مفهوم الحوسبة السحابية وخدمة التعافي من الكوارث

د. إسلام جمال صابر إبراهيم
مدرس بقسم علوم المعلومات
كلية الآداب – جامعة بني سويف
Gamaleslam685@art.bsu.edu.eg

المستخلص:

تهدف هذه الدراسة إلي التعرف علي الحوسبة السحابية من حيث مفهومها بالنسبة لتخصص الوثائق والأرشيف ونماذجها وطبقاتها بالإضافة إلي تناول تصنيفات الكوارث التي تصيب الوثائق الإلكترونية المخزنة بالسحابة مع طرح مواصفات خطة التعافي من الكوارث التي يجب توافرها ووصولاً إلي خدمة التعافي من الكوارث بالحوسبة السحابية، وتوصي الدراسة بضرورة تواصل اختصاصي الوثائق والأرشيف مع متخصصي تكنولوجيا المعلومات وغيرهم من المهنيين، وإنشاء شراكات جديدة ومن ثِم تطوير أدوار ومهام جديدة للإخصائيين والمتخصصين، ويجب أن تكون هناك مسؤولية مشتركة ومواجهة التحديات التي تواجه حفظ الوثائق والسجلات، والمساءلة الناشئة عن تقنيات المعلومات والاتصالات.

الكلمات المفتاحية: الحوسبة السحابية؛ السحابة؛ التعافي من الكوارث؛ اختصاصيو الوثائق والأرشيف

تاريخ استلام البحث: 2022/05/14 تاريخ إجازة البحث: 2022/06/01

تمهيد:

لقد أصبح اتساع نطاق الحوسبة السحابية يسير في تزايد يوماً بعد يوم؛ نظرًا لقدرتها على مشاركة الموارد الموزعة عالميًا، وتمكين المستفيدين من الوصول إلى الكثير من الخدمات عبر الإنترنت في جميع أنحاء العالم، كما تقوم أكبر شركات تكنولوجيا المعلومات بتطوير مراكز البيانات الخاصة بها في القارات الخمس لدعم الخدمات السحابية المختلفة.

وبالتزامن يتم اليوم في كل مؤسسة إنشاء قدر كبير من البيانات في تنسيق إلكتروني، وأصبحت هذه البيانات تتطلب الأمن لخدمات التخزين، وأصبحت قضايا النسخ الاحتياطي للبيانات لمواجهة الكوارث واستمرارية الأعمال، أساسية في الشبكات السحابية، لأن أهمية البيانات الرقمية وقيمتها الاجتماعية في ازدياد مستمر، وتتطلب كل مؤسسة خطة لاستمرارية العمل أو خطة لمواجهة الكوارث، والنسخ الاحتياطي للبيانات التي تقع ضمن قيود التكاليف مع تحقيق متطلبات الاسترداد المستهدفة، تواجه الكثير من الشركات والمؤسسات في منطقة الشرق الأوسط والعالم بأسره لخطر فقدان البيانات الرقمية، والتي تعتبر واحدة من أهم الأصول بالنسبة لأي شركة أو مؤسسة، ويعتبر فقدان تلك البيانات بمثابة كارثة فعلية إذا لم يكن هناك خطة محكمة لاستعادة النظام وتلك الخطة تسمى خطة التعافي من الكوارث (Disaster Recovery Plan, DRP) أو خطة استمرارية العمل (Business Continuity Plan, BCP)، والتي تعتبر بمثابة خطة تأمينيه لاستعادة البيانات والمعلومات مما يسمح للشركة أو المؤسسة بالعودة إلى نشاطها الطبيعي (Caraman, M. C; etal, 2012) (Bushey ,Jessica;etal, 2015)

مشكلة الدراسة:

يمثل استعادة النظام بعد الكوارث مشكلة تواجه منصات تكنولوجيا المعلومات، هذه المشكلة أكثر أهمية في الحوسبة السحابية لأن مقدمي الخدمة السحابية (CSPs) يتعين عليهم تقديم الخدمات لمستفيديهم، حتى لو كان مركز البيانات معطلاً بسبب حدوث كارثة أو اخطاء فنية.

