مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٨) العدد(١) ٢٠٢٤
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (8) No. (1) 2024

التحديّات الأمنية لتبنّي الحوسبة السحابيّة في القطاع الحكوميّ (مراجعة منهجيّة)

أ.د. فادي غصنة*

د. ناجي محمد**

م. مرح مفلح***

(تاريخ الإيداع ٢٠٢٣/٩/٧ . قُبِل للنشر في ٢٠٢٤/١/٢٢)

□ ملخّص□

تعدّ الحوسبة السحابيّة من أهم النماذج التكنولوجيّة سريعة النمو القادرة على تقديم الكثير من الخدمات عند الطلب عبر الإنترنت، وقد اتجهت أغلب المؤسسات الحكوميّة اليوم إلى اعتمادها لما لها من تأثير على أدائها، خاصةً مع الزيادة الكبيرة والمتسارعة في حجم البيانات، والضرورة الحتميّة للحكومة الإلكترونيّة. ماتزال المخاوف الأمنيّة عائقاً كبيراً أمام تبنّي هذا النموذج وخاصةً أمام الحكومات للاستفادة من مزاياها. يهدف هذا البحث إلى عرض أهم التحديّات الأمنيّة التي تواجه تبنّي الحوسبة السحابيّة في المؤسسات الحكوميّة ضمن مراجعة منهجية للأدبيات Systematic Literature Review (SLR)وتحليل لأهم الأبحاث ذات الصلة، من خلال دراسة العديد من المقالات والأبحاث التي تركّز على أمن السحابة، وتحديد مجموعة القضايا الأمنية الأكثر شيوعاً. أظهرت المراجعة أهمية تنفيذ الأمن كخدمة وضرورة تصنيف التحديّات الأمنيّة لتسهيل فهم الترابط بينها ومعالجتها من خلال وضع إطار عمل تكاملي لحلول هذه التحديّات متضمناً أفضل الممارسات في هذا المجال.

كلمات مفتاحية: الحوسبة السحابيّة، الحكومة الإلكترونيّة، الأمن، التحديّات.

*أ.د. فادي غصنة: أستاذ في قسم هندسة تكنولوجيا الاتصالات–كلية هندسة تكنولوجيا المعلومات والاتصالات–جامعة طرطوس.

**د. ناجي محمد: أستاذ مساعد في قسم هندسة تكنولوجيا الاتصالات–كلية هندسة تكنولوجيا المعلومات والاتصالات–جامعة طرطوس.

***م. مرح ناجي مفلح: طالبة دكتوراه في قسم هندسة تكنولوجيا الاتصالات– كلية هندسة تكنولوجيا المعلومات والاتصالات–جامعة طرطوس.

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٨) العدد(١) ٢٠٢٤
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (8) No. (1) 2024

Security Challenges for Cloud Computing Adoption in the Governmental Sector (Systematic Literature Review SLR)

Dr. Fadi Ghosna*
Dr. Naji Mohammad**
Eng. Marah Mfleh***

(Received 7/9/2023 . Accepted 22/1/2024)

□ ABSTRACT □

Cloud computing is one of the most important and rapidly growing technological models capable of providing many services on demand over the Internet, most government agencies today have tended to adopt it because of its impact on their performance, especially with the large and rapid increase in the volume of data, and the inevitable necessity of e-government. Security concerns remain a major obstacle to adopt this model, especially for governments to benefit from its advantages. This research aims to present the most important security challenges facing the adoption of cloud computing in government agencies using a systematic literature review (SLR) and analysis of the most relevant research, by examining many articles and researches that focus on cloud security, and recognizing frequented security issues. The review showed the importance of implementing security as a service and the need to classify security challenges to facilitate understanding of the interrelationship between them and to address them by developing an integrated framework for solutions to these challenges, including best practices in this field.

Keywords: Cloud Computing, E-Government, Security, Challenges.

*Dr. Fadi Ghosna: Professor in the Department of Communications Technology Engineering - Faculty of Information and Communications Technology Engineering -Tartous University.
**Dr. Naji Mohammad: Assistant Professor in the Department of Communications Technology Engineering - Faculty of Information and Communications Technology Engineering –Tartous University.
***Eng. Marah Naji Mfleh: PhD student in the Department of Communications Technology Engineering - Faculty of Information and Communications Technology Engineering -Tartous University.

١. مقدمة

الحوسبة السحابيّة هي إحدى النماذج التكنولوجيّة سريعة النمو التي أصبحت تتبناها العديد من المؤسسات والشركات وحتى الأفراد، نظراً لميزة عدم الحاجة إلى نشر البنية التحتية التي يحتاجها العملاء لتلبية متطلباتهم الحاسوبيّة [1]. وقد اتجهت أغلب المؤسسات الحكوميّة اليوم إلى اعتمادها لما لها من تأثير على أدائها، خاصةً مع الزيادة الكبيرة والمتسارعة في حجم البيانات، والضرورة الحتمية للحكومة الإلكترونيّة باعتبارها شرط أساسي لأيّ دولة لتوفير مشاركة أفضل للمواطنين وتحسين العلاقات الدوليّة [2] مما يتطلب توفير بنية تحتية هائلة وذات جودة في تخزين ومعالجة البيانات، ويتطلب التحكم في استخدام الحوسبة السحابيّة وضبط آليات تشغيلها وتحديد الأدوار والمسؤوليات والتحديّات من قبل مدراء الحكومة الإلكترونيّة والمعنيين لتكون على أكمل وجه [3].

١.١ مفاهيم الحوسبة السحابية

يشير مصطلح الحوسبة السحابيّة إلى "المصادر والأنظمة الحاسوبيّة المتوافرة عند الطلب عبر الشبكة والتي تستطيع توفير عدد من الخدمات الحاسوبيّة المتكاملة دون التقيّد بالموارد المحلية بهدف التيسير على المستخدم. وبذلك أصبحت نموذجاً لتسهيل الوصول ومشاركة مصادر الحوسبة المختلفة مثل المخدمات Infrastructure as a Service (IaaS)، وأنظمة التشغيل ومنصات خاصة للتطوير Platform as a Service (PaaS)، والبرمجيات والخدمات Software as a Service (SaaS) وكذلك التخزين كخدمة data Storage as a Service (dSaaS)". وبتعريفٍ آخر مقدّم من قبل المعهد الوطني للمعايير والتكنولوجيا National Institute of Standards and Technology (NIST) وتحالف أمن السحابة Cloud Security Alliance(CSA) ، تعدّ الحوسبة السحابيّة "نموذجاً لتمكين الوصول المريح للشبكة عند الطلب إلى مجموعة مشتركة من موارد الحوسبة القابلة للتكوين (مثل الشبكات والمخدمات والتخزين والتطبيقات) التي يمكن توفيرها وإصدارها بسرعة بأقل جهد إداري أو تفاعل مع مزود الخدمة [4, 1]. تشمل الخصائص الخمس الرئيسية للحوسبة السحابيّة التي حددتها NIST [5]:

- الخدمة الذاتيّة عند الطلب On Demand Self-Service: يمكن للمستخدم الحصول على إمكانات الحوسبة من جانب واحد، مثل وقت المخدم والتخزين عبر الشبكة، حسب الحاجة دون أي تفاعل بشري مع مزود الخدمة.
- الوصول الواسع للشبكة Broad Network Access: يتم الوصول إليها من خلال آليات قياسيّة متنوعة لمختلف أنواع العملاء بغض النظر عن حجم الطلب. مع الحفاظ على حزمة ترددية عريضة وزمن استجابة منخفض.
- المرونة السريعة Rapid Elasticity: تتيح لنا زيادة (أو خفض) الموارد بسرعة.
- تجميع الموارد Resource Pooling: يتم تجميع موارد الحوسبة الخاصة بالمزود لخدمة جميع العملاء باستخدام نموذج متعدد الإيجار، مع تخصيص موارد مادية وافتراضية مختلفة وإعادة تخصيصها ديناميكيًا وفقًا للطلب.
- الخدمة المقاسة Measured Service: تشير إلى أن مزودي الخدمات السحابيّة يتحكمون في استخدام موارد الحوسبة ويحسنّونها من خلال تخصيص الموارد المؤتمت وموازنة الأحمال وأدوات القياس.

