Journal Of the Iraqia University (74-5) September (2025)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

# دور استخدام الحوسبة السحابية على فاعلية أمن نظم المعلومات المحاسبية دراسة استطلاعية لآراء عينة من الأكاديميين والمهنيين في تخصص المحاسبة في مدينة اربيل

ئفان صلاح عزالدين١، أ.م.د. أرشد صديق عبدالله٢

٢،١ قسم التقنيات المحاسبة، الكلية التقنية الإدارية أربيل، جامعة أربيل التقنية،

# The Role of Cloud Computing in the Effectiveness of Accounting Information Systems Security - An Exploratory Study of the Opinions of a Sample of Academics and Professionals in the Accounting Field in Erbil

Evan Salah Ezzullddin1, Dr. Arshad Sedeeq Abdullah2
evan.ezzulddin@epu.edu.iq, Arshad.s.abdullah@epu.edu.iq
1, 2 Department of Accounting Techniques, Erbil Technical Administrative College, Erbil Polytechnic University, Erbil, Iraq

مستخلص

تشهد بيئات الأعمال تحولاً رقمياً متسارعاً، جعل من الحوسبة السحابية خياراً استراتيجياً للعديد من الوحدات الاقتصادية، لا سيما في مجال نظام المعلومات المحاسبية، لما توفره من مزايا تقنية متعددة، وتكلفة تشغيلية منخفضة، وكفاءة عالية. إلا أن استخدامها يثير مجموعة من التحديات الأمنية، تتعلق بسرية وسلامة وتوافر البيانات المالية، خاصة في ظل تزايد التهديدات السيبرانية. وتكمن مشكلة الدراسة في ضعف الثقة بأمن نظام المعلومات المحاسبية في بيئة الحوسبة السحابية. وتهدف الدراسة إلى تحليل مدى اسهام الحوسبة السحابية في دعم أمن نظام المعلومات المحاسبية، وتقييم فاعليتها في حماية البيانات المالية. كما تسعى لتوضيح الأبعاد التقنية والمفاهيمية التي تساهم في تعزيز الأمان، اعتماداً على آراء عينة من الأكاديميين والمهنيين في مدينة أربيل. وقد تم جمع البيانات عبر استبانة وزعت على (١٤٠) شخصاً، استرجع منها (١٣٦) صالحة للتحليل الإحصائي باستخدام برنامج (SPSS). وأظهرت نتائج الدراسة وجود علاقة ارتباط معنوية قوية بين استخدام الحوسبة السحابية وفاعلية أمن نظام المعلومات المحاسبية، مما يعكس وعي مشترك لدى أفراد العينة بأهمية اعتماد هذه التقنية في تعزيز أمن المعلومات في البيئة المحاسبية، وأوصت الدراسة بضرورة تبني أفضل الممارسات الأمنية، وتطبيق الإجراءات حماية فعالة، الى جانب إجراء تقييمات دورية للمخاطر المتحملة، لضمان القدرة على الاستجابة الفعالة لأي تهديدات قد تنشأ مستقبلاً.**الكلمات الإفتتاحية:** الحوسبة السحابية، نظام المعلومات المحاسبية، أمن المعلومات.

Abstract:

Business environments are undergoing a rapid digital transformation, making cloud computing a strategic option for many economic units, particularly in the field of accounting information systems, due to its multiple technical advantages, low operating costs, and high efficiency. However, its use raises a number of security challenges related to the confidentiality, integrity, and availability of financial data, especially amid increasing cyber threats. The problem of the study lies in the lack of trust in the security of accounting information systems within the cloud computing environment. The study aims to analyze the extent to which cloud computing contributes to supporting the security of accounting information systems and to evaluate its effectiveness in protecting financial data. It also seeks to clarify the technical and conceptual dimensions that enhance security, based on the views of a sample of academics and professionals in the city of Erbil.Data were collected through a questionnaire distributed to (140) individuals, of which (136) were deemed valid for statistical analysis using SPSS software. The results of the study showed a strong significant correlation between the use of cloud computing and the effectiveness of accounting information system security, reflecting a shared awareness among the sample members of the importance of adopting this technology to enhance information security in the accounting environment. The study recommended the adoption of best security practices, the implementation of effective

protection measures, and the conduct of regular risk assessments to ensure the ability to respond effectively to any future threats.**Keywords:** Cloud computing, Accounting information system, Information security.

## المقدمة

شهد العالم في العقود الأخيرة تحولات جذرية وعميقة في مختلف المجالات، لا سيما في قطاع الأعمال والاقتصاد، وذلك بالتزامن مع تسارع هائل في التطورات التكنولوجية والرقمية. لم تقتصر هذه التحولات على تعديلات سطحية أو تحسينات شكلية فقط، بل مثلت ثورة شاملة أعادت بناء بيئة العمل وطرق إدارة الموارد وتبادل المعلومات، مما أثر بشكل مباشر على كفاءة الوحدات الاقتصادية وقدرتها التنافسية في الأسواق المحلية والدولية. وفي سياق هذا التحول الرقمي، ظهرت مجموعة من المفاهيم والتقنيات الحديثة التي أصبحت مكونات أساسية في البنية الرقمية الحديثة، من أبرز هذه التقنيات الحوسبة السحابية، التي تمثل تحولاً جذرياً في إدارة البيانات والمعلومات، حيث تعتمد على بيئة افتراضية قائمة على الإنترنت لتخزينها ومعالجتها وإتاحتها بسهولة وفعالة، ما يقلل الاعتماد على البنية التحتية التقليدية المكلفة والمعقدة.كما يعد الذكاء الاصطناعي كأداة قوية لتحليل كميات ضخمة من البيانات واستخلاص الأنماط والتنبؤ بالاتجاهات المستقبلة، إلى جانب ذلك ساهم إنترنت في ربط الأجهزة والأنظمة المختلفة عبر الشبكة، مما يتيح جمع بيانات متسقة ومتنوعة من البيئات الفعلية في الوقت الحقيقي، مما يعزز من قيمة المعلومات ودعم اتخاذ القرارات بشكل علمي ومنهجي. وسط هذا التنوع التقني المتسارع، تبرز الحوسبة السحابية كواحدة من أكثر الابتكارات تأثيراً وأهمية في المجال الوحدات الإقتصادية، فقد تجاوزت دورها التقليدي المتمثل في تقديم خدمات التخزين والمعالجة عبر الإنترنت لتصبح ركيزاً استراتيجياً من البنية التحتية التقنية، تمكن الوحدات الاقتصادية من التوسع بمرونة والسرعة في الاستجابة للتغيرات والإحتياجات المتجددة. وبفضل الحوسبة السحابية، تمكن المستخدمين من الوصول إلى التطبيقات والخدمات والبيانات من أي مكان وفي أي وقت، مما ساهم في رفع كفاءة العمل وسهل التعاون بين الفرق وعزز من خفض التكاليف التشغيلية.وتكتسب الحوسبة السحابية أهمية متزايدة في ظل بيئة اقتصادية عالمية تتسم بالعولمة والمنافسة الشديدة بين الوحدات الاقتصادية بمختلف أحجامها وأنواعها. إذ تتطلب هذه البيئة الديناميكية مستوى عالياً من المرونة التشغيلية والقدرة على التكيف السريع مع المستجدات التقنية والظروف المتغيرة المفاجئة، وهو ما توفره الحوسبة السحابية من خلال تقديم حلول تقنية متطورة تدعم عمليات التوسع بسلاسة، وضمان استمرارية تقديم الخدمات، والارتقاء بمستوى الأمان المعلوماتي عبر تقنيات الحماية المتقدمة. علاوة على ذلك، تؤكد العديد من الدراسات إلى أن تبني الحوسبة السحابية يسهم بشكل مباشر في تعزيز كفاءة وفعالية نظم المعلومات داخل الوحدات الاقتصادية، حيث يتيح الحصول على بيانات دقيقة ومحدثة، مما يمكن لصناع القرار من اتخاذ قرارات أكثر فاعلية ومدروسة.إلا أن هذه المزايا الكبيرة التي تقدمها الحوسبة السحابية تصاحبها تحديات ملحوظة، يأتي في مقدمتها التحديات الأمنية الناتجة عن طبيعة البيئة السحابية التشاركية والموزعة، ما يجعل حماية البيانات عملية معقدة تتطلب إعتماد تدابير أمنية متقدمة ومرنة تتكيف مع التهديدات المتطورة. وتزداد هذه التحديات تعقيداً في نظام المعلومات المحاسبية التي تتعامل مع بيانات مالية حساسة، ما يستدعي ضرورة ضمان مستويات عالية من السرية وسلامة البيانات، وتوافرها المستمر دون انقطاع، لأن أي خلل في هذه الجوانب قد يؤدي إلى خسائر مالية جسيمة وتأثير سلبي على السمعة الوحدة الإقتصادية.تعتبر نظام المعلومات المحاسبية (Accounting Information System – AIS) من الركائز الأساسية في الوحدات الاقتصادية، إذ تلعب دوراً محورياً في تسجيل المعاملات المالية، معالجتها، تحليلها، وإعداد تقارير دقيقة تدعم التخطيط والرقابة واتخاذ القرار. وتشكل هذا النظام حلقة وصل بين البيانات التشغيلية والمعلومات المالية، مما يجعلها أداة لا غنى عنها لتحقيق الشفافية المالية، وتعزيز الرقابة الداخلية، ودعم مبادئ المساءلة المالية. ومع توجه الوحدات الاقتصادية نحو دمج نظام المعلومات المحاسبية ضمن بيئات الحوسبة السحابية، تنشأ تحديات متعلقة بضمان أمنها وملاءمة البنية التحتية الأمنية، بحيث تتحقق الاستفادة من مزايا الحوسبة السحابية من جهة مثل: المرونة، وسهولة الوصول، وخفض التكاليف، ويحفظ أمن البيانات وسريتها وخصوصيتها من جهة أخرى.

## منهجية الدراسة

### مشكلة الدراسة

شهدت نظم المعلومات المحاسبية (Accounting Information Systems) في السنوات الأخيرة بالكثير من الاهتمام، نظراً لأهمية المحاسبة باعتبارها بمثابة نظام معلومات يحدد الأحداث الاقتصادية والوضع المالي ويراقبها ويسجلها وينقلها من الوحدات الاقتصادية إلى الأطراف ذات العلاقة، وعلى الرغم من الانتشار الواسع لاستخدام الحوسبة السحابية في نظام المعلومات المحاسبي لما توفره من مزايا التشغيلية، إلا أن الوحدات الإقتصادية تعاني من ضعف الثقة في أمن نظم المعلومات المحاسبية المحوسبة، ونظراً لتزايد التهديدات السيبيرانية والإعتماد على مزودي خدمات خارجيين، تبرز حاجة لتحليل مدى فاعلية الحوسبة السحابية في تعزيز أمن نظام المعلومات المحاسبية، لأن وجود بيانات مالية حساسة يصبح

الحفاظ على سرية المعلومات المحاسبية وسلامتها وتوافرها تحدياً كبيراً، بناءً على ذلك، ولحل هذه المشكلة يجب الإجابة على التساؤلات التالية:

هل هناك دور الحوسبة السحابية على فاعلية أمن نظام المعلومات المحاسبية؟ وتتفرع من المشكلة الرئيسية للدراسة المشاكل الفرعية الآتية:

١- كيف تساهم الحوسبة السحابية في تحسين أمن نظام المعلومات المحاسبية؟

٢- ما مدى فاعلية تكنولوجيا الحوسبة السحابية في حماية البيانات المالية والمحاسبية؟

**١.٢أهمية الدراسة**

١. **الأهمية العلمية:** تستمد الدراسة أهميتها العلمية من خلال تقديم إطار نظري يسلط الضوء على دور الحوسبة السحابية على فاعلية أمن نظام المعلومات المحاسبية. كما تبرز أهمية هذه الدراسة في كون تكنولوجيا الحوسبة السحابية تعد من الابتكارات الحديثة التي تعتمدها الوحدات الاقتصادية حالياً في إعداد القوائم والتقارير المالية.

٢. **الأهمية العملية:** تقتصر الأهمية العملية للدراسة من خلال اختبار دور الحوسبة السحابية على فعالية أمن نظام المعلومات المحاسبية وذلك من خلال استطلاع اراء عينة من الأكاديميين والمهنيين في مدينة اربيل.

**٣.١ أهداف الدراسة**

تسعى الدراسة الى تحقيق الاهداف الآتية:

١. بيان النظريات والمفاهيم الفلسفية المرتبطة بتطور وتبني الحوسبة السحابية، مع التركيز على الأبعاد المفاهيمية والتكنولوجية التي تعزز من فهم استخداماتها وتطبيقاتها.

٢. التعرف على العناصر الرئيسية التي تساهم في توفير مستويات عالية من الأمان في بيئة الحوسبة السحابية.

٣. توضيح تأثير الحوسبة السحابية على تحسين الأمان والكفاءة في نظم المعلومات المحاسبية.

٤. التعرف على مدى دور الحوسبة السحابية على فاعلية أمن نظام المعلومات المحاسبية من خلال استخدام تكنولوجيا، وذلك من خلال استطلاع اراء عينة من الأكاديميين والمهنيين في مدينة اربيل.

