المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 7 - الإصدار 75
تاريخ النشر: 20 يناير 2026 م

الجوانب الأمنية للحوسبة السحابية (مراجعة أدبيات الموضوع للفترة من 2021م – 2024م)

Security Aspects of Cloud Computing (Literature Review Article Period 2021-2024)

إعداد: الباحث/ علي بن أحمد سليمان الجهني

باحث دكتوراه علم المعلومات (ادارة المعرفة)، قسم علم المعلومات، كلية الآداب والعلوم الإنسانية، جامعة الملك عبدالعزيز، المملكة العربية السعودية

Email: ali.altubiani@gmail.com

الملخص:

تهدف هذه الدراسة إلى التعرف على أبرز الجوانب الأمنية المتعلقة بأمن الحوسبة السحابية، وذلك من خلال استعراض أهم التهديدات والثغرات الأمنية التي تشكل خطراً على أمن وسلامة، وسرية البيانات، وطرق وأساليب الحماية للحد من تلك المخاطر، بالإضافة إلى التعريف بمفهوم الأمن المرتبط بكلاً من البيانات والمعلومات، والمعرفة، وكذلك التعريف بمفهوم تقنيات وخدمات الحوسبة السحابية، وأبرز مجالات البحث حولها. واخيراً استعراض أهم الدراسات العلمية المحكمة والمنشورة حول هذا الموضوع وذلك اعتماداً على منهج المراجعة الأدبية المنهجية (Systematic Literature Review). وتوصلت الدراسة إلى عدد من الاستنتاجات ومن أهمها إن الاستجابة للحوادث والتعافي منها من أهم الجوانب الأمنية للحوسبة السحابية، حيث تمثل الاستجابة للحوادث في الوقت المناسب أهم المكونات الأساسية في مجال أمن الحوسبة السحابية. وكذلك توصلت الدراسة إلى ضرورة نشر الوعي حول أمن البيانات في الحوسبة السحابية للمستخدمين حيث تشير العديد من الدراسات إن أغلب المخاطر والتهديدات تقع لسوء التعامل مع البيانات في الحوسبة السحابية من قبل المستخدمين، وفي ضوء ما توصلت له الدراسة من نتائج يوصي الباحث باعتماد منهجية تقييم مخاطر سحابية قبل التبنّي، وتبني سياسات واستراتيجيات للاستجابة السريعة للحوادث ومعالجتها، واختيار مزودي خدمات سحابية وفق معايير موثوقة وقابلة للتحقق مع التركيز على الشفافية والامتثال والسجل الأمني لمزود الخدمة، وشهادات الامتثال واتفاقيات مستوى خدمة واضحة، وكذلك تعزيز وتوحيد سياسات الوصول وإدارة الهوية واعتماد المصادقة متعددة العوامل خصوصا للحسابات الإدارية، ورفع الوعي الأمني بشكل مستمر وتدريب الكوادر والمستخدمين.

الكلمات المفتاحية: الحوسبة السحابية، الجوانب الأمنية، البيانات، المعلومات، المعرفة

المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 7 - الإصدار 75
تاريخ النشر: 20 يناير 2026 م

Security Aspects of Cloud Computing (Literature Review Article Period 2021-2024)

Abstract:

This study aims to identify the most prominent security aspects related to cloud computing security by reviewing the key threats and vulnerabilities that pose risks to data security, integrity, and confidentiality, as well as the methods and mechanisms of protection to mitigate these risks. It also introduces the concept of security as it relates to data, information, and knowledge, in addition to defining cloud computing technologies and services and highlighting the main research domains associated with them. Finally, the study reviews the most important peer-reviewed and published scientific studies on this topic, based on the Systematic Literature Review (SLR) methodology.

The study reached several conclusions, most notably that incident response and recovery are among the most critical security aspects of cloud computing. Timely incident response represents one of the fundamental components of cloud security. The study also emphasizes the necessity of raising user awareness regarding data security in cloud environments, as numerous studies indicate that most risks and threats result from improper handling of cloud-based data by users.

In light of these findings, the researcher recommends adopting a cloud risk assessment methodology prior to deployment, establishing policies and strategies for rapid incident response and remediation, and selecting cloud service providers based on reliable and verifiable criteria, with a focus on transparency, compliance, and the provider's security track record, as well as on compliance certifications and clear service level agreements (SLAs). The study further recommends strengthening and standardizing access control and identity management policies, adopting multi-factor authentication particularly for administrative accounts and continuously enhancing security awareness through ongoing training for staff and users.

Keywords: Cloud computing, security aspects, data, information, knowledge

1. المقدمة:

تعد الجوانب الأمنية من أكثر الموضوعات أهمية في مجال التقنيات الرقمية، لكون هذه التقنيات لا غنى عنها في كثير من الأحيان، حيث أنها دخلت في كافة المجالات والأنشطة على مستوى الأعمال والمنظمات، وكذلك على المستوى الشخصي للأفراد. وتعتبر تقنية وخدمات الحوسبة السحابية أحد أبرز هذه التقنيات فأغلب نظم المعلومات التي يتم استخدامها تعتمد على تقنية وخدمات الحوسبة السحابية في تشغيل نظم المعلومات التي تستخدمها الكثير من المنظمات. بالإضافة الى تعدد النظم والبرمجيات التي تقدم هذه الخدمات وتلبي حاجات المستخدمين سواء على المستوى الفردي للأشخاص أو المستوى التنظيمي للمنظمات.

أصبحت الحوسبة السحابية جزءًا لا يتجزأ من حياة كل مستخدم بشكل مباشر وغير مباشر. وترتبط مع عمليات واستخدام الحوسبة السحابية بيانات المستخدمين والمؤسسات مما يستدعي مخاوف أمنية كبيرة لمزودي خدمات الحوسبة السحابية للحفاظ على البيانات وحمايتها من الاختراق والتسرب، وفي الآونة الأخيرة برز مفهوم سرية البيانات والخصوصية من أهمّ شواغل الأمن في الحوسبة السحابية، خصوصا للبيانات السرية والحكومية وبيانات الشركات والمؤسسات الكبرى مما يستدعي إلى الاهتمام الكبير بالجوانب الأمنية لخدمات الحوسبة السحابية ومعرفة الخوادم غير الموثوقة والموثوقة، بالإضافة إلى استخدام آليات أمان مثل التشفير، والتجزئة، والتوقيع الرقمي، وبنية المفتاح العام، وإدارة الوصول إلى الهوية، وتسجيل الدخول الموحد.

1.1. مشكلة الدراسة:

وعلى ضوء ما سبق يمكن تلخيص مشكلة هذه الدراسة وحصر اشكاليتها في مراجعة ادبيات الموضوع حول الجوانب الأمنية التي تتعلق بأمن البيانات، المعلومات، والمعرفة بشكل عام في البيئات الرقمية، وتحديداً باستخدام تقنيات وخدمات الحوسبة السحابية. وتحاول هذه الدراسة التعريف بمفهومي أمن البيانات، المعلومات، والمعرفة اولاً، وثانياً تقنيات وخدمات الحوسبة السحابية، ثم استعراض أحدث ما توصل اليه الانتاج الفكري العربي والاجنبي حول ادبيات الموضوع فيما يتعلق بالتهديدات أو الثغرات الأمنية في بيئة الحوسبة السحابية وأنجع الحلول والتدابير اللازمة لسد تلك الثغرات والتصدي للهجمات المختلفة لضمان سلامة المحتوى سواء اكان بيانات، معلومات، أو معرفة، بالإضافة لضمان وتأمين جانب خصوصية بيانات المستخدمين بالدرجة الأولى، ومن ثم سلامة النظم وضمان استمرارها وعدم تعطلها. ويمكن التعبير عن اشكالية الدراسة من خلال التساؤل الرئيسي التالي:

- ما هي أبرز مجالات البحث حول الجوانب الأمنية في بيئة الحوسبة السحابية؟

وللإجابة على التساؤل الرئيسي يمكن طرح عدد من التساؤلات الفرعية، وهي كالتالي:

1. ما هو مجال أمن المعرفة؟
2. ماهي تقنية خدمات الحوسبة السحابية؟
3. ماهي المجالات العلمية الأكثر اهتماماً بالموضوع؟
4. ماهي أبرز التهديدات الأمنية في بيئة الحوسبة السحابية؟
5. ماهي أهم الحلول المقترحة لزيادة الأمن في بيئة الحوسبة السحابية؟
6. ماهي مجالات البحث المستقبلية حول أمن الحوسبة السحابية؟

2.1. أهمية الدراسة:

تكمن أهمية هذه الدراسة كونها تسبر غور الجوانب الأمنية في بيئة الحوسبة السحابية، من خلال التعرف على أهم المجالات البحثية حول هذا الموضوع، كما أنها تستعرض أبرز التهديدات والثغرات الأمنية التي تهدد أمن البيانات، المعلومات، والمعرفة التي يتم تخزينها، تداولها، ومشاركتها بواسطة تقنيات وخدمات منصات الحوسبة السحابية، ومن ثم التعريف بأفضل الحلول والتدابير التي توصي بها الدراسات العلمية المختارة ضمن حدود هذه الدراسة.