يوجد كذلك أربعة نماذج لنشر السحابة: [6, 5]

✓ السحابة الخاصة Private Cloud: يتم استخدام موارد الحوسبة والتحكم فيها بواسطة مؤسسة خاصة. بحيث يقتصر الوصول إلى الموارد على العملاء الذين ينتمون إلى تلك المؤسسة المالكة للسحابة. تتمثل الميزة الرئيسية لهذا النموذج في زيادة أمن وخصوصيّة البيانات.

✓ السحابة المجتمعيّة Community Cloud: البنية التحتية السحابيّة مشتركة بين عدد من المنظمات ذات الاهتمامات والمتطلبات المتماثلة. مما يساعد في الحدّ من تكاليف النفقات اللازمة لتأسيسها بحيث يتم تقاسمها بين هذه المنظمات.

✓ السحابة العامة Public Cloud: يتم توفير الموارد ديناميكياً على أساس الخدمة الذاتيّة عبر الإنترنت، وعبر تطبيقات/ خدمات الويب. يمكن للعملاء الوصول بسرعة إلى هذه الموارد، والدفع فقط مقابل الاستخدام. تتمثل مخاطرها في الأمن والامتثال التنظيمي وجودة الخدمة.

✓ السحابة الهجينة Hybrid Cloud: عبارة عن مزيج نموذجي من السحابة العامة والخاصة. من خلال هذه البيئة، يمكن للمؤسسة توفير وإدارة موارد معينة داخل الشركة وتوفير موارد أخرى من خلال مزود خارجي.

٢.١ الحوسبة السحابيّة والحكومة الإلكترونيّة

يمكن تعريف الحكومة الإلكترونيّة على أنها طرق جديدة تُستخدم لإعادة هندسة أعمال الحكومة، وتشمل إتاحة الوصول إلى المعلومات على شبكة الإنترنت، وتقديم جميع الخدمات على الويب بطريقة سهلة وسريعة وموثوقة بغض النظر عن المسافات والوقت. وهي عبارة عن مشروع ضخم لأنظمة المعلومات تبنيه الحكومة، وتقدم خدماتها لأربعة أنواع من العملاء: الشركات، والمواطنين، والموظفين، والحكومة نفسها، وبناءً على ذلك يمكن أن تكون الحوسبة السحابية نموذجاً مناسباً لتنفيذ بنية الحكومة الإلكترونيّة بكفاءة عالية وبتحقيق رضا المستخدمين. [5 ,7 ,8 ,9]

تقدّم تقنيات الحوسبة السحابيّة العديد من المزايا للقطاع الحكوميّ والحكومة الإلكترونيّة: [2 ,5 ,8]

أ.قابلية التوسّع: يمكن شراء موارد الحوسبة السحابيّة مثل المخدمات تلقائياً بأيّ كمية وفي أيّ وقت لتناسب العدد المتزايد من المستخدمين.

ب. التوافرية: تتم استضافة تطبيقات الحوسبة السحابيّة عبر الإنترنت أي أنها متوفرة بدرجة عالية ويمكن استخدامها في أي وقت ومن أي مكان.

ج. توفير التكاليف: لا تحتاج أنظمة الحوسبة السحابيّة إلى شراء وتركيب معدات وبرمجيات تكنولوجيا المعلومات في المبنى الخاص بها.

د. النسخ الاحتياطيّ والاسترداد: نظرًا لأن جميع البيانات مخزنة في السحابة، فإن النسخ الاحتياطيّ والاستعادة أسهل بكثير من الطريقة التقليديّة.

هـ. تخزين غير محدود: يمنحك تخزين المعلومات في السحابة سعة تخزين غير محدودة تقريباً.

و. التكنولوجيا الخضراء: الحوسبة السحابيّة جيدة نسبياً في استهلاك الطاقة وتوفر أنظمة بيئية عبر الخدمات الافتراضيّة.

ز. مركزية البيانات: يمكن أن يؤدي اعتماد السحابة في الحكومات إلى إنشاء مجموعة بيانات مركزيّة من الموارد والبرامج والبنية التحتيّة المشتركة.

يمكن تعريف السحابة الحكوميّة Gov Cloud كما قدّمتها الوكالة الأوروبية المتحدة لأمن الشبكات والمعلومات ENISA عام ٢٠١٣، على النحو الآتي:

✓ (ماذا) هي بيئة تعمل على تشغيل خدمات متوافقة مع التشريعات الحكوميّة المتعلقة بالأمن والخصوصيّة والمرونة.

- ✓ (كيف) هي طريقة آمنة وجديرة بالثقة (السحابة الخاصة أو السحابة العامة) لتشغيل الخدمات في ظل حوكمة الهيئة العامة.
- ✓ (لمن) هي نموذج نشر لبناء وتقديم الخدمات لمؤسسات الدولة (التسليم الداخلي للخدمات) والمواطنين والمؤسسات (تقديم الخدمات الخارجية إلى المجتمع). [10]

٣.١ التحديّات الأمنيّة للحوسبة السحابيّة

إن هناك العديد من الفوائد لتطبيق واستخدام الحوسبة السحابيّة، وكذلك هناك العديد من المشكلات والتحديّات التي تؤثر على قابلية تبنّيها والتي يجب استهدافها أو مواجهتها لا سيما تلك المتعلّقة بأمن المعلومات، والسياسات المطلوبة لضمان سلامتها. يمكن تعريف التحديّات على أنّها عقبات يمكن أن تعيق أو تؤخر اعتماد الحوسبة السحابيّة أو تحدّ من استخدامها في المؤسسات. يمكن تلخيص مجموعة التحديّات التي تواجه تطبيق الحوسبة السحابيّة وخاصةً في القطاع الحكوميّ بـ (الأمن والخصوصية، الامتثال التنظيمي، قابلية التشغيل البينيّ، ترحيل البيانات، والتدقيق). يعد الأمن أحد أكبر التحديّات التي تعيق الاعتماد واسع النطاق للحوسبة السحابيّة، تنشأ المشكلات الأمنيّة عادةً بسبب وجود مقدميّ الخدمات ومراكز البيانات بمناطق موزعة جغرافياً، بحيث يتم تخزين المعلومات الحساسة للعملاء في المخدمات والمواقع البعيدة مع احتمالية التعرض لأطراف غير مصرّح لها وبالتالي اختراقها. كذلك تعدّ الثقة بين العملاء ومقدميّ الخدمات السحابيّة مشكلة أخرى تواجه مخاوف أمنية، وهي مرتبطة بشكل مباشر بمصداقية مقدميّ الخدمات السحابيّة. تواجه تطبيقات الحوسبة السحابيّة جميع نقاط الضعف في الشبكة، بسبب البيئة المتصلة. وفي الوقت نفسه، إلى جانب نقاط الضعف في الشبكات ونقاط ضعف الشبكة الافتراضيّة، تحتاج التطبيقات السحابيّة أيضاً إلى التعامل مع التهديدات المحتملة من المشاركين في السحابة، مثل مزوديّ الخدمة غير المعروفين أو مستخدميّ البيانات غير المتوقعين. وهذا يعني أن معظم التطبيقات تواجه تهديدات من الداخل والخارج. [11, 5, 3]

تأتي في مقدمة التحديّات المخاوف الأمنية العامة ((Confidentiality, Integrity, Availability (CIA))، والامتثال القانوني، وفقدان البيانات وتسربها، وكذلك الوصول غير المصرّح به من خلال إساءة استخدام بيانات الموظفين وضوابط الوصول غير المناسبة كأكبر تهديد منفرد، ويتبع ذلك سرقة الحسابات وواجهات برمجة التطبيقات غير الآمنة.