**٤.١.١ فرضيات الدراسة**

للإجابة عن أسئلة الدراسة ولتحقيق أهداف الدراسة أعلاه، تم صياغة فرضيات الدراسة كالاتي:

١. توجد موافقة ذات دلالة إحصائية معنوية من قبل أفراد عينة الدراسة على العبارات الخاصة باستخدام الحوسبة السحابية.

٢. توجد موافقة ذات دلالة إحصائية معنوية من قبل أفراد عينة الدراسة على العبارات الخاصة بأمن نظام المعلومات المحاسبية.

٣. توجد علاقة ذات دلالة إحصائية معنوية بين استخدام تكنولوجيا الحوسبة السحابية وأمن نظام المعلومات المحاسبية من وجهة نظر الأكاديميين والمهنين في مدينة أربيل.

٤. هناك تأثير معنوي ذو دلالة إحصائية بين استخدام تكنولوجيا الحوسبة السحابية وفاعلية أمن نظام المعلومات المحاسبية.

٥. توجد فروق ذات دلالة إحصائية معنوية في آراء المهنيين والأكاديميين في مدينة أربيل بشأن استخدام الحوسبة السحابية.

٦. توجد فروق ذات دلالة إحصائية معنوية في آراء المهنيين والأكاديميين في مدينة أربيل بشأن أمن نظام المعلومات المحاسبية.

**٥.١.١ حدود الدراسة**

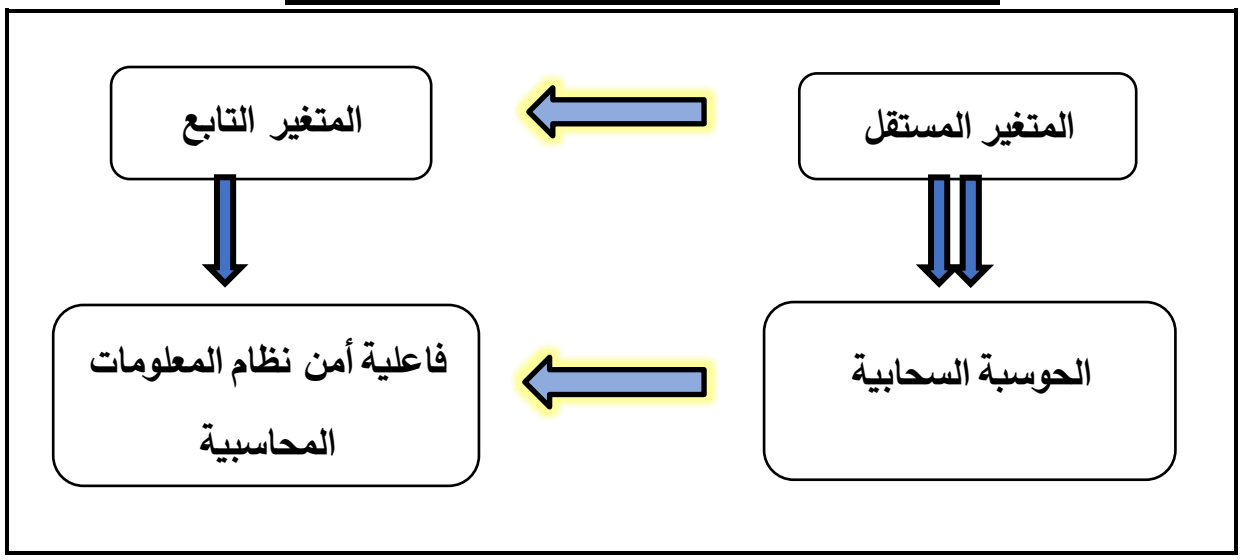
١. **الحدود المكانية:** تتمثل الحدود المكانية للدراسة تصميم استمارة الاستبانة و توزيعها عينة من الاكاديميين و المهنيين في مدينة أربيل.

٢. **الحدود الزمانية:** تتمثل الحدود الزمانية للدراسة على سنة (٢٠٢٥)م.

٣. **الحدود الموضوعية:** تقتصر الحدود الموضوعية للدراسة على دور الحوسبة السحابية على فاعلية أمن نظام المعلومات المحاسبية.

**٦.١.١ انموذج الدراسة**

يوضح الأنموذج التالي متغيرات الدراسة و العلاقة بينهما و يتكون من متغير مستقل وهو (**الحوسبة السحابية**) و متغير التابع (**فاعلية أمن نظام المعلومات المحاسبية**)، وكما موضح أدناه:




الشكل (1)
أنموذج الدراسة
مصدر: من اعداد الباحثان

٢.الإطار النظري الدراسة

٢:١ مفهوم وتعريف الحوسبة السحابية

٢:١:١ مفهوم الحوسبة السحابية

تتضمن الحوسبة السحابية تقديم خدمات عبر الإنترنت يمكن للمستخدمين الوصول إليها من خلال متصفح الويب، ولا يتطلب إستخدامه خبرة متطورة من قبل المستخدمين ولا يتطلب أي بنية تحتية أو تكاليف الصيانة، كما هو حال في ألبانيا فقد تم تنفيذ الحوسبة السحابية ليس فقط في القطاع العام في الخدمات مثل الحكومة الإلكترونية والتعليم ولكن في القطاع الخاص أيضاً، وذلك بفضل مزاياها مثل سهولة وسرعة الوصول إلى البيانات وكفاءة أعلى من حيث التكلفة وزيادة المرونة مقارنة بالأنظمة التقليدية الأخرى (Shkurti, 2014: 1-12). ان الخدمات السحابية أدوات مفيدة ومساعدة للحكومات والضوابط الضريبية لأن وصول السلطات الضريبية إلى قواعد البيانات السحابية لأنشطة الوحدات الإقتصادية يزيد في مستوى الإبلاغ الضريبي داخل اقتصاد أي بلد، وتعد هذه نقطة مهمة ينبغي أخذها بعين الاعتبار عند مناقشة الخدمات السحابية او محاولة الاستفادة منها في مجال معين. وقد عرف المعهد الوطني للمعايير والتكنولوجيا المعلومات (NIST) أن الحوسبة السحابية هي نموذج لتمكين وصول ملائم للشبكة عند الطلب إلى ملف تجمع مشترك لموارد الحوسبة السحابية القابلة للتكوين مثل: (الشبكات، الخوادم، التخزين، التطبيقات والخدمات) التي يمكن أن يتم توفيرها بسرعة أكبر وإدراتها بأقل جهد إداري (عبدالزهرة، ٢٠٢٣: ٤)ويشير الباحثان الى أن الحوسبة السحابية تعد من أبرز التقنيات الحديثة التي تعتمد على شبكة الإنترنت كمصدر أساسي لتوفير الخدمات الرقمية، حيث تتيح تخزين البيانات والملفات ضمن مساحات تخزينية كبيرة قابلة للمشاركة مع مستخدمين آخرين عبر أجهزة حاسوب موزعة في مواقع جغرافية متعددة، مع إمكانية معالجة هذه البيانات باستخدام أحدث أدوات التحليل ومعالجة البيانات مثل تطبيقات الذكاء الاصطناعي.

**٢:١:٢ تعريف الحوسبة السحابية**

الحوسبة السحابية تعد نتيجة لتطور تقنيات الإنترنت وإرتفاع سرعاته بشكل ملحوظ، وتتجسد في قيام العديد من الوحدات الإقتصادية بإتاحة تطبيقاتها عبر الشبكة، دون الحاجة إلى امتلاك بنية تحتية تقنية محلية. كما أنها تتيح سهولة الوصول إلى هذه الخدمات دون الحاجة إلى المعرفة التقنية أو الإمكانيات المادية الكبيرة من قبل المستخدمين (زرزار وبن وريدة، ٢٠١٩: ١٨٤-٢٠٥).كما عرفت ايضاً بانها " تكنولوجيا تعتمد على نقل المعالجة ومساحة التخزين الخاصة بالحاسوب الى بيئة السحابة حيث يمكن الوصول اليه عن طريق شبكة الانترنت، وبذلك تتحول برامج تكنلوجيا المعلومات من منتجات تقليدية الى خدمات " (khanoam, 2017: 3).ويرى الباحثان أن التعاريف الشائعة لمفهوم الحوسبة السحابية تعبر بصورة عامة عن الفكرة الأساسية المتمثلة في نقل الموارد التقنية والبرمجيات من البيئة المحلية إلى بيئة افتراضية تدار عبر شبكة الإنترنت.

**٢:٢ أنواع خدمات الحوسبة السحابية**

تعد خدمات الحوسبة السحابية من الركائز الأساسية للبنية التحتية الرقمية في العصر الحديث، وقد قام المعهد الوطني للمعايير والتكنولوجيا (NIST)بتصنيف هذه الخدمات الى ثلاث فئات رئيسة، وهي (الشمراني والأسمري، ٢٠٢١: ١٣٣ , Mell & Grance, 2011: 2):

١. **البرمجيات كخدمة (SaaS)**في إطار نموذج (SaaS)، لا يتحمل المستخدم مسؤولية إدارة البنية التحتية الأساسية التي تشمل الخوادم وأنظمة التشغيل أو وسائط التخزين، بل يقتصر دوره على استخدام التطبيق وضبط الإعدادات الشخصية ضمن صلاحيات محدودة، ومن أبرز الأمثلة على هذا النموذج: خدمات البريد الإلكتروني عبر الويب مثل(Gmail,office 365 ) (Alharthi et al., 2022: 212).

٢. **النظام الأساسي كخدمة (PaaS)**في نموذج (PaaS) يتحكم المستخدم في التطبيقات التي يقوم بإنشائها وإعدادات بيئة التشغيل الخاصة بهذه التطبيقات، بينما تظل مسؤولية تشغيل وصيانة الشبكات والخوادم وأنظمة التشغيل على عاتق مزودو الخدمة، ويعد هذا النوع من الخدمة مناسباً للتركيز على تطوير التطبيقات دون الانشغال بإدارة البنية التحتية (Zhang and Chen, 2021: 58).

٣. **البنية التحتية كخدمة (IaaS)**يتمتع المستخدم في هذا النموذج (IaaS) بتحكم واسع في أنظمة التشغيل، التخزين، والتطبيقات، مع إمكانيات محدودة في إدارة إعدادات الشبكة مثل: انشاء جدران الحماية، ومع ذلك، تبقى مسؤولية إدارة وصيانة البنية التحتية المادية على عاتق مزودو الخدمة (Singh et al., 2023: 19).يمثل هذا التصنيف إطاراً واضحاً لفهم نماذج خدمات الحوسبة السحابية، كما يمكن الوحدات الإقتصادية من اختيار النموذج الذي يتوافق مع متطلباتها التقنية والإدارية (Mell & Grance, 2011: 3)على ضوء ما سبق يرى الباحثان أن نماذج الحوسبة السحابية الثلاثة (Saas,PaaS,IaaS) تمثل مستويات مختلفة من التحكم والتجريد لتلبية احتياجات الوحدات الإقتصادية حسب حجمها وقدراتها التقنية. حيث يوفر (SaaS) حلولاً جاهزة وبكلفة منخفضة تناسب أغلب الوحدات الإقتصادية، خصوصًا في القطاع الخاص المحلي، بينما يتيح ( PaaS)تطوير التطبيقات دون إدارة البنية التحتية، ويمكن (IaaS) من تحكم ومرونة عالية للجهات ذات الكوادر الفنية المتقدمة. ويشير الباحثان إلى أن التحول الرقمي يتطلب رفع القدرات التقنية للوحدات الإقتصادية للانتقال تدريجياً نحو نماذج أكثر تقدمًا تحقق توازناً بين الأداء والمرونة والأمان.

**٣:٢ مقارنة تحليلية بين الحوسبة السحابية والحوسبة التقليدية**

تعد الحوسبة السحابية (Cloud Computing) من النماذج التقنية الحديثة التي أحدثت تحولاً كبيراً في البنية التحتية لتكنولوجيا المعلومات في الوحدات الإقتصادية، مقارنةً بالحوسبة التقليدية التي تعتمد على الموارد المحلية. فيما يلي تحليل علمي مقارن بين النموذجين:

١. **الوصول المرن إلى الموارد والخدمات**توفر الحوسبة السحابية إمكانية الوصول المرن إلى التطبيقات والبيانات من أي مكان وفي أي وقت عبر اتصال بالإنترنت، بخلاف الحوسبة التقليدية التي تتطلب التواجد الفيزيائي في موقع العمل أو وجود جهاز محدد. وهذا يعزز من مرونة العمليات التشغيلية والتنقل ويخدم نماذج العمل عن بعد(Zhang etal., 2010: 9).

٢. **المرونة في التوسع والتعديل**تتميز الحوسبة السحابية بإمكانية التوسع الديناميكي للموارد حسب احتياجات المستخدم الفعلية، مما يمكن المستخدم من تعديل السعة التخزينية أو قوة المعالجة بشكل فوري دون تغيير مادي في الأجهزة، ولكن التوسع في الحوسبة التقليدية تتطلب شراء أو تركيب معدات جديدة (Armbrust et al., 2010: 53).

٣. **نقل عبء الصيانة والدعم الفني**في بيئة الحوسبة السحابية، يتولى مزودو الخدمة مسؤولية صيانة البنية التحتية والتحديثات الأمنية والفنية، مما يخفف من الأعباء التشغيلية على المستخدم النهائي، في المقابل، تتطلب الحوسبة التقليدية موارد بشرية وتقنية داخلية لصيانة الأجهزة والبرمجيات (Buyya etal., 2010: 35).