ولعل أهم اسباب اختيار موضوع " خدمة التعافي من الكوارث بالحوسبة السحابية **" للدراسة والبحث ما يلي:-**

1. حداثة الموضوع، مما يتطلب إبراز أهمية تطبيقه في مجال الحفظ الوثائقي و الأرشيفي
2. محاولة لسد الفجوة الموجودة؛ نظراً لقلة الدراسات العربية المتخصصة في هذا المجال.

أهمية الدراسة:

عادةً ما يفضل المستفيد تخزين كمية كبيرة من الوثائق الإلكترونية المختلفة في الخدمات السحابية (السحابة)، ولسوء الحظ إذا كانت الخدمات السحابية (السحابة) تالفة؛ فسيؤدي ذلك إلى فقد جميع البيانات والوثائق، وبالتالي ينبغي أن تكون هناك بعض الآليات لاستعادة البيانات والوثائق الإلكترونية المختلفة المخزنة بالسحابة، وتوفير البيانات في وقت فشل الخدمات السحابية (السحابة) أو فقدان البيانات.

أهداف الدراسة:

و تهدف الدراسة إلى:-

1. التعرف علي خدمات الحوسبة السحابية بالنسبة للوثائق الإلكترونية.
2. تحليل المخاطر المتعلقة بإدارة الوثائق عند استخدام التخزين السحابي.
3. التعرف علي خدمة التعافي من الكوارث.

منهج الدراسة:

اعتمد الباحث في دراسته هذه علي المنهج الوصفي التحليلي، ومنهج دراسة الحالة للتخزين السحابي، كما استعان الباحث بأدوات البحث التي أمدته بالمعلومات وساعدت في تطبيق المناهج وهي الملاحظة، وتحليل المضمون.

تساؤلات الدراسة:

وقد حاولت الدراسة الإجابة علي التساؤلات الآتية:-

1. ماهية الحوسبة السحابية، وأنواع خدمات الحوسبة السحابية بالنسبة للوثائق الإلكترونية؟
2. ما أنواع مخاطر الحوسبة السحابية بالنسبة للأرشيفات؟
3. ماذا يقصد بخدمة التعافي من الكوارث؟

الدراسات السابقة:

لا توجد دراسات عربية مثيلة، ولكن توجد دراسات تعرضت للحوسبة السحابية من نواحٍ عدة دون التعرض لممارسات التعافي من الكوارث، ومن هذه النماذج ما يلي:

1. Duranti , Luciana ; Jansen , Adam. Records In The Cloud :Authenticity And Jurisdiction .- IEEE, 2013.

تتناول الدراسة القضايا المحيطة بمراقبة أصالة الوثائق الموجودة علي الحوسبة السحابية، وكانت نتائج الدراسة أن الاعتماد السريع علي تكنولوجيات الحوسبة السحابية كان في الغالب تدبيرا من تدابير توفير التكاليف، وأوصت الدراسة بضرورة صياغة عقود نموذجية تساعد مقدمي الخدمات السحابية والمستخدمين على حد سواء في تسوية المخاوف بشأن أصالة الوثائق التي تم إنشاؤها أو إدارتها أو تخزينها في السحابة .

2. Duranti , Luciana. Digital Records and Archives in the Commercial Cloud .- Cambridge, Mass.: The MIT Press, 2015.

وتتناول الدراسة القضايا الرئيسة المتعلقة بالحوسبة السحابية التجارية حتي تكون جديرة بالثقة بها، وكانت من نتائج الدراسة أن المعلومات الرقمية في نمو متزايد وتنتشر عبر منصات متعددة على الإنترنت، وتصبح غير قابلة للإدارة ويختار منتجوها ببساطة السماح لها بالتراكم، وبالتالي توصي الدراسة بضرورة وضع سياسة لتنظيمها مع ضمان حماية الامتياز القانوني أو الأسرار التجارية عند استخدام الطرف الثالث وعدم إتاحة الوثائق المخزنة له نتيجة لالتزامات التعاقدية بالإضافة إلي إجراء عمليات مراجعة للحسابات السحابية لضمان .