3.1. أهداف الدراسة:

تهدف هذه الدراسة من خلال مراجعة الأدبيات السابقة للجوانب الأمنية للحوسبة السحابية إلى مجموعة من الأهداف نلخصها في التالي:

- التعريف بمفهوم أمن البيانات، المعلومات، والمعرفة.
- التعرف على مفهوم تقنيات وخدمات الحوسبة السحابية.
- التعرف على أبرز مجالات البحث في أمن الحوسبة السحابية.
- التعرف على المجالات العلمية الأكثر اهتماماً بالموضوع.
- استعراض أبرز التهديدات الأمنية في بيئة الحوسبة السحابية.
- التعرف على أهم الحلول المقترحة لتحقيق الأمن في بيئة الحوسبة السحابية.
- التعرف على مجالات البحث المستقبلية حول أمن الحوسبة السحابية.

4.1. حدود الدراسة:

الحدود موضوعية: تركز هذه الدراسة على الجوانب الأمنية في بيئة الحوسبة السحابية فيما يتعلق بالتهديدات والثغرات الأمنية، والتوصيات المقترحة لمعالجتها من وجهة نظر الوعي المعلوماتي حولها.

الحدود زمانية: تقتصر هذه الدراسة على عشرة دراسات علمية محكمة يختارها الباحث خلال الفترة من 2021-01-01 إلى نهاية 2024-10-13م.

5.1. مصطلحات الدراسة

البيانات Data

لتحديد مفهوم البيانات كمصطلح فان البيانات DATA هي جمع للكلمة اللاتينية DATUM ومعناها مادة، وحدة، أو مفردة معلومات، وقد شاع استخدام مفردة DATAT للمفرد والجمع.

يشير مصطلح البيانات Data إلى إي من أو كل الحقائق، الارقام، الحروف، أو الرموز التي تشير إلى أو تصف موضوعاً ما، فكرة، حالة، أو أية عوامل أخرى. فالبيانات تكون تمثيل للحقائق، المفاهيم، أو التعليمات في شكل معياري يناسب عملية الاتصال، الترجمة، أو المعالجة بواسطة الإنسان أو الحاسب. احيانا تعتبر البيانات هي ذات الطابع الرقمي فقط في حين أنها ليست محدودة بالطابع الرقمي فقط.

وفي أبسط وأشمل تعريف للبيانات يمكن القول انها هي المادة الاولية الخام والمسجلة كأرقام أو رموز تتم معالجتها حتى تظهر في شكل معلومات. وتجدر الاشارة إلى أن البيانات بحد ذاتها لا تعني شيئاً مفهوماً له دلالة كافية (السريحي، 2019).

المعلومات Information

يشير ولفرد لانكستر (1979) إلى أن المعلومات شيء لا يمكن سماعة أو رؤيته أو الاحساس به فهي شي غير محدد المعالم، ولكنها تغير في الحالة المعرفية للأفراد في أي موضوع وذلك عن طريق تزويدهم واحاطتهم علماً بهذا الموضوع.

ويعرف معجم ويبستر (2026) المعلومات بأنها المقومات الجوهرية في أي نظام للتحكم. وهي بيانات مجهزة ومقيمة خاصة إذا تم استقاؤها من مجموعة من الوثائق أو الاشكال. وهي الجزء الذي يكون له معنى من الاشارة لتمييزه عن التشويش.

وللتمييز ما بين البيانات والمعلومات يشير موسى (2011) إلى أن هناك معياراً واحداً للتمييز بينهما ويتمثل في تحقيق الغرض من الاستخدام فإذا كانت البيانات في صورة تحقق الغرض من استخدامها مباشرة تكون في هذه الحالة معلومات.

المعرفة Knowledge

المعرفة هي العلم بالأشياء ومضامينها وتفسير الظواهر. تشتمل المعرفة على كل شيء سواء المعرفة بالطبيعة، الادارة، السياسة، الاقتصاد أو أي مجال من مجالات المعرفة البشرية بكافة مناحي الحياة.

يصنف بولاني (1966) المعرفة لفرعين أساسيين، وهما:

المعرفة الضمنية Tacit Knowledge: وتتعلق بكل ما هو موجود في عقل وقلب الفرد من مهارات، خبرات، افكار، وغيرها من المخزون الذهني للفرد، والتي من الصعب التعبير عنها بسهولة بالنقل، المشاركة، أو التحويل للأخرين. وقد تكون تلك المعرفة فنية أو إدراكية.

المعرفة الصريحة Explicit Knowledge: وتتعلق بكل ما هو موجود ومخزن في مصادر المعلومات التقليدية أو الرقمية، وهذا النوع من المعرفة يمكن الوصول إليه بسهولة واستخدامه ويمكن تقاسمه مع الأخرين.

يميز بولاني بين نوعي المعرفة في إطار اننا نعرف أكثر مما يمكن أن نقول في إشارة إلى أن المعرفة الضمنية هي الأكثر أهمية وهي الأكثر تحدياً في مجالات إدارة المعرفة وتطبيقاتها (بامفلح، 2022).

أمن البيانات Data Security

أمن البيانات Data security: وتعني حماية البيانات من أي قوة مدمرة أو من أي فعل غير مرغوب به من قبل مستخدمين غير مخولين.

أمن المعلومات Information Security

ارتبط مفهوم أمن المعلومات تاريخياً بأمن الاتصالات والذي حددته توصيات أمن انظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة الاميركية بما يلي:

"هو المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات، ولضمان أصالة وصحة هذه الاتصالات".

وتضمنت النشاطات المحددة آنذاك أربعة أجزاء رئيسية لأمن الاتصالات وهي: أمن التشفير Cryptosecurity، أمن النقل Transmission Security، أمن الإشعاع Emission Security، والأمن الفيزيائي Physical Security، كما تضمن تعريف أمن الاتصالات خاصيتين اساسيتين وهما السرية والتحقق من الهوية، كما اضافت في التسعينيات خاصيتي التكامل والتوافر إليهما.

توجد العديد من التعريفات التي تناولت مفهوم أمن المعلومات ومنها:

يعبر عن أمن المعلومات بأنه "الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية".

كما يعـرف بأنه "مجموعة من الإجراءات والتـدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي، للحفاظ على المعلومات والأجهزة والبرمجيات، إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال".

ويعرف ايضاً على أنه "استخدام كافة الاجراءات والوسائل التي تضمن الحماية اللازمة لكافة البرامج والأجهزة المستخدمة في معالجة المعلومات وضمان سلامتها لأنها تمثل المورد والميزة الاساسية التي ينبغي لأي مؤسسة الحفاظ عليها" (الطائي، 2015).

وتعرف لجنة أنظمة الأمن القومي الأميركي (2010) أمن المعلومات بأنها حماية المعلومات وعناصرها بما في ذلك الانظمة والاجهزة التي تستخدم وتخزن وترسل هذه المعلومات، ووفقاً لقانون الولايات المتحدة يعرف بأنه "حماية المعلومات ونظم المعلومات من الوصول لغير المصرح لهم، والاستخدام، الافصاح، التعديل أو احداث الخلل والتدمير".

تناول عدنان مريزق وعمار بوقلاش (2010) تعريفات الأمن المعلوماتي من عدة زوايا، فمن الزاوية الاكاديمية يعرف الأمن المعلوماتي بأنه " ذلك العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها. ومن زاوية تقنية هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن زاوية قانونية فأن أمن المعلومات هو محل دراسات وتدابير لحماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة انشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها.

