لأهم الهجمات والمخاطر والتحديات التى يمكن أن تواجه تكنولوجيا إنترنت الأشياء وذلك كما يلى:

2-2-1 هجمات تكنولوجيا إنترنت الأشياء

يوجد العديد من الهجمات على نظم المعلومات فمنها من يستهدف الأجهزة أو الشبكة أو النظام أو التطبيقات من خلال بث البرامج الضارة أو حتى التعرض للمستخدمين أنفسهم من خلال الهندسة الاجتماعية والتصيد الاحتيالى وإختراق برامج التشفير، كما يمكن أن يكون المهاجم من داخل أو خارج الشركة (Kremer et al., 2019; Mohankumar,2019; Atlam and Wills,2020; Demirkan et al., 2020; IoT Alliance Auslralia,2020; Efosa et al., 2021; Muravskyi et al., 2021). تتمثل أهم الهجمات التى يمكن أن تتعرض لها تكنولوجيا إنترنت الأشياء فى هجمات مادية، وهجمات متعلقة بالبرمجيات، وهجمات الشبكات، وأخيراً هجمات التشفير. وذلك كما يلى (Atlam and Wills, 2020).

تتعلق **الهجمات المادية** بإتلاف والعبث بالعقد الخاصة بأجهزة الأستشعار وإستبدالها من قبل المستخدم الضار (المهاجم). يرجع ذلك إلى إستخدام المهاجم علامة تحديد هوية التردد اللاسلكى لتوجيه إشارات مشوشة (noise signals) ، مما يؤثر على جودة الإتصال، كما يمكن للمهاجم أيضاً إستخدام **تداخل الترددات الراديوية** على أجهزة تحديد الهوية بموجات الراديو للتأثير أيضاً على جودة الإتصال. يمكن أيضاً استخدام **هجوم حقن العقد الخبيثة** من خلال قيام المهاجم بتشغيل عقدة ضارة جديدة بين العقد المتصلة بتكنولوجيا إنترنت الأشياء، مما يسمح للمهاجم بالتحكم فى تدفق البيانات بين مختلف العقد. يستطيع المهاجم أيضاً حدوث **أضرار مادية** بالأجهزة المتصلة بإنترنت الأشياء، إلا أن ذلك الهجوم يتطلب قربه من تلك الأجهزة. وأخيراً يمكن حدوث العديد من الهجمات من خلال **الهندسة الإجتماعية** والوصول إلى المعلومات الحساسة للمستخدمين من خلال إستغلال المهاجم عدم وعى المستخدمين للأمن السيبرانى لإنترنت الأشياء.

يمكن أن تتم **هجمات البرامج** من خلال قيام المهاجم **بإنشاء نصوص برمجية ضارة** (برامج نصية ضارة) تهدف إلى الوصول للبيانات الحساسة، وكذلك **هجمات التصيد:** وفيها يحصل المهاجم على البيانات الحساسة من خلال رسائل البريد الالكترونى، بالإضافة إلى **الهجمات من خلال إرسال الفيروسات وبرامج التجسس**. وأخيراً **هجمات رفض الخدمة** Denial of service حيث يمنح المهاجم الوصول الكامل للبيانات الحساسة ومنع وصول المستخدمين للبيانات.

كما تتمثل **هجمات الشبكة** فى **تحليل حركة المرور**: من خلال إستكشاف المهاجم للبيانات الحساسة، **وهجمات الإنتحال:** من خلال إنتحال إشارات RFID للحصول على البيانات المخزنة. وكذلك **هجوم الاستنساخ:** من خلال نسخ بيانات REID على علامة RFID أخرى. بالاضافة إلى

الوصول غير المصرح به من خلال إختراق عقد RFID **وتعطيل خدمة الشبكة**. وكذلك **هجوم رجل فى المنتصف** Man in –the– middle عن طريق وضع عقد ضارة بين عقدتين متصلتين مما يسمح بمراقبة كل حركة المرور المرسلة بين عقد الاتصال. وأخيراً يوجد **هجمات معلومات التوجيه** حيث يستخدم موجه الشبكة معلومات جدول التوجيه لإعادة توجيه البيانات إلى الوجهات المرغوبة وتغيير محتوياتها مما يؤدى إلى تعطيل خدمة الشبكة.

أما بالنسبة لهجمات التشفير فهى تتم من خلال **كسر الشفرات وإختراق هيكل التشفير** لتكنولوجيا إنترنت الأشياء وإستخدام تقنيات معينة للوصول إلى مفتاح التشفير وفك التشفير المستخدمة فى عملية تشفير البيانات.

وبالنسبة لتنفيذ الهجمات على منصات إنترنت الأشياء فإنها قد تكون داخلياً أو خارجياً. تؤدى **الهجمات الداخلية** التى يقوم بها المستخدمون عند دخولهم إلى الشبكة إلى حدوث مخاطر كثيرة للشركة؛ نظراً لامتلاكهم إمتيازات الوصول داخل النظام الأساسى بشكل كبير على جميع طبقات إنترنت الأشياء. كما قد تكون **الهجمات الخارجية** من قبل الأفراد من خارج الشركة – الذين لا يتمتعون بإمتيازات وصول لمعلومات الشركة–. من المتوقع أن الهجمات الداخلية على إنترنت الأشياء قد تكون أكثر حدة، نظراً لأن الهجمات الداخلية تكون أقل تحكماً من الهجمات من خارج الشركة. أى أنه يمكن منع الهجمات الخارجية من خلال جدار حماية الشبكة[4] firewall وأنظمة الكشف عن التسلل، ولكن يمكن للهجمات الداخلية الوصول إلى هدفها دون المرور بأى أداة أو وسيلة أمنية وبالتالي من المرجح أن تكون الهجمات داخل الشبكة ناجحة.

2-2-2 المخاطر والتحديات التى تواجه تبنى تكنولوجيا إنترنت الأشياء

ترتبط المخاطر الناتجة عن تبنى تكنولوجيا إنترنت الأشياء بالطبقات التى تتكون منها تلك التكنولوجيا (Duncan et al., 2017; CPA, 2019; Haddadpajouh et al., 2021)، والتى يمكن تقسيمها إلى ثمانية عوامل خطر كما يلى (Chang et al.,2016; Chang et al.,2020). تتعلق **المخاطر البيئية** بالمخاطر الخارجة عن سيطرة الشركة وتهدد عملها مثل وجود قناة إتصال لاسلكى غير آمنة. تحدث **المخاطر العملية** أثناء القيام بعمليات الشركة مثل إنتهاك

[4] يقصد بجدار الحماية : برنامج أو جهاز يقوم على حماية جهاز الحاسب أثناء إتصاله بشبكة الإنترنت من المخاطر، حيث يتولى جدار الحماية فحص كل المعلومات والبيانات الواردة من الإنترنت، أو من أى شبكة أخرى، ثم بعد ذلك يقوم بالسماح لها بالمرور والدخول إلى جهاز الحاسب، إذا كانت متوافقة مع إعدادات جدار الحماية، أو يقوم بإستبعادها وطردها إذا كانت من البرامج الخبيثة.

الخصوصية، والتصنت على الرسائل. أما بالنسبة **لمخاطر إتخاذ القرار** فهى تتعلق بالمشكلات المرتبطة بجمع المعلومات ومدى مصداقيتها. كما تنتج **المخاطر التشغيلية** فى حالة إساءة إستخدام البنية التحتية السحابية أو الإستغلال غير القانونى لمعلومات الشركة. تنتج أيضاً **مخاطر التفويض** من فشل الخدمات السحابية مما يؤثر على أمن وخصوصية المعلومات. كما يؤدى إنقطاع شبكة الإنترنت إلى حدوث **مخاطر معالجة البيانات**، لذا يتطلب الأمر إتخاذ التدابير الإحتياطية فى حالة إنقطاع الشبكة. وتأتى **المخاطر الأخلاقية** بسبب وجود طاقم عمل معادى وتحريف البيانات سواء على مستوى طبقة التطبيق أو على مستوى طبقة الشبكة، مما يؤدى إلى الإضرار بمصالح الشركة. وأخيراً تشير **مخاطر التمويل** إلى فقدان الأصول أو عدم التوازن بين التمويل وتوزيع رأس المال العامل مما يؤدى إلى وجود أزمة فى تشغيل عمليات الشركة. وقد ينتج ذلك بسبب سرقة أو تلف المعدات المرتبطة بأجهزة الإستشعار مثل الماسح الضوئى، وتحديد الهوية بموجات الراديو RFID ؛ لأن صيانة تلك الأجهزة مكلف للغاية.

تتمثل التحديات التى تواجه تكنولوجيا إنترنت الأشياء – والتى تمثل مشكلة خطيرة عند ربطها بنظام المعلومات المحاسبى– فى مشكلتى الأمن والخصوصية. تواجه تكنولوجيا إنترنت الأشياء تحديان رئيسيان وهما تحدى الأمن والخصوصية. تتعلق **التحديات الأمنية** بمخاطر هجمات القرصنة على البنية التحتية الحيوية والتى قد تؤدى إلى حدوث أضرار جمة. تتمثل التحديات الأمنية لإنترنت الأشياء فى إتسام إنترنت الأشياء بقدرات معالجة وتخزين محدودة، وإستخدام المستخدمين لكلمات مرور ضعيفة مما قد يؤدى إلى إمكانية وصول المهاجمين الذين يستطيعون معالجة بيانات الجهاز أو حتى إتلافه مادياً إلى معلومات الشركة. لذا يجب حماية قناة الإتصال التى تربط عقد الإتصال المختلفة مثل أجهزة إنترنت الأشياء والخدمات السحابية من أى هجوم. ويرجع ذلك إلى إرسال أجهزة إنترنت الأشياء البيانات بتنسيق نصى غير مشفر مما يجعلها هدفاً سهلاً لأنواع مختلفة من هجمات الشبكة.

يرجع **تحدى الخصوصية:** إلى أن نمو إنترنت الأشياء يساعد على إضافة مليارات من أجهزة الإستشعار والأجهزة إلى الإنترنت، مما ينتج عنه قدراً هائلاً من المعلومات حول الأشخاص أو الشركات سواء بموافقتهم أو بدونها وإساءة إستخدامها. مثل تجسس المنافسون على الشركات المنافسة لهم فى السوق؛ بغرض فهم هيكل تكلفة المنافس أو مستويات الانتاج (Lee and Lee,2015; Leloglu,2017; Devi and Mohankumar,2019; Payne,2019, Atlam and Wills,2020; Chang et al., 2020; Mahlous and Ara,2020; Khadam et

al., 2020; Romansky and Noninska,2020; Tavana et al., 2020; Busulwa .and Evans,2021; Martens et al., 2021; Popescu et al., 2021)

يتضح مما سبق ضرورة وجود العديد من المتطلبات الأمنية الأخرى التى يلزم تنفيذها لكل مستوى من مستويات بنية إنترنت الأشياء (Atlam and Wills ,2020). كما أنه قد يكون لدى الشركات أطر عمل ومعايير حالية للرقابة الداخلية مثل تقرير COSO ، وتقرير COBIT ، والأيزو 13000 الخاص بإرشادات إدارة المخاطر ومع ذلك فإن التهديدات والمخاطر المتعلقة بإنترنت الأشياء تختلف عن أى وقت مضى، وأن إدارة أمن المعلومات والشبكات فى بيئة إنترنت الأشياء لا تزال فى مهدها (Chang et al., 2020) . مما يتطلب الأمر ضرورة تطوير آليات الحماية الممكنة فى تلك البيئة؛ نظراً لوجود الكثير من عوامل الخطر. وهذا ما أكدته دراسة المعهد الوطنى للمعايير والتكنولوجيا على وجود ثلاثة إعتبارات قد تؤثر على إدارة الأمن السيبرانى ومخاطر الخصوصية لأجهزة إنترنت الأشياء مقارنة بأجهزة تكنولوجيا المعلومات التقليدية. تتمثل تلك الإعتبارات فى تفاعل العديد من أجهزة إنترنت الأشياء مع العالم المادى بطرق لا تتفاعل معها أجهزة تكنولوجيا المعلومات التقليدية، كما أنه لا يمكن الوصول إلى العديد من أجهزة إنترنت الأشياء أو إدارتها أو مراقبتها بنفس الطرق التى يمكن بها لأجهزة تكنولوجيا المعلومات التقليدية، وأخيراً تختلف كفاءة وفاعلية الأمن السيبرانى وقدرات الخصوصية لأجهزة إنترنت الأشياء عن أجهزة تكنولوجيا المعلومات التقليدية، مما يتطلب الأمر تحديد ضوابط إضافية للتخفيف من حدة المخاطر .(Boeckl et al., 2019)

لذا سوف يتم فى الجزء التالى من البحث التعرض لأهمية تطبيق الشركات للمدخل المقترح والمتمثل فى المورد البشرى– العملية– التكنولوجى لحماية أمن البيانات والمعلومات المحاسبية فى بيئة إنترنت الأشياء.

3- المورد البشرى – العملية – التكنولوجى كمدخل لحماية خصوصية وأمن البيانات والمعلومات المحاسبية عند تبنى تكنولوجيا إنترنت الأشياء

يتضح مما سبق أهمية وجود برنامج قوى للأمن السيبرانى يتطلب نهجاً متعدد الأوجه يجمع بين مجموعة من المهارات والعمليات والأدوات التكنولوجية (Ernst and Young,2011; Janes,2012; Duncan et al., 2017; ENISA,2019; Janvrin and Wang ,2019; Cui et al., ,2020). أى أنه يمكن القول أن الأمن السيبرانى عموماً يمكن تقسيمه إلى **عوامل تقنية** والتى هى خطوط الدفاع الأولى **والعوامل البشرية** غير الفنية (بما فيهم المحاسبين) والتى

تشمل العوامل البشرية من الناحية السلوكية والثقافة التنظيمية، لأنه عندما يكون الموظفون على دراية بسياسات وإجراءات أمن المعلومات الخاصة بشركتهم، فإنهم يكونوا أكثر كفاءة لإدارة مهام الأمن السيبرانى من أولئك الذين ليس لديهم دراية بسياسات الأمن السيبرانى لشركتهم. بالإضافة إلى أهمية تحديد الشركات **للعمليات** التى تقوم بها لحماية البيانات والمعلومات المحاسبية فى بيئة إنترنت الأشياء؛ فهى تعد مفتاح تنفيذ الإستراتيجية الفعالة للأمن السيبرانى فى بيئة إنترنت الأشياء. لذا سوف يتم توضيح المدخل المقترح لحماية أمن البيانات والمعلومات المحاسبية عند تبنى تكنولوجيا إنترنت الأشياء بمزيد من التفصيل فى الجزء التالى من البحث.

3-1. المورد البشرى: يعد المورد البشرى بلا شك نقطة حاسمة فى أمن المعلومات. يوجد قول مأثور يوضح أن التهديد الرئيسى يكمن بين الكرسى ولوحة المفاتيح مما يوضح أن إدراك المستخدمين يعد فى واقع الأمر مصدر المشكلات الأمنية فى بعض الأحيان. ويرجع ذلك إلى كونهم هدفاً للهجوم، بالإضافة إلى تجنبهم إستخدام آليات الحماية المتاحة بسبب التعقيد المفرط وعدم كفاية مستوى تعليمهم وتدريبهم (Duncan et al., 2017; Kremer et al., 2019; Lartey et al., 2021). لذا يتم فى الجزء التالى من البحث توضيح أهم الضوابط والاجراءات المرتبطة بالمورد البشرى التى يمكن تتخذها الشركات لحماية نظام المعلومات المحاسبى عند تطبيق تكنولوجيا إنترنت الأشياء.