لا تتصدر مخاوف أمن السحابة قائمة العوائق المحدّدة فحسب، بل إنها تتزايد بشكل أكبر. ومع ذلك، فإن اعتماد الحوسبة السحابيّة آخذ في الازدياد مما يدفع المؤسسات وفُرق الأمن لإيجاد طريقة "لإنجاز سحابة آمنة". [12, 13, 14]

٢. هدف البحث

يهدف هذا البحث إلى عرض أهم التحديّات الأمنيّة التي تواجه تبنّي الحوسبة السحابيّة في المؤسسات الحكوميّة من خلال مراجعة منهجيّة Systematic Literature Review (SLR) وتحليل لأهم الأبحاث ذات الصلة. تنعكس أهمية هذا البحث على محورين: صانعيّ السياسات ومدراء الحكومة الإلكترونيّة لوضع تصوّر شامل عن التحديّات الأمنية التي تتطلب إيجاد حلول وتحديد أدوار ومسؤوليات المعنيّين قبل البدء باستثمار إمكانيات الحوسبة السحابيّة، وطلاب الدراسات العليا والباحثين بحيث يشكل إطاراً مرجعيّاً للتخصص والبحث في العديد من التحديّات الفردية التي ماتزال مفتوحة.

٣. طرائق البحث وموادّه

على الرغم من وجود العديد من الأبحاث التي تناولت تحديّات الحوسبة السحابيّة عموماً لم تلحظ مراجعة الأدبيات التي قمنا بها أي مراجعة منهجيّة للتحديّات الأمنية للحوسبة السحابيّة في البيئة الحكوميّة على وجه الخصوص، وكذلك لم نجد إطار عمل شامل لتغطية هذه التحديّات ذات الأهمية العاليّة في مواجهة تبنّي الحوسبة السحابيّة. حيث قمنا بمراجعة العديد من المقالات والأبحاث التي تركّز على الحوسبة السحابيّة وأمن السحابة لتوضيح وتلخيص القضايا والتحديّات الأمنية الحاليّة التي تواجهها.

1.3 المراجعة المنهجية

أجرينا مراجعة أدبيّة منهجيّة SLR للتحديّات المحتملة للحوسبة السحابيّة، من خلال جمع المستندات والوثائق التي تصفها، وتم التركيز على التحديّات الأمنية وخاصةً تلك التي تواجه استثمار الحوسبة السحابيّة في القطاع الحكوميّ.

1.1.3 منهجية SLR

تم اعتماد إرشادات مراجعة الأدبيات المنهجيّة (SLR) التي قدمها كيتشنهام (٢٠٠٧) لإجراء مراجعة الأدبيات. SLR هي طريقة لتحديد وتقييم وتفسير جميع الأبحاث المتاحة من خلال الدراسات الأولية ذات الصلة بسؤال بحث معين أو ظاهرة معينة. يمكن تصنيف منهجيّة SLR إلى ثلاث مراحل رئيسيّة، وهي: ١) تخطيط SLR؛ ٢) إجراء SLR؛ و٣) تقرير نتائج SLR. هذه الإجراءات مفصّلة في الأقسام التالية.

2.1.3 تخطيط SLR

تظهر الحاجة إلى SLR هنا لتلخيص مجموعة المعرفة الحاليّة حول موضوع التحديّات الأمنية للحوسبة السحابيّة في القطاع الحكوميّ، وكذلك الاطلاع على بعض الأطر والأساليب المقدّمة لتعزيز الأمن السحابيّ الحكوميّ. تشمل مرحلة التخطيط صياغة أسئلة البحث، التي تحتاج إلى إجابة، بناءً على جمع وتحليل البيانات، نختار سؤالين بحثيين لـ SLR لدينا:

١) ماهي التحديّات الأمنيّة التي تؤثر على تبنّي الحوسبة السحابيّة في القطاع الحكوميّ؟

٢) ماهي التجارب والممارسات والأطر المقدّمة في هذا الصدد؟

كما تشمل مرحلة التخطيط اختيار مصادر البيانات والدراسات ومن ثم تصفية النتائج.

تم إجراء البحث باستخدام قواعد البيانات الآتية:

- Springer، IEEE Explore، Research Gate، Google Scholar، Science Direct.

3.1.3 إجراء SLR

استخدمنا في البحث مجموعات مختلفة من مصطلحات البحث الأوليّة المشتقة من أسئلة البحث المقترحة. تم استخدام الكلمات الرئيسية التالية: ("الحوسبة السحابيّة" أو "السحابة الحكوميّة" أو "الحوسبة السحابيّة في الحكومة الإلكترونيّة" أو "الحوسبة السحابيّة في القطاع الحكومي") و ("مشكلات" أو "تحديّات" أو "عوائق" أو "مخاطر" تبنّي الحوسبة السحابيّة) و ("أمن الحوسبة السحابيّة" أو "أمن السحابة" أو "أمن السحابة الحكوميّة") و ("إطار عمل الحوسبة السحابيّة"). حددنا أيضاً معايير التضمين والاستبعاد لـSLR التي تم إجراؤها كالتالي:

معايير الاشتمال: ١. الدراسات التي تعرض أي تحديّات أمنية لتبنّي الحوسبة السحابيّة في القطاع الحكوميّ، بما في ذلك وقائع المؤتمرات وأوراق المجلات، ٢. الدراسات التي تقدّم أي تجارب أو نماذج أو أطر عمل لتبنّي الحوسبة السحابيّة في القطاع الحكوميّ، ٣. الدراسات المنشورة بين ٢٠١٠ و2023.

معايير الاستبعاد: ١. الدراسات التي ليست باللّغة الإنجليزيّة أو العربيّة، ٢. الدراسات غير المتعلّقة بأسئلة البحث، ٣. الدراسات المكرّرة (حسب العنوان أو المحتوى).

في البداية، تم اختيار ١١٠ ورقة، وبعد تطبيق معايير الإدراج والاستبعاد السابقة، تم اختيار ٥١ ورقة للتحليل والدراسة تمت فهرستها ضمن مراجع البحث.

4.1.3 تقرير نتائج SLR

يتم هنا تقديم نتائج SLR مع الأخذ بالحسبان كل سؤال بحث تمت صياغته في القسم السابق.

١.٤.١.٣ التحديات الأمنية التي تؤثر على تبنّي الحوسبة السحابيّة في القطاع الحكوميّ

قامت الدراسات الناتجة عن SLR بتحليل العديد من القضايا والتحدّيات المؤثرة على تبنّي الحوسبة السحابيّة ومنظوماتها، وقمنا بتجميعها في ١٩ قضية كما هو في الجدول (١)، ويلي الجدول لمحة موجزة عن كلّ من هذه التحدّيات وفقاً لتلك الدراسات.