ويشير (دوادي & بن حود، 2020) إلى أن حماية المعلومات يلزم وضع إطار قوي وشامل لأمن التطبيقات من اجل التحليل والتجسس كما يجب أن يكون هذا الإطار أمن وقادر على سرد وتغطية جميع جوانب الامان، ووضع نظام معلوماتي يشتمل على ثلاث مكونات رئيسية والتي تمثل ما اصطلح على تسميته بمثلث الأمن المعلوماتي، وهي:

- **السرية: Confidentiality** وهي وسيلة للتحكم بالسماح بوصول المستخدمين للمعلومات والتفاعل معها. كما انها تضمن ان يتم السماح فقط بالقيام بذلك للمستخدمين المصرح لهم ومنع غيرهم من القيام بذلك. يمكن تحقيق السرية من مجموعة واسعة من الضوابط الأمنية ومنها: التشفير، التحكم بالوصول، واخفاء المعلومات.
- **الإتاحة أو التوافر: Availability** وهي توفر القدرة على الوصول الى المعلومات أو الموارد لمن له الحق في الدخول عليها فقط في موقع محدد ووفق تنسيق صحيح عندما لا يعمل النظام بشكل منتظم حيث يتم اختراق المعلومات وتوفر البيانات

مما يؤثر على المستخدمين بالإضافة الى الوظائف الأخرى التي تتعلق بالوقت فإذا لم يكن نظام الكمبيوتر قادرا على تقديم المعلومات بكفاءة وبسرعة يتعرض للخطر مرة اخرى، ويمكن ضمان توفر البيانات من خلال التخزين المحلي أو خارج الموقع كالتخزين السحابي.

- **التكاملية وسلامة المحتوى: Integrity & Content Safety** ويقصد به أن يكون المحتوى سليماً ولم يتم العبث به، إي أنه لم يتم تدمير أي جزء من أجزائه في أي مرحلة من مراحله عن طريق الدخول غير المشروع إليه من أي أحد من العابثين الذين يقومون بالدخول إلى محتوى المعلومات لتدميره سواء تدمير كلي أو جزئي.

أمن المعرفة Knowledge Security

تناول Renaud (2019) مصطلح أمن المعرفة في إطار الحفاظ على رأس المال الفكري Intellectual Capital على مستوى المنظمات، ويشير الى ارتباطه بأمن المعلومات من حيث الاجراءات والاساليب الا ان هناك اختلاف جوهري بينهما ويتمثل في كون المعرفة شيء غير ملموس كالمعلومات وأكثر تعقيداً منها مما يجعل الحفاظ عليها وتأمينها امراً صعباً الى حد ما مقارنة بالمعلومات. ويشير Cook إلى أن أبرز التحديات التي تتعلق بأمن المعرفة والمتمثلة في سرقة المعرفة واختلاسها أو فقدان المعرفة. ويعرف Ilvonen أمن المعرفة بأنه تامين رأس المال الفكري IC من خلال عملية الحفاظ على معرفة الأشخاص الذين يعملون في منظمة أمنة، ويشير إلى وجود ارتباط ما بين أمن المعرفة وحوكمة أمن المعلومات.

2. منهجية الدراسة:

اعتمدت هذه الدراسة منهج المراجعة الأدبية المنهجية (Systematic Literature Review) بوصفه الأنسب لدراسة الجوانب الأمنية للحوسبة السحابية؛ إذ يتيح هذا المنهج جمع الأدبيات وتحليلها بصورة منظمة وشفافة، وتم تنفيذ المراجعة عبر خطوات متتابعة تشمل: تحديد كلمات مفتاحية ومترادفاتها بالعربية والإنجليزية، ثم البحث في قواعد البيانات العلمية مثل IEEE Xplore و ACM Digital Library و ScienceDirect (Elsevier) و دار المنظومة ومستودعات الرسائل العلمية، يلي ذلك فحص العناوين والملخصات لاستبعاد غير الملائم، ثم قراءة النصوص الكاملة للدراسات المقبولة واستخلاص البيانات الأساسية وبعد ذلك جرى تحليل الدراسات بشكل وصفي وموضوعي لإبراز الاتجاهات البحثية والفجوات والتوصيات، وتم اعتماد معايير اشتمال تمثلت بأن تكون الدراسة منشورة بين 2021–2024، و أن تكون في مجلة محكّمة أو مؤتمر علمي دولي أو مراجعة علمية أو رسائل جامعية ذي صلة مباشرة بأمن السحابة.

وتم استبعاد المقالات غير المحكمة والمواد التسويقية/المدونات، والدراسات التي تتناول الحوسبة السحابية دون تركيز أمني واضح، وتم اختيار الفترة 2021–2024 كونها تمثل مرحلة حديثة شهدت تسارعًا كبيرًا في تبني السحابة والتحول نحو الحاويات والسحابة المتعددة والحوسبة الآمنة والسرية، وما رافق ذلك من ظهور تهديدات وأطر ومعايير وأدوات حماية حديثة.

3. الإطار النظري:

1.3. الحوسبة السحابية Cloud Computing

في عصر التطور الرقمي الذي يشهده عالم اليوم أصبح استخدام التقنيات الحديثة أحد أهم المقومات الرئيسية لنجاح أو فشل المنظمات، وعلى مستوى تطبيق أفضل الممارسات المرتبطة بالتقنيات، تعتبر الحوسبة السحابية من أفضل النماذج التي تسمح بالوصول الشبكي السهل، وحسب الطلب إلى مجموعة مشتركة من الموارد الحاسوبية القابلة للتكوين مثل الشبكات، الخوادم،

التخزين، التطبيقات، والخدمات البرمجية التي يمكن توفيرها وإطلاقها بشكل سريع بأقل جهد إداري، أو تفاعل بشري مع مقدم الخدمة. وتتألف الحوسبة السحابية من خمس خصائص رئيسية (الخدمة الذاتية حسب الطلب، الوصول الشبكي الواسع، تجميع الموارد، المرونة والسرعة، وقياس الخدمة)، وثلاثة نماذج للخدمة (البرمجيات كخدمة، المنصات كخدمة، والبنية التحتية كخدمة)، وأربعة نماذج للنشر وهي الحوسبة السحابية (العامة، الخاصة، المشتركة، والهجينة).

يعرف الأرشيف القومي الأميركي الحوسبة السحابية "بأنها تقنية تسمح للمستفيدين بالوصول الى واستخدام البيانات المشتركة، وخدمات الحوسبة عبر الإنترنت أو شبكة افتراضية خاصة، فهو يمنح المستفيدين إمكانية الوصول إلى الموارد دون الحاجة إلى أنشاء بنية أساسية لدعم هذه الموارد داخل بيئاتهم أو شبكاتهم الخاصة، وتتضمن التفسيرات العامة للحوسبة السحابية تأجير مساحة التخزين على خوادم هيئة أخرى أو استضافة مجموعة من الخدمات. وتشير التفسيرات الأخرى للحوسبة السحابية الى تطبيقات وسائل التواصل الاجتماعية خاصة والبريد الإلكتروني المستند الى السحابة وأنواع أخرى من تطبيقات الويب". (صابر، 2022).

وتعتمد الحوسبة السحابية على نقل تكنولوجيا المعالجة ومساحة التخزين الخاصة بالحاسوب الى السحابة وهي جهاز خادم يتم الوصول إليه عن طريق الإنترنت وبهذا تتحول برامج تكنولوجيا المعلومات من منتجات الى خدمات. كما تعتمد البنية التحتية للحوسبة السحابية على مراكز البيانات المتطورة والتي تقدم مساحات تخزين كبيرة للمستخدمين. (عالم، 2023).