1. **اختيار الموظفين ذوى الصفات الأخلاقية:** من خلال الإهتمام بإختيار الموظفين المشهود لهم بالأخلاق الحميدة، والإهتمام بتحديد وتوثيق وإعتماد متطلبات حماية البيانات المحاسبية المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند إنتهاء عملهم فى الشركة.
2. **خلق ثقافة الوعى بأهمية الأمن السيبرانى لنظام المعلومات المحاسبى وفهم المحاسبون لطبيعة إنترنت الأشياء والمخاطر التى يمكن أن تتولد منها:** من خلال الإهتمام بتوعية العاملين بأهمية حماية البيانات والمعلومات المحاسبية المرتبطة بتكنولوجيا إنترنت الأشياء، والتأكيد على مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد إنتهاء خدمتهم. حيث يؤثر تجاهل المحاسبين بأمن نظام المعلومات المحاسبى على إستقرار نظم المعلومات المحاسبية فى الشركات، على الرغم من إهتمام تلك الشركات بشراء آلات ومعدات أكثر تقدماً وفعالية (Gansler and Lucyshyn,2005; Ernst and Young,2011; Janes ,2012; Lee,2020; Bhol et al., 2021; Lartey et al., 2021; Shao et al., 2021). يرجع ذلك إلى تخريب المطلعين الضارين أفضل التقنيات، كما يمكن للمستخدمين غير المهتمين بأمن المعلومات

والشبكات إدخال الفيروسات فضلاً عن إختراق كلمات المرور الخاصة بهم. وفى جميع الأحوال لا يمكن التنبؤ بالسلوك البشرى والأخطاء المترتبة عليه، كما يمكن أن تكلف هذه الأخطاء الأفراد والشركات تكلفة كبيرة وبصفة خاصة فى الفضاء الإلكترونى. لذا يتطلب الأمر الإهتمام بتدريب الأفراد وزيادة وعيهم بالأمن السيبرانى فى ظل إستخدام تكنولوجيا إنترنت الأشياء (Bauer et al., 2017; Cui et al., 2020; Alghamdie,2021; Martens et al., 2021). وقد يرجع ذلك إلى أنه لا ينطوى ضمان الأمن السيبرانى على حماية البيانات المحاسبية فقط، بل يجب أيضاً جعل المحاسبين والعمليات المحاسبية هى الأساس فى عمليات الأمان (Eaton et al., 2019; Zadorozhnyi et al., 2020) . لذا يتطلب الأمر تعزيز المعرفة وزيادة وعى الأفراد بشأن الأمن السيبرانى عند إستخدام تكنولوجيا إنترنت الأشياء وضرورة تعزيز المعرفة متعددة الوظائف حول تكنولوجيا المعلومات وأمن إنترنت الأشياء (ENISA,2019). كما يمكن إشتراك المحاسبين ذوى المعارف الإضافية متعددة التخصصات وذوى الخبرة والمهارة فى مجال العمل فى حماية البيانات المحاسبية ورقابة تلك النظم (Zadorozhnyi et al., 2020).

3. **مشاركة المحاسبون فى تحديد الأهداف التنظيمية لإدارة البيانات وتحليلها:** يتطلب الأمر ضرورة تعمق المحاسبون ومعرفة المزيد من علم البيانات والرياضيات والإحصاء والترميز والخوارزميات والإهتمام بالذكاء الإصطناعى وتعلم الآلة ولغات البرمجة. أى يجب أن يتسم المحاسبون بالمعرفة والمهارات فى إدارة علم البيانات[5]، بالإضافة إلى تحديدهم للبيانات الحساسة ومراقبتها وحمايتها مما يساعد على منع فقدان البيانات الحساسة للشركة (WatchGuard,2010; Pendly,2018). يرجع ذلك إلى أهميتهم فى تحسين إدارة بيانات شركتهم وتحليل البيانات (Payne,2019). ويؤكد ذلك على أهمية المحاسبين فى المشاركة فى تحديد الأهداف التنظيمية لإدارة البيانات وتحليلها وعلم البيانات وإستخدام مخرجات البيانات لتحسين عملية صنع القرار (Busulwa and Evans, 2021) .

يتضح مما سبق أهمية مساعدة المحاسبون للمديرين على القيام بالأدوار الخاصة بخصوصية وحماية معلومات الشركة من خلال ضمان وصول المديرين إلى أفضل المعلومات لتمكينهم من توقع أو إكتشاف أى مخاطر / أحداث / سلوكيات / مواقف متعلقة بالخصوصية، وتمكنهم من إمداد المديرين بالمعلومات التى تساعدهم على الحصول على رؤية واضحة عن إلمام الموظفين والموردين

[5] تشير إدارة البيانات إلى عمليات وممارسات الشركة لجمع البيانات والتحقق منها وتخزينها وإستخدامها على النحو الأمثل.

والعملاء وأصحاب المصالح الأخرى بخصوصية معلومات الشركة وتحديد المخاطر الناتجة عن إستخدام الإنترنت. لذا يمكن اشتقاق فرض البحث الأول:

H1: يؤدى إهتمام الشركات بوضع الضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبطة بالمورد البشرى (المحاسبين بصفة خاصة) عند تبنى تكنولوجيا إنترنت الأشياء إلى حماية نظام المعلومات المحاسبى المرتبط به.

3-2. العملية: لا يقتصر المهاجمون لنظام المعلومات المحاسبى فى ظل تبنى تكنولوجيا إنترنت الأشياء على الأفراد من خارج الشركة فقط، بل قد يكون من داخل الشركة أيضاً. لذلك تحتاج الشركات إلى تنفيذ مجموعة من الضوابط لحماية معلومات الشركة من الإستخدام غير المصرح به. كما يتطلب الأمر أيضاً تفكير الشركات فى وجود نظام حوكمى قوى وإدارة المخاطر لديها -من خلال تحديد البيانات التى يجب تأمينها، وتحديد الإرشادات حول كيفية جمع البيانات وإستخدامها وتخزينها بشكل آمن، ومنع الإنتهاكات غير المرغوب فيها، وتحديد المسئولين فى حالة حدوث إختراق للبيانات أو لنظام المعلومات الخاص بالشركة ككل- (Saif et al., 2015; Taveras,2019). بالإضافة إلى مراجعة مسار تسجيل المستندات ذات الصلة بجميع عمليات الشركة (Wang,2016). لذا يتناول الجزء التالى من البحث أهم الضوابط والإجراءات المرتبطة بالعمليات الداخلية التى يمكن تتخذها الشركات لحماية نظام المعلومات المحاسبى عند تطبيق تكنولوجيا إنترنت الأشياء.

1. **إنشاء إدارة للأمن السيبرانى وتنظيم أنشطتها:** يجب أن تضع إدارة الشركة وفريق الأمن السيبرانى إستراتيجية الأمن السيبرانى وتضع السياسات والإجراءات والعمليات التى يجب أن تقوم بها لحماية نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء. بحيث لا ينبغى النظر إلى حماية نظام المعلومات المحاسبى المرتبط بإنترنت الأشياء من منظور الضعف فقط، وإنما يتم النظر إليه على إنها إستراتيجية تعتمد على تأمين الشركة لمعلوماتها وهياكلها بإستخدام وعى وفهم عميقين للمعلومات والعمليات وتقنيات الإتصال الحالية التى تشكل أساس الشركة ككل. ويجب أن تكون تلك الإستراتيجيات مرنة لتمكنها من الإستمرار فى التكيف مع التغيرات المستقبلية، ويتم مراجعتها بإستمرار لضمان ملائمتها لسير العمل. كما يجب تحديد العمليات الخاصة بحماية المعلومات والتى تشتمل على السياسات اللازمة لحماية البيانات والإجراءات الخاصة بأمن نظام المعلومات المحاسبى المرتبط بإنترنت الأشياء بوضوح، وتحديد التعليمات والأوامر الخاصة بأداء المهمة والمصفوفات والأدوار، وكيفية تحسين العمل من خلال الإهتمام

بالتحسين المستمر للعمليات (Ernest and Young,2011; Chelakkara, 2020 ; Cui et al., ,2020). وأخيراً الإهتمام بالإختبار المنتظم لنظام المعلومات المحاسبى لتحديد التهديدات المحتملة.

2. **توثيق مسئوليات المحاسبين فى كتيبات:** من خلال وضع دليل أخلاقيات المحاسبين المرتبطة بالأمن السيبرانى وإهتمام المحاسبين بتشفير البيانات من خلال تطبيق الخوارزميات لتحويل المعلومات المقروءة إلى بيانات لا معنى لها ولا يفهمها إلا مستخدمى البيانات المصرح لهم بذلك (ITU,2008; Maistry et al., 2015; Pendley,2018; Kremer et al., 2019; Cui .et al., ,2020; Lee,2020; Zadorozhnyi et al., 2020; Lartey et al., 2021) وكذلك تصميم وتنفيذ الضوابط للتخفيف من حدة المخاطر وإعداد تقارير الأمن السيبرانى فى ظل تبنى تكنولوجيا إنترنت الأشياء وتحديد التفاصيل الأمنية اللازمة لمستخدمى نظام المعلومات المحاسبى الإلكترونى والتأكيد على إلتزام مستخدمى نظام المعلومات وموظفى الشركة بقواعد التعامل مع المعلومات المحاسبية ومراقبة فعالية جدار الحماية (Firewall) ، وتقديم التأكيدات بخصوص تلك التقارير (Eaton et al., 2019).

3. **وضع نظام واضح لتوثيق الأشخاص الذين يمكنهم الوصول إلى المعلومات المحاسبية:** يقصد بها تحديد الشركات لمجموعة القواعد والممارسات المنظمة داخل نظام معين لكيفية تشغيل وإدارة وتوزيع الموارد المختلفة. بحيث يمكن التعرف على كل من يصل إلى نظام معلومات الشركة والتحقق من هوية الشخصauthentication[6] أو الجهاز الذى يحاول الوصول إلى النظام. يمكن أيضاً وضع ضوابط التفويض authorization[7] أى تقييد وصول المستخدمين المصادق عليهم إلى إجراءات معينة من النظام (Chelakkara, 2020; Jaidi, 2017; Sangani and Zarger, 2017) . يساعد الإهتمام بالتحقق من الهوية والمصادقة وضوابط الوصول أيضاً على تحقيق الأمن داخل طبقة الإدراك والتطبيق. يرجع ذلك إلى أن تحديد الهوية والمصادقة يعد أول خدمتين لتحقيق الأمن (Duncan et al., 2017). أى يجب أن تحدد السياسة المحاسبية أو اللوائح الداخلية المشتقة إجراءات إدارة الوصول إلى المعلومات وتدريب الأفراد على المصادقة الرقمية وتحديد صلاحيات المستخدمين وتوقيعهم على المستندات وتدريبهم

[6]يقصد بـ authentication هوية المستخدم : أى التأكد من أن المستخدم موجود فى قاعدة بيانات المستخدمين فى الشركة من خلال كتابة الأسم وكلمة المرور أو إضافة خطوات أخرى من الخصائص البيومترية للمستخدم.

[7]يقصد بـ authorization التصريح أو المصادقة: التصريح لمستخدم معين بالدخول وتحديد صلاحياته لإستخدامات معينة على النظام.

على وضع واستخدام كلمات مرور قوية، بالإضافة إلى إستخدام الأدوات الحديثة مثل بصمات الأصابع والتعرف على الوجه (الخصائص البيومترية) (NIST,2018) ، بالاضافة إلى تشكيل وإعداد قائمة واضحة بالأشخاص الذين لديهم حق الوصول إلى المعلومات وتحديد الآلية المناسبة لمساءلة هؤلاء الأشخاص.

4. **تطبيق الشركات لأطر عمل ومعايير الرقابة الداخلية وحوكمة تكنولوجيا المعلومات وتطبيق نموذج نضج قدرات الأمن السيبرانى:** يمكن للشركات إستخدام تقرير COSO، وتقرير COBIT كأطر للرقابة الداخلية. كما يتطلب الأمر أيضاً الإهتمام بتحقيق أمن وحماية نظام المعلومات المحاسبى فى ظل بيئة إنترنت الأشياء من خلال تطبيق معايير أمن المعلومات والأمن السيبرانى مثل معيار PAS 555 ، والأيزو 27032 ، والأيزو 27001 . يمكن أيضاً إهتمام الشركات بالتحسين المستمر لحماية نظام المعلومات المحاسبى عبر شبكة الإنترنت من خلال **تطبيق نموذج نضج قدرات الأمن السيبرانى** وبصفة خاصة الإصدار الثانى لعام 2021 (Busulwa and Evans,2021; U.S. Department of energy,2021). يوفر نموذج نضج قدرات الأمن السيبرانى معياراً يمكن من خلاله تقييم الشركة للمستوى الحالى لنضج ممارستها وعملياتها وتحديد الأهداف والأولويات الخاصة بتحسين الأمن السيبرانى لها من خلال تحديد أربعة مستويات نضج. تبدأ مستويات النضج من المستوى صفر إلى المستوى 3 والتى يتم تطبيقها بشكل مستقل على كل مجال من العشرة مجالات الخاصة بالنموذج. يتسم النموذج بالتركيز على الشركة بأكلمها، كما يساعد على تحديد الفجوات فى القدرات ووضع الخطط لمعالجتها وتنفيذ الخطط، ومعالجة الثغرات الأمنية مما يؤدى إلى التحسين المستمر لعمليات إدارة مخاطر الأمن السيبرانى المتعلقة بإنترنت الأشياء وحماية نظام المعلومات المحاسبى المرتبط به.

5. **إدارة المخاطر السيبرانية بين أعضاء سلسلة التوريد والتحقق من موثوقية وسمعة مزود الخدمة:** بالنظر إلى إستخدام إنترنت الأشياء فى الصناعة يتضح تأثيره ليس فقط على الشركة بل يمتد آثاره إلى أصحاب المصالح ذات العلاقة بالشركة (ENISA,2019)، مما يتطلب الأمر إدارة المخاطر السيبرانية المرتبطة بالأطراف الخارجية (NIST,2018). يتطلب الأمر أيضاً ضرورة مشاركة المعلومات بين الأطراف ذات العلاقة عند تعرضها للتهديدات السيبرانية، مما يساعد الشركات على فهم المخاطر وتوجيهها بشكل أفضل وتحديد التدابير الوقائية (Gansler and LycyShyn ,2005; Walton et al., 2021). كما يتطلب الأمر أيضاً التحقق من موثوقية وسمعة مزود الخدمة المرتبطة بوظائف المحاسبة.

مما سبق يتضح أهمية العمليات التى تقوم بها الشركة لحماية المعلومات المحاسبية فى ظل تبنى تكنولوجيا إنترنت الأشياء. لذا يمكن اشتقاق فرض البحث الثانى:

H2: يؤدى اهتمام الشركات بوضع الضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبطة بالعملية عند تبنى تكنولوجيا إنترنت الأشياء إلى حماية نظام المعلومات المحاسبى المرتبط به.

3-3 التكنولوجى: يشكل التكنولوجى والتقنية دوراً هاماً فى حياة الأفراد والشركات حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية (ENISA, 2019; IoT Alliance Australia, 2020; Lee, 2020). وتشمل حماية الأجهزة بمختلف أشكالها الذكية والحاسبات الآلية والشبكات من خلال الإعتماد على جدران الحماية وإستخدام برامج مكافحة الفيروسات بالإضافة إلى العديد من التقنيات الأخرى مثل الذكاء الاصطناعى وتعلم الآلة والبلوك تشين.

ويمكن تقسيم تقنيات وضوابط الأمن السيبرانى التى يمكن إستخدامها فى بيئة إنترنت الأشياء إلى ثلاثة مجموعات وهم التقنيات التى تضمن سرية المعلومات، والتقنيات التى تكتشف وتتصدى للتهديدات ونقاط الضعف، والضوابط التكنولوجية التى يمكن أن تساعد على مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. ويساعد القيام بما سبق على تحقيق الأمن السيبرانى فى كل طبقة من طبقات إنترنت الأشياء.