الجدول (١): التحدّيات الأمنية للحوسبة السحابية

القضية/ التحدّي	تسلسل الدراسات
١. الاختراقات الداخلية Malicious insiders	٥، ١٢، ١٣، ٢٨، ٣٦، ٣٧، ٤٢، ٤٧، ٤٨
٢. التشفير وإدارة المفاتيح Encryption and Key Management	٣، ٦، ١١، ١٢، ١٣، ١٤، ١٧، ١٨، ٢٠، ٢٤، ٣٣، ٣٤، ٣٧، ٣٩، ٤٣، ٤٤، ٥٠
٣. منع أو حجب الخدمة Denial of service (DOS)	٣، ١٢، ١٣، ١٦، ١٧، ١٨، ٢٤، ٢٨، ٣٢، ٣٦، ٣٩، ٤٢، ٤٣، ٤٨، ٥٠
٤. واجهات الربط غير الآمنة Insecure interfaces and APIs	١٢، ١٣، ١٧، ١٨، ٢٨، ٣٦، ٣٧، ٤٢
٥. فقدان وتسرب البيانات Data loss or leakage	٥، ١٢، ١٣، ١٧، ٣١، ٣٢، ٣٦، ٣٧، ٤٢، ٤٧
٦. سلامة وتكاملية البيانات Integrity	٣، ١٤، ١٦، ١٧، ٢٠، ٢٤، ٢٨، ٢٩، ٣٠، ٣١، ٣٢، ٣٣، ٣٥، ٣٧، ٣٩، ٤٢، ٤٣، ٤٤، ٤٨، ٤٩، ٥٠، ٥١
٧. التوافرية Availability	٣، ٥، ١٢، ١٤، ١٦، ١٧، ١٩، ٢١، ٢٨، ٢٩، ٣٠، ٣١، ٣٢، ٣٤، ٣٥، ٣٦، ٣٧، ٣٨، ٤١، ٤٣، ٤٩، ٥٠، ٥١
٨. فقدان النسخ الاحتياطية Loss of backups	٣، ١٢، ١٤، ٣٢، ٣٤، ٣٧، ٥٠
٩. خصوصية وسرية البيانات Confidentiality and Data Privacy	٢، ٣، ٥، ٦، ٨، ١١، ١٢، ١٣، ١٦، ١٧، ١٨، ١٩، ٢٠، ٢١، ٢٤، ٢٨، ٢٩، ٣٠، ٣١، ٣٢، ٣٣، ٣٤، ٣٧، ٣٨، ٣٩، ٤٠، ٤٢، ٤٥، ٤٧، ٤٨، ٤٩، ٥٠، ٥١
١٠. الامتثال التنظيمي Regulatory compliance	٢، ٣، ١٢، ١٤، ١٦، ١٧، ٢٨، ٣٠، ٣٢، ٣٣، ٣٤، ٣٥، ٣٦، ٤٢، ٤٨، ٥٠
١١. المصادقة، التعريف وإدارة الوصول Identification, Authentication and Access Management	٢، ٣، ٦، ١١، ١٣، ١٤، ١٦، ١٧، ١٨، ٢١، ٢٤، ٢٨، ٣١، ٣٢، ٣٥، ٣٧، ٣٨، ٤١، ٤٢، ٤٣، ٤٤، ٤٨، ٤٩، ٥٠
١٢. التشبيك الافتراضي الآمن Secure Virtual Networking	١٧، ١٨، ٣٢، ٣٧، ٤٦، ٤٨
١٣. موقع البيانات Data location	٣، ٥، ١٤، ١٧، ٢٤، ٢٨، ٢٩، ٣٢، ٣٣، ٣٥، ٣٦، ٣٨، ٣٩،
١٤. التفويض أو الترخيص Authorization	٣، ٦، ١١، ١٣، ١٤، ١٦، ١٧، ٢١، ٢٤، ٢٨، ٣١، ٣٢، ٣٧، ٤٣، ٤٤، ٤٩، ٥٠، ٥١
١٥. أمن الشبكة Network security	١٤، ١٦، ١٧، ٢٤، ٣٠، ٤٨
١٦. قضايا التكنولوجيا المشتركة Shared Technology Issues	٥، ١٢، ١٣، ١٨، ٢٨، ٣٣، ٤٢، ٤٨
١٧. عدم التنصل Non-repudiation	١٧،٥٠
١٨. حوكمة الأمن Security Governance	١٢، ٥٠
١٩. فصل البيانات Data Segregation	٣٦، ٤٨، ١٤

١. الاختراقات الداخلية: يمكن للموظفين العاملين في مزود الخدمة السحابيّة الوصول الكامل إلى موارد المؤسسة. لذلك يجب أن يكون لدى مزوديّ الخدمات السحابيّة تدابير أمنية مناسبة لتتبع إجراءات الموظفين بحيث لا يمكنهم جمع معلومات سريّة من العملاء دون أن يتم اكتشافهم.

٢. التشفير وإدارة المفاتيح: يعد التشفير أحد أكثر الطرق فعالية للحفاظ على سلامة وسريّة المعلومات. لكن يعدّ إنشاء مفاتيح التشفير وإدارتها لنموذج السحابة غير معياريّ. وهذا التشفير في شكله الحالي كافٍ لتخزين البيانات ونقلها، ولكنّه يمنع بشكل أساسي معالجتها أي أنه يعزز المخاطر المحتملة.

٣. منع أو حجب الخدمة: وهو نوع من الهجوم حيث تبدأ مجموعة من المتسلّلين بالهجوم على هدف واحد وحجب الخدمات عن المستخدم المستهدف. يمكن تعطيل الخدمة في بيئة سحابيّة افتراضيّة: إما باستخدام وحدة المعالجة المركزيّة، أو ذاكرة الوصول العشوائي، أو مساحة القرص أو النطاق الترددي للشبكة.

٤. واجهات الربط غير الآمنة: تقدّم الخدمات السحابيّة على الإنترنت من خلال واجهات برمجة التطبيقات (API)، الممكن مهاجمتها والإضرار بسرية وسلامة الخدمة. أي يجب أن توفر السحابة واجهات آمنة، مما يجعل هذه الهجمات عديمة الفائدة.

٥. فقدان وتسرب البيانات: قد يتم فقد البيانات المخزنة في السحابة بسبب فشل القرص الصلب، أو حذفها عن طريق الخطأ، وقد يقوم المهاجم بتعديل البيانات. لذا، فإن أفضل طريقة للحماية من فقدان البيانات من خلال الاحتفاظ بنسخة احتياطية منها، مما يحل مشاكل فقدان البيانات وعواقبها.

٦. سلامة البيانات: تشير إلى دقة واتساق (صحة) البيانات خلال دورة حياتها. بحيث تصبح البيانات المخترقة دون فائدة لمالكيّ البيانات، ناهيك عن المخاطر التي يمثلها فقدان البيانات الحساسة. لهذا السبب، فإن سلامة البيانات هي مطلب إلزامي للعديد من حلول الأمن في السحابة.

٧. توافرية البيانات: يعني أن تكون خدماتنا وتطبيقاتنا السحابيّة متاحة دائماً عندما نحتاج إليها، وهو أحد أسباب الانتقال إلى السحابة. وهو مطلب إلزامي لأمن المعلومات والبيانات.

٨. فقدان النسخ الاحتياطية: ماذا يحدث للبيانات في حالة وقوع كارثة، هل يستطيع مزود السحابة نقل بيانات العميل بالكامل إلى بيئة مختلفة في هذه الحالة؟ وهل يضمن استعادة كاملة، وإذا كان الأمر كذلك، فما المدة التي تستغرقها هذه العملية؟

٩. خصوصيّة وسريّة البيانات: تعد مشكلة شائعة في تطبيق الحوسبة السحابيّة. بحيث تشكل البيانات التي تحمل معلومات حساسة أهدافاً للمهاجمين، ويكون لمالكيّ البيانات تحكم قليل في بياناتهم عند تخزين/ تشغيل البيانات على مخدم السحابة عن بعد، وتبادلها مع مزوديّ الخدمة.

١٠. الامتثال التنظيمي: يشير إلى الانضباط والتأكد من أن مزود الخدمة السحابيّة يتّبع القوانين التي تفرضها الهيئات الإدارية في موقعه الجغرافيّ أو القواعد التي تتطلّبها معايير الصناعة المعتمدة. ولتحقيقه يقوم الأشخاص والعمليات بالتدقيق لاكتشاف ومنع الانتهاكات.

١١. المصادقة وإدارة الوصول: تمثل تتبع هوية المستخدم والتحكم بالوصول إلى المعلومات، وتحديد من لديه حق الوصول المميز إلى البيانات، ومن الذي يقرر تعيين المسؤولين عن ذلك. تعد هذه العملية أكثر تعقيداً في بيئة السحابة نظراً لوجود مالك البيانات والموارد في مجالات إدارية مختلفة.

١٢. التشبيك الافتراضي الآمن: الإضافة إلى الحوسبة السحابيّة، تقدم الافتراضيّة تحديات أمنية جديدة من خلال تمكين الاتصال بين المكونات الافتراضيّة المختلفة. إلى جانب تأمين الاتصال نفسه في الشبكات الافتراضيّة، يجب أيضاً تأمين إدارة الاتصال فقد تظهر هجمات جديدة وتحتاج إلى التعامل معها.