٤. **خفض التكاليف التشغيلية**يتيح النموذج السحابي للوحدات الإقتصادية خفض التكاليف الرأسمالية، من خلال الاستغناء عن شراء الخوادم والبرمجيات، ولكن تتلطب الحوسبة التقليدية استثمارات كبيرة في البنية التحتية التكنولوجية (Khajeh-Hosseini etal., 2010: 451).

٥. **ضمان التوافر واستمرارية الخدمة**توفر مزودات الحوسبة السحابية اتفاقيات مستوى الخدمة(Service level agreements – SLA) تضمن استمرارية تشغيل الخدمات بنسبة تتجاوز ٩٩.٩٪، ومع ذلك انقطاعات الخدمة على نطاق واسع تظل واردة، كما حدث في عدد من الأعطال لدى Amazon Web Services, Google Cloud في السنوات الأخيرة (Gill et al., 2019: 480).

٦. **الاستفادة من البنية التحتية العلمية السحابية**وفرت الحوسبة السحابية إمكانية الوصول إلى موارد حوسبية ضخمة مناسبة للبحث العلمي، من خلال إتاحة موارد حوسبية عالية الأداء خاصة في مجالات النمذجة والمحاكاة وتحليل البيانات الكبيرة. وسحابات مثل (AWS, Google cloud platform)أصبحت منصات مثالية لدعم البحوث المعقدة، لكن قضايا الأمان وحماية الملكية الفكرية لا تزال تحديات بارزة (Gholami and).

(Laure, 2016: 463)ويرى الباحثان أن الحوسبة السحابية تعد خيارًا استراتيجياً هاماً للوحدات الاقتصادية بمختلف أحجامها، حيث توفر مرونة في الموارد التقنية وخفض التكاليف، خاصة للوحدات الصغيرة والمتوسطة. كما تعزز الأمان والتعاون عن بعد، ويزيد الإنتاجية. ومع ذلك، يواجه المستخدمين تحديات تتعلق بالأمان والخصوصية والاعتماد على المزودين والفجوات التقنية.

**٤:٢ الإتجاهات المستقبلية في الحوسبة السحابية**

مع التطور السريع للتكنولوجيا الرقمية، أصبحت الحوسبة السحابية إحدى الركائز الأساسية للتحول الرقمي في الوحدات الإقتصادية. لذالك لم تعد تستخدم كأداة لتخزين البيانات وتشغيل التطبيقات فقط، بل يستخدم اليوم كبنية تحتية ذكية ومرنة تواكب تطورات العصر، ومن اتجاهات المستقبلية في الحوسبة السحابية كالتالي:

١. **الذكاء الاصطناعي المدعوم بالسحابة**دمج البنى السحابية مع تقنيات الذكاء الاصطناعي لتقديم خدمات تحليل وتنبؤ آلي، إدارة الموارد بشكل تلقائي، وتعزيز الأمن عبر اكتشاف الأنماط والتهديدات بشكل سريع، وتركز الدراسات على كيفية تكامل بين نظم التوزيع السحابية مع الذكاء الاصطناعي لتحسين الأداء والكفاءة التشغيلية (Zangana and Zeebaree, 2024: 11).

٢. **الحوسبة الطرفية مع الذكاء الاصطناعي** أوضحت الدراسات إلى أن نقل جزء من قدرات المعالجة إلى "أطراف الشبكة"، مدعوماً بخوارزميات الذكاء الاصطناعي، يساهم في تقليص زمن الاستجابة، تحسين مستوى الخصوصية، بالإضافة الى تخفيف العبء عن البنى السحابية المركزية (Zhou et al., 2019: 1738-1740).

٣. **الحوسبة متعددة السحب والهجينة** يتجه دراسات نحو نماذج سحابية تجمع بين أكثر من مزود، سواء بنية هجينة التي تجمع بين السحابة العامة والسحابة الخاصة أومتعددة السحب. تساهم هذه النماذج في تحسين المرونة وتوزيع المخاطر، بإضافة الى إعداد بيئات ديناميكية (Zhou et al., 2019: 1738-1740).

٤. **الأمن السحابي المعزز بالذكاء الاصطناعي** في ظل تزايد التهديدات السيبرانية يستخدم الذكاء الاصطناعي لتعزيز أمن الحوسبة السحابية من خلال قدرته على رصد التهديدات في الوقت الحقيقي والتصدي التلقائي لها لتقليل مخاطر امنية ضمن إطار مفاهيم امنية حديثة مثل نموذج "الثقة المعدومة (Zero Trust)" وعمليات الذكاء للعمليات (AIOps) (Zangana and Zeebaree, 2024: 11).

٥. **الحوسبة السحابية المستدامة** يؤدي التزايد في استخدام الذكاء الاصطناعي على تعزيز كفاءة الطاقة في مراكز البيانات من خلال تطبيق حلول ذكية مثل انظمة التبريد الذكي وإدارة الموارد الطاقية، مما يحقق أهداف الاستدامة من خلال خفض الانبعاثات الكربونية (Huang etal., 2023: 4).

٦. **دمج الحوسبة الكمية في السحابة** تسعى الوحدات الإقتصادية دمج الحوسبة الكمية مع خدمات الحوسبة السحابية لدعم عمليات تحليل بيانات معقدة وتنفيذ عمليات التشفير المتقدمة. وعلى الرغم من هذا التوجه لا يزال في مراحل مبكرة، فإن الأبحاث الأكاديمية تضع الأسس لهذه الدمج لتمكين التكامل بينهما في المستقبل (Zangana and Zeebaree, 2024: 12).ويرى الباحثان أن الاتجاهات المستقبلية في الحوسبة السحابية تمثل فرصة استراتيجية مهمة للوحدات الاقتصادية الراغبة في تعزيز تنافسيتها في ظل التحول الرقمي العالمي، ويشددان على أهمية الحلول الأمنية القائمة بالذكاء الاصطناعي لحماية البيانات، بالإضافة إلى ضرورة تبني الحوسبة السحابية المستدامة لتحقيق التوازن بين التطور التكنولوجي والإستدامة البيئية. ورغم التحديات التنظيمية والتقنية يرى الباحثان أن اعتماد هذه الاتجاهات بشكل متكامل سيحدث تحولاً نوعياً ويفتح آفاق جديدة للنمو والابتكار في بيئة الإقتصادية الرقمية.

**٥:٢ مفهوم وتعريف أمن نظام المعلومات المحاسبية**

**١:٥:٢ مفهوم أمن نظام المعلومات المحاسبية**

يعد أمن نظام المعلومات المحاسبية من القضايا الجوهرية في عصر التحول الرقمي المتسارع، نظراً لما ينطوي عليه من أهمية في حماية البيانات المالية وضمان دقة وموثوقية المعلومات المحاسبية. فمع تصاعد التهديدات السيبرانية وتزايد اعتماد الوحدات الإقتصادية على النظم الإلكترونية، تبرز الحاجة ملحة إلى تبني استراتيجيات أمنية شاملة تحد من مخاطر الاختراق والتلاعب، وتساهم في تعزيز الثقة في التقارير المالية (عباس، ٢٠٢٤: ١٢).يرتبط مفهوم أمن نظام المعلومات المحاسبية بعدة عناصر أساسية، من ابرزها حماية البيانات، وتأمين الملفات المحاسبية، وضبط آليات المعالجة المالية، وهو ما يعد عاملاً محورياً في دعم استمرارية الأعمال التجارية والحفاظ على دقة وموثوقية المعلومات. وقد أكدت الأدبيات

المتخصصة على أهمية إدماج تقنيات الأمن السيبراني ضمن هذه النظم لضمان فاعليتها في بيئات الأعمال الحديثة (أبو عمرو وآخرون، ٢٠٢٣: ٤٤).

**٢:٥:٢ تعريف أمن نظام المعلومات المحاسبية**

يعد أمن نظام المعلومات المحاسبية من المفاهيم الأساسية في بيئة الأعمال الرقمية الحديثة، ويعرف على أنه مجموعة من السياسات والإجراءات والضوابط التقنية والتنظيمية المصممة لحماية البيانات المحاسبية من التهديدات الداخلية والخارجية، مع ضمان سرية المعلومات وسلامتها وتوافرها، بما يساهم في تعزيز موثوقية التقارير المالية ويدعم عملية اتخاذ القرار بشكل دقيق. وقد أشارت أحد الدراسات أن هذه الإجراءات تشكل الإطار الأساسي للسيطرة على المخاطر المتعلقة بالبيانات المالية في النظم المحوسبة (Ahmed etal., 2019: 8).من منظور مختلف، يرى (Zadorozhnyi and Muravskyi, 2020)أن حماية نظام المعلومات المحاسبية ترتكز على منع الوصول غير المصرح به، والتصدي لمحاولات الاحتيال أو الإضرار المتعمد للبيانات، مع ضمان استمرارية توافر المعلومات ودقتها، وخاصة في بيئات العمل الرقمية المعقدة التي تتطلب درجة عالية من المرونة والأمان (Zadorozhnyi and Muravskyi, 2020: 118). وفي السياق ذاته، يوضح (AICPA, 2017) أن أمن نظام المعلومات المحاسبية يتمثل في قدرة النظام على تقييد الوصول للمستخدمين المصرح لهم فقط، ومنع أي تعديل أو إتلاف غير مصرح به للبيانات، ويعد هذا الجانب عنصراً محورياً من نظام الرقابة الداخلية الذي يضمن موثوقية التقارير المالية (AICPA, 2017: 3).ويرى الباحثان أن أمن نظام المعلومات المحاسبية يعد مفهوماً شاملاً لا يقتصر فقط على الجوانب التقنية، بل يشمل جميع الأبعاد المتعلقة بحماية البيانات المحاسبية من كافة التهديدات المحتملة، سواء كانت داخلية أو خارجية، مادية أو إلكترونية. وتؤمن بأن تحقيق هذا الأمن يعتمد على تكامل الضوابط التقنية والتنظيمية، بما يضمن الحفاظ على سرية المعلومات، وسلامتها، وتوافرها.

**٦:٢ مبادئ أمن نظام المعلومات المحاسبية**

وضع كل من المعهد الأمريكي للمحاسبين القانونيين (AICPA)، والمعهد الكندي للمحاسبين القانونيين (CICA) إطاراً مفاهيمياً يعنى بتعزيز موثوقية نظام المعلومات المحاسبية، وضمن هذا الإطار تم تحديد خمسة مبادئ أساسية، وفيما يلي عرض مفصل لكل مبدأ:

**1. مبدأ الأمن (Security)** يتمثل هذا المبدأ في ضرورة حماية نظام المعلومات المحاسبية من الوصول غير مصرح به، ويشمل ذلك الأشخاص، برمجات ضارة، أو محاولات الاختراق الخارجي. يطبق هذا من خلال الأدوات الأمنية التقنية مثل: جدران الحماية، أنظمة كشف التسلل، والمصادقة متعددة العوامل. كما يتضمن وضع سياسات صارمة للتحكم في الصلاحيات الممنوحة للمستخدمين، وفصل المهام، ومراقبة الأنشطة (المطيري، ٢٠١٩: ١٢٩).

**2. مبدأ السرية (Confidentiality)** يركز هذا المبدأ على حماية المعلومات الحساسة من الكشف غير المصرح به، مثل السجلات المالية، العقود، أو بيانات العملاء. وتشمل ممارسات الحماية استخدام تقنيات التشفير، وضوابط التحكم في مشاركة الملفات، وتدريب المستخدمين على حفظ سرية المعلومات داخل بيئة العمل (Gelinas et al., 2018: 389).

**3. مبدأ الخصوصية (Privacy)** يرتبط هذا المبدأ بكيفية جمع واستخدام وتخزين البيانات الشخصية للعملاء والموظفين، ويشمل ذلك أسماءهم، عناوينهم، وأرقام الهواتف أو البريد الإلكتروني الخاصة بهم للتواصل. تلزم القوانين الحديثة الوحدات الإقتصادية بالإفصاح الواضح عن سياسة الخصوصية، والحصول على الموافقة من قبل اصحاب البيانات قبل معالجتها، بما يضمن احترام الحقوق الرقمية والالتزام بالمعايير الأخلاقية (البرقاوي،٢٠٢١: ٤٩).

**4. مبدأ تكاملية الإجراءات (Processing Integrity)** يشير هذا المبدأ إلى ضرورة أن تتم معالجة البيانات بدقة واكتمال ووفق توقيت مناسب داخل النظام. ويعد وجود ضوابط داخلية آلية، وسجلات مراجعة دقيقة، ونظام تحقق متعدد الطبقات يكشف الانحرافات، تعد من أهم الأساليب لتحقيق هذا المبدأ، لضمان عدم التلاعب، أو حدوث أخطاء في نتائج المعالجات المحاسبية (Bodnar and Hopwood, 2013: 271).