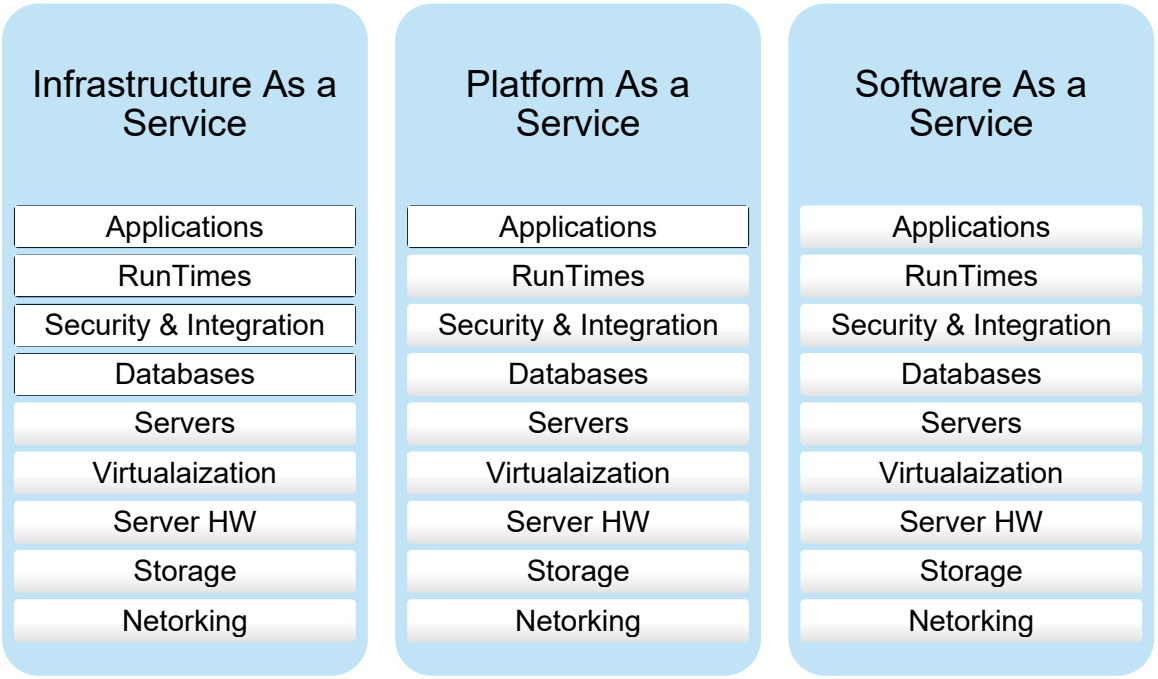
وتعرف أمازون التخزين السحابي بأنه نموذج حوسبة سحابية يتيح تخزين البيانات والملفات على الإنترنت من خلال مُزود الحوسبة السحابية الذي يمكنك الوصول إليه من خلال الإنترنت العام أو اتصال شبكة خاصة مخصصة لذلك. ويتولى المُزود تخزين خوادم التخزين والبنية التحتية والشبكة، وإدارتها والاحتفاظ بها بأمان بهدف ضمان وصولك إلى البيانات عندما تحتاج إليها على نطاق غير محدود تقريبًا وبسعة مرنة. يغنيك التخزين السحابي عن الحاجة إلى شراء البنية التحتية لمخزن بياناتك وإدارتها بنفسك، ما يمنحك المرونة وقابلية التوسع والثبات، ويتيح لك أيضًا الوصول إلى البيانات في أي وقت ومن أي مكان. (أمازون، 2024).

يمكن تقسيم أنواع الحوسبة السحابية الى ثلاث أنواع، حيث يعتمد هذا التقسيم على الاختلافات الجوهرية في النشر الذي يتلاءم مع احتياجات المنظمة، كالتالي: (العزاني، 2022)

1. **السحابة العامة: Public Cloud** هي أحد أنواع الحوسبة السحابية، وكما يشير اسمها فهي متاحة لعامة الناس، حيث يمتلك مزود الخدمة موارد الحوسبة السحابية ويجعل هذه الموارد متاحة للمستخدمين ويمكن لاي متصل بالأنترنت الوصول الى التطبيقات المتاحة واستخدامها.
2. **السحابة الخاصة: Private Cloud** يتم انشاؤها خصيصاً لمنظمات أو مجموعة من المستخدمين في مجال محدد، بحيث تقتصر في تقديم خدماتها على المشتركين فقط مثل تطبيقات التعلم الإلكتروني المملوكة للجامعات.
3. **السحابة المختلطة: Hybrid Cloud** في هذا النوع يتم الجمع بين نوعي السحابة العامة والخاصة معاً في تخصصات أو مجالات متنوعة، وبالتالي تتيح خدماتها وتطبيقاتها السحابية للجميع باستثناء بعض الأصول المهمة والاستراتيجية.

وفقاً لما قدمه المعهد القومي للمعايير والتكنولوجيا (NITS) من تصنيف لخدمات الحوسبة السحابية حيث صنفها الى ثلاثة أنواع مختلفة من نماذج الخدمات الأساسية المقدمة، كما في الشكل التالي:

شكل رقم (1) نماذج خدمات الحوسبة السحابية (IaaS – PaaS – SaaS) ومكوّناتها



المصدر: من إعداد الباحث اعتماداً على IBM Cloud, Cloud service models

يتضح من الشكل السابق وجود ثلاث تصنيفات لأنواع الخدمات التي يمكن تقديمها من خلال الحوسبة السحابية، وهي كما يلي:

1. **البنية التحتية كخدمة Infrastructure as a Service (IaaS):** وتعبر عن الأساس الذي تقوم عليه الحوسبة السحابية، وفي كثير من الأحيان يطلق عليها مسمى الأجهزة الذكية كخدمة (Haas Hardware As a Service)، وذلك لما تتضمنه تلك الخدمة من خدمات التخزين، الشبكات، الخوادم، أجهزة المستخدمين، وقواعد البيانات، والتي يتم الحصول عليها وقت الحاجة الى امتلاك وتحمل تكاليف تلك الخدمات، أو توافر الخبرات الخاصة بكيفية عملها، أو التحكم فيها، أو صيانتها وتحديثها.
2. **المنصة كخدمة Platform as a Service (PaaS):** يطلق عليها المستوى الثاني أو الطبقة الوسطى من الحوسبة السحابية ككل، وغالباً ما يتم الاعتماد على تقنية المنصة كخدمة من جانب المبرمجين والمطورين، ويتم تقديم كافة الإمكانيات لهم لاختبار، نشر، تطوير، وإدارة التطبيقات البرمجية الخاصة بهم، وتعتبر الصلاحية الكاملة والتحكم الكامل خاص بالمطورين من خلال التحكم الكامل في استخدام الواجهة البرمجية لتلك التطبيقات، ومن أمثلة المنصة كخدمة للحوسبة السحابية تطبيقات مايكروسوفت وتطبيقات جوجل.
3. **البرمجيات كخدمة Software as a Service (SaaS):** تعتبر البرمجيات كخدمة اعلى مستويات الحوسبة السحابية، ويتمثل ذلك في مدى قدرتها على الاستخدام الأمثل للخدمات المتاحة، كما يمكن الوصول إليها من خلال الأجهزة المختلفة للمستخدمين سواء حاسب شخصي، جهاز لوحي، أو أجهزة الاتصال المحمولة والذكية، ويمكن الاعتماد على أي متصفح للإنترنت وحسب احتياجات وإمكانيات المستخدم وبشكل متكافئ لجميع المستخدمين.

كما توفر تقنية البرمجيات كخدمة خدمات التطبيقات والبيانات وجميع المتطلبات الأساسية اللازمة من قبل مزودي الخدمة السحابية، وتعتبر البرمجيات كخدمة من أوائل نماذج خدمات الحوسبة السحابية ولا تزال هي النموذج الأكثر انتشاراً ومن الأمثلة عليها برامج البريد الإلكتروني، العملاء، واللوجستيات. (عمار، 2020).

2.3. أمن الحوسبة السحابية Cloud Computing Security

يشير أمن الحوسبة السحابية إلى مجموعة واسعة من السياسات والتقنيات والضوابط الخاصة بحماية البيانات، التطبيقات، والبنية التحتية، وذلك نظراً لتشجيع استخدام الحوسبة السحابية المكثف للبرمجيات والتطبيقات المختلفة التي تعمل في كل مكان وزمان والقائمة على تقنية شبكة الانترنت، تخزين البيانات، وإيصال الخدمات من قبل طرف خارجي يقوم باستضافة البيانات المهمة أو تنفيذ العمليات الحرجة في اماكن غير معلومة، بالإضافة الى سعة حجم السحابة، تنوعها، وتشتتها الجغرافي الذي يؤدي الى تعريض البيانات للعديد من المخاطر الأمنية.

مخاطر الحوسبة السحابية:

تعرف منظمة المعايير الدولية ISO المخاطر بأنها "عبارة عن أحداث مستقبلية غير مؤكدة يمكن أن تؤثر في عملية تحقيق الأهداف الاستراتيجية، التشغيلية، والمالية. وتعرف بأنها " احتمال وقوع حدث، خسارة، ضرر، أو عواقب وخيمة أو تأثير في عدم اليقين المصاحب لبيئة الأعمال على تحقيق أهدافها وهذا التأثير إما أن يكون ايجابياً أو سلبياً. فالتأثير الإيجابي يمكن أن يحول المخاطر الى فرصة يمكن استغلالها، بينما التأثير السلبي قد يحول المخاطر الى تهديد ربما يتسبب في عملية إعاقة تحقيق الأهداف.