١٣. موقع البيانات: هل يسمح مزود السحابة بأيّ سيطرة على موقع البيانات؟ وفي أيّ موقع جغرافي يتم تخزين معلومات المستخدم؟ بحيث نظرًا لقوانين الامتثال وخصوصيّة البيانات في مختلف البلدان، فإن موقع البيانات له أهمية قصوى.

١٤. التفويض: هو عملية إعطاء شخص ما القدرة على الوصول إلى مورد معين. وهو مطلب مهم لأمن المعلومات في الحوسبة السحابيّة لضمان الحفاظ على سلامة البيانات. يستخدم لممارسة التحكم وتطبيق الامتيازات على تدفقات العمليات داخل السحابة.

١٥. أمن الشبكة: تواجه الحوسبة السحابيّة جميع أنواع الهجمات الموجهة للشبكة باعتبارها تقنية مستندة إلى الويب. يمكن تصنيف هذه الهجمات إلى سلبية Passive ونشطة Active. الهجوم السلبي هو الذي يجذب المعلومات من خلال اعتراضه مباشرةً لحركة المرور عبر الشبكة مثل تحليل حركة المرور Traffic analysis. أما الهجوم النشط فهو الذي يتمكن فيه المهاجم من الوصول بشكل غير قانوني عبر استخدام شيفرات خبيثة مثل الفيروسات Virus.

١٦. قضايا التكنولوجيا المشتركة: يستخدم مزودو الخدمات السحابية بنية تحتيّة مشتركة لا يتم تجهيزها غالباً لاستيعاب البنية متعددة المستأجرين. مثلاً تعمل برامج Hypervisor على عدّة أجهزة افتراضيّة وتشغّل تطبيقات متعددة. في حال حصول هجوم على هذه البرامج يستطيع المهاجم الوصول إلى بيانات تطبيق آخر يعمل على نفس الجهاز الافتراضيّ وبالتالي الوصول إلى جميع الأجهزة الافتراضيّة على نفس المخدم.

١٧. عدم التنصّل: هو التأكيد على أن الشخص لا يستطيع إنكار صحة شيء ما. وهو مفهوم قانوني يستخدم على نطاق واسع في أمن المعلومات ويشير إلى أصل وسلامة البيانات. يستخدم لأجله التوقيع الرقمي Digital Signature والطابع الزمني Timestamps.

١٨. حوكمة الأمن: يجب على مزود الخدمة السحابيّة الكشف عن تفاصيل هندسة الأمن التي إما تساعد أو تعيق إدارة الأمن وفقًا لمعيار المؤسسة. وكذلك تحديد مسؤوليات الحوكمة وإدارة الأمن للمستخدم مقابل تلك الخاصة بمزود السحابة بوضوح.

١٩. فصل البيانات: نتيجة لتعدد الإيجارات، يمكن لعدّة مستخدمين تخزين بياناتهم من خلال تطبيقات السحابة، أي ستتواجد بياناتهم في نفس الموقع، ويصبح من الممكن التطفّل على بيانات أحدهم بواسطة آخر ولفصلها عادةً تستخدم أنماط تشفير مختلفة للبيانات.

نلاحظ أنه من المّمكن تصنيف هذه التحديّات، وقد اخترنا لذلك إطار TOE (Technology, Organization, Environment) الذي اقترحه (Tornatzky & Fleischer, 1990)، حيث يحدد الإطار ثلاث مجموعات من العوامل (التكنولوجيّة والتنظيميّة والبيئيّة) التي تؤثر على تبنيّ واعتماد التقانات في قطاعات الأعمال. يظهر الجدول (٢) تصنيف هذه التحديّات:

الجدول (٢): تصنيف التحديّات الأمنية للحوسبة السحابية وفقاً لإطار TOE

تصنيف TOE	القضية/التحديّ
التكنولوجيا Technology	التشفير وإدارة المفاتيح، منع أو حجب الخدمة، واجهات الربط غير الآمنة، فقدان وتسرّب البيانات، سلامة البيانات، التوافرية، قضايا التكنولوجيا المشتركة، عدم التنصل.
التنظيم Organization	الاختراقات الداخلية، فقدان النسخ الاحتياطيّة، خصوصيّة وسريّة البيانات، الامتثال التنظيميّ، المصادقة، التعريف وإدارة الوصول، التفويض، حوكمة الأمن.
البيئة Environment	التشبيك الافتراضيّ الآمن، موقع البيانات، أمن الشبكة، فصل البيانات.

استعرض العديد من الباحثين هذه التحديّات مع بعض الحلول المقترحة كمايلي:

عرض [15] (David, 2010) في بحثه ماهيّة الحوسبة السحابيّة وأهميتها واستخداماتها في الحكومات في جميع أنحاء العالم، من الولايات المتحدة إلى أوروبا وآسيا. بعد ذلك، النظر إلى الموارد –الأشخاص والحوسبة –التي ينطوي عليها التحوّل إلى

الحوسبة السحابيّة وفق ما سمّاه "إستراتيجيّة الهجرة السحابيّة" المكوّنة من ست خطوات للمؤسسات الحكوميّة ومن ثم الآثار المترتبة على مؤسسات القطاع العام ومجتمع تكنولوجيا المعلومات مع تقدم ثورة الحوسبة السحابيّة.

أوضح [16] (Ashish & Aparna, 2011) مشكلة الخصوصية وفقاً لسيناريو السحابة المختلف بعدّة حالات: (أ) كيفية جعل المستخدمين متحكمين دائماً ببياناتهم عند تخزينها ومعالجتها في السحابة، وتجنب السرقة والاستخدام غير المصرح به، (ب) كيفية ضمان تكرار البيانات في مواقع مناسبة متعددة، وتجنب فقدان البيانات، والتسرب، والتعديل أو التلفيق غير المصرح به، (ج) من هو الطرف المسؤول عن ضمان المتطلبات القانونيّة للمعلومات الشخصيّة، و (د) إلى أي مدى يمكن تحديد المتعاقدين في السحابة المشاركين في المعالجة والتحقق منهم بشكل صحيح.

بيّن [17] (Subra k., 2011) بأنه من المهم إجراء تحليل فجوة لإمكانيات الخدمة السحابيّة قبل اتخاذ القرار بتشغيل السحابة. يجب أن يقيس هذا التحليل مستوى نضج المنصة السحابيّة وشفافيته وامتثاله لمعايير أمن المؤسسة (مثل ISO 27001) والمعايير التنظيمية مثل PCI DSS وHIPAA وSOX. يمكن أن تساعد نماذج نضج أمن السحابة في تسريع إستراتيجيّة ترحيل التطبيقات إلى السحابة. أوضح كذلك مجموعة من حلول أمن السحابة. مثلاً، لتحقيق التوافرية بشكل مستمر، يجب تصميم التطبيقات السحابيّة لتحمّل الاضطرابات في البنية التحتيّة المشتركة الموجودة داخل مركز البيانات أو منطقة جغرافية ما وقد يساعد الاقتران Loose coupling للتطبيقات والمكونات في هذه الحالة. شرح أيضاً أهمية ترحيل عمليات الأمن مثل إنشاء سياسة جدران الحماية وتوفير الشهادات وتوزيع المفاتيح والاختبارات إلى نموذج خدمة ذاتية بهدف التخلّص من نقاط اللمس البشريّة وتحقيق سيناريو الأمن كخدمة وبالتالي تخفيف التهديدات وتحسين الكفاءة التشغيليّة وتضمين عناصر التحكم بالأمن في التطبيقات السحابيّة.