3-3-1 التقنيات التى تضمن سرية البيانات والمعلومات المحاسبية المرتبطة بتكنولوجيا إنترنت الأشياء: تهتم هذه التقنيات بضمان سرية البيانات والمعلومات المحاسبية المتولدة من تكنولوجيا إنترنت الأشياء، وتتمثل فى الآتى:

- **إستخدام التشفير:** يساعد التشفير على إخفاء البيانات والمعلومات فى شكل لا يمكن قراءته بسهولة، لذا يجب توفير مفتاح لفك التشفير أيضاً عند الحاجة اليه. أى أن التشفير يعد أداة فعالة لحماية البيانات والمعلومات أثناء نقلها وتخزينها عبر الإنترنت (Ernst and Young, 2011; Janes,2015; Maistry et al., 2015, Romney and Steinbart,2018; Kremer et al., 2019).
- **النسخ الاحتياطى المنتظم للمعلومات المحاسبية دون الاتصال بالإنترنت لجهاز التخزين الرئيسى وتجنب استخدام البرامج التى لا حاجة لها:** يتم الإهتمام بالنسخ الاحتياطى المنتظم للمعلومات المحاسبية وذلك حتى يمكن للشركة إستعادة المعلومات المحاسبية فى حالة حدوث إنتهاك لتلك المعلومات من خلال الإنترنت. يجب أيضاً القيام بإجراء فحص دورى لمدى فعالية إستعادة النسخ الإحتياطية (Maistry et al., 2015). يساعد أيضاً تجنب إستخدام البرامج

التى لا حاجة لها من عدم إعطاء الفرصة للمهاجمين من الدخول على نظام المعلومات المحاسبى. كما يجب الإهتمام بفحص نظام المعلومات المحاسبي بإنتظام ومدى إرتباط البيانات المحاسبية بإنترنت الأشياء (Zhang,2019). لذا يعد وجود نسخ احتياطية أمراً ضرورياً للتعافى من الهجمات وتخزينها على مسافة بعيدة عن الأنظمة الموجودة والمعرضة للهجمات.

- **حماية البريد الإلكترونى:** من خلال إستخدام خاصية منع البريد الالكترونى من إرسال المحتوى والمرفقات والبيانات الحساسة خارج شبكة الإنترنت، بالإضافة إلى تحليل وتصفية رسائل البريد الالكترونى وبصفة خاصة رسائل التصيد الإلكترونى والرسائل الاقتحامية Spam بإستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الالكترونى (Ernst and Young, 2011; Janes, 2012; IoT Alliance Australia,2020).
- **إستخدام العلامات المائية الرقمية:** يمكن إستخدام العلامات المائية الرقمية كعنصر رقابة وقائى يساعد الشركة على تحديد المعلومات السرية وإخفائها ضد الإستخدام غير القانونى. يتم ذلك من خلال وضع العلامات المائية على المستندات النصية التى يتم إنشاؤها يومياً ومشاركتها من خلال تطبيق إنترنت الأشياء وأن تكون المعلومات غير ظاهرة للمستخدمين غير المصرح لهم بإستخدامها (Contreras and Coatrieux,2017; Kermer et al., 2019; Khadam et al., 2020). لذا يساعد وضع العلامة المائية على النص المستخرج من أجهزة إنترنت الأشياء على توافر المعلومات وسهولة وصول المستخدم لها وتكاملها وحمايتها والمحافظة عليها وزيادة جودتها.
- **إدارة حساب المستخدم والتأكد من قوة كلمات المرور:** يتم إدارة حساب المستخدم من خلال تعيين حسابين للموظفين الذين يحتاجون إلى صلاحيات إدارية على جهاز كمبيوتر معين. أحدهما يكون له جقوق إدارية عندما يحتاج إلى تنفيذ بعض الإجراءات مثل تثبيت برنامج جديد والذى يتطلب حقوقاً إدارية والأخر له امتيازات محدودة لأداء واجباتهم اليومية الروتينية. لذا فإنه إذا قام الموظف بزيارة موقع ويب تم اختراقه أو فتح بريداً الكترونياً مصاباً، فيسحصل المهاجم على حقوق محدودة فقط على الجهاز (Romney and Steinbart, 2018) . يتطلب الأمر أيضاً التأكد من قوة كلمات المرور لأجهزة إنترنت الأشياء عن طريق تغييرها من الإعدادات الإفتراضية للشركة المصنعة إلى النماذج التى تلبى سياسات تكنولوجيا المعلومات التنظيمية (CPA,2019).
- **إستخدام تقنية البلوك تشين كدفتر أستاذ رقمى لا مركزى:** تتكون تقنية البلوك تشين من كتل من المعاملات التى تتم بين الأطراف وتوزيع الآلاف من النسخ على جميع الأعضاء المشتركين

فى تلك التقنية. لذا يؤدى إستخدام نظام المعلومات المحاسبى المستند على تقنية البلوك تشين فى بيئة إنترنت الأشياء إلى عدم وجود تدخل يدوى فى أى مرحلة داخل عمليات نظام المعلومات المحاسبى، ولا يمكن تزوير أو الغاء أى بيانات مسجلة فى دفتر الأستاذ الموزع، بالإضافة إلى أهميته فى إرسال وتسجيل كميات كبيرة من البيانات المحاسبية. أى أن إستخدام تقنية البلوك تشين يمكن أن تعد أحد الحلول لقضايا الخصوصية وأمن البيانات والمعلومات المحاسبية فى ظل إستخدام تكنولوجيا إنترنت الأشياء وتعزيز إستخدام إنترنت الأشياء على المستوى العالمى (Altam et al., 2018; Payne,2019; Liu and Zhang,2020; Mahlous and Ara,2020; Zadorozhnyi et al., 2020; Abad-Segura et al., 2021). ويرجع ذلك إلى وجود آلاف من النسخ الإحتياطية بمجرد نشرها على البلوك تشين مما يؤدى رؤية جميع المعاملات لجميع الأعضاء داخل الشبكة (Demirkan et al., 2020; Sarwar et al., 2021). كما يساعد تطبيق تقنية البلوك تشين على إدارة أمن المعلومات المحاسبية (Demirkan et al., 2020 ; Shao et al., 2021) ، وتحسين جودة المعلومات المحاسبية (Wu et al., 2017) .

3-3-2 التقنيات التى تكتشف وتتصدى للتهديدات ونقاط الضعف (الحماية متعددة الطبقات)

يمكن استخدام العديد من التقنيات التي يمكن أن تكتشف وتتصدى للتهديدات السيبرانية فى الوقت المناسب فى ظل إستخدام نظام المعلومات المحاسبى المستند على تكنولوجيا إنترنت الأشياء. تتمثل تلك التقنيات فى تحليل السجلات وإستخدام جدران الحماية وأنظمة كشف التطفل والتتبع الخلفى، وأنظمة منع التطفل بالإضافة إلى إستخدام الذكاء الاصطناعى وتعلم الآلة.

- يعد **تحليل السجل:** عملية تهتم بفحص السجلات لتحديد الأدلة على الهجمات المختلفة على أجهزة الكمبيوتر. لذا يتطلب الأمر تحليل السجلات بصورة روتينية (Romney and Steinbart,2018). أى يجب إدارة سجلات الأحداث وتحليل ومراقبة السجلات من أجل الاكتشاف الإستباقى للهجمات السيبرانية وإدارة مخاطرها بفاعلية لمنع أو تقليل الأثار المترتبة على حدوث الهجمات.
- **إستخدام جدران الحماية:** وهو ذلك الجهاز الذي تقوم الشركات المتخصصة في برامج الحاسب الآلى بوضعه فى جهاز الكمبيوتر. وذلك بهدف حماية البرامج وكذلك الملفات من الإختراق والسرقة من بعض الجهات الخارجية (Ducan et al., 2017).

- **إستخدام أنظمة كشف التطفل:** للتحقق وتسجيل الأحداث الخاصة التى تشير إلى هجوم وتنبيه مسئولى النظام عندما تصبح الأمور خطيرة.
- **إستخدام أنظمة منع التطفل:** من خلال إيقاف تشغيل الإتصال بالإنترنت أو تسجيل الخروج من المستخدم عندما يصبح الشخص مشبوهاً بدرجة كافية وفقاً لنظام الكشف عن التطفل، كما يشمل أيضاً أشكالاً من الحد من الضرر مثل حرمان المستخدم من موارد معينة أو تخفيض أولويتها أو تأخيرها. يمكن أيضاً إستخدام التتبع الخلفى وهو شكل من أشكال دفاع الشبكة يحاول العثور على وجود مصدر هجوم خارجى لإيقافه بسهولة (Maistry et al., 2015; Kremer et al., 2019).
- **إستخدام الذكاء الإصطناعى:** يمكن إستخدام الذكاء الإصطناعى لإكتشاف المتطفلين على أنظمة معلومات الشركة وتحديد نقاط الضعف من خلال تحليل أنماط حركة المرور. يرجع ذلك إلى أهمية إستخدام وتطوير خوارزميات معقدة لحماية الشبكات والأنظمة بما فيها أنظمة إنترنت الأشياء؛ بسبب تعرض الأشياء للهجوم سواء من الأجهزة أو البرامج أو الشبكة التى يتصل بها (Kuzlu et al., 2021). كما يتضح أهمية إستخدام الذكاء الإصطناعى وتعلم الآلة[8]، وذلك للكشف عن نمط سلوك المستخدم الضار فى بيئة إنترنت الأشياء (Sanagani and Zarger,2017; Ghumro et al., 2020).

3-3-3 الضوابط التكنولوجية التى يمكن أن تساعد على مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى

- **ضوابط الأمن المادى:** أى حماية الأصول المعلوماتية والتقنية من الوصول المادى غير المصرح له والفقدان والسرقة. ويتم ذلك من خلال وضع موظف إستقبال أو حارس أمن عند المدخل الرئيسى للتحقق من هوية الموظفين، وكذلك مراقبة حركة الدخول والخروج إلى الغرف التى تحتوى على أجهزة كمبيوتر مرتبطة بإنترنت الأشياء. وتقييد الوصول إلى الأسلاك المستخدمة فى الشبكات المحلية للشركة وعدم كشف الكابلات والأسلاك، وأخيراً تقييد الوصول المادى إلى طابعات الشبكة لأنها فى الغالب تخزن صوراً للمستندات على محركات الأقراص الصلبة الخاصة بها.
- **ضوابط تصميم البرمجيات** وإزالة التعليمات البرمجية والفيروسات وتدريب المبرمجين على التعامل مع جميع المدخلات من المستخدمين الخارجيين على إنها غير جديرة بالثقة، والتحقق منها

[8] هو أحد فروع الذكاء الاصطناعى يهتم بتصميم وتطوير خوارزميات وتقنيات تسمح للحاسب بإمتلاك خاصية التعلم.

بعناية قبل تنفيذ المزيد من الإجراءات، وإستخدام البرامج الجيدة والإبتعاد عن البرامج المليئة بالثغرات الأمنية، بالإضافة إلى تعطيل ميزة التحديث التلقائى للبرامج.

- **ضوابط خاصة بمزود الخدمة والإهتمام بالحوسبة الضبابية:** يجب أن تحدد الشركة متطلبات الأمن والحماية مثل ضمان الضوابط المناسبة حول التخزين والنقل والوصول، وأن يوافق مزود الخدمة على متطلبات محددة لأمن السحابة فى الإتفاقيات التعاقدية أى اتفاقية مستوى الخدمة مع الأطراف الخارجية التى قد تتأثر بإصابتها ببيانات الجهة أو الخدمة المقدمة لها. بالإضافة إلى إهتمام الشركات بتخزين البيانات عبر الحوسبة الضبابية[9] Fog computing. حيث ترسل الأجهزة المرتبطة بإنترنت الأشياء هذه البيانات إلى الأجهزة القريبة منها مثل الهواتف الذكية، وتتواصل معها فى وقت قصير مقارنة بالوقت المطلوب للإرسال إلى السحابة.
- **ضوابط لإدارة أمن الشبكات وإنشاء شبكة خاصة بإنترنت الأشياء ومراجعة السجلات:** يتم ذلك من خلال إنشاء شبكة خاصة منفصلة لأجهزة إنترنت الأشياء والتى لا يتم مشاركتها مع الشبكة التى يمكن لأجهزة الموظفين الوصول إليها. والإهتمام بعزل والتقسيم المادى لأجزاء الشبكات بشكل آمن. والإهتمام بتحقيق أمن الشبكات اللاسلكية وحمايتها وعدم ربط الشبكات اللاسلكية بالشبكة الداخلية للشركة إلا بناء على دراسة متكاملة للمخاطر المترتبة على ذلك والتعامل معها بما يضمن حماية الأصول التقنية للشركة. وأخيراً يجب تحديد الحد الأدنى لعدد الشبكات التى يجب السماح إليها بالوصول إلى تطبيقات إنترنت الأشياء؛ لضمان التحكم ورقابة الشبكات التي تنقل حركة مرور إنترنت الأشياء.

يتضح مما سبق أهمية وجود تقنيات وضوابط تكنولوجية لحماية نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء، لذا يمكن اشتقاق فرض البحث الثالث.

H3: يؤدى وضع الشركات للتقنيات التكنولوجية والضوابط الخاصة بحماية أمن الشبكات والمعلومات عند تبنى تكنولوجيا إنترنت الأشياء إلى حماية نظام المعلومات المحاسبى المرتبط به.

وسوف يتم إختبار فروض البحث عن طريق إجراء دراسة تجريبية كما يلى:

[9] يقصد بالحوسبة الضبابية : البنية التي تستخدم واحد أو أكثر من العملاء أو الأجهزة القريبة من المستخدم لإتمام كمية كبيرة من التخزين. يتمثل الهدف الأساسى منها فى العمل على رفع كفاءة نقل البيانات وتقليل التكرار فيها، لكي تصل إلى السحابة لمعالجتها وتخزينها، كما تستخدم أيضاً في زيادة الأمان مما يؤدى إلى تحسين عملية النقل إلى السحابة.

4- الدراسة التجريبية

4-1 هدف الدراسة التجريبية

تهدف الدراسة إلى إختبار فروض البحث المتعلقة بأهمية ضوابط أمن الشبكات والمعلومات المتمثلة فى بعد المورد البشرى، والعملية، والتكنولوجى فى حماية نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء.

4-2 أهمية الدراسة التجريبية

ترجع أهمية الدراسة إلى إهتمام العالم كله بالتحول الرقمى واهتمام الشركات الصناعية بصفة خاصة ببناء مصانع ذكية، مما يترتب عليه ضرورة زيادة الضوابط الرقابية لحماية نظام المعلومات المحاسبى المرتبط بإستخدام الشركات للتكنولوجيا الحديثة.

4-3 أدوات وإجراءات الدراسة

عند إجراء الدراسة التجريبية تم الإعتماد على توزيع قوائم الاستقصاء (المرفقة فى ملحق البحث) على المستقصى منهم. بدأت قائمة الاستقصاء بمقدمة بسيطة توضح الهدف من موضوع البحث والمصطلحات المرتبطة به وأسئلة عن خصائص عينة الدراسة، ثم الحالات التجريبية وأخيراً أسئلة عامة تتعلق بموضوع البحث لتوضح مدى تقبل المستقصى منهم للمخاطر، وقد اتسمت القائمة بالوضوح والبساطة. تم الإعتماد عند إجراء الدراسة التجريبية على توزيع حالتين إفتراضيتين على المستقصى منه مع القيام بالتبديل بين الحالات وبين الأسئلة داخل كل حالة؛ لتجنب تعلم المستقصى منه من الحالات الموزعة عليه- لشركة تتبع تكنولوجيا إنترنت الأشياء وتقوم بربط نظام المعلومات المحاسبى بتلك التكنولوجيا-. تتمثل الحالة الأولى فى شركة تتبنى تكنولوجيا إنترنت الأشياء دون الإهتمام بتوفير الضوابط الوقائية الكافية لمواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. فى حين تتمثل الحالة الثانية فى شركة تتبنى تكنولوجيا إنترنت الأشياء مع الإهتمام بتوفير الضوابط الوقائية الكافية لمواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى، وعلى المستقصى منهم الإجابة على الأسئلة التى تلى كل حالة.