**5. مبدأ الجهوزية (Availability)** يتعلق هذا المبدأ بقدرة النظام المحاسبي على البقاء متاحاً لتلبية المتطلبات التشغيلية في جميع الأوقات، بما في ذلك أثناء حالات الطوارئ أو الكوارث التقنية. ويتطلب ذلك تنفيذ عمليات نسخ احتياطية، وإجراء صيانة دورية، وخطط لاستعادة النظام في حال توقفه، لضمان استمرارية الخدمة وتجنب الانقطاعات المفاجئة التي قد تعطل العمليات المحاسبية (الزعبي، ٢٠١٧: ٥٥٢).ويرى الباحثان أن المبادئ الخمسة لأمن نظام المعلومات المحاسبية التي حددها كل من (AICPA) و (CICA) تعد اطاراً أساسياً لحماية البيانات وتعزيز موثوقية النظام. فكل مبدأ يعالج بعداً حيوياً، بدءاً من ضبط الوصول وحماية الخصوصية والسرية المعلومات، وصولاً إلى ضمان استمرارية التشغيل.

**٧:٢ التحديات التي تواجه أمن نظام المعلومات المحاسبية**

في ظل تسارع التحول الرقمي واعتماد الوحدات الإقتصادية بشكل متزايد على نظام المعلومات المحاسبية، أصبح تأمين هذه النظم ضرورة جوهرية للحفاظ على سرية البيانات، استمرارية العمليات التشغيلية، وتعزيز ثقة أصحاب المصلحة. وتأتي هذه التحديات من مصادر متعددة، تشمل الثغرات التقنية، العوامل البشرية، وضعف الضوابط التنظيمية، ما يتطلب من الوحدات اعتماد استراتيجيات أمنية شاملة ومتعددة الأبعاد (كاطع وغالي، ٢٠٢٤: ٩١).

**١:٧:٢ التحديات التقنية**

١. **الثغرات البرمجية**الثغرات الناشئة عن ضعف في التصميم النظام أو التكامل بين الأنظمة المحاسبية والأنظمة الأخرى (مثل انظمة الموارد البشرية أو سلاسل الإمداد)، وتشكل هذه الثغرات نقاط ضعف يمكن استغلالها بسهولة. وتشمل هذه الثغرات أخطاء التشفير، أو قصور في آليات التحقق من صحة البيانات (Dunn etal., 2016: 212).

٢. **ضعف التحديثات والصيانة**عدم تثبيت التحديثات الأمنية في الوقت المناسب يجعل نظام المعلومات المحاسبية عرضة لهجمات تستغل الثغرات المكتشفة مسبقاً. وقد تؤدي هذه الممارسات إلى خسائر مالية في حالة حدوث اختراق واسع النطاق (Kim and Solomon, 2018: 187).

٣. **الهجمات السيبرانية المتقدمة**الهجمات المعقدة مثل: البرمجيات الخفية (Fileless Malware) أو الهجمات المستمرة المتقدمة (Advanced persistent threats–APTs)، تستهدف نظام المعلومات المحاسبية بدقة باستخدام تقنيات يصعب كشفها دون أدوات تحليل أمنية متقدمة تعتمد على الذكاء الاصطناعي (السويدي، ٢٠٢٢: ٦٣).

**٢:٧:٢ التحديات البشرية**

١. **ضعف الوعي الأمني**عدم إدراك الموظفين للمخاطر الأمنية الرقمية يجعلهم أكثر عرضة لارتكاب أخطاء، مثل: استخدام كلمات مرور ضعيفة أو الاستجابة لروابط مشبوهة في رسائل بريد ألكتروني، وهو ما قد يعرض الوحدة الإقتصادية لخرق مباشر (Delso–Vicente etal., 2025: 28).

٢. **إساءة استخدام الصلاحيات**عند منح صلاحيات واسعة للموظفين دون رقابة صارمة، يمكن أن تستغل من بعض الموظفين للوصول إلى معلومات غير مصرح لهم بها، مما قد يؤدي إلى التلاعب المالي أو تسريب البيانات الحساسة (safa etal., 1019: 1–18).

٣. **مقاومة التغيير**يظهر بعض الموظفين مقاومة عند إدخال تغييرات أمنية جديدة، سواء بدافع التعود أو قلة الفهم لأهميتها، ما قد يؤدي إلى تعثر السياسات الأمنية أو التحايل عليها (Delso–Vicente etal., 2025: 28).

**٣:٧:٢ التحديات التنظيمية والتشريعية**

١. **غياب السياسات الأمنية**يؤدي عدم وجود سياسات مكتوبة وواضحة يخلق فجوة في المسؤوليات الأمنية، ويجعل الاستجابة في حالة الهجوم الأمني أكثر ارتباكاً وتأخيراً (von Solms and van Niekerk, 2013: 103).

٢. **ضعف التدقيق والمراقبة**غياب المراقبة المستمرة والتدقيق الأمني الدوري يمنع اكتشاف الإختراقات في الوقت المناسب، ما يضاعف الأثر السلبي لأي خرق قد يحدث (الربيدي وسلطان، ٢٠٢٥: ١١٧).

٣. **صعوبة الامتثال للتشريعات**تواجه الوحدات الإقتصادية صعوبات في الالتزام بالمعايير الدولية مثل ISO 27001 أو قوانين المتعلقة بحماية البيانات بسبب غياب البنية التشريعية الكافية أو نقص الموارد المتخصصة (Alkalbani etal., 2016: 5).

٤. **ضعف الميزانية المخصصة للأمن**تعد الميزانية المحدودة من أبرز العوائق التي تواجه الوحدات الإقتصادية في تأمين نظمها المعلوماتية، إذ تؤدي إلى الاعتماد على أدوات منخفضة الكفاءة أو عدم توظيف خبراء مختصين (Alkalbani etal., 2016: 5).يرى الباحثان أن التحديات الأمنية التي تواجه نظام المعلومات المحاسبية داخل الوحدات الاقتصادية تتمثل في ضعف البنية التحتية التقنية، وقلة الوعي الكافي الأمني بين الموظفين، وغياب السياسات تنظيمية واضحة لتوزيع الصلاحيات. كما تعاني هذه الوحدات من محدودية الموارد المالية والبشرية وعدم تطبيق الرقابة المستمرة، مما يجعلها أكثر عرضة للاختراقات والمخاطر الأمن السيبرانية.

**٨:٢ الاستجابة للتحديات الأمنية في أنظمة المعلومات المحاسبية (AIS)**

**١. تبني استراتيجيات أمان استباقية**

يتطلب ضمان أمن أنظمة المعلومات المحاسبية اعتماد نهج استباقي يقوم على دمج مفهوم "الأمن حسب التصميم (Security by Design)" ضمن كافة مراحل تطوير النظام، بدءاً من التحليل والتخطيط وليس بعد ظهور التهديدات أو الثغرات. وهذا النهج يمكن من تصميم أنظمة تكون محمية بشكل مدمج، مما يقلل من الحاجة لتعديلات لاحقة قد تكون مكلفة أو محدودة الفعالية (Harris, 2020: 160).

٢. **تعزيز الكفاءة الأمنية للموارد البشرية**يعد العامل البشري من أبرز الثغرات في أمن نظام المعلومات المحاسبية، لذا من الضروري الاستثمار في برامج تدريبية مستمرة تهدف إلى رفع مستوى الوعي الأمني لدى الموظفين، يمكن أن تتضمن هذه البرامج محاكاة لهجمات التصيد الإلكتروني ومواقف استجابة فورية للتهديدات. تشير الدراسات إلى أن انخفاض مستوى الوعي الأمني في الوحدات الإقتصادية العربية كان وراء عدد من الحوادث السيبرانية الفعلية، مما يبرز أهمية التثقيف والتدريب كحائط صد أساسي (Harris, 2020: 160).

٣. **إعداد خطط شاملة للاستجابة الحوادث**تعزز خطط الاستجابة للحوادث من قدرة الوحدات الإقتصادية على التعامل مع الخروقات الأمنية بطريقة سريعة ومنهجية، وتحد من التأثيرات التشغيلية والمالية لتلك الحوادث. وتشمل هذه الخطط تحديد الإجراءات الفورية الواجب اتخاذها، وتوزيع الأدوار والمسؤليات، وتفعيل آليات التعافي، والتحليل اسباب الثغرات بعد وقوعها، مما يجعلها جزءاً لا يتجزأ من منهجية إدارة المخاطر (Gelinas, Dull, and Wheeler, 2019: 175).

٤. **الالتزام بالأطر والمعايير الدولية**تتبنى المنظمات الرائدة في مجال أمن المعلومات أطراً والمعايير الدولية مثل (ISO 27001) و (NIST) و (COBIT) لتطوير سياسات وإجراءات أمنية قوية وفعالة لإدارة أمن المعلومات، وفي السياق العربي، شددت الهيئة الوطنية للأمن السيبراني على أهمية مواءمة هذه الأطر وتكييفها مع البيئة المحلية، بما يساهم في تحسين مستوى الجاهزية الأنظمة وضمان الامتثال للمتطلبات التنظيمية والأمنية (الهيئة الوطنية للأمن السيبراني، ٢٠٢١: ١١).

٥. **التقييم المستمر والمراجعة الأمنية**لا يمكن تحقيق منظومة الأمن السيبراني دون إجراء مراجعات دورية تشمل التدقيق الداخلي المنتظم، واختبارات اختراق منتظمة، وتحليل الثغرات، تمثل هذه الممارسات أداة فعالة لضمان التحصين المستمر وكشف نقاط الضعف غير الظاهرة، مما يمكن من تصحيحها قبل استغلال تلك الثغرات من قبل المهاجمين (Andress, 2020: 150)ويرى الباحثان أن مواجهة التحديات الأمنية في أنظمة المعلومات المحاسبية تتطلب اتباع نهج استباقي شامل متعددة الأبعاد، يبدأ من دمج الأمان في تصميم النظام ضمن مراحل التصميم الأولى، مروراً بتأهيل العنصر البشري وتوعيته بمخاطر الأمن السيبراني، ووصولاً إلى إعداد خطط إستجابة واضحة للحوادث الأمنية، كما يؤكد الباحثان على أهمية الالتزام بالأطر والمعايير الدولية وتكييفها وفق البيئة التنظيمية المحلية، إلى جانب ضرورة إجراء مراجعات أمنية دورية، واختبارات إختراق منتظمة لضمان الاستعداد الدائم، والكشف المبكر عن الثغرات.

**٩:٢ فاعلية أمن نظام المعلومات المحاسبية في ظل استخدام الحوسبة السحابية**

تعد الحوسبة السحابية من الظواهر التقنية التي باتت تحظى بأهمية متزايدة في مختلف المجالات، لا سيما في نظام المعلومات المحاسبية. مع تزايد الاعتماد على هذه التقنية، تبرز الحاجة إلى دراسة مدى تأثيرها على فاعلية أمن هذه النظم، من خلال تحليل شامل لمزايا الحوسبة السحابية، والمخاطر الأمنية المصاحبة لها، بالإضافة الى إستراتيجيات المناسبة التي يمكن اعتمادها لضمان حماية وسلامة البيانات المحاسبية.وفي إطار أمن نظام المعلومات المحاسبية، تعتبر المواصفات الرقمية من أهم العناصر، اذ تسهم تقنيات الحوسبة السحابية في تعزيز مستوى الأمان من خلال توظيف تقنيات متقدمة مثل تشفير البيانات والتحكم في الوصول لضمان حماية بيانات المحاسبية الحساية (Li, 2023: 2). كما أن لمزودي خدمة الحوسبة السحابية دوراً هاماً في تقديم الإرشادات والدعم الأمني للوحدات الإقتصادية، من خلال إعتماد أفضل الممارسات الأمنية وتنفيذ معايير حماية فعالة (Alshawabkeh etal., 2022: 1155).ومن الجدير بالذكر أن استراتيجيات الحماية في نظام المعلومات المحاسبية يجب أن تكون متعددة الأبعاد، بحيث تشمل التدابير التقنية، والإجراءات الإدارية، والتدريب المستمر على الأمن السيبراني، من أجل مواجهة التهديدات المتزايدة في البيئة السحابية (Alrabei, 2023: 114). ومن ثم تطوير استراتيجيات فعالة للأمن السيبيراني، تتضمن تدابير أمان قوية متقدمة، وآليات المراقبة فعالة يعد أمراً ضرورياً لحماية البيانات المحاسبية من الاختراقات والعبث (الربيدي والحميري، ٢٠٢٥: ١٨).كما توصي العديد من الدراسات بضرورة تبني إطار متكامل لتقييم المخاطر في البيئات السحابية لضمان سلامة المعلومات المحاسبية وحمايتها من التهديدات المحتملة، ويجب أن تكون الاستراتيجيات الأمنية مصممة بما يتناسب مع متطلبات العمل المحددة وتحتوي على آليات للتحقق من صحة البيانات وضمان سريتها وسلامتها (Alrabei, 2023: 114).ويرى الباحثان أن العلاقة بين الحوسبة السحابية وفاعلية أمن نظام المعلومات المحاسبية يعتمد بدرجة كبير على استراتيجيات الأمنية المعتمدة لضمان حماية البيانات الحساسة. لأن نجاح استخدام الحوسبة السحابية لا يقتصر على مزاياها التقنية فقط، بل تحتاج

الوحدات الإقتصادية إلى فهم عميق للتحديات التي تواجهها، وتقييم للمخاطر المحتملة بشكل دوري والتأكد من تنفيذ أفضل الممارسات الأمنية لتفادي التهديدات المحتملة في بيئة الحوسبة السحابية. ولا شك أن الحوسبة السحابية ستواصل لعب دور محوري في مستقبل أمن نظام المعلومات المحاسبية، نظراً لقدرتها على منح الوحدات الإقتصادية المرونة والتكيف مع التطورات السريعة في بيئة الأعمال الرقمية.