وتعرف مخاطر الحوسبة السحابية بأنها " مخاطر تكنولوجيا أمن المعلومات الخارجية والداخلية الناجمة في معظم الحالات عن اختيار أسلوب السحابة غير المناسب، الوصول غير المصرح به للسحابة، فشل نقل المعلومات، فقدان سلامة البيانات المخزنة على السحابة، معاملات غير كاملة لم ترحل للسحابة، فشل أو مشكلات في السحابة، ونظم السحابة الإلكترونية غير المتوافقة.

يمكن تصنيف مخاطر الحوسبة السحابية الى الأنواع التالية: (سلطان، 2023)

- مخاطر تقديم الخدمة: ويضم كلاً من تقييم المخاطر الافتراضية، تقييم مخاطر SaaS، تقييم مخاطر PaaS، وتقييم مخاطر LaaS.
- مخاطر النشر: وتضم كلاً من فهم مخاطر السحابة العامة، فهم مخاطر السحابة الخاصة، وفهم مخاطر السحابة الهجينة.
- مخاطر نموذج الأعمال: ويتألف من تقييم المخاطر السحابية للزبون، تقييم المخاطر السحابية لمزود الخدمة.
- مخاطر حوكمة الشركات وحوكمة تقنية المعلومات.
- مخاطر الأمن والخصوصية: وتشتمل على القيام بإجراء تحليل لمخاطر الخصوصية أو مخاطر أمن المعلومات.
- مخاطر أخرى: وهي عبارة عن مخاطر مختلفة ربما لا يمكن حصرها ويندرج ضمن هذا النوع من المخاطر مخاطر تكنولوجيا المعلومات، مخاطر الالتزام، مخاطر استمرارية الخدمة، ومخاطر خصوصية الهيكل التنظيمي.

4. مراجعة الدراسات السابقة:

بالرجوع إلى الإنتاج الفكري باللغة العربية والإنجليزية حول موضوع الجوانب الأمنية للحوسبة السحابية، تبين للباحث أن هناك العديد من الدراسات العلمية المحكمة تناولت هذا الموضوع بعناوين مختلفة إلا أن جميعها تؤكد على التهديدات، المخاطر، والثغرات الأمنية التي ينبغي التنبه لها عند استخدام تقنيات وخدمات الحوسبة السحابية.

وتجدر الاشارة إلى منصات الحوسبة السحابية التجارية مثل أبل، قوقل، أمازون، وغيرها من المنصات قدمت العديد من التوصيات حول هذا الموضوع في صيغة تحديثات أمنية لمستخدمي منصاتها. في السطور التالية سيتم التركيز على عشرة دراسات علمية قام الباحث باختيارها بعناية مراعياً الجدة، الاصالة، وقوة التوصيات والمقترحات التي خرجت بها تلك الدراسات، وفيما يلي سيتم استعراض هذه الدراسات ومراجعة أبرز توصياتها ومقترحاتها.

1.4. الدراسات باللغة العربية

1- دراسة سلوى إسماعيل (2024) حول "**أثر تطبيق الحوسبة السحابية على أمن وسرية المعلومات في البنوك: دراسة ميدانية**". هدفت هذه الدراسة إلى تحليل وتقييم أثر تطبيق الحوسبة السحابية على أمن وسرية المعلومات للبنوك المسجلة لدى البنك المركزي المصري. واعتمدت الباحثة على المنهج الوصفي التحليلي مستخدمة أداة الاستبانة حيث وزعت على عينة الدراسة وعددها (265) مفردة، والمكونة من مدراء الفروع، المدراء التنفيذين، ورؤساء الأقسام، والعاملين في قطاع البنوك. اثبتت نتائج الدراسة ان استخدام الحوسبة السحابية يؤدي الى تحسين امان المعلومات المصرفية من خلال توفير حماية أفضل للبيانات والمراقبة الأمنية المتقدمة، وادارة الوصول المحكم وتعزيز سرية المعلومات المصرفية من خلال تطبيق تقنيات التشفير.

وأوصت الدراسة بضرورة ان يكون مزود الخدمة السحابية موثوق به ومعروف بتوفير مستويات عالية من الأمان والأداء، بالإضافة إلى التحقق من توافر نسخ احتياطية وآليات الاستعادة في حالات الطوارئ. وضرورة استخدام تقنيات التشفير الموثوقة لحماية وسرية البيانات المخزنة والمرسلة عبر السحابة وتوفير آليات لإدارة وتأمين مفاتيح التشفير.

2- دراسة وئام سالم (2023) حول "**أثر الحوسبة السحابية المخاطر التشغيلية في البنوك التجارية في الأردن**". هدفت الدراسة إلى قياس أثر الحوسبة السحابية بأبعادها: البنية التحتية، المنصة الالكترونية، والبرمجيات مجتمعة ومنفردة في المخاطر التشغيلية في البنوك التجارية في الأردن. وذلك باتباع المنهج الوصفي التحليلي. تم جمع البيانات الاولية من خلال استبانة وزعت على الإدارات العليا والوسطى في البنوك التجارية الأردنية، والبالغ عددها 144 فرداً. وتم استخدام أساليب الإحصاء الوصفي الاستدلالي في تحليل بيانات الدراسة واختبار فرضياتها. وتوصلت الدراسة الى وجود أثر ذو دلالة احصائية للحوسبة السحابية بأبعادها مجتمعة ومنفردة في المخاطر التشغيلية في البنوك التجارية الأردنية. أوصت الدراسة باعتماد البنوك التجارية على حوسبة سحابية تتلاءم مع أهدافها الاستراتيجية وحوكمة تكنولوجيا المعلومات، وإعداد الخطط والبدائل المناسبة للحد من المخاطر التشغيلية التي قد تواجهها البنوك والتخفيف من حدة تأثيراتها السلبية.

3- دراسة يحيى الفيفي (2022) حول "**واقع تقنية الحوسبة السحابية لدى شركات الاتصالات في المملكة العربية السعودية (التوجهات والخطط المستقبلية)**"، حيث هدفت الدراسة إلى التعرف على واقع تقنية الحوسبة السحابية لدى شركات الاتصالات السعودية بمدينة الرياض، بالإضافة الى معرفة أهم التوجهات والخطط المستقبلية لها. ولتحقيق أهداف الدراسة اتبع الباحث المنهج الوصفي المسحي، وقدم استبانة وزعت على عينة عشوائية بلغ عددها 250 شخصاً من متخذي قرار تبني هذه التقنية من الذكور والإناث في شركات الاتصالات السعودية، وهم مدراء الادارات، ورؤساء الاقسام، والموظفون التقنيون. وتوصلت الدراسة الى عدد من النتائج أهمها أن أفراد الدراسة يوافقون وبشدة على أن واقع استخدام الحوسبة السحابية لدى شركات الاتصالات السعودية، ويتضح ذلك كون هذه التقنية خياراً تقنياً واقتصادياً مهماً لها، بالإضافة إلى أن أحد أهم أولوياتها هو الحفاظ على أمن وخصوصية البيانات وأن من التوجهات والخطط المستقبلية وضع خطة وطنية للبنية الأساسية للاتصالات اللاسلكية عريضة النطاق والاستثمار في البنية التحتية لتقنية المعلومات.

4- دراسة إسلام ابراهيم (2022) بعنوان **"مفهوم الحوسبة السحابية وخدمة التعافي من الكوارث"**. تهدف هذه الدراسة الى التعرف على الحوسبة السحابية من حيث مفهومها بالنسبة لتخصص الوثائق والأرشيف ونماذجها وطبقاتها بالإضافة إلى تناول تصنيفات الكوارث التي تصيب الوثائق الإلكترونية المخزنة بالسحابة مع طرح مواصفات خطة التعافي من الكوارث التي يجب توافرها ووصولاً إلى خدمة التعافي من الكوارث بالحوسبة السحابية، وتوصي الدراسة بضرورة تواصل اختصاصي الوثائق والأرشيف مع متخصصي تكنولوجيا المعلومات وغيرهم من المهنيين وإنشاء شراكات جديدة من ثم تطوير أدوار ومهام جديدة للاختصاصيين والمتخصصين. كما يجب ان تكون هناك مسؤولية مشتركة ومواجهة التحديات التي قد تواجه حفظ الوثائق والسجلات، بالإضافة للمساءلة الناشئة عن تقنيات المعلومات والاتصالات.