4-4 وصف عينة الدراسة

تشتمل عينة الدراسة على المسئولين عن التعامل مع وإدارة البيانات (سواء الحصول على أو تخزين أو إستدعاء البيانات) وما يرتبط بها من أنظمة وتكنولوجيا وشبكات لازمة للقيام بهذه المهام

بالإضافة إلى (وما يرتبط بها من) أمن المعلومات وأمن الشبكات (على سبيل المثال لا الحصر محللى ومصممى النظم، ومهندسى البرمجيات، ومختصى قواعد البيانات، ومختصى أمن المعلومات، ومختصى أمن الشبكات، ومحللى البيانات وإستخبارات الأعمال، ومهندسى الإتصالات والشبكات،.....إلخ). وفى هذا الصدد يمكن تقسيم عينة الدراسة إلى المحاسبين فى الإدارة المالية والمختصين بالنظم وتكنولوجيا المعلومات فى العديد من القطاعات والتى تتضح من الجدول رقم (1).

تم إستلام 78 قائمة إستقصاء من إجمالى 90 قائمة إستقصاء موزعة على المشاركين فى الدراسة بنسبة إستجابة 86.7% كما يتضح من الجدول التالى:

جدول 1: بيان بالردود على الحالات التجريبية

	المهندسين المختصين بنظم وتكنولوجيا المعلومات	المحاسبين	إجمالى
الموزع	48	42	90
المستلم	42	36	78
نسبة الاستجابة	87.5	85.7	86.7
المستبعد	__	ـــــ	ـــــ
المستخدم	42	36	78

تم توزيع قوائم الإستقصاء على بعض القطاعات التى تدرك أهمية وجود شبكة شاملة من الأشياء الذكية التى لديها القدرة على التنظيم التلقائى ومشاركة المعلومات والبيانات بين الأجهزة وبعضها البعض مما يؤثر على نظام المعلومات فى الشركة. يتضح ذلك فى قطاع الأجهزة المنزلية وقطاع السيارات والجهات المختصة بوضع البنية التحتية للمدن الذكية، بالإضافة إلى قطاع الإتصالات (الشركة المصرية للإتصالات) ؛ لقيامها بإنشاء أول منصة لتكنولوجيا إنترنت الأشياء فى مصر بالتعاون مع شركة نوكيا العالمية. وأخيراً شركات الإستشارات والتدريب فى مجال المحاسبة ونظم وتكنولوجيا المعلومات لإدراكهم أهمية الأمن السيبرانى فى ظل تطبيق أدوات الثورة الصناعية الرابعة كما يتضح من الجدول التالى.

جدول 2: يوضح عدد المشاركين فى كل قطاع

القطـــاع	النسبـة	المهندسين المختصين بالنظم وتكنولوجيا المعلومات	النسبـة	المحاسبين	إجمالى عينة الدراسة والنسبة	
قطـاع الأجهـزة المنزليـة والأدوات الكهربائية	35.7	15	41.7	15	30	38.5
قطاع السيارات	16.7	7	27.8	10	17	21.8
قطـــاع الإتصـــالات وتكنولوجيـــا المعلومـــات (الشـــركة المصـــرية للإتصالات)	21.4	9	16.7	6	15	19.2
شركات المقـاولات والبنيـة التحتيـة الذكية	11.9	5	—	—	5	6.4
الإستشارات والتدريب	14.3	6	13.8	5	11	14.1
الإجمـالـــي	100	42	100	36	78	100

كما يوضح الجدول رقم (3) الخصائص الديمغرافية لعينة الدراسة وذلك كما يلى:

جدول 3: الخصائص الديمغرافية لعينة الدراسة

الخصائص الديمغرافية	ن	%
الوظيفة		
المهندسين المختصين بالنظم وتكنولوجيا المعلومات	42	53.8
المحاسبين	36	46.2
دراسات عليا		
دبلوم	44	56.4
ماجستير	8	10.3
دكتوراه	2	2.6
عدد سنوات الخبرة في العمل		
أقل من خمس سنوات	26	33.3
من 5 سنوات إلي أقل من 10 سنوات	32	41
من 10 سنوات إلي أقل من 15 سنة	15	19.3
15 سنة فأكثر	5	6.4

يتضح من الجدول السابق أن نسبة 100% من عينة الدراسة حاصلون على مؤهل عالى، وأن 69.3 % حاصلون على دراسات عليا، بالإضافة إلى 74.3 % من عينة الدراسة تتراوح خبرتهم ما بين حديثى إلى متوسطى الخبرة. لذا يوضح التحليل الوصفى لعينة الدراسة أنهم على دراية وعلم بالمستجدات الحديثة فى بيئة العمل، مما يتناسب مع موضوع البحث.

4-5 إختبار ثبات وصدق المقاييس المستخدمة فى الدراسة

يمكن إختبار ثبات وصدق المقاييس المستخدمة كالتالى:

4-5-1 بالنسبة للتحقق من مستوى الثبات فى المقاييس

تم استخدام معامل كرونباخ ألفا لمعرفة ثبات أداة القياس أو الإعتمادية على إجابات المستقصى منهم على قائمة الإستقصاء على عينة مبدئية (20 مفردة). توصلت الدراسة عند تطبيق كرونباخ الفا على العينة المبدئية إلى أن قيمة كرونباخ ألفا للإختبار الكلى يساوى 0.98 ، 0.964 للحالة الأولى والثانية على التوالى وهى قيمة عالية. يدل ذلك على أن قائمة الاستقصاء تتمتع بدرجة ثبات مرتفعة، مما يدل على الإطمئنان عند تطبيق قائمة الاستقصاء على عينة الدراسة.

4-5-2 للتحقق من مستوى الصدق فى قائمة الاستقصاء: تم قياسه من خلال صدق المحتوى والصدق الذاتى وذلك كما يلى: بالنسبة لصدق المحتوى: تم عرض القائمة فى صورتها الأولية للتحكيم من بعض المحاسبين والمهندسين المتخصصين بالنظم وتكنولوجيا المعلومات، وقد أبدى هؤلاء المحكمون مجموعة من الملاحظات على العبارات الواردة بقائمة الاستقصاء. لذا تم تعديل بعض الفقرات العديد من المرات فى ضوء مقترحاتهم. أما بالنسبة للصدق الذاتى: تم الحصول على مقياس الصدق الذاتى -بأخذ الجذر التربيعى لمعامل الثبات الكلى- والبالغ 0.989، 0.981 للحالة الأولى والثانية على التوالى ، وهى نسبة عالية مما يؤكد على الصدق الذاتى لقائمة الاستقصاء.

جدول 4: ملخص الثبات والصدق للمدخل المقترح

المتغيرات الرئيسية	عدد البنود	معامل الثبات		معامل الصدق	
		حالة (1)	حالة (2)	حالة (1)	حالة (2)
الضوابط الخاصة ببعد المورد البشرى	3	0.936	0.953	0.967	0.976
الضوابط الخاصة ببعد العمليات	5	0.967	0.955	0.983	0.977
الضوابط الخاصة ببعد الحلول التكنولوجية	3	0.966	0.833	0.982	0.912
إجمالى متغيرات البحث	11	0.98	0.964	0.989	0.981

4-6 أساليب التحليل الاحصائي

تم إجراء التحليل الاحصائى لبيانات قائمة الإستقصاء بإستخدام برنامج SPSS الإصدار 26 – أحد البرامج الجاهزة التى تستخدم لتحليل البيانات– وتم الإعتماد على إختبار كولمجروف– سمرنوف (K.S) لمعرفة مدى تبعية بيانات الدراسة للتوزيع الطبيعى، وذلك كما هو موضح فى الجدول التالى:

جدول 5: إختبار تحليل K.S لاختبار توزيع طبيعة البيانات

	معلمات التوزيع الطبيعى	عدد المشاهدات	المتوسط الحسابى	الإنحراف المعيارى	الإختبار الاحصائى	(p.value)
حالة (1)	1.99	858	1.99	0.722	0.373	0.00
حالة (2)	4.30	858	4.5	0.650	0.294	0.00

يتضح من الجدول السابق أن قيمة p. value أقل من مستوى المعنوية 5% (عند مستوى ثقة 95 %) ، وبالتالى تم رفض فرض العدم وقبول الفرض البديل بأن البيانات الخاصة بالدراسة مسحوبة من مجتمع لا يتبع التوزيع الطبيعى، وبالتالى يتم الإعتماد على الأساليب الإحصائية المرتبطة بالإختبارات اللامعلمية. تتمثل الأساليب الإحصائية فى التحليل الوصفى لكل فقرة من فقرات قائمة الإستقصاء، وإختبار Wilcoxon Signed Ranked test لعينتين مترابطتين، وإختبار مان ويتنى لإختبار معنوية الفرق بين أراء عينة الدراسة لكل بعد من الأبعاد الثلاثة فى كل من الحالتين.

4-7 نتائج اختبارات التحليل الاحصائى

تم إختبار فروض الدراسة من خلال قياس إستجابات عينة الدراسة على الأسئلة الخاصة بهذا الجزء فى قائمة الإستقصاء والقيام بعمل تحليل وصفى للعبارات المتعلقة بفروض الدراسة، بالإضافة إلى الإختبارات الخاصة بالفروض وذلك على النحو التالى:

4-7-1 نتائج التحليل الوصفى للعبارات المتعلقة بفروض الدراسة

يوضح الجدول التالى نتائج التكرارات والنسب المئوية والوسط الحسابى والإنحراف المعيارى وإتجاه الإجابات لهذه العبارات.

جدول 6: الإحصاء الوصفى لأسئلة الدراسة

		الحالة الأولى				الحالة الثانية			
		بعد المورد البشرى							
		الموافقة	المتوسط الحسابى	الإنحراف المعيارى	الإتجاه العام	الموافقة	المتوسط الحسابى	الإنحراف المعيارى	الإتجاه العام
1-1	التكرار	6	1.97	0.66	غير موافق	74	4.09	0.64	موافق بشدة
	نسب الموافقة	7.7				94.8			
2-1	التكرار	3	1.99	0.720	غير موافق	74	4.28	0.752	موافق بشدة
	نسب الموافقة	3.8				94.8			
3-1	التكرار	3	1.98	0.69	غير موافق	70	4.35	0.735	موافق بشدة
	نسب الموافقة	3.8				89.7			
إجمالى			1.98	0.690			4.24	0.709	
		بعد العملية							
1-2	التكرار	2	1.92	0.78	غير موافق	72	4.29	0.691	موافق بشدة
	نسب الموافقة	2.6				92.3			
2-2	التكرار	3	1.86	0.80	غير موافق	74	4.40	0.565	موافق بشدة
	نسب الموافقة	3.8				94.9			
3-2	التكرار	7	1.95	0.70	غير موافق	72	4.28	0.601	موافق بشدة
	نسب الموافقة	8.9				92.3			
4-2	التكرار	6	2.13	0.85	غير موافق	70	4.32	0.655	موافق بشدة
	نسب الموافقة	7.7				89.7			
5-2	التكرار	4	2.14	0.722	غير موافق	72	4.26	0.693	موافق بشدة
	نسب الموافقة	5.1				92.3			
إجمالى			2.00	0.771			4.31	0.641	
		بعد التكنولوجى							
1-3	التكرار	6	2.01	0.687	غير موافق	76	4.26	0.599	موافق بشدة
	نسب الموافقة	7.7				97.5			
2-3	التكرار	2	2.00	0.734	غير موافق	74	4.37	0.586	موافق بشدة
	نسب الموافقة	2.6				94.9			
3-3	التكرار	1	1.99	0.592	غير موافق	75	4.42	0.609	موافق بشدة
	نسب الموافقة	1.3				96.1			
إجمالى			2.00	0.671			4.35	0.598	

يشير التحليل المبدئى للمتوسطات المرتبطة ببعد المورد البشرى إلى أن هناك إتجاه عام من أفراد عينة الدراسة على عدم الموافقة على العبارات الخاصة بذلك البعد فى ظل الحالة الأولى (عدم وضع ضوابط خاصة بالمورد البشرى). يتضح أن المتوسط العام للعبارات (الإنحراف المعيارى) يبلغ 1.98 (0.690) وهو متوسط منخفض. كما يتضح من الجدول أيضاً إنخفاض التكرارات ونسب الموافقة لإستجابات عينة الدراسة لبعد المورد البشرى فى الحالة الأولى، مما يؤكد على عدم الموافقة على الضوابط التى وضعتها الشركة فى الحالة الأولى لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء. وعلى العكس من ذلك يتضح من المتوسطات المرتبطة ببعد المورد البشرى فى ظل الحالة الثانية (وضع ضوابط خاصة بالمورد البشرى) أن هناك إتجاه عام من أفراد عينة الدراسة على الموافقة بشدة على العبارات الخاصة ببعد المورد البشرى، حيث أن المتوسط العام للعبارات (الإنحراف المعيارى) يبلغ 4.24 (0.709) وهو متوسط مرتفع جداً. كما يتضح من الجدول أيضاً إرتفاع التكرارات ونسب الموافقة لاستجابات عينة الدراسة لبعد المورد البشرى فى الحالة الثانية، مما يؤكد على الموافقة على الضوابط التى وضعتها الشركة فى الحالة الثانية لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء. لذا يدل ما سبق على أهمية وضع الشركات للضوابط والإجراءات الخاصة بالمورد البشرى لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء.

يشير التحليل المبدئى للمتوسطات المرتبطة ببعد العملية إلى أن هناك إتجاه عام من أفراد عينة الدراسة على عدم الموافقة على العبارات الخاصة بذلك البعد فى ظل الحالة الأولى (عدم وضع ضوابط خاصة بعمليات الشركة لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء). يتضح أن المتوسط العام للعبارات (الإنحراف المعيارى) يبلغ 2.00 (0.771) وهو متوسط منخفض. كما يتضح من الجدول أيضاً إنخفاض التكرارات ونسب الموافقة لاستجابات عينة الدراسة لبعد العملية فى الحالة الأولى، مما يؤكد على عدم الموافقة على الضوابط التى وضعتها الشركة فى الحالة الأولى لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء. وعلى العكس من ذلك يتضح من المتوسطات المرتبطة ببعد العملية فى ظل الحالة الثانية (وضع ضوابط خاصة بعمليات الشركة لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء) أن هناك إتجاه عام من أفراد عينة الدراسة على الموافقة بشدة على العبارات الخاصة ببعد العملية، حيث أن المتوسط العام للعبارات (الإنحراف المعيارى) يبلغ 4.31 (0.641) وهو متوسط مرتفع جداً. كما يتضح من الجدول أيضاً إرتفاع التكرارات ونسب الموافقة لإستجابات عينة الدراسة لبعد العملية فى الحالة الثانية، مما يؤكد على الموافقة على الضوابط التى وضعتها الشركة فى

الحالة الثانية لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء. لذا يدل ما سبق على أهمية وضع الشركات للضوابط والإجراءات الخاصة بعمليات الشركة لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء.

يشير التحليل المبدئى للمتوسطات المرتبطة ببعد التكنولوجى أيضاً إلى أن هناك إتجاه عام من أفراد عينة الدراسة على عدم الموافقة على العبارات الخاصة بذلك البعد فى ظل الحالة الأولى (عدم وضع ضوابط خاصة ببعد التكنولوجى لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء). يتضح أن المتوسط العام للعبارات (الإنحراف المعيارى) يبلغ 2.00 (0.671) وهو متوسط منخفض. كما يتضح من الجدول أيضاً إنخفاض التكرارات ونسب الموافقة لاستجابات عينة الدراسة لبعد التكنولوجى فى الحالة الأولى، مما يؤكد على عدم الموافقة على الضوابط التى وضعتها الشركة فى الحالة الأولى لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء. وعلى العكس من ذلك يتضح من المتوسطات المرتبطة ببعد التكنولوجى فى ظل الحالة الثانية (وضع ضوابط خاصة ببعد التكنولوجى لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء) أن هناك إتجاه عام من أفراد عينة الدراسة على الموافقة بشدة على العبارات الخاصة ببعد التكنولوجى، حيث أن المتوسط العام للعبارات (الإنحراف المعيارى) يبلغ 4.35 (0.598) وهو متوسط مرتفع جداً. كما يتضح من الجدول أيضاً إرتفاع التكرارات ونسب الموافقة لاستجابات عينة الدراسة لبعد التكنولوجى فى الحالة الثانية مما يؤكد على الموافقة على الضوابط التى وضعتها الشركة فى الحالة الثانية لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء. لذا يدل ما سبق على أهمية وضع الشركات للضوابط والإجراءات الخاصة ببعد التكنولوجى لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء.