**3. النتائج والمناقشة**

**١:٣ الوصف الإحصائي للخصائص الديموغرافية لعينة الدراسة**

يهدف هذا الجزء إلى استعراض الخصائص الديموغرافية والوظيفية لعينة الدراسة، والتي تمثل خلفية أساسية لفهم طبيعة الأفراد الذين أجابوا على الاستبانة. ويساعد هذا الوصف في تفسير نتائج الدراسة من خلال التعرف على توزيع المبحوثين وفقاً لعدة متغيرات، من بينها: المؤهل العلمي، العنوان الوظيفي أو المهني، اللقب العلمي، عدد سنوات الخدمة، المشاركة في الدورات التدريبية، ومدى استخدام الحوسبة السحابية في بيئة العمل. تم عرض نتائج هذا الجزء باستخدام الجداول التكرارية والنسب المئوية، لتوضيح توزيع عينة الدراسة وفق هذه المتغيرات، وتم اختيار عينة قصدية بلغ حجمها (١٤٠) مستجيب وكانت (١٣٦) إستمارة منها صالحة للتحليل، نظراً لطبيعة الدراسة التي تتطلب توفر معرفة متخصصة بموضوع الدراسة. وقد تم توزيع العينة وفق عدد من الخصائص الديموغرافية،يمكن عرضها كالآتي:**الجدول (1) الخصائص الديموغرافية لعينة الدراسة**

| الخاصية | البيان | التكرار | النسبة المئوية |
|---|---|---|---|
| التحصيل العلمي | بكالوريوس | ٤٥ | ٪٣٣.٠٩ |
| | محاسب قانونية | ٢٤ | ٪١٧.٦٥ |
| | دبلوم عالي | ٦ | ٪٤.٤١ |
| | ماجستير | ٤١ | ٪٣٠.١٥ |
| | دكتوراه | ٢٠ | ٪١٤.٧١ |
| **المجموع** | | **١٣٦** | **٪١٠٠** |
| العنوان الوضيفي أو المهني | مراقب حسابات | ٢٥ | ٪١٨.٣٨ |
| | مدير مالي | ١٤ | ٪١٠.٢٩ |
| | محاسب | ٥٠ | ٪٣٦.٧٧ |
| | أكاديمي | ٤٧ | ٪٣٤.٥٦ |
| **المجموع** | | **١٣٦** | **٪١٠٠** |
| اللقب العلمي | بدون لقب علمي | ٨٩ | ٪٦٥.٤٤ |
| | مدرس مساعد | ١٠ | ٪٧.٣٥ |
| | مدرس | ١٢ | ٪٨.٨٢ |
| | أستاذ مساعد | ١٥ | ٪١١.٠٣ |
| | أستاذ | ١٠ | ٪٧.٣٥ |
| **المجموع** | | **١٣٦** | **٪١٠٠** |
| عدد سنوات الخدمة | ٥ سنوات وأقل | ١٦ | ٪١١.٧٦ |
| | من ٦ إلى ١٠ سنوات | ٢٣ | ٪١٦.٩١ |
| | من ١١ إلى ١٥ سنة | ٤٠ | ٪٢٩.٤١ |
| | ١٦– ٢٠ سنة | ٤٠ | ٪٢٩.٤١ |
| | ٢١ سنة فأكثر | ١٧ | ٪١٢.٥٠ |
| **المجموع** | | **١٣٦** | **٪١٠٠** |
| | نعم | ٨٦ | ٪٦٣.٢٤ |

| | | | |
|---|---|---|---|
| **المشاركة في الدورات التدريبية** | لا | ٥٠ | ٣٦.٧٦٪ |
| **المجموع** | | **١٣٦** | **١٠٠٪** |
| **استخدام الحوسبة السحابية ضمن التقنيات المُعتمدة في العمل** | نعم | ٧٥ | ٥٥.١٥٪ |
| | لا | ٦١ | ٤٤.٨٥٪ |
| **المجموع** | | **١٣٦** | **١٠٠٪** |

**المصدر:** من اعداد الباحثان بالاستناد إلى نتائج التحليل الإحصائييتبين أن النسبة الأكبر من أفراد العينة يحملون شهادة البكالوريوس، حيث بلغ عددهم (٤٥) فرداً وبنسبة (٣٣.٠٩٪) من إجمالي العينة. تليها فئة الحاصلين على شهادة الماجستير بعدد (٤١) فرداً وبنسبة (٣٠.١٥٪)، في حين جاءت فئة الحاصلين على دبلوم عالي في المرتبة الأخيرة بعدد (٦) أفراد فقط وبنسبة (٤.٤١٪) من إجمالي العينة. تعكس هذه النتائج تنوع مستويات التحصيل العلمي لدى المبحوثين، بما يسهم في إثراء نتائج الدراسة من خلال تعدد وجهات النظر. كما أظهرت النتائج أن فئة المحاسبين جاءت في المرتبة الأولى بعدد بلغ (٥٠) فرداً، وهو ما يمثل نسبة (٣٦.٧٧٪) من إجمالي العينة البالغ عددها (١٣٦). ويدل هذا التمثيل المرتفع على الطبيعة التنفيذية للوحدات الإقتصادية المستهدفة، والتي تعتمد بشكل رئيس على المحاسبين في تنفيذ أعمالها اليومية، في حين جاءت فئة المديرين الماليين في المرتبة الأخيرة بعدد بلغ (١٤) فرداً، أي بنسبة (١٠.٢٩٪) من مجموع العينة. ورغم أن هذه النسبة تمثل الفئة الأقل عدداً، إلا أن وجود المديرين الماليين يضيف بعداً إدارياً وقيادياً يعكس طبيعة السياسات والإجراءات المتبعة في إدارة الشؤون المالية، ويتبين ايضاً أن النسبة الأكبر من أفراد العينة هم من دون لقب علمي، بعدد بلغ (٨٩) فرداً، وهو ما يشكّل نسبة (٦٥.٤٤٪) من إجمالي العينة. ويدل هذا التمثيل العالي على أن معظم المشاركين هم من الممارسين التنفيذيين في الوحدات الاقتصادية، ما يعزز الجانب العملي في نتائج الدراسة، وقد أظهرت النتائج أن أكبر فئتين تمثلتا في فئتي (١١–١٥ سنة) و (١٦–٢٠ سنة)، حيث بلغ عدد الأفراد في كل منهما (٤٠) فرداً، بنسبة (٢٩.٤١٪) من إجمالي العينة لكل فئة. ويدل هذا التماثل على أن ما يقارب (٦٠٪) من المشاركين يمتلكون خبرات متوسطة إلى متقدمة في العمل، مما يضيف موثوقية على البيانات المستخلصة من استجاباتهم، كما تبين النتائج أن نسبة كبيرة من المشاركين، تبلغ (٨٦) فرداً، قد شاركوا في هذه الدورات، مما يعادل (٦٣.٢٤٪) من إجمالي العينة، وهو ما يعكس وعيًا عاليًا بأهمية التطوير المهني والتدريب المستمر في مجال التكنولوجيا الحديثة، وأخيراً، أظهرت النتائج أن (٧٥) فرداً من أصل (١٣٦) يستخدمون الحوسبة السحابية ضمن تقنيات عملهم، أي بنسبة (٥٥.١٥٪)، مما يعكس انتشاراً واسعًا لهذه التقنية في الوحدات الاقتصادية التي ينتمي إليها المشاركون، وهو مؤشر إيجابي يعكس توجه الوحدات الاقتصادية نحو الرقمنة والتطوير التكنولوجي.

**٢:٣ قياس متغيرات الإستبانة**

تم قياس متغيرات الدراسة الثلاث باستخدام مقياس ليكرت الخماسي، بمدى يتراوح بين (١) لا أتفق تماماً إلى (٥) أتفق تمامًا. وبعد جمع البيانات وتحليلها باستخدام برنامج (SPSS)، وجاءت النتائج كما يلي:

**أولاً: قياس المحور الأول المتغير المستقل (استخدام الحوسبة السحابية)الجدول (٢) التحليل الوصفي لمحور استخدم الحوسبة السحابية**

| ت | العبارة | المتوسط | الانحراف المعياري | المرتبة | نسبة الاتفاق |
|---|---|---|---|---|---|
| X1 | يعد استخدام الحوسبة السحابية في المحاسبة خطوة أساسية لمواكبة التطورات التكنولوجية الحديثة. | 4.4191 | ٠.70506 | 1 | %88.38 |
| X2 | تحدث الحوسبة السحابية تحولًا جذريًا في مجال المحاسبة من خلال تقليل التكاليف والوقت وزيادة دقة المعالجة. | 4.2500 | ٠.71751 | 3 | %85.00 |
| X3 | توفر الحوسبة السحابية سعة تخزينية افتراضية تتجاوز بكثير قدرات التخزين التقليدية. | 4.3088 | ٠.70464 | 2 | %86.18 |

| | | | | | |
|---|---|---|---|---|---|
| X4 | تعد بيئة الحوسبة السحابية مرنة، ما يسهل توسيع استخدام البرامج عبر مختلف الأجهزة. | 4.1544 | ٠.80626 | 7 | %83.09 |
| X5 | تتيح الحوسبة السحابية استخدام التطبيقات دون الحاجة لتثبيتها على أجهزة المستخدمين. | 4.0662 | ٠.86240 | 13 | %81.32 |
| X6 | توفر الحوسبة السحابية نسخاً احتياطية آلية ومنتظمة للبيانات، مما يعزز الأمان المعلومات ويقلل من احتمالات خطر فقدانها. | 4.2353 | ٠.77206 | 5 | %84.71 |
| X7 | يعتمد نجاح استخدام الحوسبة السحابية على تأهيل الموظفين وتدريبهم. | 4.2206 | ٠.79527 | 6 | %84.41 |
| X8 | تهدف الحوسبة السحابية الى تحقيق قابلية التوسع بما يتناسب مع احتياجات الوحدة الإقتصادية. | 4.0956 | ٠.84221 | 11 | %81.91 |
| X9 | عند استخدام خدمات الحوسبة السحابية تكون صيانة وتطوير البرامج من الناحية التقنية من مسؤولية الشركات المزودة للخدمة. | 4.1324 | ٠.87609 | 9 | %82.65 |
| X10 | تعتبر الحوسبة السحابية تقنية صديقة للبيئة بسبب تقليل استهلاك الأجهزة والخوادم. | 4.0809 | ٠.79866 | 12 | %81.62 |
| X11 | تساعد الحوسبة السحابية في ضمان استمرارية الأعمال حتى في حالات الكوارث. | 4.0956 | ٠.79702 | 10 | %81.91 |
| X12 | تشجع الحوسبة السحابية الوحدات الاقتصادية على رفع الوعي الأمني لدى موظفيها لضمان حماية البيانات والأنظمة. | 4.1397 | ٠.72186 | 8 | %82.79 |
| X13 | تعزز الحوسبة السحابية قدرة الوحدات الاقتصادية على التوسع الرقمي والتقني. | 4.2353 | ٠.63521 | 4 | %84.71 |
| المتوسط | | ٤.١٨٧٢ | ٠.٧٧١٩ | ---- | ٪٨٣.٧٤ |

**المصدر:** من اعداد الباحثان من واقع الدراسة الميدانية لسنة ٢٠٢٥المتوسط العام لمتغير استخدام الحوسبة السحابية بلغ (٤.١٨٧٢) مع انحراف معياري مقداره (٠.٧٧١٩)، مما يشير إلى درجة عالية من الاتفاق بين أفراد العينة حول أهمية وفوائد استخدام الحوسبة السحابية في العمل، حيث بلغت نسبة الاتفاق الكلية (٨٣.٧٤٪)، وهي نسبة تعكس قناعة قوية لدى المشاركين بأهمية هذا المتغير وتأثيره.تتصدر العبارة "يعد استخدام الحوسبة السحابية في المحاسبة خطوة أساسية لمواكبة التطورات التكنولوجية الحديثة (X1) " المرتبة الأولى، بمتوسط عالٍ جداً (٤.٤١٩١) ونسبة اتفاق بلغت (٨٨.٣٨٪)، مما يدل على إدراك المشاركين لأهمية تبني الحوسبة السحابية كضرورة ملحة في مجال المحاسبة لمواكبة التطور الرقمي.وفي المرتبة الثانية جاءت العبارة المتعلقة بالسعة التخزينية الافتراضية التي توفرها الحوسبة السحابية (X3)، حيث أقر المشاركون بأنها تفوق قدرات التخزين التقليدية بنسبة (٨٦.١٨٪). هذا يؤكد على أحد أبرز مزايا الحوسبة السحابية في مجال إدارة البيانات.أما العبارة الثالثة (X2) فترتبط بتحويلات الحوسبة السحابية في تقليل التكاليف والوقت وزيادة دقة المعالجة، حيث أظهرت نسبة اتفاق عالية بلغت (٨٥٪)، مما يدل على تأييد المشاركين لهذه الفوائد التشغيلية.بقية العبارات، على اختلاف تفاصيلها، جاءت بمستويات اتفاق تتراوح بين (٨١.٣٢٪) و(٨٤.٧١٪)، مع متوسطات مرتفعة تشير إلى أن كافة الجوانب التي تعكس استخدام الحوسبة السحابية تلقى قبولاً واسعاً بين أفراد العينة، من حيث المرونة، الأمان، الاستمرارية، القابلية للتوسع، والتأهيل والتدريب.