اقترح [18] (Kashif et al., 2013) نموذجاً وإطاراً أمنياً لبيئة الحوسبة السحابيّة الآمنة حدّد من خلالها متطلبات الأمن والهجمات والتهديدات والمخاوف المرتبطة بنشر السحابات. وقد اعتبر بأن أمن الحوسبة السحابيّة ليس مجرد مشكلة تقنية وحسب، بل يتضمن أيضاً قياس الخدمات والإشراف والقوانين واللوائح والعديد من الجوانب الأخرى. دعا كذلك إلى إيجاد طرق لتحليل المخاطر النوعيّة والكميّة في الحوسبة السحابيّة لكي تُمكّن هذه الأساليب المؤسسات من تحقيق التوازن بين المخاطر الأمنيّة المحددة والفوائد المتوقعة من الانتقال إلى السحابة.

طوّر [19] (Nouf et al, 2014) نموذجاً متكاملاً لفحص أهم العوامل التي تؤثر على قرار المؤسسات بتبنّي السحابة، وقد ظهرت العوامل الأمنية في مقدمة العوامل المؤثرة على هذا القرار مثل التوافرية، الموثوقيّة، السريّة، الامتثال التنظيمي وغيرها، ولكنّه لم يتابع مراجعة هذا النموذج وتأكيده ضمن هذا البحث.

قدّم [20] (Lo'ai et al., 2015) إطار عمل للحوسبة السحابيّة يصنّف فيه البيانات بناءً على أهميتها، أي يتم تشفير البيانات الأكثر أهمية باستخدام خوارزمية تشفير أكثر أمناً وأحجام مفاتيح أكبر، بينما قد لا يتم تشفير البيانات الأقل أهمية. ساهم هذا النهج في تخفيض تكلفة المعالجة وتعقيد تخزين البيانات ومعالجتها بسبب عدم الحاجة إلى تطبيق نفس تقنيات التشفير المتطورة على بيانات المستخدمين بأكملها.

عرضت [12] (Ibtissam et al., 2018) عدداً من الحلول لمعالجة بعض التحديّات الأمنيّة المذكورة سابقاً. مثلاً، للتغلب على تحديّات الخصوصيّة والحماية، من الممكن استخدام بنية تختّص باستراتيجيات موقع البيانات، والخدمات السحابيّة وموردي الخدمات الموثوقين. من أجل قضايا الامتثال التنظيمي، ذكرت مفهوم السوق السحابيّة التي تمكّن المستخدمين من التبادل مع السوق وطلب الموارد التي تتوافق مع احتياجات تطبيقاتهم من خلال وسيط السحابة. ولتجنب تقييد البائع، اقتُرحت بنية متعددة الطبقات تقدّم نموذجاً موحداً للموارد من بيئات سحابية مختلفة.

نوّه [21] (Jaydip K., 2019) إلى أن تشفير البيانات السحابيّة لا يعدّ الحلّ الذي يمكن أن يحافظ على الثقة في أمن السحابة. يمكن إجراء ذلك من خلال تطبيق تقنيات الأمن الأخرى مثل المصادقة والتحقق من الهوية والتشفير والتحقق من السلامة والتحكم بالوصول والحذف الآمن وإخفاء البيانات، وجميع هذه التقنيات قابلة للتطبيق على السحابة. أشار على سبيل المثال إلى التقنيات الأساسية لتكاملية البيانات وهي Provable Data Prossession (PDP) عبارة عن تقنية لضمان تكامل البيانات السحابيّة على مخدم بعيد، وتقنية Proof Of Retrievability (POR) للتحقّق والحصول على أدلة على أن البيانات السحابيّة المخزنة من قبل المستخدم على المخدم لم تتغير. أما بالنسبة للحذف الآمن فيمكن استخدام تقنيات مختلفة مثل التنظيف Clearing، والتي يتم من خلالها حذف الوسائط قبل أن تتم إعادة استخدام هذه الوسائط، وفي نفس الوقت تقديم الحماية للبيانات المحتواة ضمن الوسائط قبل حذفها. والتعقيم Sanitization، بحيث لا يتم توفير الحماية للبيانات السابقة هنا. وفيما يخص التسلّل تم تحديد نوعين من أنظمة كشف التسلّل، نظام الكشف المستند إلى الشبكة (NIDS) الموجود في الأجهزة أو الجزء المتصل بالحاسب من شبكة المنظمة ويراقب حركة مرور الشبكة والهجمات المستمرة، ونظام الكشف المستند إلى المضيف بحيث يتم تثبيت النظام (HIDS) على نظام أو مخدم محدد ومراقبة الأنشطة غير القانونية على هذا النظام.

أوضح [1] (Taera O., 2020) أنه من أجل منع المخاطر الأمنيّة الموجودة في الحوسبة السحابيّة، يجب استخدام آليات أمن مختلفة تتراوح من أمن مركز البيانات الماديّ إلى أمن محدد ومعقد لواجهة برمجة التطبيقات. على سبيل المثال، التشفير التام بين الأطراف، والمراقبة النشطة وفحص نقاط الضعف في الموارد المشتركة، واستخدام SSL على المخدمات السحابيّة لتأمين بيانات المستخدمين الخاصين وغيرها.

عرضت [3] (Hedaia A., 2020) العلاقة بين الأمن السيبرانيّ والأمن القوميّ ومجموعة العوامل التي قد تؤثر على الأمن القوميّ عندما تتحول الحكومات إلى الحوسبة السحابيّة، وخاصةً في حال مشاركة طرف ثالث وعدم وجود أطر تنظيمية واضحة داخل البلدان وفيما بينها. تكمن أهميّة هذ البحث في ضرورة مساعدة الحكومات من الناحية التجريبيّة على البقاء آمنة أثناء الاستمتاع بمزايا الحوسبة السحابيّة وبسبب أهمية البيانات كمورد استراتيجيّ وطنيّ. نوّهت إلى أن الحلول المستندة إلى Blockchain هي طريقة شائعة لتأمين البيانات في البيئات السحابيّة وكذلك تشفير البيانات.

عرضت [22] (Kristin B, 2023) مجموعة من العوامل لتأمين البيانات في بيئات السحابة والتي ينبغي على المؤسسات مراعاتها عند الانتقال إلى التطبيقات السحابيّة. أولها التفكير في أتمتة أمن السحابة كجزء من استراتيجية التحوّل الرقمي للمؤسسة. ثانياً، تطبيق إطار العمل الأمني وفقاً لنهج عدم الثقة zero-trust approach بمصادقة جميع المستخدمين –داخل وخارج شبكة المؤسسة– قبل الوصول إلى تطبيقاتها وبياناتها. ثالثاً، الحوسبة السريّة التي تحمي البيانات المستخدمة في بيئات آمنة ومعزولة على الأجهزة وبالتالي تمنع الوصول غير المصرّح به وتعديل التطبيقات والبيانات. تكون موارد هذه الحوسبة على شكل مفاتيح تشفير غير مرئية، وتظلّ غير قابلة للاكتشاف بواسطة أي برنامج أو شخص أو مزود خدمة سحابيّة. رابعاً، دعم بنية الأمن المفتوحة عبر مقدميّ الخدمات السحابيّة، وأخيراً التوسّع في اعتماد Multicloud والتي تقدّم العديد من المزايا للمؤسسات، مثل انخفاض التكاليف، تحسين تقديم الخدمات، وتلبية متطلبات الامتثال، وتحسين الأداء، وتحسين المرونة وقابلية التوسّع. يمكن للاستراتيجيّة متعددة السحابة كذلك تحسين الأمن بشكل أكبر من خلال تمكين المرونة المحسّنة والتعافي المحسّن من الكوارث وخيارات تجاوز الفشل الأفضل التي تقلّل من وقت التعطّل.

تبيّن معنا بعد مراجعة الدراسات السابقة، أنّ عدداً قليلاً من الدراسات قامت بتحديد العوامل الأمنيّة التي تؤثر على تبنيّ الحوسبة السحابيّة في المؤسسات الحكوميّة على وجه الخصوص، لذا فإن هذا المجال البحثي يحتاج للمزيد من الاهتمام من خلال إجراء تحليل معمّق والتحقيق في المخاطر الأمنيّة التي تؤثر على اعتماد الحوسبة السحابيّة في المؤسسات الحكوميّة.