5- دراسة محمود رحال وآخرون (2021)، الموسومة بـ **"نموذج هجين أمن لحماية البيانات في الحوسبة السحابية بدمج AES، RSA، وCP-ABE"**. تقترح هذه الدراسة نموذجاً متكاملاً لنظام الرعاية الصحية في الحوسبة السحابية يحقق أمن وسرية البيانات المنقولة عبر الحوسبة السحابية، من خلال دمج خوارزميتي AES وRSA مع خوارزمية التحكم في الوصول CP-ABE بغرض الاستفادة من مزايا كل منها، بحيث تتم عملية التشفير عن طريق خوارزمية مقترحة تعتمد على خوارزمية RSA والمعامل XOR وخوارزمية AES. يتميز النموذج المقترح بتلبية متطلبات التحكم بالوصول، التوثيق، والتحقق لكل من المرسل والمستقبل من خلال زيادة سرية خوارزمية AES عبر توليد مفتاح ديناميكي وتأمين سرية هذا المفتاح بمستويين للتشفير، الأول باستخدام خوارزمية CP-ABE والمستوى الثاني باستخدام خوارزمية RSA، واظهرت النتائج تفوق هذا النظام الهجين من ناحية تحقيق متطلبات الأمن في الحوسبة السحابية. حيث يعتمد النموذج الهجين على دمج خوارزميات AES، RSA، و-CP ABE كما تقدم بهدف الاستفادة من مزايا كل منها.

وتشير الدراسة الى مزايا التوثيق والتحقق التي تحققها خوارزمية RSA غير المتناظرة، بالإضافة الى ميزة ادارة المفاتيح من خلال استخدامها في تشفير المفتاح السري لخوارزمية AES المتناظرة، وكذلك مزايا سرعة التشفير وفك التشفير لخوارزمية AES. كما تساعد مزايا التحكم في الوصول لخوارزمية CP-ABE غير المتناظرة، وذلك من خلال الاستفادة من مزاياها الهامة فيما يتعلق بتقييد الوصول للبيانات.

2.4. الدراسات باللغة الانجليزية

6- دراسة لـ Uma Maheswari وآخرون (2023) والمعنونة بـ **"خصوصية البيانات وامانها في بيئات الحوسبة السحابية "** قدمت الدراسة مراجعة شاملة للقضايا والحلول والتطورات المستقبلية المتعلقة بخصوصية البيانات وامانها في الحوسبة السحابية، وتؤكد الدراسة على صعوبة الحفاظ على خصوصية البيانات وامانها اثناء معالجة وتخزين هذه البيانات في مراكز البيانات الخارجية والمتمثلة في بيئة الحوسبة السحابية. ناقشت الدراسة المخاطر، التهديدات، انتهاكات البيانات، والوصول غير المشروع الى المعلومات الحساسة، كما دعت الى تعمق أكثر في المعايير القانونية والامتثال التي يجب على المنظمات اتباعها لحماية بيانات مستخدميها في السحابة. تقترح الدراسة منهجية شاملة لتعزيز خصوصية البيانات وامانها في بيئات الحوسبة السحابية، بهدف حماية المعلومات الحساسة من الوصول غير المصرح به وانتهاكات البيانات وغيرها من الانشطة الخبيثة، ومن هذه الحلول تشفير البيانات Data Encryption من خلال تعزيز البيانات بشكل كبير من خلال التشفير. تستخدم المنهجية طرق تشفير قوية مثل تشفير المفتاح المتماثل والمفتاح الرئيسي، لتشفير البيانات أثناء تخزينها، نقلها، ومعالجتها.

وتساهم اداة تشفير البيانات في ضمان عدم الاطلاع على البيانات من قبل غير المصرح لهم في الوصول اليها، وإذا ما تم الوصول اليها فإنها ستظل غير مفهومة وغير قابلة للاستخدام دون مفاتيح فك التشفير والمطابقة، وكذلك ضوابط الوصول Access Controls: يعد التحكم في الوصول الى البيانات جانباً مهماً واساسياً من جوانب خصوصية البيانات وامانها. توصل النظام المقترح إلى آليات تحكم الوصول الدقيق لتقييد المستخدمين غير المصرح لهم من الوصول الى البيانات الحساسة المخزنة في السحابة، ويستخدم لذلك نماذج التحكم في الوصول القائم على السمات (ABAC)، والنماذج المعتمدة على الدور (RBAC)، وتدقيق البيانات Data Auditing: تساعد عملية تدقيق البيانات في الحفاظ على المساءلة وضمان سلامة البيانات، وتتيح إمكانيات التدقيق القوية للبيانات من خلال تنفيذ إطار تسجيل شامل يسجل ويراقب جميع انشطة المستخدمين، بما في ذلك اذونات الوصول الى البيانات، التعديلات، واحداث النظام المختلفة بحيث تخزن في سجلات بشكل أمن تمكن مدير النظام من الرجوع اليها وتحليها والتحقيق في الانشطة غير المصرح بها، ونقل البيانات الأمن Secure Data Transfer: يتطلب نقل البيانات حماية أكثر لتجنب السرقة أو التعديل غير المصرح به في تلك البيانات، ويقدم النموذج نظام اتصالات مشفر بين المستخدمين وخوادم السحابة باستخدام بروتوكولات اتصال آمنة مثل أمان طبقة النقل (TLS) تضمن عدم التلاعب في البيانات المنقولة بين أجهزة المستخدمين والسحابة.

7- دراسة Swetha Gadde وآخرون (2023)، حول **"مشاركة البيانات الأمنة في الحوسبة السحابية: مسح شامل لحلول المصادقة الثنائية والتشفير"**، طرحت الدراسة مراجعة تحليلية للمصادقة الثنائية وتدابير التشفير داعية الى تنفيذها بشكل مشترك لتعزيز أطر الأمان في أنظمة السحابة. كما قامت الدراسة بمراجعة دقيقة للإنتاج الفكري حول الموضوع والثغرات الأمنية المتعلقة بالحوسبة السحابية وآليات الأمان والتحديات الأساسية التي يفترض أن تأخذ بعين الاعتبار فيما يتعلق بعمليات التحسين والتطوير والابتكار لمواجهة الاخطار والتهديدات المتعلقة بأمن وحماية البيانات في البيئات الرقمية ومنها الحوسبة السحابية. حددت الدراسة الفجوة المعرفية في نقص المراجعات المنهجية التي تفصل بين البحث المتطور والمعاصر المرتبط بعمليات نقل البيانات، وتوصي بإنشاء قنوات تواصل تعاونية ما بين المجال الأكاديمي وأصحاب المصلحة لمزودي منصات الحوسبة السحابية.

8- دراسة أسماء البكري (2023) بعنوان **"سرية تخزين البيانات السحابية باستخدام التشفير الخفي والمرئي"**. هدفت هذه الدراسة إلى مراجعة عدة تقنيات للتشفير الخفي والتشفير المرئي التي تم اقتراحها لتحسين أمان السحابة وجعلها أكثر اماناً ضد الهجمات الالكترونية والتنصت، بغرض التحقق من قدرات البيانات المؤمنة والتي يتم استخدامها بشكل متكرر من قبل الباحثين، بالإضافة الى التحقق من مزايا وعيوب كل مجال من مجالات البيانات المؤمنة من اجل تعزيز اليات الامان من خلال دمج هذين الاسلوبين معاً في الحوسبة السحابية. استنتجت الدراسة أن أساليب التشفير المرئي يمكن دمجها مع التشفير الخفي والحوسبة السحابية لتأمين البيانات، حيث أن التشفير المرئي والخفي يعتبران من أهم تقنيات التشفير التي تحقق اتصال ونقل أمن للبيانات، وتوصي الدراسة بضرورة دمج هذين الفرعين المختلفين ليصبح من الصعب على المهاجم التلاعب بسرية البيانات.