مفهوم الحوسبة السحابية من وجه نظر التخصص:-

يعرف الأرشيف القومي الأمريكي الحوسبة السحابية بأنها : تقنية تسمح للمستفيدين بالوصول إلى، واستخدام البيانات المشتركة، وخدمات الحوسبة عبر الإنترنت أو شبكة افتراضية خاصة، فهو يمنح المستفيدين إمكانية الوصول إلى الموارد دون الحاجة إلى إنشاء بنية أساسية لدعم هذه الموارد داخل بيئاتهم أو شبكاتهم الخاصة، و تتضمن التفسيرات العامة للحوسبة السحابية "تأجير" مساحة التخزين على خوادم هيئة أخرى أو استضافة مجموعة من الخدمات،

وتشير التفسيرات الأخرى للحوسبة السحابية إلى تطبيقات وسائل التواصل الاجتماعية خاصةً والبريد الإلكتروني المستند إلى السحابة وأنواع أخرى من تطبيقات الويب ***(David S, Ferriero, 2021)***.

أما تعريف مشروع انترابارس للحوسبة السحابية:.بأنها :خدمة أو مجموعة من الخدمات المقدمة عبر الإنترنت حسب الطلب من موقع بعيد بدلاً من الإقامة على سطح مكتب / كمبيوتر محمول أو خوادم الهيئة؛ وذلك من خلال تعاقد المؤسسات مع مقدم الخدمة لتقديم التخزين ومعالجة و / أو التطبيقات عبر الويب ***(The International Council On Archives "ICA", 2012)***.

وفي الو اقع أن مصطلح الحوسبة يعبر عن جميع الممارسات المتعلقة بتخزين المعلومات وتبادلها عبر الفضاء الإلكتروني؛ نتيجة التطور التكنولوجي والتقني و استخدام الانترنت بشكل واسع، **وبالتالي** فأن الحوسبة السحابية اعم واشمل من الخدمات؛ أي أن الحوسبة السحابية هي البنية التحتية من المعدات المادية والبرمجيات التي تقدم الخدمات السحابية.

نماذج نشر الحوسبة السحابية (Deployment Models):-

يمكن تقسيم الحوسبة السحابية من حيث تقديم الخدمة السحابية إلي أربعة أنواع رئيسة وهي:

أولاً السحابة الخاصة (Private Cloud): هي حوسبة سحابية من حيث المفهوم التقني، ولكنها ليست مفتوحة للعامة، وإنما مغلقة لعدد محدد من العملاء مثل حوسبة سحابية لبنك أو لجامعة او لحكومة ، ويتم تشغيل البنية التحتية السحابية فقط للهيئة وقد تتم إداراتها من جانب الهيئة أو طرف ثالث كما انها قد توجد داخل موقع الهيئة أو خارجة ***(عبد العزيز، أماني محمد، 2012)***، وتُعد السحابة الخاصة من أقل نماذج النشر خطورة ومن الممكن أن يحقق استخدام نموذج السحابة الخاصة ما يلي:-

- ضمان الثقة من خلال توفير السيطرة الكاملة علي سحابة المؤسسة الخاصة.
- أقصي درجات الرقابة علي البيانات والأمن وجودة الخدمة ومستوي عال من السيطرة علي الموارد؛ نظراً لامتلاك الشركة للبنية التحتية للسحابة.

- إيصال تطبيقات متدرجة واحتياجات عمل مختلفة لمن يحتاجها من المستفيدين.
- إدارة بنية مركز البيانات كحزمة واحدة من موارد الحوسبة الافتراضية(Telecommunication Standardization Sector Of Itu., 2014).