تدعم أيضاً نتائج الإحصاء الوصفى للسؤال رقم 4 لكل من الحالة الأولى والثانية ما توصل إليه نتائج الإحصاء الوصفى للأسئلة من 1 : 3 بفرعياتهم لكل من الحالة الأولى والثانية. توصلت نتائج الإحصاء الوصفى لهذا السؤال إلى أن عدد الموافقين (نسبة الموافقة) على مدى توقعهم لزيادة المنافع المتحققة للشركة من ربط نظام المعلومات المحاسبى بتكنولوجيا إنترنت الأشياء بمرور الوقت تساوى 15 مفردة (بنسبة 19 %) ، 78 مفردة (بنسبة 100 %) للحالة الأولى والثانية على التوالى. يدل ذلك على زيادة موافقة الأفراد على المنافع المتولدة من تبنى تكنولوجيا إنترنت الأشياء عند إهتمام الشركات بوضع الضوابط الخاصة ببعد المورد البشرى– العملية– التكنولوجى لحماية نظام المعلومات المحاسبى المرتبط بهذه التكنولوجي. كما يتضح أيضاً من نتائج الإحصاء الوصفى

للسؤال العام أن 49 مفردة من عينة الدراسة (بنسبة 62.9 %) يتسمون بتجنبهم للمخاطر. مما يؤكد ذلك على أهمية المدخل المقترح لمواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى وزيادة المنافع المتحققة للشركة من ربط نظام المعلومات المحاسبى بتكنولوجيا إنترنت الأشياء بمرور الوقت، وبصفة خاصة عند إتسام مستخدمى تلك التكنولوجى بتجنبهم للمخاطر؛ لأنه يحميهم من المخاطر المتوقعة من تلك التكنولوجى.

4-7-2 الإختبارات الإحصائية المرتبطة بإختبار فروض البحث: (إختبار Wilcoxon Signed Ranked test لعينتين مترابطتين).

أولاً: نتائج إختبار فرض البحث الأول والذى ينص على أنه لا توجد فروق ذات دلالة إحصائية بين وضع الشركات للضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبطة بالمورد البشرى (المحاسبين بصفة خاصة) وعدم وضع تلك الضوابط عند تبنى تكنولوجيا إنترنت الأشياء لحماية نظام المعلومات المحاسبى. يتم ذلك من خلال مقارنة إجابات عينة الدراسة على الأسئلة من 1-1 : 1-3 المرتبطة ببعد المورد البشرى فى كل من الحالتين. لذا يلخص الجدول التالى نتائج الإحصاء الوصفى والإختبارات الاحصائية المستخدمة لإختبار فرض البحث الأول:

جدول 7: نتائج إختبار ويلكوكسون للمقارنة بين الحالة الأولى والثانية لبعد المورد البشرى

	المتوسط	الانحراف المعيارى	أقل قيمة	أعلى قيمة		الرتب	عدد الرتب	متوسط الرتب	مجموع الرتب	إختبار ويلكوكسون (Z)	الدلالة
حالة (1)	1.98	0.690	1	5	حالة (2) – حالة (1)	السالبة	5	12	60	13.227-	0.00
						الموجبة	221	115.8	25591		
حالة (2)	4.24	0.709	1	5		الروابط	8				
						الإجمالي	224				

يتضح من الجدول السابق أن المتوسط الحسابى لإجابات عينة الدراسة فى الحالة الأولى (عدم وضع الضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبطة بالمورد البشرى (المحاسبين بصفة خاصة) يساوى 1.98 وهو أقل من المتوسط الحسابى فى الحالة الثانية (وضع الضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبطة بالمورد البشرى) 4.24 ، كما يتضح من الجدول أيضاً أنه عند قياس الفرق بين وضع الضوابط الخاصة بالمورد البشرى (الحالة الثانية) وعدم وضع تلك الضوابط (الحالة الأولى) أن عدد الرتب السالبة (5) أقل من عدد الرتب الموجبة (221). مما يؤكد على أن متوسط الحالة الأولى أقل من متوسط الحالة الثانية. كما يلاحظ من نتائج هذا الإختبار أن قيمة P.Value تساوى صفر وهى أقل من مستوى المعنوية 5%. وبالتالى

نقبل الفرض البديل بأن متوسط الإجابات الخاصة بالحالة الأولى يختلف معنوياً عن متوسط الإجابات الخاصة بالحالة الثانية فيما يتعلق ببعد المورد البشرى. ولتحديد إتجاه العلاقة يتم مقارنة إشارات الرتب الموجبة والسالبة، ويلاحظ أن متوسط الرتب الموجبة (115.8) أكبر من متوسط الرتب السالبة (12) ، مما يدل على أن متوسط الإجابات فى الحالة الثانية أكبر من الحالة الأولى أى فى صالح الضوابط المقترحة الخاصة بالبعد البشرى. ويؤكد ذلك على أهمية تطبيق الضوابط الخاصة بالمورد البشرى عند تبنى تكنولوجيا إنترنت الأشياء فى حماية نظام المعلومات المحاسبى .

يؤكد ما سبق على إتفاق نتائج إختبار ويلكوكسون لعينتين مترابطتين مع نتائج التحليل الوصفى، حيث توصلت نتائج ويلكوكسون إلى رفض فرض العدم وقبول الفرض البديل (قيمة P. Value تساوى صفر وهى أقل من مستوى المعنوية 5 %). أى توصلت نتائج الإختبار إلى أن تطبيق الضوابط الخاصة بالمورد البشرى (المحاسبين) يؤدى إلى مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. يدل ذلك على أهمية بعد المورد البشرى وإختيار الموظفين ذوى الصفات الأخلاقية، وأهمية خلق ثقافة الوعى بأهمية الأمن السيبرانى لنظام المعلومات المحاسبى وفهم المحاسبون لطبيعة إنترنت الأشياء والمخاطر التى يمكن أن تتولد منها. كما يتضح من تحليل البيانات أيضاً أهمية المحاسبون فى معرفة المزيد من علم البيانات وإكتساب المهارات التى تؤهلهم لذلك؛ لتحديد البيانات الحساسة ومراقبتها وحمايتها فى ظل تبنى تكنولوجيا إنترنت الأشياء. يؤكد ما سبق على أهمية مواكبة المحاسبون للتطورات فى بيئة الأعمال الحديثة وإدراكهم للمخاطر المرتبطة بها فى ظل تبنى الشركات لتكنولوجيا إنترنت الأشياء وهو ما توصلت اليه بعض الدراسات (WatchGuard,2010; Payne , 2018; Cui et al., 2020; Zadorozhnyi et al., 2020; Alghamdie,2021; Busulwa and Evans, 2021) .

ثانياً: نتائج إختبار فرض البحث الثانى والذى ينص على أنه لا توجد فروق ذات دلالة إحصائية بين وضع الشركات للضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبطة بعملياتها وعدم وضع تلك الضوابط عند تبنى تكنولوجيا إنترنت الأشياء لحماية نظام المعلومات المحاسبى. يتم ذلك من خلال مقارنة إجابات عينة الدراسة على الأسئلة من 2-1 : 2-5 المرتبطة ببعد العملية فى كل من الحالتين. ويلخص الجدول التالى نتائج الإحصاء الوصفى والإختبارات الاحصائية المستخدمة لإختبار فرض البحث الثانى:

جدول 8: نتائج إختبار ويلكوكسون للمقارنة بين الحالة الأولى والثانية لبعد العمليات

	المتوسط	الانحراف المعيارى	أقل قيمة	أعلى قيمة		الرتب	عدد الرتب	متوسط الرتب	مجموع الرتب	إختبار ويلكوكسون (Z)	الدلالة
حالة (1)	2.00	0.771	1	5	حالة (2) – حالة (1)	السالبة	7	18.5	129.50	16.861-	0.00
						الموجبة	362	188.22	68135.5		
حالة (2)	4.31	0.641	1	5		الروابط	21				
						الإجمالي	390				

يتضح من الجدول السابق أن المتوسط الحسابى لإجابات عينة الدراسة فى الحالة الأولى (عدم وضع الضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبطة بعملياتها) يساوى 2.00 وهو أقل من المتوسط الحسابى فى الحالة الثانية (وضع الضوابط الخاصة بحماية أمن الشبكات والمعلومات المرتبطة بعملياتها) 4.31 ، كما يتضح من الجدول أيضاً أنه عند قياس الفرق بين وضع الضوابط الخاصة بالعملية (الحالة الثانية) وعدم وضع تلك الضوابط (الحالة الأولى) أن عدد الرتب السالبة (7) أقل من عدد الرتب الموجبة (362) . مما يؤكد على أن متوسط الحالة الأولى أقل من متوسط الحالة الثانية. كما يلاحظ من نتائج هذا الإختبار أن قيمة P. Value تساوى صفر وهى أقل من مستوى المعنوية 5%. وبالتالى نقبل الفرض البديل بأن متوسط الإجابات الخاصة بالحالة الأولى يختلف معنوياً عن متوسط الإجابات الخاصة بالحالة الثانية فيما يتعلق ببعد العملية. ولتحديد إتجاه العلاقة يتم مقارنة إشارات الرتب الموجبة والسالبة، ويلاحظ أن متوسط الرتب الموجبة (188.22) أكبر من متوسط الرتب السالبة (18.5) ، مما يدل على أن متوسط الإجابات فى الحالة الثانية أكبر من الحالة الأولى أى فى صالح الضوابط المقترحة الخاصة ببعد العملية. ويؤكد ذلك على أهمية تطبيق الضوابط الخاصة بعمليات الشركة عند تبنى تكنولوجيا إنترنت الأشياء فى حماية نظام المعلومات المحاسبى .

أى يتضح مما سبق إتفاق نتائج إختبار ويلكوكسون لعينتين مترابطتين مع نتائج التحليل الوصفى، حيث توصلت نتائج ويلكوكسون إلى رفض فرض العدم وقبول الفرض البديل (قيمة P. Value تساوى صفر وهى أقل من مستوى المعنوية 5 %). توصلت نتائج الإختبار إلى أن تطبيق الضوابط الخاصة بالعملية يؤدى إلى مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. يدل ذلك على أهمية بعد العملية والأبعاد الفرعية المنبثقة من ذلك البعُد التى تقوم بها الشركات لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء. أى يؤدى إهتمام الشركات ببعُد العملية إلى حماية نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت

الأشياء. لذا تتفق نتائج الدراسة مع الدراسات السابقة (Ernest and Young, 2011; Cui et al., 2020; Lartey et al., 2021) .

ثالثاً: نتائج إختبار فرض البحث الثالث والذى ينص على أنه لا توجد فروق ذات دلالة إحصائية بين وضع الشركات للضوابط المرتبطة بالتقنيات التكنولوجية والضوابط الخاصة بحماية أمن الشبكات والمعلومات وعدم وضع تلك الضوابط عند تبنى تكنولوجيا إنترنت الأشياء لحماية نظام المعلومات المحاسبى. يتم ذلك من خلال مقارنة إجابات عينة الدراسة على الأسئلة من 3-1: 3-3 المرتبطة ببعد التكنولوجى فى كل من الحالتين. لذا يلخص الجدول التالى نتائج الإحصاء الوصفى والإختبارات الاحصائية المستخدمة لإختبار فرض البحث الثالث:

جدول 9: نتائج إختبار ويلكوكسون للمقارنة بين الحالة الأولى والثانية لبعد التكنولوجى

	المتوسط	الانحراف المعيارى	أقل قيمة	أعلى قيمة		الرتب	عدد الرتب	متوسط الرتب	مجموع الرتب	إختبار ويلكوكسون (Z)	الدلالة
حالة (1)	2.00	0.671	1	5	حالة (2) – حالة (1)	السالبة	1	8	8	13.238-	0.00
						الموجبة	223	112.97	25192		
حالة (2)	4.35	0.598	2	5		الروابط	10				
						الإجمالي	234				

يتضح من الجدول السابق أن المتوسط الحسابى لإجابات عينة الدراسة فى الحالة الأولى (عدم وضع الشركة للضوابط المرتبطة بالتقنيات التكنولوجية والضوابط الخاصة بحماية أمن الشبكات والمعلومات) يساوى 2.00 وهو أقل من المتوسط الحسابى فى الحالة الثانية (وضع الضوابط المرتبطة بالتقنيات التكنولوجية والضوابط الخاصة بحماية أمن الشبكات والمعلومات) 4.35 ، كما يتضح من الجدول أيضاً أنه عند قياس الفرق بين وضع الضوابط الخاصة بالتقنيات التكنولوجية والضوابط الخاصة بحماية أمن الشبكات والمعلومات (الحالة الثانية) وعدم وضع تلك الضوابط (الحالة الأولى) أن عدد الرتب السالبة (1) أقل من عدد الرتب الموجبة (223) . مما يؤكد على أن متوسط الحالة الأولى أقل من متوسط الحالة الثانية. كما يلاحظ من نتائج هذا الإختبار أن قيمة P. value تساوى صفر وهى أقل من مستوى المعنوية 5%. وبالتالى نقبل الفرض البديل بأن متوسط الإجابات الخاصة بالحالة الأولى يختلف معنوياً عن متوسط الإجابات الخاصة بالحالة الثانية فيما يتعلق ببعد الضوابط المرتبطة بالتقنيات التكنولوجية والضوابط الخاصة بحماية أمن الشبكات والمعلومات. ولتحديد إتجاه العلاقة يتم مقارنة إشارات الرتب الموجبة والسالبة، ويلاحظ أن متوسط الرتب الموجبة (112.97) أكبر من متوسط الرتب السالبة (8) ، مما يدل على أن متوسط الإجابات فى الحالة الثانية أكبر من الحالة الأولى أى فى صالح الضوابط المقترحة الخاصة

بالتقنيات التكنولوجية والضوابط الخاصة بحماية أمن الشبكات والمعلومات. ويؤكد ذلك على أهمية تطبيق الضوابط الخاصة بحماية أمن الشبكات والمعلومات عند تبنى تكنولوجيا إنترنت الأشياء فى حماية نظام المعلومات المحاسبى.

أى يتضح مما سبق إتفاق نتائج إختبار ويلكوكسون لعينتين مترابطتين مع نتائج التحليل الوصفى، حيث توصلت نتائج ويلكوكسون إلى رفض فرض العدم وقبول الفرض البديل (قيمة p.value تساوى صفر وهى أقل من مستوى المعنوية 5 %). توصلت نتائج الإختبار إلى أن تطبيق الضوابط المتعلقة بالتقنيات التكنولوجية والضوابط الخاصة بحماية أمن الشبكات والمعلومات يؤدى إلى مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. يدل ذلك على أهمية بعد التكنولوجى والأبعاد الفرعية المنبثقة من ذلك البعُد التى تقوم بها الشركات لحماية نظام المعلومات المحاسبى عند تبنى تكنولوجيا إنترنت الأشياء. لذا يؤدى إهتمام الشركات ببعُد التكنولوجى والضوابط المرتبطة بذلك البعُد إلى حماية نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء. لذا تتفق نتائج الدراسة مع الدراسات السابقة (Ernst and Young, 2011; Janes, 2012; Contreras and Coatrieux,2017; Ducan et al., 2017; Sanagani and Zarger,2017; Altam et al., 2018; CPA, 2019; Ghumro et al., 2020).