9- دراسة Sijad Ali وآخرون (2024) بعنوان **"تعزيز الأمن السحابي: الكشف عن الإمكانيات الوقائية لمشاركة الاسرار المتماثلة في الحوسبة السحابية الأمنة"**. تؤكد الدراسة على ان امان الحوسبة السحابية وحماية البيانات أصبح من الامور الحاسمة وبشكل متزايد في الآونة الاخيرة، حيث تظهر الأبحاث مؤخراً كيف يمكن دمج تقنيات المشاركة السرية والتشفير المتجانس لحماية المعلومات الخاصة ضمن سيناريوهات الحوسبة السحابية. تقدم الدراسة استراتيجية خاصة لحماية البيانات وذلك من خلال تقسيمها الى عدة خوادم، ومن خلال هذا التوزيع ترى أنه من غير المرجح أن تتعرض تلك البيانات أو النظام لنقاط فشل فردية

وبالتالي يكون له مستوى أعلى من الأمان. لضمان خصوصية المعلومات وبياناتها يقيد تشفير البيانات من إمكانيات الوصول لغير المصرح لهم، وكميزة إضافية يستخدم التشفير المتجانس لتمكين عمليات البيانات المشفرة دون الوصول المباشر الى النسخ الاصلية. توصلت الدراسة إلى أن هذه الاستراتيجية تحقق التوازن الفعال ما بين الامان وكفاءة العمليات وذلك من خلال حماية البيانات الحساسة التي يتطلب الكشف عنها مع ضمان عدم سوء الاستخدام اثناء المعالجة، بالإضافة الى الحفاظ على سرية البيانات الاصلية عند المشاركة المشفرة.

10- دراسة Ankush Pawar وآخرون (2023). حول **"دراسة وتحليل مختلف نماذج الأمان السحابي والمصادقة وتخزين البيانات: نظرة في التحديات"**. قدمت الدراسة مراجعة تفصيلية لخمسين ورقة بحثية تقدم اساليب الحفاظ على الخصوصية وهي الأساليب المعتمدة على المصادقة، امان الحوسبة السحابية، تخزين البيانات، أمن البيانات، والتشفير. الهدف الرئيسي لهذه الدراسة هو مناقشة بعض الموضوعات البحثية المرتبطة بأمن السحابة وبالتالي مساعدة المطورين والباحثين على فهم مزايا مجال الحوسبة السحابية بشكل أفضل والمساهمة في تطويره. تم ترتيب ورقة الاستطلاع لهذه الدراسة كما يلي:

1.4. التعقيب على الدراسات السابقة:

تعكس الدراسات السابقة تنوّعًا واضحًا في مقاربة الجوانب الأمنية للحوسبة السحابية بين المنظور التطبيقي المؤسسي (البنوك والاتصالات والوثائق) والمنظور التقني الخوارزمي. فدراسة سلوى إسماعيل (2024) تقدّم دليلًا ميدانيًا على أن تبنّي السحابة قد يرتبط بتحسين السرية والأمن عبر التشفير والرقابة وإحكام إدارة الوصول، لكنها في جوهرها تُبرز أن النتيجة الأمنية ليست تلقائية بل مشروطة بموثوقية المزوّد ونضج النسخ الاحتياطي وإدارة مفاتيح التشفير. وبالمثل، تنتقل دراسة وئام سالم (2023) من أمن المعلومات إلى المخاطر التشغيلية وتؤكد أثر نماذج الخدمة (IaaS/PaaS/SaaS) في المخاطر، ما يدعم رؤية أن الأمن السحابي جزء من حوكمة تقنية المعلومات وإدارة المخاطر أكثر من كونه قرارًا تقنيًا فقط. أما دراسة يحيى الفيفي (2022) فتضيف بعدًا استراتيجيًا من حيث الجاهزية والتوجهات والخطط الوطنية وتؤكد أن الأمن والخصوصية يشكلان أولوية عند صانعي القرار، لكنها تظل أقرب لوصف الواقع من قياس فعالية ضوابط أمنية بعينها. وفي سياق مختلف، تركّز دراسة إسلام إبراهيم (2022) على التعافي من الكوارث في مجال الوثائق والأرشيف وتُحسن الربط بين الحفظ الرقمي والمسؤولية المشتركة والتكامل المهني مع مختصي تقنية المعلومات؛ وهي نقطة مهمة لأن كثيرًا من إخفاقات الأمن السحابي تنشأ من فجوة الأدوار والإجراءات لا من التقنية وحدها.

ترسم الدراسات السابقة العربية خريطة متكاملة في الجوانب الأمنية ي الحوسبة السحابية تبدأ بختيار المزوّد، والخطط البديلة، والاستعادة، والامتثال، إلى مستوى التشغيل من حيث إدارة الوصول والمراقبة، ومستوى التقنية كالتشفير والتحكم بالوصول. ومع ذلك، يظهر تفاوت منهجي فالدراسات الميدانية تعتمد أساسًا على الاستبانة وتلتقط الإدراك ودرجة التبنّي أكثر من قياس مؤشرات أمنية موضوعية كحوادث فعلية، أو اختبارات اختراق، بينما الدراسة التقنية (محمود رحال وآخرون، 2021) تقدّم مساهمة أكثر تجريبية عبر نموذج تشفير هجين (RSA/AES/CP-ABE) يعالج السرية والتحكم بالوصول وإدارة المفاتيح—لكنها غالبًا تُختبر في بيئة محدودة ولا تناقش بما يكفي تحديات النشر الواقعي مثل الأداء تحت أحمال كبيرة، التكلفة، إدارة الهوية في السحابة، وأمن واجهات البرمجة وسلاسل التوريد البرمجية. ونجد فجوات بحثية في الدراسات السابقة تتمثل بالحاجة لدمج قياسات أمنية موضوعية مع المسوح الميدانية بدل الاكتفاء بالرأي، وربط نماذج التشفير المقترحة بمتطلبات تشغيلية سحابية حديثة، ودراسة الأمن السحابي من منظور المسؤولية المشتركة والحوكمة والامتثال كإطار مُفسِّر للنتائج.

بينما انتقلت الدراسات الأجنبية من الطرح المؤسسي العام إلى تركيز أكثر عمقًا على آليات الحماية التقنية ودورة الحياة السحابية لسلسلة حماية البيانات من تخزين البيانات إلى نقلها إلى معالجة البيانات وتدقيقها والتحكم والوصول إلى البيانات، فمراجعة Uma Maheswari وآخرون (2023) ركزت على تحدي فقدان السيطرة على البيانات داخل مراكز بيانات خارجية، مما يستلزم امتثال قانوني أعلى، وركزت دراسة أسماء البكري (2023) زاوية متخصصة أقل شيوعًا في المراجعات العامة عبر دمج التشفير الخفي والتشفير المرئي لتحسين سرية التخزين والنقل.

من خلال ما سبق نجد الحاجة لمقارنات معيارية تُظهر قابلية التطبيق والأثر العملي، وتعزيز طبقات الأمن التقنية والحوكمة السحابية ونموذج المسؤولية المشتركة والامتثال. وكذلك مواكبة التوجهات البحثية الحديثة في الجوانب الأمنية للحوسبة السحابية مثل البنى الوقائية عبر تقنيات مشاركة الأسرار مع التشفير كالتشفير المتجانس لتقليل نقطة الفشل الواحدة.

5. الخاتمة:

وفقاً لما تم عرضه والتطرق اليه في هذه الورقة ابتداءً بمشكلة البحث التي تتمحور حول مراجعة أحدث أدبيات موضوع الجوانب الأمنية المتعلقة بتقنيات وخدمات الحوسبة السحابية، واهمية الموضوع والتي تنحصر في معرفة التهديدات والثغرات الأمنية للحوسبة السحابية وطرق وأساليب الحماية والحد من تلك المخاطر، بالإضافة الى أهداف هذه الدراسة والتي تتعلق بالتعريف بمفهوم أمن كلاً من البيانات، المعلومات، والمعرفة، بالإضافة الى التعريف بمفهوم تقنيات وخدمات الحوسبة السحابية وأبرز مجالات البحث حولها. واخيراً استعراض أهم الدراسات العلمية المحكمة والمنشورة حول هذا الموضوع.

1.5. ملخص نتائج البحث:

على ضوء ما سبق استنتج الباحث ما يلي:

- يعد أمر الاستجابة للحوادث والتعافي منها من أهم الجوانب الأمنية للحوسبة السحابية، حيث تمثل الاستجابة للحوادث في الوقت المناسب أهم المكونات الاساسية في مجال أمن الحوسبة السحابية.
- ترتبط معظم مخاطر أمن الحوسبة السحابية بأمن البيانات السحابية، سواء من حيث نقص الرؤية للبيانات، عدم القدرة على التحكم في البيانات، أو تعرضها للسرقة أو الفقد في السحابة.
- معظم المشكلات التي تتعلق بأمن الحوسبة السحابية ترجع أسبابها الى نقص الوعي من قبل المستخدمين في التعامل بحذر مع البيانات التي يتم تداولها في السحابة.
- يشتمل أمن الحوسبة السحابية على ركائز اساسية وهي الرؤية والامتثال، الأمان القائم على الحوسبة وحماية الشبكة، إدارة الهوية، والوصول.
- يعتبر قطاع البنوك والمنظمات المالية الاكثر اهتماماً بمجال أمن المعلومات والمعرفة في بيئة الحوسبة السحابية.