ثانياً السحابة العامة (Public Cloud) : ويطلق عليها أيضاً السحابة الخارجية (External Cloud)، وهي حوسبة سحابية متاحة لجميع من يريد الخدمة المقدمة علي شبكة الانترنت، وهي المنتشرة في وقتنا الحالي مثل خدمات (Google)، وتتم إتاحة البنية التحتية للحوسبة السحابية لجميع المستفيدين او مجموعة كبيرة منهم، وهي مملوكة للهيئة المسئولة عن الخدمات السحابية ***(Mell ;Grance , 2011)***، وقد تتولى ملكية الخدمات السحابية العامة و إدارتها وتشغيلها شركة تجارية أو مؤسسة أكاديمية أو هيئة حكومية أو مزيج منها، وتوجد هذه الخدمة في مقر مقدم الخدمات السحابية، والخدمة السحابية العامة حدودها واسعة للغاية، بحيث لا يواجه عميل الخدمة السحابية سوى قيود محدودة، إن وجدت لدى نفاذه إلى الخدمات السحابية العامة ويحقق استخدام السحابة العامة الفوائد التالية:-

-زيادة كفاءة وفاعلية العمل من خلال توفير موارد الحوسبة عبر الانترنت لأي مكان حسب الحاجة.
- خفض نسبة المخاطر عن طريق نقل مسئولية أمن البيانات إلي الشركات المضيفة Host Company.
- خفض تكلفة دعم تقنية المعلومات؛ نظراً لتوفر أحدث إصدارات البرمجيات؛ دون الحاجة إلي الدعم الداخلي لفريق تقنية المعلومات (Rabai;Jouini, 2015) .

ثالثاً (سحابة مجتمع ما أو مشاركة) (Community Cloud) : هي حوسبة سحابية تكون الخدمات مقتصرة علي مؤسسات أو شركات لها نفس الهدف من الخدمة، حيث تكون هناك مؤسستان أو أكثر لها نفس الهدف، وتسعي لتحقيقه من خلال الحوسبة السحابية، وتشترك هذه الشركات في النفقات والمصروفات مقابل توفير أمن المعلومات بشكل كبير مثل : الخدمات السحابية التي تقدمها شركات الاتصالات للمؤسسات و الشركات، والبنوك التي تتصل مع شركات تحويل الأموال مثل وسترنيون(Westernuion) وهي شركة أوروبية لتحويل الأموال ولديها فروع في جميع أنحاء العالم، وتوجد بجميع محافظات جمهورية مصر العربية (Mell ;Grance , 2011).

وقد تكون البنية التحتية السحابية مشتركة بين الكثير من الهيئات، كما أنها تدعم مجتمعاً محدداً يتفق في اهتمامات مشتركة (مثل المهام أو الأهداف، ومتطلبات الأمن، والسياسة ...الخ)، وقد تتم الإدارة من جانب الهيئة أو طرف ثالث، كما أنها قد توجد داخل موقع الهيئة أو خارجه. وتقصر الخدمات السحابية بالسحابة المشاركة على مجموعة من عملاء الخدمات السحابية ممن لديهم مجموعة شواغل مشتركة، على عكس الطابع المنفتح للخدمات السحابية العامة، في حين تتميز الخدمات سحابة مجتمع ما؛ بقاعدة مشاركة أوسع من الخدمات السحابية الخاصة، وتشمل هذه الشواغل المشتركة، على سبيل المثال لا الحصر المهمة ومتطلبات أمن المعلومات والسياسات، والاعتبارات المتعلقة بلوائح العمل (Governance & Standards Division,2017).

رابعاً السحابة الهجينة (Hybrid Cloud) : وهي حوسبة سحابية تكون فيها الخدمات مقدمة من مقدمي الخدمة، وهي بين خصائص السحب العامة والخاصة؛ بحيث يستفيد العميل من خدمات السحابة الخاصة وهي ضمن سحابة عامة، كمواقع التسوق الضخمة مثل سوق امازون الإلكتروني .