4-7-3 إختبار مان ويتنى لإختبار معنوية الفرق بين أراء عينة الدراسة وفقاً لمجال عملهم

يعتبر مان ويتني من الإختبارات اللامعلمية، وهو بديل لإختبار t لعينتين مستقلتين. يستخدم هذا الإختبار لقياس معنوية الفرق بين أراء عينة الدراسة وفقاً لمجال عملهم. يتم قياس معنوية الفرق بين أراء المحاسبين والمهندسين المختصين بالنظم وتكنولوجيا المعلومات لمدى أهمية الضوابط الخاصة ببعُد المورد البشرى، والعملية، والتكنولوجى فى حماية نظام المعلومات المحاسبى من مخاطر تكنولوجيا إنترنت الأشياء فى ظل الحالتين كما فى الجدول التالى:

جدول 10: إختبار مان ويتنى لإختبار الفروق بين أراء عينة الدراسة

	قيمةp. value	الدلالة	قيمةp. value	الدلالة
	الحالة الأولى		الحالة الثانية	
بعد المورد البشرى	0.206	غير دال	0.242	غير دال
بعد العملية	0.984	غير دال	0.673	غير دال
البعد التكنولوجى	0.146	غير دال	0.850	غير دال

يتضح من الجدول السابق عدم وجود فروق معنوية بين المحاسبين والمهندسين المختصين بالنظم وتكنولوجيا المعلومات فى الأبعاد الثلاثة (بعد المورد البشرى، العملية، التكنولوجى) لكل من الحالة الأولى والثانية. وقد يرجع ذلك إلى أن عينة الدراسة على دراية وعلم بالمستجدات الحديثة في بيئة العمل وإدراكهم لمدى حماية نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء. لذا تؤكد نتائج الدراسة على أهمية الضوابط الخاصة بالمورد البشرى – العملية– التكنولوجى فى مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى.

5- خلاصة البحث ونتائجه وتوصياته

إستهدف البحث إقتراح مدخل لمواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. توصل البحث فى شقه النظرى إلى أهمية تبنى تكنولوجيا إنترنت الأشياء فى الشركات؛ لما لها من تأثير على تحسين العمليات التشغيلية وتخفيض تكاليف الشركات، بالإضافة إلى الوصول إلى معلومات فور حدوث الحدث مما يساعد على إتخاذ القرارات السليمة فى الوقت المناسب. وعلى الرغم من توضيح بعض الدراسات لأهمية تبنى تكنولوجيا إنترنت الأشياء، إلا أن البعض الأخر نظر إلى تلك التكنولوجيا من ناحية المخاطر المرتبطة بها وبصفة خاصة مخاطر الأمن والخصوصية؛ والذى قد يرجع إلى المشاكل التقنية التى تواجه تلك التكنولوجيا. وخلصت الدراسة من الشق النظرى إلى اقتراح مدخل يعتمد على بعد المورد البشرى– العملية – التكنولوجى لمواجهة تلك المخاطر على نظام المعلومات المحاسبى. كما توصلت نتائج الدراسة التجريبية إلى: أهمية المدخل المقترح فى حماية نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء. كما أن الإهتمام بوضع تلك الضوابط المتضمنة فى المدخل المقترح يؤدى إلى زيادة المنافع المتوقعة من تبنى تكنولوجيا إنترنت الأشياء بمرور الوقت.

لذا توصى الباحثة بضرورة إهتمام الشركات بوضع الضوابط التى تساعدها على حماية نظام المعلومات المحاسبى المرتبط بتبنى تلك التكنولوجيا. كما توصى الباحثة بضرورة إهتمام أقسام المحاسبة بكليات التجارة فى الجامعات المصرية بدراسة المقررات البينية فى المجالات المختلفة لتوضيح منافع ومخاطر تبنى أدوات الثورة الصناعية الرابعة على نظام المعلومات المحاسبى.

فى ضوء ما توصل اليه البحث من نتائج وتوصيات، فقد ظهرت بعض المجالات البحثية المرتبطة بموضوع البحث والتى يمكن تناولها فى البحوث المستقبلية ومنها: إستكشاف العوامل التى قد تزيد (تخفض) من منافع (تكاليف) الإستثمار بالأمن السيرانى عند تبنى الشركات لتكنولوجيا إنترنت الأشياء، ودراسة محددات تبنى الشركات لنظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء بما في ذلك خصائص الصناعة وخصائص الشركة ، وكذلك دراسة الفرص والتحديات التى تواجه إرتباط نظام المعلومات المحاسبى بتكنولوجيا إنترنت الأشياء، وأخيراً تقييم الإستثمار فى نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء من حيث المنافع والتكاليف والمخاطر.

المراجع

أولاً: المراجع باللغة العربية

الاستراتيجية الوطنية للامن السيبرانى ،2017 ، المجلس الأعلى للأمن السيبرانى، رئاسة مجلس الوزراء، جمهورية مصر العربية.

خميس، محمد مصطفى، 2021، " أثر تطبيق تقنية إنترنت الأشياء فى ظل تبني الحوسبة السحابية على نظام إدارة المخزون" ، مجلة الإسكندرية للبحوث المحاسبية، العدد الأول، المجلد الخامس، 1-40.

ثانياً: المراجع باللغة الأجنبية

Abad-Segura, E., Infante-Moro, A., González-Zamar, M. D., & López-Meneses, E. (2021). Blockchain technology for secure accounting management: Research trends analysis. *Mathematics*, *9*(14), 1–26.

Alghamdie, M. I. (2021). A novel study of preventing the cyber security threats. *Materials Today: Proceedings*, article in press, 1-5. https://doi.org/10.1016/j.matpr.2021.04.078

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *International Journal of Intelligent Systems and Applications*, *10*(6), 40–48.

Atlam, H. F., & Wills, G. B. (2020). *IoT Security, Privacy, Safety and Ethics*. *Internet of Things*. Springer International Publishing, 123-149.

Bagay, D. (2020). Information security of Internet things. *Procedia Computer Science*, *169*(2019), 179–182.

Bauer, H., Scherf , G. ,Tann, V & Klinkhammer, L. (2019). Perspectives on transforming cybersecurity. *McKinsey Global Institute*, *32* (March), 1–128. https://www.mckinsey. com/~/media /McKinsey /McKinsey Solutions/Cyber Solutions/Perspectives on transforming cybersecurity/Transforming cybersecurity_March2019.ashx

Bhimani , A., Willcocks, L. (2014). Digitisation, 'Big Data' and the transformation of accounting information. Accounting and Business Research, Volume 44, 2014 - Issue 4: International Accounting Policy Forum, 469-490.

Bhol, S., Mohanty, J., & Kumar Pattnaik, P. (2021). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings*. In press, 1-6.

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., O'Rourke , D., Piccarreta, B., & Scarfone, K. (2019). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, 1-44. https://doi.org/10.6028/NIST.IR.8228

Busulwa, R., & Evans, N. (2021). Digital Transformation in Accounting. *Digital Transformation in Accounting*. https: //doi.org/ 10. 4324/9780429344589

Chelakkara , S. (2020). People, Process And Technology In Cybersecurity. Ampcus Cyber , 1-9.

CPA,.(2019). Internet of Things Technology Spotlight.1-6,https://cpacanada. ca.

Contreras, J. F., & Coatrieux, G. (2017). Protection of Relational Databases by Means of Watermarking: Recent Advances and Challenges. *Advances in Security in Computing and Communications*, 1-6.

CyberEdge Group. (2019). Cyberthreat Defense Report. *CyberEdge Group*, 1–50. Retrieved from https://cyber-edge.com/

Cao, H., & Zhu, Z. (2012). Research on future accounting information system in the Internet of Things era. *ICSESS 2012 - Proceedings of 2012 IEEE 3rd International Conference on Software Engineering and Service Science*, 741–744. https:// doi.org/ 10.1109/ ICSESS. 2012.6269573

Chang, S. I., Chang, L. M., & Liao, J. C. (2020). Risk factors of enterprise internal control under the internet of things governance: A

qualitative research approach. *Information and Management*, *57*(6), 1-18.

_____., Huang, A., Chang, L. M., & Liao, J. C. (2016). Risk factors of enterprise internal control: Governance refers to Internet of Things (IoT) environment. *Pacific Asia Conference on Information Systems , PACIS 2016 - Proceedings, 1-11.*

Contreras, J. F., & Coatrieux, G. (2017). Protection of Relational Databases by Means of Watermarking: Recent Advances and Challenges. *In book: Advances in Security in Computing and Communications, Chapter: 05, Publisher: InTech , by :Jaydip Sen.*

Cui, C., Kaduskar , N., Miller, D., & Tate, A. (2020). Building the foundation of your cybersecurity program ,1-24. https:// rhisac. org/ wp-content/uploads/RH-ISAC_ Building the Foundation _ White Paper.pdf

Dai Y., & Ge , X. (2015). Optimization Of The Internal Accounting Control Based On The internet Of Things. Chapter in Management, Information And Educational Engineering,1st edition, https:// Www. Taylorfrancis. Com /Books /Mono /10.1201/B18558 /Management-Informationeducational -Engineering? Refid= Ae 66407f-B34e-428e-B7b8- 29608 f4799 da & Context = Ubx)

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189–208.

Devi, S., & M. Mohankumar. (2019) . An empirical study on cyber security threats and attacks. International Journal of Scientific Research and Review, Volume 07, Issue 03, 2271-2276.

Duncan, B., Happe, A., & Bratterud, A. (2017). Cloud Cyber Security: Finding an Effective Approach with Unikernels. *Advances in Security in Computing and Communications*. 31-119.

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, *13* (2), C1–C9.

Efosa, E., Oseikhuemhen, J., & Onyinye , E. (2021). Cyber Security : The perspective of Accounting Professionals in Nigeria, Accounting & Taxation Review, Vol. 5, No. 2 ,15-29.

ENISA. (2019). Industry 4.0 Cybersecurity:Challenges & Recommendations. 1-13. https:// www. enisa. europa. eu/ publicat-ions/industry-4-0-cybersecurity-challenges-and-recommendations

Ernst & Young. (2011). Data Loss Prevention Keeping Your Sensetive Data Out of the Puplic Domain. Insights on Governance Risk and Compliance. 1-24.

_____. (2018). Is cybersecurity about more than protection? *EY Global Information Security Survey*, 1-36, https://assets.ey.com/ content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-infor-mation-security-survey-2018-19.pdf.

Gansler, J. S., & Lucyshyn, W. (2005). Improving the security of financial management systems: What are we to do? *Journal of Accounting and Public Policy*, *24* (1), 1–9.

Ghumro, A., Memon, A. K., Memon, I., & Simming, I. A. (2020). A Review of Mitigation of Attacks in IoT using Deep Learning Models, *18*(1), Quest Research Journal, Vol. 18, No. 1, 36–42.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34* (7), 808–834.

HaddadPajouh, H., Dehghantanha, A., M. Parizi, R., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things (Netherlands)*, *14*, 1–19. https://doi.org/10.1016/j.iot.2019.100129

Hatane, S. E., Johari, I. V. D., Valencia, J., & Prayugo, L. E. (2019). The Acceptance of Accounting Students on the Use of Internet of

Things, *103* (Teams 19), 273–278. https://doi.org/10.2991/teams-19.2019.44

Interpol African Cyberthreat Assesment Report. (2021). Interpol's key insight into cybercrime in Africa. 1-34, https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa.

Iot Alliace Australia. (2020). Ensuring your IoT is secure a user's guide . 1-34, https://iot.org.au/wp/wp-content/uploads/2021/02/IoTAA-IoT-Users-Security-Awareness-Guide.pdf .

ITU. (2008). Data networks, open system communications and security Telecommunication security. 1-64, https://docplayer.net/12447473-Series-x-data-networks-open-system-communications-and-security-cyberspace-security-identity-management.html.

Jaidi, F. (2017). Advanced Access Control to Information Systems: Requirements, Compliance and Future Directives. *Advances in Security in Computing and Communications* , 83-97.

Janes, P. (2012). *People, Process, and Technologies Impact On Information Data Loss. SANS Institute.* 1-58 , https:// www. scribd. com/ document/493224074/Paper-SANS-People-Process-and-Technologies-Impact-on-Information-Data-Loss-DLP-2012.

Janvrin, D. J., & Wang, T. (2019). Implications of cybersecurity on accounting information. *Journal of Information Systems*, *33* (3), A1–A2.

Khadam, U., Iqbal, M. M., Alruily, M., Al Ghamdi, M. A., Ramzan, M., & Almotiri, S. H. (2020). Text Data Security and Privacy in the Internet of Things: Threats, Challenges, and Future Directions. *Wireless Communications and Mobile Computing*, *1-15,*https://doi.org/10.1155/2020/7105625https://doi.org/10.1155/2020/ 7105625

Kremer, S., Mé, L., Rémy, D., & Roca, V. (2019). Cybersecurity: Current challenges and Inria's research directions., 1-172. Retrieved from https://hal.inria.fr/hal-01993308

Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, *1*(1).1-15. https://doi.org/10.1007/s43926-020-0000

Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, *7*(3), 1-13.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440.

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 1-21.

Leloglu, E. (2017). A Review of Security Concerns in Internet of Things. *Journal of Computer and Communications*, *05* (01), 121–136.

Liu, Y. H., & Zhang, S. (2020). Information security and storage of Internet of Things based on block chains. *Future Generation Computer Systems*, *106*, 296–303.

Mahlous, A. R., & Ara, A. (2020). The Adoption of Blockchain Technology in IoT: An Insight View. *Proceedings - 2020 6th Conference on Data Science and Machine Learning Applications, CDMA 2020*, (March), 100–105.

Maistry, T. N., Ramkurrun, N., Cootignan, M., & Catherine, P. C. (2015). Cyber security : Threats , Vulnerabilities and Countermeasures - A Perspective on the State of Affairs in Mauritius, Proceedings of the Second International Conference on Data Mining, Internet Computing, and Big Data, Reduit, Mauritius,54–68.

Martens, C. D. P., Silva, L. F. da, Silva, D. F., & Martens, M. L. (2021). Challenges in the implementation of internet of things projects and actions to overcome them. *Technovation*, (November), article in press.1-16. https://doi.org/10.1016/j.technovation.2021.102427

Moll, J., & Yigitbasioglu, O. (2019). The role of internet-related technologies in shaping the work of accountants: New directions for accounting research. *British Accounting Review*, *51*(6), 1-20.

Muravskyi, V., Pochynok, N., & Farion, V. (2021). Classification of cyber risks in accounting. *Herald of Economics*, (2), 129-144.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, *535*, 9–25. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

O'Leary, D. E. (2013). 'Big Data', the 'Internet of Things' and the 'Internet of Signs.' *Intelligent Systems in Accounting, Finance and Management*, *20*(1), 53–65.

Onyshchenko, O., Shevchuk , K., Shara, Y., Koval, N., & Demchuk, O. (2022). Industry 4.0 And Accounting: Directions, Challenges, Opportunities. Independent Journal Of Management & Production (Ijm&P), V. 13, n. 3, Special Edition ISE, S&P, 161-195.

Payne,R. (2019). The Internet Of Things And Accounting: Lessons From China.ICAEW thought leadership business and management,10-37.

Pendley, J. (2018). Finance and Accounting Professionals and Cybersecurity Awareness. The Journal of Corporate Accounting & Finance, 53-58.

Ponemon Institute. (2019). Cost of a Data Breach Report . IBM security , 1-78, https://www.ibm.com/downloads/cas/RDEQK07R.

Popescu, T. M., Popescu, A. M., & Prostean, G. (2021). Iot security risk management strategy reference model (IoTSRM2). *Future Internet*, *13* (6), 1-43.

Qiu, F. (2016). Overall framework design of an intelligent dynamic accounting information platform based on the internet of things. *International Journal of Online Engineering*, *12* (5), 14–16. https://doi.org/10.3991/ijoe.v12i05.5728

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5),5288-5303.

Romney, M., & B., Steinbart, J. (2018). Accounting information systems-(14th Ed). Harlow: Pearson.

Saif, I., Peasley, S., & Perinkolam, A. (2015). Safeguarding the Internet of Things. *Deloitte Review*, (17), 100–117. Retrieved from https:// dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html

Sangani, N. K., & Zarger, H. (2017). Machine Learning in Application Security. *Advances in Security in Computing and Communications*, 61-78.