2.5. التوصيات والمقترحات:

استنادًا إلى ما عُرض في المراجعة الأدبية حول الجوانب الأمنية للحوسبة السحابية، يقدم الباحث مجموعة من التوصيات أهمها:

- اعتماد منهجية تقييم مخاطر سحابية قبل التبنّي، وتبني سياسات واستراتيجيات للاستجابة السريعة للحوادث ومعالجتها.
- اختيار مزودي خدمات سحابية وفق معايير موثوقة وقابلة للتحقق مع التركيز على الشفافية والامتثال والسجل الأمني لمزود الخدمة، وشهادات الامتثال واتفاقيات مستوى خدمة واضحة.

- تعزيز وتوحيد سياسات الوصول وإدارة الهوية واعتماد المصادقة متعددة العوامل خصوصا للحسابات الإدارية.
- بناء منظومة تدقيق ومراقبة مركزية وتبني سياسات احتفاظ بالسجلات وتحليل مستمر للكشف المبكر.
- رفع الوعي الأمني بشكل مستمر وتدريب الكوادر والمستخدمين حيث أن المخاطر الأمنية السحابية والاختراق مرتبط بالأخطاء البشرية والإجراءات وقلة الوعي.

6. المراجع والمصادر:

1.6. المراجع العربية:

إبراهيم، إسلام. (2022). مفهوم الحوسبة السحابية وخدمة التعافي من الكوارث. المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات. تم الاسترداد من https://search-ebscohost-com.sdl.idm.oclc.org/login.aspx?direct=true&db=awr&AN=161665835&site=eds-live

السريحي، حسن. (2019). مقدمة في علم المعلومات: رؤية حديثة. جدة: مكتبة الشقري للتوزيع والنشر.

العزاني، محمد عبد العزيز. (2022). الحوسبة السحابية وأثرها في التعليم الالكتروني. جامعة عدن-كلية الاقتصاد والعلوم الادارية.

الطائي، محمد؛ الكيلاني، وينال. (2015). إدارة أمن المعلومات. عمان: دار الثقافة للنشر والتوزيع.

الفيفي، يحيى. (2022). واقع تقنية الحوسبة السحابية لدى شركات الاتصالات في المملكة العربية السعودية: "التوجهات والخطط المستقبلية": دراسة وصفية. مجلة العلوم الهندسية وتكنولوجيا المعلومات.

الهيئة السعودية للبيانات والذكاء الاصطناعي;. (2024). الحوسبة السحابية: تجارب عالمية .

أمازون. (2023). ما المقصود بالتخزين السحابي؟

بامفلح، فاتن. (2022). استرجاع المعرفة في ظل التطبيقات الذكية. القاهرة: الدار المصرية اللبنانية.

حسين، أمل. (2023). أثر التكامل بين سلاسل الكتل والحوسبة السحابية على جودة التقارير المالية الرقمية: مدخل مقترح. مجلة الإسكندرية للبحوث المحاسبية.

حسين، سلوى رشدي. (2024). أثر تطبيق الحوسبة السحابية على أمن وسرية المعلومات في البنوك: دراسة ميدانية. مجلة التجارة والتمويل.

دوادي، دلندة، & بن حود، زهرة. (2020). أمن المعلومات المصرفية (رسالة ماستر، جامعة قاصدي مرباح – ورقلة، كلية الحقوق والعلوم السياسية، الجزائر).

راشد، عبد النبي داود؛ العليمات، ابراهيم محمد؛ أبو سليم، خليل سليمان. (2021). أثر نظام تخطيط موارد المؤسسة ERP في تدقيق مخاطر الحوسبة السحابية في الشركات الأردنية المساهمة العامة. المجلة الدولية أبحاث في العلوم التربوية والإنسانية والآداب واللغات.

سالم، وئام. (2023). أثر الحوسبة السحابية المخاطر التشغيلية في البنوك التجارية في الأردن. مجلة جدارا للبحوث والدراسات. تم الاسترداد من https://search-ebscohost-com.sdl.idm.oclc.org/login.aspx?direct=true&db=awr&AN=177450611&site=eds-live

سلطان، تيسير جواد. (2023). أثر فاعلية التدقيق الداخلي في ادارة مخاطر الحوسبة السحابية. مجلة الغري للعلوم الادارية والاقتصادية.

صابر، اسلام. (2022). مفهوم الحوسبة السحابية والتعافي من الكوارث. المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات.

صابر، اسلام. (بلا تاريخ). مفهوم الحوسبة السحابية وخدمة التعافي من الكوارث .

عالم، ناهد محمد;. (2023). الحوسبة السحابية واستخداماتها في أرشيف العصر الرقمي. مجلة كلية الآداب: جامعة بني سويف.

عمار، اسماعيل;. (2021). دور تقنية الحوسبة السحابية في تحسين جودة الخدمة التعليمية: دراسة تطبيقية على مؤسسات التعليم العالي. المجلة العلمية للدراسات والبحوث المالية والتجارية.

مريزق، عدمان، & بوقلاشي، عماد. (2010). الأمن المعلوماتي في ظل التجارة الإلكترونية: إشارة إلى حالتي تونس والجزائر. مجلة الاقتصاد الجديد، 1(2)، 7–25.

مهروسة، زكريا؛ رحال، محمود; الزين، نيروز. (2021). نموذج هجين أمن لحماية البيانات في الحوسبة السحابية بدمجRSA ، AES، و .ABE-Cمجلة العلوم الهندسية وتكنولوجيا المعلومات.

موسى، نبيل عزت. (2011). اساسيات نظم المعلومات في التنظيمات الإدارية. جدة: مكتبة الملك فهد الوطنية.

2.6. المراجع الأجنبية:

Albakri, Asmaa; Karan, Oguz. (2023). Cloud Data Storage Confidentiality Using Steganography and Visual Cryptograph: A Review. Jornal of Education and Science (EDUSJ).

Ali, Sijjad; Wadho, Shuaib; Yichiet, Aun; Lee Gan, Ming; Kang Lee, Chen. (2024). Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing. www.sciencedirect.com.

Alnaamneh, Qais Aymen. (2022). Enhanced Certain Trusted Model and Secured for Cloud Market Infrastructure. Alzarqaa: Alhasheimiah Univercity.

Balaram, Ankush; Ghumber, Shashikant; Jogdand, Rashmi. (2023). Study and Analysis of Various Cloud Security, Authentication, and Data Storage Models: A Challenging Overview. International Journal of Decision Support System Technology (IJD).

Committee on National Security Systems. (2010). National information assurance (IA) glossary (CNSS Instruction No. 4009). Fort Meade, MD: CNSS.

Gadde, Swetha; Rao, Gutta Srinivasa; Vesam, Venkata Srinvasu; Yarlagadda, Madhulika; Patibandla, R.S.M Lakshmi. (2023). Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions. International Information and Engineering Technology Association (IIETA).

Lancaster, F. W. (1979). Information retrieval systems: Characteristics, testing, and evaluation (2nd ed.). New York, NY: Wiley.

Maheswari, J. Uma; Vijayalakshmi, S.; Gandhi, Rajiv; Alzubaidi, Laith. (2023). Data Privacy and Security in Cloude Computing Environments. EDP Science.

Merriam-Webster, Incorporated. (2026). Information. In Merriam-Webster.com dictionary. Retrieved January 13, 2026, from https://www.merriam-webster.com/dictionary/information

Polanyi, M. (1966). The tacit dimension. Chicago, IL: University of Chicago Press.

Rnaud, Karen; Solms, Basie Von; Solms, Von Rossouw. (2019). How does intellectual capital align with cyber security? Journal of Intellectual Capital.

Zawaidh, Firas; Ghanem, Waheed; Saany, Syarilla. (2022). The Layers of Cloud Computing Infrastructure and Security Attacking Issues. Journal of Pharmaceutical Negative Results.

Doi: http://doi.org/10.52133/ijrsp.v7.75.10