٢.٤.١.٣ لمحة عن التجارب والأطر المقدّمة لتبنّي وتأمين الحوسبة السحابيّة في القطاع الحكوميّ

تتنقل المؤسسات الحكوميّة في جميع أنحاء العالم إلى الحوسبة السحابيّة بعد تجربة القطاع الخاص الناجحة مع هذا التحوّل. حيث صاغت العديد من البلدان استراتيجيات منفصلة لضمان انتقال ملموس وأكثر منهجية إلى الحوسبة السحابيّة مثل المملكة المتحدة وأستراليا وإسبانيا والإمارات العربية والسعودية ومصر وسورية مؤخراً. وقد عبّرت بعض الأبحاث عن أهميّة الحوسبة السحابيّة لما تقدمّه من الميزات للحكومات، ودرست قابلية تطبيقها مع مراعاة التحديّات الأمنية على اعتبار أهميّة البيانات كمورد استراتيجيّ وطنيّ [3, 15, 29, 30]، ومن بينها:

- اعتمدت الحكومة الأستراليّة في عام ٢٠١٤ سياسة للخدمات السحابيّة مماثلة لما هو قائم في الولايات المتحدة والمملكة المتحدة. تضمّنت وثيقة سياسات رسميّة بغية مساعدة المؤسسات الحكوميّة في إدارة، وتنفيذ، وشراء الخدمات السحابيّة وكذلك تلبية متطلبات الخصوصيّة والأمن. طوّرت فيما بعد الحكومة الأستراليّة في العام ٢٠٢١ استراتيجيّة السحابة الآمنة الخاصة بها للانتقال للحوسبة السحابيّة وتحقيق أقصى استفادة مما تقدمه من خدمات. تم استخدام هذه الاستراتيجيّة كنقطة انطلاق للوصول لنموذج السحابة الأنسب وتقييم جاهزيّة الخدمة، واسترشد تنفيذ السحابة بسبعة مبادئ منها اتخاذ قرارات قائمة على المخاطر عند تطبيق الأمن السحابيّ، ومراقبة صحة استخدام السحابة في الوقت الحقيقي لضمان الأمن. [23]
- اقترحت وزارة العلوم وتكنولوجيا المعلومات والاتصالات في كوريا في العام ٢٠١٣ قانوناً بشأن تنمية الحوسبة السحابيّة وحماية مستخدميها ("قانون تنمية الحوسبة السحابيّة") الذي يرمي إلى تسهيل استخدام المؤسسات العامة للحوسبة السحابيّة، وتعزيز صناعتها، وبناء بيئة آمنة للمستخدمين. وقد أقرت الجمعية الوطنية القانون ودخل حيز التنفيذ في العام ٢٠١٥. ويتألف من أربع ركائز رئيسيّة هي "الأحكام العامة"، "إرساء الأساس لتنمية الحوسبة السحابيّة"، "تيسير استعمال خدمات الحوسبة السحابيّة"، و"تعزيز موثوقية خدمات الحوسبة السحابيّة وحماية المستخدمين". [23]
- قامت ENISA في العام ٢٠١٥ بتقديم نموذج لإطار أمني عام للسحب الحكوميّة. يعتمد الإطار المقترح على مجموعة من أدبيات أمن الحوسبة السحابيّة الحاليّة، وأفضل الممارسات الأمنيّة الأخرى ذات الصلة، وعلى دراسات الحالة الواقعيّة القليلة الحاليّة للسحابات الحكوميّة في أوروبا. خلصت النتيجة النهائيّة إلى إطار أمني صُمّم على شكل أربع مراحل، وتسعة أنشطة أمنية وأربعة عشر خطوة توضّح بالتفصيل مجموعة الإجراءات التي يجب على كل دولة اتباعها لتحديد وتنفيذ سحابة حكوميّة آمنة. تم التحقق من صحة إطار العمل الأمني تجريبياً من خلال تحليل أربع دراسات حالة خاصة بالسحابة الحكوميّة وهي إستونيا واليونان وإسبانيا والمملكة المتحدة. [10]
- قدّم [25] (Madini A., 2018) نموذجاً أمنياً لتبنّي الحوسبة السحابية في المؤسسات الحكوميّة في السعوديّة، وهو عبارة عن إطار عمل لفهم وتقييم الأمن في اعتماد السحابة بحيث يتم التركيز على المخاطر والفوائد الاجتماعيّة عند تنفيذ الأمن.

• قدّمت [26] (Amira T., 2019) بحثها لاقتراح إطار عمل مرجعيّ لمساعدة شركات تكنولوجيا المعلومات في مصر وصنّاع القرار في مجال الأعمال على تحليل الآثار الأمنية للحوسبة السحابيّة على أعمالهم. تضمّن البحث قائمة بالخطوات والإرشادات لتقييم ومقارنة عروض السلامة لمقدميّ الخدمات السحابيّة المختلفين عند التفكير في الانتقال إلى السحابة، بحيث يجب أن يكون لدى العملاء فهم واضح لفوائد الأمن والمخاطر المحتملة، وتطوير توقعات حقيقية مع مزود السحابة.

- أقرّت وزارة الاتصالات والتقانة في الجمهوريّة العربيّة السوريّة بالتعاون مع الإسكوا السياسة الوطنيّة للحوسبة السحابيّة في العام ٢٠٢٢ بهدف تسريع وتيرة اعتماد الحوسبة السحابيّة في القطاع العام؛ وتشجيع مزوّدي خدمات الاتصالات للاستثمار في الحوسبة السحابيّة في سورية؛ ووضع إطار تنظيمي لخدماتها في السوق المحليّة، وتوّفر خدمات تنافسيّة؛ وحماية المستخدم النهائيّ من خلال نماذج أمن معياريّة وتحفيز الإبداع والابتكار في مجال التحوّل الرقميّ، وبالتالي إيجاد بيئة آمنة للتطبيقات تضمن كفاءة الاستثمار في البنى التحتيّة المعلوماتيّة وتحقيق أهداف التحوّل الرقميّ. [27]

٤. <u>الاستنتاجات والتوصيات</u>

وفقًا لتحليل SLR وتصنيف التحديّات الأمنيّة نستنتج أنّه من الممّكن إيجاد حلول متكاملة لها، مثلاً التحديّات التنظيمية معاً، الأمر القابل للتطبيق من خلال إطار عمل متكامل يشمل حلول التحديّات الأمنيّة المتوافرة وأفضل الممارسات في هذا المجال. يمكن اعتبار الأمن السحابيّ نموذج مسؤولية مشتركة يُظهِر لكلّ من مزوّد الخدمة السحابيّة والعميل مسؤوليات الأمن الخاصة بهما، بحيث يعتمد التقسيم الدقيق للمسؤوليات على نوع الخدمة المقدّمة، وأهميّة البيانات التي من المّمكن تشفير الأكثر أهمية منها باستخدام خوارزمية تشفير أكثر أمناً وأحجام مفاتيح أكبر. يمكن أيضاً العمل على ترحيل عمليات الأمن مثل إنشاء سياسات جدران الحماية وتوفير الشهادات وتوزيع المفاتيح والاختبارات إلى نموذج خدمة ذاتيّة بهدف التخلّص من نقاط اللمس البشريّة وتحقيق سيناريو الأمن كخدمة وتضمين عناصر التحكم في الأمن في التطبيقات السحابيّة. قد يضمن ذلك اتباع السياسات الأمنيّة للمؤسسات وإيقاف فقدان البيانات والتعرف على الاختراقات الأمنيّة والتعامل معها بهدف إيجاد بيئة آمنة للتطبيقات السحابيّة في القطاع الحكوميّ وهذا ما سنعمل عليه في الأبحاث القادمة.