**ثانياً: قياس المحور الثاني للمتغير التابع (أمن نظام المعلومات المحاسبية)الجدول (٣) نتائج قياسات أمن نظام المعلومات المحاسبية**

| ت | العبارة | المتوسط | الانحراف المعياري | المرتبة | نسبة الاتفاق |
|---|---|---|---|---|---|
| Y1 | يعد الأمان والخصوصية في نظام المعلومات المحاسبية من ابرز القضايا الأساسية في الوحدات الاقتصادية. | 4.2868 | ٠.80653 | ١ | %85.74 |
| Y2 | تعزز الضوابط الأمنية من مصداقية نظام المعلومات المحاسبية مثل أنظمة التشفير وتحديد صلاحيات الوصول. | 4.2206 | ٠.85800 | ٥ | %84.41 |
| Y3 | تساعد التدابير الأمنية على تقليل أخطار البرمجيات الخبيثة أو الفيروسات التي قد تهدد سلامة النظام المعلومات المحاسبية. | 4.2574 | ٠.75027 | ٤ | %85.15 |
| Y4 | تلتزم النظام المحاسبية بسياسات الأمان العامة للوحدة الإقتصادية. | 4.1838 | ٠.84505 | ٨ | %83.68 |
| Y5 | تسهم الالتزام بالمعايير القانونية في تعزيز أمن نظام المعلومات المحاسبية. | 4.1618 | ٠.80019 | ١٠ | %83.24 |
| Y6 | تطبق الوحدات الاقتصادية سياسات مراقبة صارمة على نظام المعلومات المحاسبية. | 4.0956 | ٠.71883 | ١٤ | %81.91 |
| Y7 | تؤدي فاعلية أمن نظام المعلومات المحاسبية الى تحقيق الميزة التنافسية. | 4.1471 | ٠.73565 | ١٢ | %82.94 |
| Y8 | يعد أمان النظام المحاسبي من التحديات الأساسية للوحدات الاقتصادية، لا سيما في ظل تزايد التهديدات السيبرانية وتطور أساليب الهجمات الإلكترونية. | 4.1544 | ٠.84221 | ١١ | %83.09 |
| Y9 | تعتبر حماية المعلومات المحاسبية ضرورة لتفادي المسؤولية القانونية. | 4.1985 | ٠.85911 | ٦ | %83.97 |
| Y10 | يعتمد فاعلية أمن نظام المعلومات المحاسبية على وجود فريق مؤهل ومزود بأدوات مناسبة. | 4.1618 | ٠.78146 | ٩ | %83.24 |
| Y11 | فاعلية امن نظام المعلومات المحاسبية تؤدي الى تحقيق موثوقية و شفافية و بالتالي القدرة على اتخاذ القرارات الرشيدة. | 4.1838 | ٠.79071 | ٧ | %83.68 |
| Y12 | يسهم أمن نظام المعلومات المحاسبية في تسهيل عمليات التدقيق الداخلي والخارجي. | 4.1397 | ٠.76180 | ١٣ | %82.79 |
| Y13 | توفر بعض نظام المعلومات المحاسبية الحديثة أدوات لتحديد صلاحيات الدخول بدقة بما يعزز من حماية البيانات المحاسبية. | 4.2574 | ٠.73026 | ٣ | %85.15 |
| Y14 | تساعد نظم الأمان على حماية البرامج المحاسبية من التلاعب والتلف. | 4.2794 | ٠.73727 | ٢ | %85.59 |

| المتوسط | ٤.١٩٤٩ | ٠.٧٨٠ | --- | ٨٣.٩٠٪ |
|---|---|---|---|---|

**المصدر:** من اعداد الباحثان من واقع الدراسة الميدانية لسنة ٢٠٢٥وقد بلغ المتوسط العام لمتغير أمن نظام المعلومات المحاسبية (٤.١٩٤٩) مع انحراف معياري مقداره (٠.٧٨٠)، ونسبة اتفاق كلية بلغت (٨٣.٩٠٪)، مما يشير إلى إجماع واضح من أفراد العينة على أهمية وتأثير جوانب الأمن المختلفة في النظام المحاسبي.وتتصدر العبارة المتعلقة بأهمية الأمان والخصوصية في نظام المعلومات المحاسبية (Y1) الترتيب الأول بمتوسط (٤.٢٨٦٨) ونسبة اتفاق (٨٥.٧٤٪)، مما يعكس إدراكاً قوياً من المشاركين للحساسية التي تحملها بيانات النظام وضرورة حمايتها.في المرتبة الثانية جاءت العبارة التي تؤكد على دور نظم الأمان في حماية البرامج المحاسبية من التلاعب والتلف (Y14) بمتوسط (٤.٢٧٩٤) ونسبة اتفاق (٨٥.٥٩٪)، مما يبرز أهمية الحماية التقنية للبرامج التي تُستخدم في معالجة البيانات.كما أظهرت العبارة الثالثة (Y13) التي تشير إلى توفر أدوات حديثة لتحديد صلاحيات الدخول بفعالية، نسبة اتفاق مرتفعة (٨٥.١٥٪)، مما يدل على اعتراف المشاركين بضرورة التحكم الدقيق في وصول المستخدمين إلى البيانات.على صعيد آخر، عبّرت العبارات ذات المرتبة الأدنى، مثل تطبيق سياسات المراقبة الصارمة (Y6)، عن اتفاق أقل نسبياً (٨١.٩١٪)، رغم أن النسبة لا تزال مرتفعة، ما قد يشير إلى تفاوت في تطبيق الإجراءات الأمنية بين الوحدات الاقتصادية.بشكل عام، تعكس هذه النتائج إدراكاً عالياً وشمولياً لمختلف أبعاد أمن نظام المعلومات المحاسبية، من الجوانب التقنية والتنظيمية إلى جوانب حماية البيانات والامتثال القانوني، مما يؤكد أهمية هذا المتغير في تعزيز فعالية النظام المحاسبي وكفاءته التشغيلية.

**٣:٣ اختبار فرضيات الدراسة**

**١:٣:٣ الفرضية الأولى: توجد موافقة ذات دلالة إحصائية معنوية من قبل أفراد عينة الدراسة على العبارات الخاصة باستخدام الحوسبة السحابية.الجدول (٤) نتائج اختبار ويلكوكسن للفرضية الأولى**

| المتغير | المتوسط | المتوسط الفرضي | الخطأ القياسي | قيمة (Z) المعيارية | القيمة الاحتمالية |
|---|---|---|---|---|---|
| الحوسبة السحابية | ٤.١٨٧٢ | ٣ | ٤٥٩.٩٧٦ | ٩.٣٨٧ | < 0.001 |

**المصدر:** من اعداد الباحثان من واقع الدراسة الميدانية لسنة ٢٠٢٥يتضح من نتائج الجدول (٤) أن متوسط استجابات أفراد عينة الدراسة لمدى موافقتهم على عبارات استخدام الحوسبة السحابية قد بلغ (٤.١٨٧٢)، وهي قيمة أعلى من المتوسط الفرضي المعتمد (٣). كما أظهرت نتائج اختبار ويلكوكسن قيمة معيارية (Z) بلغت (٩.٣٨٧) وقيمة احتمالية (P–value) أقل من (٠.٠٠١)، وهي أقل من مستوى الدلالة المعتمد (0.05). وبناءً على ذلك، يمكن رفض الفرضية العدمية وقبول الفرضية البديلة، مما يشير إلى وجود موافقة ذات دلالة إحصائية معنوية من قبل أفراد العينة على العبارات المتعلقة باستخدام الحوسبة السحابية.

**٢:٣:٣ الفرضية الثانية: توجد موافقة ذات دلالة إحصائية معنوية من قبل أفراد عينة الدراسة على العبارات الخاصة بأمن نظم المعلومات المحاسبية.الجدول (٥) نتائج اختبار ويلكوكسن للفرضية الثانية**

| المتغير | المتوسط | المتوسط الفرضي | الخطأ القياسي | قيمة (Z) المعيارية | القيمة الاحتمالية |
|---|---|---|---|---|---|
| أمن نظم المعلومات المحاسبية | ٤.١٩٤٩ | ٣ | ٤٥٩.٩٣٦ | ٩.٢٥١ | < 0.001 |

**المصدر:** من اعداد الباحثان من واقع الدراسة الميدانية لسنة ٢٠٢٥يوضح الجدول (٥) أن متوسط استجابات أفراد عينة الدراسة نحو مدى موافقتهم على عبارات أمن نظم المعلومات المحاسبية قد بلغ (٤.١٩٤٩)، وهي قيمة تفوق المتوسط الفرضي (٣). كما أظهرت نتائج اختبار ويلكوكسن قيمة معيارية (Z) مقدارها (٩.٢٥١) مع قيمة احتمالية (P–value) أقل من (٠.٠٠١)، وهي أقل من مستوى الدلالة المعتمد (0.05). وعليه، يتم رفض الفرضية العدمية لصالح الفرضية البديلة، مما يشير إلى وجود موافقة معنوية ذات دلالة إحصائية من قبل أفراد العينة على العبارات المرتبطة بأمن نظم المعلومات المحاسبية.

**٣:٣:٣ الفرضية الثالثة: توجد علاقة ارتباط معنوية ذات دلالة إحصائية بين استخدام الحوسبة السحابية ومستوى أمن نظم المعلومات المحاسبية، وذلك من وجهة نظر المهنيين والأكاديميين العاملين في مدينة أربيل.الجدول (٦) نتائج اختبار الفرضية الثالثة**

| المتغيران | معامل ارتباط سبيرمان | القيمة الاحتمالية |
|---|---|---|
| استخدام الحوسبة السحابية | **٠.٧٩٤ | < 0.001 |

| | | |
|---|---|---|
| ومستوى أمن نظم المعلومات المحاسبية | | |

**المصدر:** من اعداد الباحثان من واقع الدراسة الميدانية لسنة ٢٠٢٥يتضح من نتائج الجدول (٦) أن قيمة معامل ارتباط سبيرمان بين استخدام الحوسبة السحابية ومستوى أمن نظم المعلومات المحاسبية بلغت (٠.٧٩٤)، وهي قيمة موجبة مرتفعة تشير إلى وجود علاقة ارتباط قوية بين المتغيرين. كما أن القيمة الاحتمالية المصاحبة للاختبار بلغت أقل من (٠.٠٠١)، وهي أقل من مستوى الدلالة المعتمد (٠.٠٥)، مما يشير إلى أن هذه العلاقة ذات دلالة إحصائية معنوية. وبالتالي، يتم رفض الفرضية العدمية وقبول الفرضية البديلة، مما يؤكد وجود علاقة ارتباط قوية ومعنوية بين استخدام الحوسبة السحابية ومستوى أمن نظم المعلومات المحاسبية وفقاً لآراء أفراد العينة في مدينة أربيل.

**٤:٣:٣ الفرضية الرابعة: يوجد تأثير معنوي ذو دلالة إحصائية لاستخدام الحوسبة السحابية في مستوى أمن نظم المعلومات المحاسبية، بحسب تقديرات المهنيين والأكاديميين في مدينة أربيل.الجدول (٧) نتائج اختبار الفرضية الرابعة**

| أمن نظم المعلومات المحاسبية | القيمة الثابته | ميل الإنحدار | قيمة-t | القيمة الاحتمالية | قيمة-F | القيمة الإحتمالية | معامل التحديد |
|---|---|---|---|---|---|---|---|
| الحوسبة السحابية | ٠.٠٣٥ | ١.٠١٠ | ٢٦.٤٥٤ | < 0.001 | ٦٩٩.٨١ | < 0.001 | ٠.٨٣٩ |

**المصدر:** من اعداد الباحثان من واقع الدراسة الميدانية لسنة ٢٠٢٥تشير نتائج اختبار الانحدار إلى أن قيمة الميل (معامل الانحدار) بلغت (١.٠١٠)، وهي قيمة موجبة تدل على وجود علاقة طردية قوية بين استخدام الحوسبة السحابية ومستوى أمن نظم المعلومات المحاسبية. بمعنى آخر، كلما زاد الاعتماد على تقنيات الحوسبة السحابية، ارتفع مستوى أمن نظم المعلومات المحاسبية من وجهة نظر أفراد العينة. أما بالنسبة لاختبار معنوية النموذج، فقد أظهرت قيمة (t) المحسوبة لمعامل الانحدار (٢٦.٤٥٤)، وهي قيمة كبيرة جداً مقارنة بالقيم الجدولية، مع قيمة احتمالية (p-value) أقل من (٠.٠٠١)، مما يشير إلى أن معامل الانحدار معنوي إحصائياً عند مستوى دلالة (٠.٠٥)، ويدعم وجود تأثير معنوي للحوسبة السحابية على أمن نظم المعلومات المحاسبية.كما أظهرت نتائج اختبار (F) الخاص بملاءمة نموذج الانحدار قيمة مرتفعة جداً بلغت (٦٩٩.٨١)، مع قيمة احتمالية أقل من (٠.٠٠١)، ما يعني أن النموذج ككل معنوي إحصائياً، ويصلح لقياس العلاقة بين المتغيرين. وعلى صعيد القوة التفسيرية للنموذج، بلغ معامل التحديد ($R^2$) قيمة (٠.٨٣٩)، وهو ما يشير إلى أن ٨٣.٩٪ من التغيرات الحاصلة في مستوى أمن نظم المعلومات المحاسبية يمكن تفسيرها من خلال استخدام الحوسبة السحابية، بينما تعزى النسبة المتبقية إلى عوامل أخرى لم يتضمنها النموذج.بناءً على ما سبق، يمكن تأكيد صحة الفرضية الرابعة التي تنص على وجود تأثير معنوي ذو دلالة إحصائية لاستخدام الحوسبة السحابية في مستوى أمن نظم المعلومات المحاسبية في بيئة العمل بمدينة أربيل. وتعكس هذه النتيجة أهمية الحوسبة السحابية كأحد العوامل المؤثرة في تعزيز أمن الأنظمة المحاسبية، بما يتفق مع التوجهات الحديثة في دعم البنية التحتية لتقنية المعلومات.