وتكون البنية التحتية للحوسبة السحابية بمثابة تركيبة من اثنين أو أكثر من السحاب (الخاصة، أو المجتمعية، أو العامة) التي تظل بمثابة كيانات فريدة من نوعها، لكن يتم ربطها من خلال التكنولوجيا التي تساعد في إمكانية نقل البيانات والتطبيقات (مثل عمليات النقل لكي يتحقق التوازن بين انواع السحاب) (الاتحاد الدولي للاتصالات، 2017).

وقد ينشأ عن ذلك مخاطر بسبب دمج أكثر من نموذج للنشر، وهنا يقع على عاتق مستفيد السحابة مسؤولية تصنيف المعلومات ليتم تخزينها على نموذج النشر الخاص بها،

ويمكن أن تتولى الهيئة نفسها أو طرف ثالث ملكية الخدمة السحابية الهجين وإداراتها، وتشغيلها، وقد تكون موجودة في مقر العميل أو بعيداً عنه، وتمثل الخدمات السحابية الهجينة الحالات التي قد يلزم فيها التفاعل بين نموذجي نشر متمايزين، وإن ظلا مرتبطين بواسطة تكنولوجيات ملائمة، وبذلك تعكس الحدود التي تعيّنها الخدمة السحابية الهجين نموذجي النشر الأساسيين لها.

ويفيد هذا النوع المؤسسات التي لا ترغب في استخدام بيئة خارجية لتخزين البيانات الخاصة بها، حيث يمكن تخزين المعلومات الحساسة أو التي يكثر استخدامها في البنية التحتية الخاصة والبيانات الأقل حساسية في السحابة العامة (Bera, Sova Pal, 2016).

طبقات الحوسبة السحابية:-

توجد ثلاث طبقات أو مستويات أساسية، يمكن من خلالها تقديم الخدمات السحابية في جميع المجالات، وهي كالتالي:-

الطبقة الأولي البرمجيات كخدمة ((Software as a Service (Saas): المصطلح يعني تطبيق أو خدمة على الإنترنت، وهي تقنية تُمكن من الوصول إلى البرمجيات والقيام بوظائفها عن بعد، كخدمة مبنية على الويب، مما تحرر من عبء الإدارة المعقدة للبرمجيات والعتاد (إبراهيم، إسلام جمال صابر، 2021).

حينما نستعمل تطبيقاً معيناء (Application) فليس لدي المستفيد ان يتحكم في أي شيء له علاقة بهذا التطبيق؛ إلا أنه يستخدمه ويوظفه في أداء مهامه المختلفة، حيث تدار هذه الطبقة من قِبل مقدم الخدمة، ولتقريب هذا المعني نقول: عندما يستخدم أحدنا خدمة البريد الإلكتروني المتاحة من G-mail مثلاً، فإنه لا يملك ان يتحكم في نظام التشغيل القائم عليه هذا التطبيق، ولا في الخادم المعتمد عليه ، وكذلك الحال عند استخدام تطبيق وثائق جوجل Google Docs علي سبيل المثال؛ فإن العميل يستفيد من هذا التطبيق في كتابة وثائقه وحفظها؛ بصيغة الوورد أو الباوربوينت ...الخ، كما يمكنه رفع ملفاته الشخصية عبر هذا التطبيق، وكذلك تحميل ما كُتب من تلك الوثائق إلي حاسبه الآلي الشخصي، فضلاً عن إمكانية مشاركة هذه الوثائق، وتلك الملفات مع غيره من الزملاء والموظفين والإداريين؛ إلا أنه لا يملك التحكم في نظام التشغيل القائم عليه هذا التطبيق.