٥. المراجع

1. TAERA, O. (2020). Proposing Cloud Security Framework Based On It Governance (Doctoral dissertation, ST. MARY'S UNIVERSITY).
2. Almarabeh, T., Majdalawi, Y. K., & Mohammad, H. (2016). Cloud computing of e-government. Communications and Network, *8*(01), 1-8.
3. Abd Al Ghaffar, H. T. A. N. (2020). Government cloud computing and national security. Review of Economics and Political Science,Emerald.
4. Abd Al Ghaffar, H. T. A. N. (2020). Government cloud computing and national security. Review of Economics and Political Science.
5. Assaf, A., IisHamsir, A. W., & Muhammad, M. (2021). Benefits and Risks of Cloud Computing in E-Government Tasks: A Systematic Review. In E3S Web of Conferences (Vol. 328, p. 04005). EDP Sciences.
6. Mall, S., & Saroj, S. K. (2018). A new security framework for cloud data. Procedia computer science.
7. Mohamed, M. A., Galal-Edeen, G. H., & Hassan, H. A. (2013, June). Towards Adoption of Government Enterprise Architecture: The Cases of Egypt and Syria. In Proc. 13th European Conference on eGovernment (ECEG 2013), Academic Conferences Limited (p. 345).
8. Mohammed, F., Ibrahim, O., Nilashi, M., & Alzurqa, E. (2017). Cloud computing adoption model for e-government implementation. Information Development, 33(3), 303-323.
9. Stieninger, M. et al. (2018). Factors influencing the organizational adoption of cloud computing: a survey among cloud workers. International Journal of Information Systems and Project Management.
10. Dekker, M. (2015). Security Framework for Governmental Clouds—ENISA.
11. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.
12. M'rhaoaurh, I., Okar, C., Namir, A., & Chafiq, N. (2018). Challenges of cloud computing use: A systematic literature review. In MATEC Web of Conferences (Vol. 200, p. 00007). EDP Sciences.
13. Sun, X. (2018, May). Critical security issues in cloud computing: a survey. In 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), (pp. 216-221). IEEE.
14. Verma, A., & Kaushal, S. (2011, July). Cloud computing security issues and challenges: a survey. In International Conference on Advances in Computing and Communications (pp. 445-454). Springer.
15. Wyld, D. C. (2010). The cloudy future of government IT: Cloud computing and the public sector around the world. International Journal of Web & Semantic Technology, 1(1), 1-20.
16. Agarwal, A., & Agarwal, A. (2011). The security risks associated with cloud computing. International Journal of Computer Applications in Engineering Sciences, 1(Special Issue on), 257-259.
17. Kumaraswamy, S. (2011). Introduction to Cloud Security Architecture from a Cloud Consumer's Perspective.
18. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of internet services and applications, 4(1), 1-13.

19. Alkhater, N., Walters, R., & Wills, G. (2014, November). An investigation of factors influencing an organisation's intention to adopt cloud computing. In International Conference on Information Society (pp. 337-338). IEEE.

20. Tawalbeh, L., Al-Qassas, R. S., Darwazeh, N. S., & Jararweh, Y. (2015). Secure and efficient cloud computing framework. In 2015 International Conference on Cloud and Autonomic Computing (pp. 291-295). IEEE.

21. Kumar, J. (2019). Cloud computing security issues and its challenges: a comprehensive research. Int. J. Recent Technol. Eng, 8(1), 10-14.

22. Burnham, K., (2023). 5 Things to Know about Cloud Security in 2023, http://buildbold*cloud*.com/.

23. Access to Cloud Computing: Challenges and Opportunities for Developing Countries, Study Period 2014-2017, International Telecommunication Union ITU.

24. Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. International Journal of Network Security & Its Applications, 6(1), 25.

25. Alassafi, M. O. (2018). A security model for cloud computing adoption in Saudi Arabian government organisations (Doctoral dissertation, University of Southampton).

26. Farag Frahat, F., & Tahon, A. H. (2019). A Proposed Framework for Security Aspects of Cloud Computing Services in Information Technology Companies. Egyptian Society journal for Information Systems and Computer Technology. 22, 5-11.

27. National Strategy for Cloud Computing in the Syrian Arab Republic (2022), Ministry of Communications and Technology, https://moct.gov.sy/.

28. Ahuja, S. P., & Komathukattil, D. (2012). A survey of the state of cloud security. Network and Communication Technologies, 1(2), 66.

29. Al Hadwer, A., Tavana, M., Gillis, D., & Rezania, D. (2021). A systematic review of organizational factors impacting cloud-based technology adoption using Technology-organization-environment framework. Internet of Things 15, 100407.

30. Ali, A. I. M. (2021). E-Governance System Challenges and Cloud Computing Benefits in E-Governance, technium science.

31. Ali, K. E., Mazen, S. A., & Hassanein, E. E. (2018). A proposed hybrid model for adopting cloud computing in e-government. Future Computing and Informatics Journal, 3(2), 286-295.

32. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information sciences, 305, 357-383.

33. Ali, O., & Osmanaj, V. (2020). The role of government regulations in the adoption of cloud computing: A case study of local government. Computer law & security review, 36, 105396.

34. Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly.

35. Ali, O., Shrestha, A., Osmanaj, V., & Muhammed, S. (2020). Cloud computing technology adoption: an evaluation of key factors in local governments. Information Technology & People.

36. Bisong, A., & Rahman, M. (2011). An overview of the security concerns in enterprise cloud computing. arXiv preprint arXiv:1101.5613.

37. Gill, S. H., Razzaq, M. A., Ahmad, M., Almansour, F. M., Haq, I. U., Jhanjhi, N., & Masud, M. (2022). Security and privacy aspects of cloud computing: a smart campus case study. Intell. Autom. Soft Comput, 31, 117-128.

38. Joshi, P. R., Islam, S., & Islam, S. (2017). A framework for cloud based e-government from the perspective of developing countries. Future Internet, 9(4), 80.

39. Abied, O., Ibrahim, O., & Kamal, S. N. I. M. (2022). Adoption of Cloud Computing in E-Government: A Systematic Literature Review. *Pertanika Journal of Science & Technology*, *30*(1).

40. Mohammed, F., Alzahrani, A. I., Alfarraj, O., & Ibrahim, O. (2017). Cloud computing fitness for e-government implementation: importance-performance analysis. IEEE access, 6, 1236-1248.

41. Mosa, A., El-Bakry, H., & AbuElkheir, M. (2015). Cloud computing in e-government: a survey. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 3(2).

42. Munir, K., & Palaniappan, S. (2013). Framework for secure cloud computing. Advanced International Journal on Cloud Computing: Services and Architecture (IJCCSA), 3(2), 21-35.

43. Odun-Ayo, I., Ajayi, O., & Misra, S. (2018). Cloud computing security: issues and developments.

44. Okoampa-Larbi, R., Twum, F., & Hayfron-Acquah, J. B. (2017). A Proposed Cloud Security Framework for Service Providers in Ghana. International Journal of Computer Applications, 975, 8887.

45. Pinheiro Junior, L., Alexandra Cunha, M., Janssen, M., & Matheus, R. (2020, June). Towards a framework for cloud computing use by governments: Leaders, followers and laggers. In The 21st Annual International Conference on Digital Government Research (pp. 155-163).

46. Schoo, P. et al. (2010, September). Challenges for cloud networking security. In International Conference on Mobile Networks and Management (pp. 298-313). Springer, Berlin, Heidelberg.

47. Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments. Procedia Engineering, 15, 2852-2856.

48. Tsochev, G. R., & Trifonov, R. I. (2022). Cloud computing security requirements: A Review. In IOP Conference Series: Materials Science and Engineering (Vol. 1216, No. 1, p. 012001). IOP Publishing.

49. Vu, K., Hartley, K., & Kankanhalli, A. (2020). Predictors of cloud computing adoption: A cross-country study. Telematics and Informatics, 52, 101426.

50. Youssef, A. E., & Alageel, M. (2012). A framework for secure cloud computing. International Journal of Computer Science Issues (IJCSI), 9(4), 487.

51. Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly, 28(2), 239-251.