Sarwar, M. I., Iqbal, M. W., Alyas, T., Namoun, A., Alrehaili, A., Tufail, A., & Tabassum, N. (2021). Data Vaults for Blockchain-Empowered Accounting Information Systems. *IEEE Access*, *1-22*.

Sen, J.(2017). Advances in security in computing and communications. Intech publisher, 1st edition.

Shao, H., Zhang, Z., & Wang, B. (2021). Research on accounting information security management based on blockchain. *Mobile Information Systems*, *1-11*. https://doi.org/10.1155/2021/9926106

Solms, B., & Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26* (1), 2–9.

Suraj, S. (2021). Cyber Security and Internet of Things.Campbellsville Univ-ersity,(May),1-27,conference paper, https: // www.researchgate.net/ publication/351576013_Cyber_Security_and_Internet_of_ Things.

Tavana, M., Hajipour, V., & Oveisi, S. (2020). IoT-based enterprise resource planning: Challenges, open issues, applications, architecture, and future research directions. *Internet of Things (Netherlands)*, *1-27*. https://doi.org/10.1016/j.iot.2020.100262

Taveras, P. (2019). Cyber Risk Management, Procedures and Considerations to Address the Threats of a Cyber Attack. *ForenSecure: Cybersecurity and Forensics Conference*, (April), 1–10. Retrieved from https://www.researchgate.net/publication/332411201_Cyber_Risk_Management_Procedures_and_Considerations_to_Address_the_Threats_of_a_Cyber_Attack

Thangaiah, S., Sharma, V., & Sundharam, V. N. (2018). Internet of Things (IoT) Integration with Enterprise Resource Planning Application in Manufacturing Industries. *International Journal of Mechanical Engineering and Technology (IJMET*, *9*(7), 877–884.

The Association of Chartered Certified Accountants.(2019). Audit and Technology. Chartered Accountants Australia and New Zealand 1-22. Retrieved from https:// www.accaglobal.com/ content/dam/ ACCA_Global/professional-insights/audit-and-tech/pi-audit-and-technology.pdf

U.S. Department of Energy .(2021). Cybersecurity Capability Maturity Model, Version 2.0, Carnegie Mellon University , 1-81, https://www. energy. gov/ sites/ default/ files/ 2021- 07/C2M2% 20Version%202.0% 20July% 202021_508.pdf .

Valentinetti, D., & Flores Muñoz, F. (2021). Internet of things: Emerging impacts on digital reporting. *Journal of Business Research*, *131*(January), 549–562.

Van Niekerk , A., & Rudman, R. (2019). Risks, controls and governance associated with internet of things technologies on accounting information. Southern African Journal of Accountability and Auditing ResearchVol. 21, No. 1,15-30.

Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research current state and future directions. *Journal of Information Systems*, *35*(1), 155–186.

Wang, Y. (2016). Research on the accounting information construction path based on internet of things and data mining. *RISTI (Revista Iberica de Sistemas e Tecnologias de Informacao)*, (E6), 222-233.

Watchguard. (2010). Data Loss Protection Data Loss Prevention : Keep Sensitive Data-In-Motion Safe. *Watchguard*, (November), 1-11.

Wu, J., Xiong, F., & Li, C. (2019). Application of internet of things and blockchain technologies to improve accounting information quality. *IEEE Access*, *7*, 1-10.

Yilmaz, N. K. , & Hazar, H. (2019). The rise of internet of things (IoT) and its applications in finance and accounting. *Pressacademia*, *10*(10), 32–35. https://doi.org/10.17261/pressacademia.2019.1139

Zadorozhnyi, Z., Muravskyi, V., Shevchuk, O., & Muravskyi, V. (2020). the Accounting System As the Basis for Organising Enterprise Cybersecurity. *Financial and Credit Activity: Problems of Theory and Practice*, *3* (34), 147-156. https://doi.org/ 10.18371/ fcaptp. v3i34. 215462

Zhang, Y. (2019). Security Risk of Network Accounting Information System and Its Precaution. Advances in Computer Science Research, volume 87,418–422.

ملحق البحث: الدراسة التجريبية

عزيزى المشارك / عزيزتى المشاركة

تحية طيبة وبعد ،،،

تقوم الباحثة بعمل دراسة تجريبية على حالة افتراضية لاحدى الشركات فى مجال صناعة الاجهزة الالكترونية وذلك بهدف انجاز بحث بعنوان " مدخل مقترح لمواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى – دراسة تجريبية ". لذا يركز البحث على دراسة أهمية المورد البشرى – العملية– التكنولوجى لمواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى. والمطلوب من سيادتكم دراسة الحالة جيداً والإجابة على الأسئلة التى تليها . وأود أن أؤكد لسيادتكم أن هذه الدراسة تلتزم بالقواعد الأكاديمية للأبحاث. وسوف تعامل جميع الإجابات بسرية كاملة ، كما يتم تحليل البيانات على أساس إجمالى.

وأتقدم لسيادتكم بخالص الشكر والتقدير على موافقتكم على المشاركة فى هذه الدراسة ومساهمتكم القيمة فى البحث العلمى

أولاً: البيانات الشخصية

- **المؤهل الدراسى: □ مؤهل متوسط □ بكالوريوس تجارة □ بكالوريوس هندسة □ بكالوريوس حاسبات ومعلومات □ بكالوريوس علوم**
- **الدراسات العليا : □ دبلوم □ ماجستير □ دكتوراه**
- **المنصب الإدارى الذى يشغله المشارك (إن وجد).....**
- **عدد سنوات العمل فى الشركة.....**

ثانياً: المصطلحات المرتبطة بالدراسة

– **إنترنت الأشياء:** شبكة شاملة من الأشياء الذكية – يقصد بالأشياء أى جهاز يمكن تعريفه على الإنترنت من خلال الصاق عنوان الإنترنت IP مثل السيارات، الأدوات المنزلية، الألآت، والسلع والمنتجات– . ويكون لها القدرة على التنظيم التلقائى ومشاركة المعلومات والبيانات. أى أنه يتم التواصل فى ظل تبنى تكنولوجيا إنترنت الأشياء بين الأجهزة وبعضها البعض عن طريق الإنترنت دون تدخل الإنسان. تتكون إنترنت الأشياء من أربعة مكونات رئيسية أجهزة استشعار، واتصال بالشبكة والإنترنت، وبرامج لمعالجة البيانات، وواجهة المستخدم. تقوم أجهزة الاستشعار

بجمع البيانات من البيئة المتواجدة فيها، ثم يقوم بارسال هذه البيانات إلى السحابة (الحوسبة السحابية) لتخزين البيانات عبر شبكة الإنترنت، ثم يتم معالجتها باستخدام أحد برامج تحليل البيانات ومن ثم إرسال نتائج التحليل إلى مستخدم هذه البيانات ونظام المعلومات المحاسبى.

- **القرصنة الالكترونية:** اختراق لأجهزة الحاسب عبر شبكة الإنترنت أو أجهزة إنترنت الأشياء. يقوم بهذه العملية شخص أو مجموعة من الأشخاص لديهم خبرة واسعة في البرمجيات، إذ يمكنهم بواسطة برامج مساعدة الدخول إلى تلك الأجهزة والتعرف على محتوياتها.
- **الأمن السيبرانى:** عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية. تهدف هذه الهجمات السيبرانية عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها؛ بغرض إحداث ضرر للمستهدفين سواء شركات أو أفراد.
- **تكنولوجيا البلوك تشين:** نظام لسجل إلكتروني مشترك، آني، ومشفر، وغير مركزي لمعالجة وتخزين المعاملات المالية، ومعلومات سلسلة التوريد. يمكن لجميع المشاركين في السلسلة رؤية تفاصيل كل سجل، وتتبع المعلومات عبر شبكة آمنة لا تستدعي التحقق من طرف ثالث.
- **حوكمة تكنولوجيا المعلومات:** العمليات التي تضمن الاستخدام الكُفء والفعال لتكنولوجيا المعلومات في تمكين الشركات من تحقيق أهدافها الاستراتيجية. وهى تساعد على حماية تقنيات المعلومات بكافة مكوناتها من الآت وبرمجيات وشبكات من أى تلاعب أو أضرار مادية أو الكترونية وتنفيذ الضوابط الرقابية ووضع الأهداف لحماية تلك التقنيات.

ثالثاً: الحالات التجريبية

حالة (1)

تعد الشركة (س) واحدة من أبرز الشركات فى تصنيع الاجهزة الالكترونية فى مصر. تمتلك الشركة العديد من الفروع فى مصر وبعض الدول العربية. تهتم الشركة بالتحول الرقمى ايماناً منها بأهمية تحقيق رؤية مصر 2030 من خلال القيام بتحويل مصانعها إلى مصانع ذكية وتكامل سلسلة التوريد لديها. لذا قامت بتطبيق تكنولوجيا إنترنت الأشياء وربط الأجهزة المرتبطة به بنظام المعلومات المحاسبى للشركة (أوراكل) ، وذلك لامكانية تتبع المنتجات وإدارة المخزون وتخفيض التكاليف بالاضافة إلى إنشاء المستندات المحاسبية الكترونياً وإعداد التقارير المالية بسرعة وفى وقت حدوث الحدث.

وفى سبيل قيام الشركة بتبنى تكنولوجيا إنترنت الاشياء وربطه بنظام المعلومات المحاسبى قامت باجراء الضوابط التالية:

الضوابط الخاصة ببُعد المورد البشرى

1. اختيار بعض المحاسبين والموظفين عشوائياً وبعض الأطراف المتعاملة مع إنترنت الاشياء (400 محاسب فقط من إجمالى 4000 محاسب على مستوى فروع الشركة) لتدريبهم على تكنولوجيا إنترنت الأشياء وربطه بنظام المعلومات المحاسبى.
2. خلق ثقافة الوعى بأهمية الأمن السيبرانى لنظام المعلومات المحاسبى من خلال وضع الشركة للتعليمات على بعض جدران الشركة.
3. قامت الشركة بتكوين فريق يتكون من الإدارة العليا ومهندسى علم البيانات فقط لتحديد الأهداف التنظيمية لإدارة البيانات المحاسبية وتحليلها.

الضوابط الخاصة ببعُد العمليات

1. إنشاء بعض التعليمات البسيطة لسياسات الأمن السيبرانى ووضعها بصورة غير واضحة داخل السياسة العامة للشركة.
2. الاستمرار فى تطبيق نفس اللوائح المتعلقة بالتنظيم الداخلى للعمل فى الشركة قبل تبنى تكنولوجيا إنترنت الأشياء مع وضع بعض القواعد البسيطة وغير التفصيلية لمسؤليات المحاسبين لحماية نظام المعلومات المحاسبى فى ظل تبنى تكنولوجيا إنترنت الأشياء مثل عدم إعطاء كلمات المرور لأى شخص سواء داخل أو خارج الشركة.
3. بالنسبة لنظام تحديد هوية وصلاحيات المستخدم user authentication and authorization: يتم دخول المستخدمين إلى نظام المعلومات المحاسبى الخاص بالشركة بخطوة واحدة ثابتة (الأسم وكلمة المرور password) ، كما أن كافة مستخدمى قاعدة بيانات الشركة لهم كافة الصلاحيات سواء فى الإطلاع أو تعديل البيانات.
4. بالنسبة لعدد الأطر والمؤشرات التى استخدمتها الشركة لإدارة المخاطر والرقابة الداخلية: استخدمت الشركة إطاراً واحداً للرقابة الداخلية للشركة وذلك لضمان تحقيق أهداف الشركة بفعالية وكفاءة وإصدار تقارير مالية موثوق بها، والإمتثال للقوانين واللوائح والسياسات.
5. بالنسبة لإدارة المخاطر السيبرانية بين أعضاء سلسلة التوريد والإتفاق مع مزود خدمة الحوسبة السحابية: قامت الشركة بالتعاون مع سلاسل التوريد على تدريب الموظفين على المخاطر الناتجة عن تبنى تكنولوجيا إنترنت الأشياء، والإتفاق وإختيار الشركات التى تقدم خدمات الحوسبة السحابية بتكلفة أقل.

الضوابط الخاصة ببعُد التكنولوجى:

1. **الاستثمار فى الأجهزة والبنية التحتية والبرامج الخاصة بتكنولوجيا إنترنت الأشياء:** تشتمل **الأجهزة والبنية التحتية** على الحواسب والسيرفرات والروترات وسويتشات ونقاط الوصول access point وأجهزة الإستشعار (المجسات) sensors ، والبلوتوث و RFID tag لتتبع حركة المنتج على طول خط الانتاج والتجميع والتخزين وهو المسئول عن تجميع البيانات من أجهزة الاستشعار، والموجهات الصناعية والتى تكون مسئولة عن إعطاء الاستجابة المناسبة لكل طلب من مستخدمى الشبكة، والواى فاى. كما قامت الشركة **بالاستثمار فى البرامج** لربط نظام تكنولوجيا إنترنت الاشياء بنظام المعلومات المحاسبى، بالاضافة إلى شراء البرامج التى تكتشف وتتصدى للتهديدات ونقاط الضعف مثل برامج مكافحة الفيروسات، وجدار الحماية.
2. التقنيات التى استخدمتها الشركة لحماية سرية البيانات والمعلومات المحاسبية المرتبطة بتكنولوجيا إنترنت الأشياء: قامت الشركة بما يلى:

–النسخ الاحتياطى غير المنتظم للمعلومات المحاسبية.

–تعيين حساب واحد لكل موظف للدخول على الشبكة (user role) يرتبط بكافة الصلاحيات الإدارية الخاصة به.

3. إستخدام التقنيات والبرامج التى تكتشف وتتصدى للتهديدات مثل برامج مكافحة الفيروسات، وجدار الحماية.
4. بالنسبة للضوابط التكنولوجية التى يمكن أن تساعد على مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى: قامت الشركة بوضع بعض الضوابط الخاصة بالأمن المادى لحماية الأصول المعلوماتية والتقنية من الوصول المادى غير المصرح له والفقدان والسرقة.

وفيما يلى أهم التكاليف والمنافع التى تحققت من تطبيق تكنولوجيا إنترنت الأشياء فى الشركة.

– بلغت تكاليف الإستثمار فى أجهزة الإستشعار والبرامج الخاصة بالنظام 57 مليون جنيه (متضمنه مبلغ 5 مليون تكاليف تدريب الموظفين على إنترنت الأشياء وربطه بنظام المعلومات المحاسبى بواقع 400 محاسب من اجمالى 4000 محاسب). كما تتحمل الشركة صيانة دورية سنوية وبوليصة تأمين سنوية بواقع 800000 جنيه. علماً بأن العمر الافتراضى لأجهزة الإستشعار والحاسبات الآلية 5 سنوات ، وأن معامل القيمة الحالية لجنيه واحد لمدة 5 سنوات بمعامل خصم 10% يساوى 3.7907 جنيه

✓ **تم الحصول على النتائج التالية فى العام الأول من تطبيق النظام**

– اعداد التقارير الخاصة بالمخزون والجودة والتقارير المالية بعد فترة من استعادة النظام نتيجة لحدوث مشاكل فى النظام وهجمات القرصنة الالكترونية على البنية التحتية لإنترنت الأشياء. وبلغت تكلفة استعادة النظام بمبلغ 1.1 مليون جنيه.