**٥:٣:٣ الفرضية الخامسة: توجد فروق ذات دلالة إحصائية معنوية في آراء المهنيين والأكاديميين في مدينة أربيل بشأن استخدام الحوسبة السحابية.**استهدفت الفرضية الخامسة التحقق مما إذا كانت هناك فروق ذات دلالة إحصائية معنوية في آراء المهنيين والأكاديميين في مدينة أربيل بشأن استخدام الحوسبة السحابية. ولتحقيق ذلك، تم استخدام اختبار (T-test) لعينة مستقلة(Independent Samples T-test)، لمقارنة متوسطات تقديرات المجموعتين.**الجدول (٨) نتائج اختبار الفرضية الخامسة**

| المحور | الوظيفة | المتوسط | فرق المتوسط | العدد | قيمة (t) | القيمة الإحتمالية |
|---|---|---|---|---|---|---|
| الحوسبة السحابية | أكاديمي | ٤.٠١٣٨ | -٠.٢٤٣١ | 39 | -٢.٣١٠ | ٠.٠٢٢ |
| | مهني | ٤.٢٥٦٩ | | 97 | | |

**المصدر:** من اعداد الباحثان من واقع الدراسة الميدانية لسنة ٢٠٢٥تشير نتائج الجدول (٨) إلى أن متوسط تقييم الأكاديميين لاستخدام الحوسبة السحابية بلغ (٤.٠١٣٨)، في حين كان متوسط تقييم المهنيين أعلى وبلغ (٤.٢٥٦٩). وبلغ فرق المتوسطات بين المجموعتين (-٠.٢٤٣١)، مما يعكس أن المهنيين كانوا أكثر ميلًا لتقدير أهمية استخدام الحوسبة السحابية مقارنة بالأكاديميين.أما من الناحية الإحصائية، فقد أظهرت قيمة (t) المحسوبة (-٢.٣١٠) أن الفروق بين المجموعتين معنوية عند مستوى دلالة (٠.٠٥)، حيث بلغت القيمة الاحتمالية (0.022) (p-value)، وهي أقل من الحد المعتمد (٠.٠٥). وبذلك يمكن رفض فرض العدم القائل بعدم وجود فروق معنوية بين آراء المجموعتين، والقبول بوجود فروق ذات

دلالة إحصائية. تدل هذه النتائج على وجود تباين جوهري في تقييم كل من الأكاديميين والمهنيين لاستخدام تقنيات الحوسبة السحابية، حيث يميل المهنيون العاملون في الميدان إلى تقدير أهمية هذه التقنيات بدرجة أعلى من الأكاديميين. ويمكن تفسير ذلك بأن المهنيين غالباً ما يتعاملون بشكل مباشر مع تطبيقات الحوسبة السحابية في بيئات العمل اليومية، ما يمنحهم تصوراً عملياً أدق حول فوائدها وتأثيرها على أنشطة المحاسبة وأنظمة المعلومات.

**٦:٣:٣ الفرضية السادسة: توجد فروق ذات دلالة إحصائية معنوية في آراء المهنيين والأكاديميين في مدينة أربيل بشأن أمن نظم المعلومات المحاسبية.**هدفت الفرضية السادسة إلى الكشف عن وجود فروق ذات دلالة إحصائية معنوية في آراء المهنيين والأكاديميين في مدينة أربيل بشأن مستوى أمن نظم المعلومات المحاسبية. ولتحقيق ذلك، تم استخدام اختبار (T–test) لعينة مستقلة، بغرض مقارنة متوسط تقديرات المجموعتين.

**الجدول (٩) نتائج اختبار الفرضية السادسة**

| المحور | الوظيفة | المتوسط | فرق المتوسط | العدد | قيمة (t) | القيمة الإحتمالية |
|---|---|---|---|---|---|---|
| أمن نظم المعلومات المحاسبية | أكاديمي | ٣.٩٤٨٧ | ٠.٣٤٥١– | 39 | ٣.٠١٣– | ٠.٠٠٣ |
| | مهني | ٤.٢٩٣٨ | | 97 | | |

**المصدر:** من اعداد الباحثان من واقع الدراسة الميدانية لسنة ٢٠٢٥وفقاً للبيانات الواردة في الجدول (٩)، بلغ متوسط تقييم الأكاديميين لمستوى أمن نظم المعلومات المحاسبية (٣.٩٤٨٧)، في حين كان متوسط تقييم المهنيين أعلى وبلغ (٤.٢٩٣٨). ويظهر فرق المتوسطات (–٠.٣٤٥١) أن المهنيين يقدّرون أمن نظم المعلومات المحاسبية بدرجة أعلى مقارنة بالأكاديميين.أما من الناحية الإحصائية، فقد بلغت قيمة (t) المحسوبة (–٣.٠١٣)، وهي قيمة تدل على وجود فرق جوهري بين متوسطات المجموعتين. كما أن القيمة الاحتمالية (p–value) المقابلة بلغت (٠.٠٠٣)، وهي أقل بكثير من مستوى الدلالة المعتمد (٠.٠٥)، مما يعني أن الفروق بين المجموعتين معنوية إحصائياً.تعكس هذه النتائج وجود تباين معنوي في تقديرات الأكاديميين والمهنيين لمستوى أمن نظم المعلومات المحاسبية، حيث يميل المهنيون إلى تقييم أنظمة أمن المعلومات المحاسبية بشكل أكثر إيجابية. ويمكن تفسير ذلك بأن المهنيين غالباً ما يتعاملون بشكل مباشر مع أنظمة المعلومات المحاسبية في بيئات العمل، مما يمنحهم رؤية أدق حول مدى فعالية أنظمة الحماية المطبقة، في حين أن الأكاديميين قد يعتمدون في تقييمهم على المعرفة النظرية أو التجريبية غير المباشرة.

## الاستنتاجات

١. أن فاعلية أمن نظام المعلومات المحاسبية عند استخدام الحوسبة السحابية تعتمد بشكل كبير على الاستراتيجيات الأمنية المتبعة، وليس فقط على المزايا التقنية التي توفرها الحوسبة السحابية. وتؤكد أن نجاح تطبيق هذه التقنية يتطلب فهماً شاملاً للتحديات والمخاطر الأمنية، مما يجعل الأمن السيبراني جزءاً أساسياً من عملية التحول الرقمي في الوحدات الاقتصادية.

٢. أظهرت نتائج التحليل الإحصائي اتفاقاً معنوياً بين أفراد عينة الدراسة تجاه العبارات المتعلقة باستخدام الحوسبة السحابية وأمن نظام المعلومات المحاسبية، مما يعكس قناعة واضحة بأهمية هذه المفاهيم في دعم بيئة العمل المحاسبي، وقد بينت نتائج إختبار ويلكوكسن لعينة واحدة أن متوسطات الاستجابات أفراد عينة الدراسة يفوق المتوسط الفرضي المعتمد (٣) بشكل يعكس فروقاً ذات دلالة إحصائية معنوية حيث بلغ متوسط الاستجابات لإستخدام الحوسبة السحابية (٤.١٨٧٢)، في حين بلغ متوسط الاستجابات لأمن نظام المعلومات المحاسبية (٤.١٩٤٩).

٣. أوضحت نتائج التحليل أن التوجهات الإيجابية للمشاركين تجاه استخدام تقنية الحوسبة السحابية وأمن نظام المعلومات المحاسبية لا تعد عشوائية، وإنما تنبع من إدراك واعٍ وفهم فعلي لدور هذه التقنيات في تعزيز كفاءة وأمان بيئات العمل المحاسبي. ويؤكد ذلك أن جميع القيم الاحتمالية الناتجة عن اختبار ويلكوكسن كانت أقل من مستوى الدلالة الإحصائية المعتمد (٠.٠٥)، مما يشير إلى أن الفروق بين المتوسطات الفعلية والمتوسط الفرضي ليست ناتجة عن الصدفة، بل تعكس دلالة إحصائية حقيقية.

٤. تشير نتائج الى وجود علاقة ارتباط معنوية قوية بين استخدام الحوسبة السحابية ومستوى أمن نظام المعلومات المحاسبية، مما يعكس وعياً مشتركاً لدى أفراد العينة بأثر استخدام هذه التقنية الرقمية في تعزيز أمن المعلومات في البيئة المحاسبية. وقد بلغ معامل ارتباط سبيرمان ( ٠.٧٩٤)، وهو معامل موجب مرتفع يدل إلى علاقة ارتباط قوية بين المتغيرين، كما أن القيمة الاحتمالية المصاحبة للاختبار كانت أقل من (٠.٠٠١)، وهي أقل من مستوى الدلالة المعتمد (٠.٠٥)، مما يؤكد دلالة هذه العلاقة إحصائياً.

٥. أشارت نتائج التحليل الإحصائي إلى أن الاعتماد على الحوسبة السحابية يمثل عاملاً مؤثراً في تعزيز أمن نظام المعلومات المحاسبية، حيث بلغ معامل الانحدار (١.٠١٠) مشيراً إلى علاقة طردية قوية. كما بينت نتائج اختبار (T = 26.454) و (F = 699.81) دلالة إحصائية معنوية عند مستوى ($p < 0.001$)، مما يدل على صلاحية النموذج لتفسير العلاقة بين المتغيرين. وأوضح معامل التحديد ($R^2 = 0.839$) أن ٨٣.٩٪ من التباين في أمن نظام المعلومات المحاسبية يعزى إلى استخدام الحوسبة السحابية، مما يدعم فعالية هذه التقنية في حماية البيانات المحاسبية.

٦. كشفت النتائج اختبار T لعينة مستقلة وجود فروق ذات دلالة احصائية معنوية بين آراء الأكاديميين والمهنيين في مدينة اربيل، حيث بلغ متوسط تقييم المهنيين (٤.٢٥٦٩) مقابل (٤.٠١٣٨) للأكاديميين، بفارق (-٠.٢٤٣١) لصالح المهنيين. وقد بلغت قيمة $T = -2.310$، مع قيمة احتمالية ($p = 0.022$):

- حيث أبدى المهنيون مواقف أكثر إيجابية تجاه استخدام الحوسبة السحابية وأمن نظام المعلومات المحاسبية.
- يعزى هذا الفرق إلى الخبرة العملية المباشرة للمهنيين مقارنة بالأكاديميين الذين يعتمدون بشكل أكبر على المعرفة النظرية.

٧. جاءت نتائج الدراسة متوافقة مع التوجهات الحديثة في أدبيات الحوسبة السحابية وأمن المعلومات، مما يعزز الرؤية بأن هذه التقنيات لم تعد خياراً إضافياً، بل ضرورة استراتيجية لضمان كفاءة وأمان الأنظمة المحاسبية.

## التوصيات

١. ضرورة التزام الوحدات الاقتصادية بتنفيذ وتحديث أفضل الممارسات والإجراءات الأمنية عند استخدام الحوسبة السحابية. وتقييم بشكل دوري للمخاطر المحتملة المرتبطة بالحوسبة السحابية، لضمان الاستجابة الفعالة لأي تهديدات قد تظهر.

٢. توصي الباحثان بضرورة وضع خطة وطنية شاملة لتبني وتكييف المعايير الدولية مثل (ISO/IEC 27001) و (SOC) و (GDPR) و (SOX)، مع توفير بنى تشريعية وتقنية داعمة، وتأسيس وحدات متخصصة بالأمن السيبراني داخل الوحدات الاقتصادية لضمان التطبيق الفعلي والفعال لهذه الأطر في البيئة المحلية.

٣. ضرورة تحقيق التكامل بين الضوابط الداخلية وأطر حوكمة البيانات لتعزيز أمن المعلومات وكفاءة الرقابة وجودة التقارير المحاسبية.

٤. يجب تطوير إطار قانوني وتنظيمي متكامل يلزم مزودي الخدمات السحابية باعتماد معايير صارمة لأمن البيانات، مع تعزيز التكامل بين الخبرات القانونية والتقنية في تصميم وتشغيل النظم السحابية، وتكثيف التدريب المتخصص للكوادر المحاسبية حول المتطلبات القانونية والامتثال الرقمي.

٥. أهمية تبني برامج تدريبية مستمرة في الأمن السيبراني تستهدف المحاسبين والمستخدمين النهائيين، إلى جانب تطبيق سياسات واضحة للمساءلة والتوعية، بما يسهم في بناء ثقافة أمنية فعالة داخل بيئة العمل المحاسبية السحابية.