فى ضوء قراءة سيادتكم للحالة السابقة ، برجاء توضيح مدى موافقتك على العبارات التالية:

رقم العبارة	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	**الضوابط التى اتبعتها الشركة لحماية أمن الشبكات والمعلومات المحاسبية المرتبطة ببعد المورد البشرى عند تبنى تكنولوجيا انترنت الأشياء**					
1-1	ما مدى موافقتكم على مدى كفاية عدد المحاسبين والموظفين الذى حددتهم الشركة لتدريبهم على نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء وكيفية حمايته؟					
2-1	ما مدى موافقتكم على الطريقة التى قامت بها الشركة لخلق وتوطيد ثقافة الأمن السيبرانى لنظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء؟					
3-1	ما مدى موافقتكم على الفريق الذى شكلته الشركة لتحديد الأهداف التنظيمية لإدارة البيانات المحاسبية وتحليلها؟					
2	**الضوابط التى اتبعتها الشركة لحماية أمن الشبكات والمعلومات المحاسبية المرتبطة ببعد العمليات عند تبنى تكنولوجيا انترنت الأشياء**					
1-2	ما مدى موافقتكم على مدى وضوح السياسات والتعليمات الخاصة بالأمن السيبرانى لنظام المعلومات المحاسبى؟					
2-2	ما مدى موافقتكم على القواعد التى حددتها الشركة المتعلقة بمسؤليات المحاسبين لحماية نظام المعلومات المحاسبى فى ظل تبنى تكنولوجيا إنترنت الأشياء؟					
3-2	ما مدى موافقتكم على نظام تحديد هوية وصلاحيات المستخدم التى قامت الشركة بتحديده؟					
4-2	ما مدى موافقتكم على مدى كفاية الأطر والمؤشرات التى استخدمتها الشركة لإدارة المخاطر بما فيها مخاطر الأمن السيبرانى والرقابة الداخلية؟					
5-2	ما مدى موافقتكم على الطريقة التى قامت بها الشركة لإدارة المخاطر السيبرانية بين أعضاء سلسلة التوريد والإتفاق مع مزود خدمة الحوسبة السحابية؟					
3	**الضوابط التى اتبعتها الشركة لحماية أمن الشبكات والمعلومات المحاسبية المرتبطة ببعد الحلول التكنولوجية عند تبنى تكنولوجيا انترنت الأشياء**					
1-3	ما مدى موافقتكم على مدى كفاية التقنيات التى استخدمتها الشركة لحماية سرية البيانات والمعلومات المحاسبية المرتبطة بتكنولوجيا إنترنت الأشياء؟					
2-3	ما مدى موافقتكم على مدى كفاية التقنيات والبرامج التى استخدمتها الشركة لتكتشف وتتصدى للتهديدات التى تواجه نظام المعلومات المحاسبى المرتبط بإنترنت الأشياء؟					
3-3	ما مدى موافقتكم على مدى كفاية الضوابط التكنولوجية التى يمكن أن تساعد على مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى؟					
		نعم			**لا**	
4	وفقاً للحالة المعروضة : هل تتوقع زيادة المنافع المتحققة للشركة من ربط نظام المعلومات المحاسبى بتكنولوجيا انترنت الأشياء بمرور الوقت ؟					

حالة (2)

تعد الشركة (س) واحدة من أبرز الشركات فى تصنيع الأجهزة الإلكترونية فى مصر. تمتلك الشركة العديد من الفروع فى مصر وبعض الدول العربية. تهتم الشركة بالتحول الرقمى ايماناً منها بأهمية تحقيق رؤية مصر 2030 من خلال القيام بتحويل مصانعها إلى مصانع ذكية وتكامل سلسلة التوريد لديها. لذا قامت بتطبيق تكنولوجيا إنترنت الأشياء وربط الأجهزة المرتبطة به بنظام المعلومات المحاسبى للشركة (أوراكل) ، وذلك لامكانية تتبع المنتجات وإدارة المخزون وتخفيض التكاليف بالاضافة إلى إنشاء المستندات المحاسبية الكترونياً وإعداد التقارير المالية بسرعة وفى وقت حدوث الحدث.

وفى سبيل قيام الشركة بتبنى تكنولوجيا إنترنت الاشياء وربطه بنظام المعلومات المحاسبى قامت بإجراء الضوابط التالية:

الضوابط الخاصة ببُعد المورد البشرى

1. تبنى سياسة الاحتواء بدءاً من إختيار وتعيين المحاسبين ذوى الأخلاق الحميدة (4000 محاسب من إجمالى 4000 محاسب على مستوى فروع الشركة) ، وتوفير بيئة عمل يشعرون بها بأنهم جزء من الشركة وتدريبهم على تكنولوجيا إنترنت الأشياء وربطه بنظام المعلومات المحاسبى.
2. خلق ثقافة الأمن السيبرانى لنظام المعلومات المحاسبى من خلال التركيز دائماً على تدريب الأفراد وزيادة مستوى وعيهم بحماية البيانات المنبثقة من إنترنت الأشياء.
3. قامت الشركة بتكوين فريق يتكون من الإدارة العليا ومهندسى علم البيانات وبعض المحاسبين للمشاركة فى تحديد الأهداف التنظيمية لإدارة البيانات المحاسبية وتحليلها.

الضوابط الخاصة ببُعد العمليات

1. إنشاء إدارة للأمن السيبرانى تهتم بوضع إستراتيجية الأمن السيبرانى والسياسات والإجراءات والعمليات التى يجب أن تقوم بها لحماية نظام المعلومات المحاسبى المرتبط بإنترنت الأشياء.
2. الاستمرار فى تطبيق اللوائح المتعلقة بالتنظيم الداخلى للعمل فى الشركة، بالإضافة إلى وضع دليل لأخلاقيات المحاسبين بخصوص الأمن السيبرانى من خلال تحديد كافة القواعد والإجراءات التفصيلية وكذلك الضوابط للتخفيف من حدة المخاطر.
3. بالنسبة لنظام تحديد هوية وصلاحيات المستخدم user authentication and authorization : يتم وضع نظام واضح لتوثيق الأشخاص الذين يمكنهم الوصول إلى المعلومات المحاسبية من خلال الدخول لنظام المعلومات المحاسبى الخاص بالشركة متعددة الخطوات تتمثل الدخول

بالطريقة المعتادة والمتعارف عليها من خلال كتابة الأسم وكلمة المرور password ، بالإضافة إلى استخدام الخصائص البيومترية مثل بصمات الأصابع والتعرف على الوجه. كما أن ليس لكل المستخدمين لهم صلاحيات سواء فى الإطلاع أو تعديل البيانات ويتم تحديد الصلاحيات وفقاً لدور كل شخص فى الشركة وصلاحياته وفقاً لمستواه الإدارى.

4. بالنسبة لعدد الأطر والمؤشرات التى استخدمتها الشركة لإدارة المخاطر والرقابة الداخلية : استخدمت الشركة إطاراً للرقابة الداخلية للشركة وذلك لضمان تحقيق أهداف الشركة بفعالية وكفاءة وإصدار تقارير مالية موثوق بها، والامتثال للقوانين واللوائح والسياسات، وإطار حوكمة تكنولوجيا المعلومات ، بالإضافة إلى إهتمامها بتوفير مؤشر يساعد على تقييم المستوى الحالى لنضج ممارسات وعمليات الشركة وتحديد الأهداف والأولويات الخاصة بتحسين الأمن السيبرانى.

5. بالنسبة لإدارة المخاطر السيبرانية بين أعضاء سلسلة التوريد والإتفاق مع مزود خدمة الحوسبة السحابية: قامت الشركة بتنفيذ الاستراتيجيات التى تساعد على التغلب على التهديدات والمخاطر اليومية والمحتملة التي تتعرض لها سلسلة التوريد نتيجة تطبيق تكنولوجيا إنترنت الأشياء، بالإضافة إلى إهتمام الشركة بالتحقق دائماً من موثوقية وسمعة مزود خدمة الحوسبة السحابية من خلال اللجوء إلى الشركات الكبيرة ذات الموثوقية العالية والسمعة الجيدة فى الحوسبة السحابية.

الضوابط الخاصة ببعُد التكنولوجى

1. **الاستثمار فى الأجهزة والبنية التحتية والبرامج الخاصة بتكنولوجيا إنترنت الأشياء وأمنه وحمايته من المخاطر**: تتكون **الأجهزة والبنية التحتية** من الحواسب والسيرفرات والروترات والسويتشات ونقاط الوصول access point وأجهزة الاستشعار (المجسات) sensors ، البلوتوث و RFID tag – لتتبع حركة المنتج على طول خط الانتاج والتجميع والتخزين وهو المسئول عن تجميع البيانات من أجهزة الاستشعار –، والموجهات الصناعية –والتى تكون مسئولة عن اعطاء الاستجابة المناسبة لكل طلب من مستخدمى الشبكة–، والواى فاى ، ووسائل الربط والاتصال والاسلاك بمختلف أنواعها ووسائل النقل اللاسلكية والاهتمام بتشفير الرسائل لمختلف الوسائط. كما قامت الشركة **بالاستثمار فى البرامج** لربط نظام تكنولوجيا إنترنت الاشياء بنظام المعلومات المحاسبى، بالاضافة إلى شراء البرامج التى تكتشف وتتصدى للتهديدات ونقاط الضعف مثل برامج مكافحة الفيروسات، وجدار الحماية وأنظمة منع التطفل وأنظمة منع الدخلاء المشتبه فيهم واستخدام تطبيق نظم الذكاء الاصطناعى وتعلم الآلة للكشف عن نمط سلوك المستخدم الضار.

2. التقنيات التى استخدمتها الشركة لحماية سرية البيانات والمعلومات المحاسبية المرتبطة بتكنولوجيا إنترنت الأشياء تم القيام بالآتى:

- تشفير المستندات ووضع العلامات المائية عليها وإخفائها من إستخدام غير المصرح لهم باستخدام تلك المستندات.
- النسخ الاحتياطى المنتظم للمعلومات المحاسبية.
- حماية البريد الإلكترونى من أى هجمات من خلال استخدام خاصية منع البريد الإلكترونى من إرسال المحتوى والمرفقات والبيانات الحساسة خارج شبكة الإنترنت وتحليل وتصفية رسائل البريد الإلكترونى وبصفة خاصة الرسائل الإقتحامية spam .
- تعيين حسابين للموظفين الذين يحتاجون إلى صلاحيات إدارية على جهاز كمبيوتر معين أحدهما يكون له جقوق إدارية والأخر له امتيازات محدودة، وقيام الشركة دائما بمتابعة فتح وغلق صلاحيات كود الموظف.
- تطبيق تكنولوجيا البلوك تشين لمعالجة وتخزين المعاملات المالية.

3. إستخدام التقنيات والبرامج التى تكتشف وتتصدى للتهديدات مثل: برامج مكافحة الفيروسات، وجدار الحماية وأنظمة منع التطفل وأنظمة منع الدخلاء المشتبه فيهم واستخدام تطبيق نظم الذكاء الاصطناعى وتعلم الآلة للكشف عن نمط سلوك المستخدم الضار.

4. بالنسبة للضوابط التكنولوجية التى يمكن أن تساعد على مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى: استخدمت الشركة ضوابط للأمن المادى لحماية الأصول المعلوماتية والتقنية من الوصول المادى غير المصرح له والفقدان والسرقة، كما قامت بوضع ضوابط لتصميم البرمجيات وتعطيل ميزة التحديث التلقائى للبرامج ، والإتفاق مع كبرى الشركات ذوى الثقة والسمعة الطيبة فى مجال الحوسبة السحابية ، بالإضافة إلى إنشاء شبكة خاصة منفصلة لأجهزة إنترنت الأشياء والتي لا يتم مشاركتها مع الشبكة التي يمكن لأجهزة الموظفين الوصول إليها.

وفيما يلى أهم التكاليف والمنافع التى تحققت من تطبيق تكنولوجيا إنترنت الأشياء فى الشركة

- بلغت تكاليف الاستثمار فى أجهزة الإستشعار والبرامج الخاصة بالنظام ونظم الحماية 102 مليون جنيه (متضمنه مبلغ 50 مليون تكاليف تدريب الموظفين على إنترنت الأشياء وربطه بنظام المعلومات المحاسبى بواقع 4000 موظف من اجمالى 4000 موظف). كما تتحمل الشركة صيانة دورية سنوية وبوليصة تأمين سنوية بواقع 800000 جنيه. علماً بأن العمر الافتراضى

لأجهزة الاستشعار والحاسبات الآلية 5 سنوات، وأن معامل القيمة الحالية لجنيه واحد لمدة 5 سنوات بمعامل خصم 10% يساوى 3.7907 جنيه.

✓ **تم الحصول على النتائج التالية فى العام الأول من تطبيق النظام**

– تحقيق وفورات فى تكاليف التشغيل بواقع 30 مليون جنيه.

– اعداد التقارير الخاصة بالمخزون والجودة والتقارير المالية لحظياً.

فى ضوء قراءة سيادتكم للحالة السابقة ، برجاء توضيح مدى موافقتك على العبارات التالية:

رقم العبارة	العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	**الضوابط التى اتبعتها الشركة لحماية أمن الشبكات والمعلومات المحاسبية المرتبطة ببعد المورد البشرى عند تبنى تكنولوجيا انترنت الأشياء**					
1-1	ما مدى موافقتكم على مدى كفاية عدد المحاسبين والموظفين الذى حددتهم الشركة لتدريبهم على نظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء وكيفية حمايته؟					
2-1	ما مدى موافقتكم على الطريقة التى قامت بها الشركة لخلق وتوطيد ثقافة الأمن السيبرانى لنظام المعلومات المحاسبى المرتبط بتكنولوجيا إنترنت الأشياء؟					
3-1	ما مدى موافقتكم على الفريق الذى شكلته الشركة لتحديد الأهداف التنظيمية لإدارة البيانات المحاسبية وتحليلها؟					
2	**الضوابط التى اتبعتها الشركة لحماية أمن الشبكات والمعلومات المحاسبية المرتبطة ببعد العمليات عند تبنى تكنولوجيا انترنت الأشياء**					
1-2	ما مدى موافقتكم على مدى وضوح السياسات والتعليمات الخاصة بالأمن السيبرانى لنظام المعلومات المحاسبى؟					
2-2	ما مدى موافقتكم على القواعد التى حددتها الشركة المتعلقة بمسؤليات المحاسبين لحماية نظام المعلومات المحاسبى فى ظل تبنى تكنولوجيا إنترنت الأشياء؟					
3-2	ما مدى موافقتكم على نظام تحديد هوية وصلاحيات المستخدم التى قامت الشركة بتحديده؟					
4-2	ما مدى موافقتكم على مدى كفاية الأطر والمؤشرات التى استخدمتها الشركة لإدارة المخاطر بما فيها مخاطر الأمن السيبرانى والرقابة الداخلية؟					
5-2	ما مدى موافقتكم على الطريقة التى قامت بها الشركة لإدارة المخاطر السيبرانية بين أعضاء سلسلة التوريد والإتفاق مع مزود خدمة الحوسبة السحابية؟					
3	**الضوابط التى اتبعتها الشركة لحماية أمن الشبكات والمعلومات المحاسبية المرتبطة ببعد الحلول التكنولوجية عند تبنى تكنولوجيا انترنت الأشياء**					
1-3	ما مدى موافقتكم على مدى كفاية التقنيات التى استخدمتها الشركة لحماية سرية البيانات والمعلومات المحاسبية المرتبطة بتكنولوجيا إنترنت الأشياء؟					

2-3	ما مدى موافقتكم على مدى كفاية التقنيات والبرامج التى استخدمتها الشركة لتكتشف وتتصدى للتهديدات التى تواجه نظام المعلومات المحاسبى المرتبط بإنترنت الأشياء؟					
3-3	ما مدى موافقتكم على مدى كفاية الضوابط التكنولوجية التى يمكن أن تساعد على مواجهة مخاطر تبنى تكنولوجيا إنترنت الأشياء على نظام المعلومات المحاسبى؟					
		نعم			لا	
4	وفقاً للحالة المعروضة : هل تتوقع زيادة المنافع المتحققة من ربط نظام المعلومات المحاسبى بتكنولوجيا انترنت الأشياء بمرور الوقت ؟					

رابعاً: أسئلة عامة تتعلق بموضوع البحث

1. إذا توافر لديك بديلين: الأول، يتضمن الحصول على مبلغ 500 جنيه بصفة مؤكدة. والثانى ، يتضمن فرصة الحصول إما على 1000 جنيه أو عدم الحصول على أى شئ على الإطلاق. يجب أن يكون هناك احتمال بنسبة (%) على الأقل لكسب الـ 1000 جنيه لكى يجعلك تفضل البديل الثانى؟