٦. يجب إعادة تقييم المعايير المهنية المحاسبية لتتكيف مع متطلبات النظم السحابية، وتطوير أطر رقابية متقدمة تضمن الحفاظ على سرية ونزاهة المعلومات ضمن هذه البيئات الرقمية الحديثة.

٧. ضرورة تبني خطط استمرارية أعمال متكاملة تشمل تقنيات النسخ الاحتياطي والتكرار الجغرافي، إلى جانب أنظمة الكشف الذكية، مع الالتزام بالتوثيق المؤسسي، بهدف تعزيز الجهوزية الرقمية وتقليل فترات التعطل في النظم المحاسبية.

## المصادر والمراجع


- زرزار، العياشي، وبن وريدة، حمزة، (2019). *الحوسبة السحابية: المفهوم والخصائص* (تجارب دول وشركات رائدة). مجلة أرصاد للدراسات الاقتصادية والإدارية، المجلد ٢(العدد ٢)، ١٨٤-٢٠٥. [أونلاين] متاح على: https://doi.org/10.52863/2261-002-002-010
- عبدالزهرة، علي، (٢٠٢٣). *جودة المعلومات المحاسبية في ظل تأثير استخدام الحوسبة السحابية*. مجلة العلوم الاقتصادية والإدارية والقانونية (JEALS)، ٧(3)، ص ٤، جامعة الكوفة: العراق. [أونلاين] متاح على: https://doi.org/10.26389/AJSRP.R071122
- الشمراني، ماجدة والأسمري، نورة، (٢٠٢١). *استخدام الحوسبة السحابية ودورها في تحديد أتعاب عملية المراجعة من وجهة نظر المراجعين الخارجيين*. المجلة العالمية للاقتصاد والأعمال، ١٠(2)، ص ٢٤٦-٢٥٨، جامعة الملك خالد: المملكة العربية السعودية. [أونلاين] متاح على: https://doi.org/10.31559/GJEB2021.10.2.2
- عباس، سجى فاضل، (٢٠٢٤). *الحوكمة الرقمية في ظل تهديدات الأمن السيبرني*، مجلة حمورابي للدراسات، (49)13، ص ٣٢٣-٣٣٨، جامعة النهرين: الإمارات. [أونلاين] متاح على: (PDF)الحوكمة الرقمية في ظل تهديدات الأمن السيبراني: دولة الامارات انموذجا

- أبو عمرو، أيمان حسين والزويلف، انعام محسن، (٢٠٢٣). *فاعلية الأطر الأمنية في نظم المعلومات المحاسبية*، مجلة جدارا للدراسات والبحوث، عدد خاص، ص ٤٤، جامعة العلوم الإسلامية العالمية: الأردن. [أونلاين] متاح على: https://doi.org/
- المطيري، فهد بن سعود، (٢٠١٩). *نظم المعلومات المحاسبية: المفاهيم والتطبيقات*، عمان: دار الحامد، ص ١٣٥.
- البرقاوي، يوسف، (٢٠٢١). *أمن المعلومات وحمايتها في بيئة الأعمال الرقمية .مجلة جامعة الأندلس للعلوم التطبيقية*، ٨(2)، ص ٤٥-٦٦.
- الزعبي، أحمد، (٢٠١٧). *أمن المعلومات في النظم المحاسبية الإلكترونية*. المجلة الأردنية في إدارة الأعمال، ١٣(4)، ص ٥٥٢ .
- كاطع، علي خلف وغالي، زينة حمزة وعزيز، حيدر عباس، (٢٠٢٤). *دور التدقيق الداخلي في تعزيز التعامل مع أمن نظم المعلومات المحاسبية المحوسبة*. مجلة العلوم المالية والمحاسبية، عدد خاص، ص ٩١-٩٨، الجامعة التقنية الجنوبية الناصرية: العراق. [أونلاين] متاح على: https://www.researchgate.net/publication/386566955_dwr_altdqyq_aldakhly_fy_tzyz_altaml_m_amn_nzm_al mlwmat_almhasbyt_almhwsbt?utm_source=chatgpt.com#full-text
- السويدي، سالم عبيد. (٢٠٢٢). *تحليل مخاطر الهجمات السيبرانية في الأنظمة المالية الذكية*، المجلة الخليجية للأمن السيبراني، ٦٣-٧٢.
- الربيدي، محمد علي والسريحي، سلطان علي أحمد والحميري، نبيل حسان عبده، (٢٠٢٥). *الدور الوسيط للضوابط الأمنية بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية*. المجلة الأدرنية في إدارة الأعمال، ٢١(١)، ص ١١٧-١٣٠، جامعة العلوم والتكنولوجية: اليمن. [أونلاين] متاح على:https://doi.org/10.35516/jjba.v21i1.270
- الهيئة الوطنية للأمن السيبراني، (٢٠٢١). *الضوابط الأساسية للأمن السيبراني* .الرياض: المملكة العربية السعودي. [أونلاين] متاح على: https://nca.gov.sa

- Shkurti, R. and Muça, E., (2014). *An analysis of cloud computing and its role in accounting industry in Albania*. Journal of Information Systems & Operations Management, 8(2), pp. 1–12. [online] Available at: https://www.researchgate.net/publication/303267851_An_analysis_of_cloud_computing_and_its_role_in_accounting_industry_in_Albania [Accessed 13 Aug. 2025].

- Mell, P. and Grance, T, (2011). *The NIST definition of cloud computing*. NIST Special Publication 800-145, p. 23. [online] Available at: https://doi.org/10.6028/NIST.SP.800-145 [Accessed 13 Aug. 2025].
- Alharthi, A., Krotov, V. and Bowman, M. (2022). *Addressing security and privacy challenges in cloud computing*. Journal of Cloud Computing, 11(1), pp. 210–225. [online] Available at: https://doi.org/10.1186/s13677-022-00274-z [Accessed 13 Aug. 2025].
- Zhang, Q. and Chen, Z. (2021). *Cloud computing models and services: A comparative study*. Elsevier.
- Singh, G., Rana, A. and Rajput, N. (2023). *Cloud computing infrastructure: Security and architecture Springer*. [online] Available at: https://doi.org/10.1007/978-981-99-1263-9 [Accessed 13 Aug. 2025].
- Zhang, Q., Cheng, L. and Boutaba, R. (2010). *Cloud computing: State-of-the-art and research challenges*. Journal of Internet Services and Applications, 1(1), pp. 7–18. [online] Available at: https://doi.org/10.1007/s13174-010-0007-6 [Accessed 13 Aug. 2025].
- Armbrust, M. et al., (2010). *A view of cloud computing*. Communications of the ACM, 53(4), pp. 50–58. [online] Available at: https://doi.org/10.1145/1721654.1721672 [Accessed 13 Aug. 2025].
- Buyya, R. Broberg, J. and Goscinski, A. (eds.), (2010). *Cloud computing: Principles and paradigms*. Wiley. ISBN: 978-0-470-88799-8. [online] Available at:Cloud Computing | Wiley Online Books
- Khajeh-Hosseini, A. Greenwood, D. and Sommerville, I. (2010). *Cloud migration: A case study of migrating an enterprise IT system to IaaS*. In: 2010 IEEE 3rd International Conference on Cloud Computing, pp. 450–457. [online] Available at: https://doi.org/10.1109/CLOUD.2010.66 [Accessed 13 Aug. 2025].
- Gill, S.S. Choudhary, A. and Buyya, R. (2019). *Transformative effects of cloud computing on businesses: A review*. Future Generation Computer Systems, 91, pp. 475–487. [online] Available at: https://doi.org/10.1016/j.future.2018.09.003 [Accessed 13 Aug. 2025].
- Gholami, A. and Laure, E. (2016). *Big data security and privacy issues in scientific cloud-based environments: A review*. Procedia Computer Science, 98, pp. 461–468. [online] Available at: https://doi.org/10.1016/j.procs.2016.09.076 [Accessed 13 Aug. 2025].
- Zangana, H.M. and Zeebaree, S.R.M. (2024). *Distributed Systems for Artificial Intelligence in Cloud Computing*. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 5(1), pp. 11–30. [online] Available at: https://ojs.unikom.ac.id/index.php/injiiscom/article/view/11883 [Accessed 13 Aug. 2025].

- Zhou, Z. Chen, X. Li, E. Zeng, L. and Zhang, J. (2019). *Edge intelligence: Paving the last mile of artificial intelligence with edge computing*. Proceedings of the IEEE, 107(8), pp. 1738–1762. [online] Available at: https://ieeexplore.ieee.org/browse/periodicals/title/ [Accessed 13 Aug. 2025].
- Huang, N. Li, X. Xu, Q. Chen, R. Chen, H. and Chen, A. (2023). *Artificial intelligence-based temperature twinning and pre-control for data center airflow organization*. *Energies*, 16(16), p. 6063.
- Ahmed, R.R. Zada, R.S.E. and Akram, S.M. (2019). *Security in accounting information systems: Risks and controls*. Journal of Information Systems, 33(1), pp. 1–15. [online] Available at: https://www.researchgate.net/publication/330856912_The_impact_of_Accounting_Information_Systems'_Quality_on_Accounting_Information_Quality
- Zadorozhnyi, Z. and Muravskyi, V. (2020). *Accounting information systems security in the digital age*. Journal of Accounting and Control, 28(2), pp. 114–120.
- AICPA. (2017). *Trust Services Principles and Criteria*. TSP Section 100, p. 3. [online] Available at: https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-
- Gelinas, U.J. Dull, R.B. and Wheeler, P.R. (2018). *Accounting Information Systems*. 11th ed. Boston: Cengage Learning, p. 387. [online] Available at:Accounting Information Systems - Ulric J. Gelinas, Richard B. Dull, Patrick Wheeler - كتب Google
- Bodnar, G.H. and Hopwood, W.S. (2013). *Accounting Information Systems*. 11th ed. Boston: Pearson, p. 271. [online] Available at: Accounting Information Systems - George H. Bodnar, William S. Hopwood - كتب Google
- Dunn, C.L. Cherrington, J.O. and Hollander, A. (2016). *Accounting Information Systems*. 14th ed. Boston: Cengage Learning, p. 212.
- Kim, D. and Solomon, M.G. (2018). *Fundamentals of Information Systems Security*. 3rd ed. Burlington: Jones & Bartlett Learning, p.187. [online] Available at: Fundamentals of Information Systems Security - David Kim, Michael G. Solomon - كتب Google
- Von Solms, R. and van Niekerk, J. (2013). *From information security to cyber security. Computers & Security*, 38, pp. 97–102. [online] Available at: https://doi.org/10.1016/j.cose.2013.04.004
- Harris, S. (2020). *CISSP All-in-One Exam Guide*. 8th ed. New York: McGraw-Hill Education. [online] Available at: CISSP All-in-One Exam Guide, Eighth Edition: 9781260142655: Computer Science Books @ Amazon.com
- Gelinas, U.J. Dull, R.B. and Wheeler, P.R. (2019). *Accounting Information Systems*. 11th ed. Boston: Cengage. [online] Available at:Accounting Information Systems - Ulric J. Gelinas, Richard B. Dull, Patrick Wheeler - كتب
- Andress, J. (2020). *Cybersecurity: The Beginner's Guide*. Birmingham: Packt Publishing. [online] Available at: Cybersecurity: The Beginner's Guide | Security | Paperback
- Alshawabkeh, A.M. Kadir, M.R.A. Nori, W.M.N. and Hassan, H. (2022). *The moderating effect of cloud computing on the relationship between accounting information systems and firms' performance in Jordan.* WSEAS Transactions on Business and Economics, 19, pp. 1155–1169. [online] Available at: https://doi.org/10.37394/23207.2022.19.101
- Li, X. (2024). *Risks and preventive measures for manufacturing enterprises in the context of cloud accounting*. Applied Mathematics and Nonlinear Sciences, 9(1), pp. 1–١٤. [online] Available at: https://doi.org/10.2478/amns.2023.1.00399
- Alrabei, A.M. (2023). *Green electronic auditing and accounting information reliability in the Jordanian Social Security Corporation: The mediating role of cloud computing*. International Journal of Financial Studies, 11(3), Article 114. [online] Available at: https://doi.org/10.3390/ijfs11030114
- Khanom, T. (2017). *The impact of using cloud computing upon the quality of accounting information and its reflection upon the development of the world standards of financial reports in Jordanian corporations*. International Journal of Professional Business Review, 8(9), pp .1–24. [online] Available at: The_Impact_of_Using_the_Cloud_Computing_Upon_the_Q.pdf
- Delso-Vicente, A.T., Sindreu-González, J., & Alfaro-Cortés, E. (2025). *Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity*. Future Business Journal, 11(1), p .28. [online] Available at: https://fbj.springeropen.com/articles/10.1186/s43093-025-00452-7
- Safa, N.S. Maple, C. Furnell, S. Azad, M.A. Perera, C. Dabbagh, M. and Sookhak, M. (2019). *Deterrence and prevention-based model to mitigate information security insider threats in organisations*. arXiv preprint, March, pp. 1-18. [online] Available at: https://arxiv.org/pdf/1903.12079.pdf
- Alkalbani, A. Deng, H. & Kam, B. 2016. *Investigating the role of socio-organizational factors in the information security compliance in organizations*. arXiv preprint arXiv:1606.00875, p. 5. [online] Available at: https://arxiv.org/abs/1606.00875