وفي هذه الطبقة يمكن للمؤسسة ان تستخدم برامج التطبيقات من خلال إحدى خدمات الاستضافة؛ مثل وثائق جوجل كما تقدم، ولكن لا يتاح لها أن تتعامل مع البني التحتية الاساسية كالشبكات والخوادم، ولن يسمح لها بإدارة البرامج ولا صيانتها، حيث تتولي شركات الاستضافة هذه المهام، كما تتميز بالتالي:-

- الوصول في الوقت الحقيقي، والتحديث من خلال الشبكة.
- واجهة المستفيد بالسحابة مماثلة لتلك الموجودة بسطح المكتب، والتي تتاح لعملاء الويب؛ بفضل تطبيقات الإنترنت الغنية (Rich Internet Applications) مثل فلاش Flash، جاكس Ajax أو جافا Java ...الخ.
- عدم الحاجة إلي قوي عاملة أو إدارة أو تحديثات للبرمجيات؛ نظراً لعدم تملك المستفيد للبرنامج.
- التكلفة تعتمد علي مستوي الاستخدام والمساحة الافتراضية، وبالرغم من أن الدفع حسب؛ الاستخدام الشهري أو شراء تراخيص؛ إلا أنها أرخص من شراء المؤسسة للتطبيق ذاته.
- نظراً لتشغيل هذه التطبيقات (وتخزين بياناتها عبر الانترنت) لم يعد المستفيدون بحاجة إلي القلق؛ بشأن إدارة ملفاتهم وحفظها ونسخها احتياطياً (Duranti,; Rogers ,2012) (InterPARES Trust Project, 2016).

ويتضح من هذا أن مستوي أو نموذج البرمجيات كخدمة يعد نموذجاً محدوداً مقيداً، يبدو فيه المستفيد محصوراً من جهة الانتفاع؛ بإمكانات التطبيقات البرمجية المعتمدة علي السحابة؛ دون التدخل في نظم تشغيلها أو معرفة الخوادم التي تخزن فيها بياناته بشكل مؤكد.

الطبقة الثانية المنصة كخدمة : Platform as a Service (PaaS) : هي خدمة أخري من خدمات السحابة قريبة الشبة بالبرمجيات كخدمة Saas، ولكنها مقدمة للمصممين والمطورين والمبرمجين التي يمكن من خلالها بناء قواعد بيانات لعمل المؤسسات، وتصميم مواقع خاصة بها، ولبناء وتشغيل التطبيقات القائمة علي الانترنت بدون تحميل أو تنصيب لأي نوع من أنواع البرمجيات، كما تتيح التحكم في التطبيقات التي تم نشرها؛ دون البنية التحتية الاساسية؛ بما في ذلك الشبكة والخوادم ونظم التشغيل أو التخزين، ومن أمثلتها منصة مطوري الشبكة الاجتماعية الفيس بوك Facebook Developers Platform، ومحرك تطبيقات Google Apps Engine، الذي يسمح للمستفيد ببناء التطبيقات؛ بغض النظر عن حجم التحميل، وكمية البيانات، ويدعم خدمة الويب الديناميكية، وتقنياتها وواجهة المستفيد، كما يوفر مساحة التخزين مع إمكانية إجراء عمليات الاستعلام Query، والفرز Sorting، وإرسال البريد الإلكتروني

E-mail باستخدام جوجل، ومنصة تشغيل Windows Azure، كبيئة لتطوير، وتشغيل تطبيقات ميكروسوفت، و Amazon Web services ، وتقدم المنصة كخدمة بيئة حوسبة متكاملة؛ بما في ذلك نظام التشغيل، وبيئة تنفيذ لغات البرمجة، وقواعد البيانات، وخوادم الويب؛ لتمكين مستفيد السحابة من تطوير، وتشغيل التطبيقات الخاصة به، ونشر تطبيقاته على البنية التحتية للسحابة، والتحكم بإعداداتها؛ دون أن يقوم المستفيد؛ بإدارة أو التحكم في البنية التحتية للسحابة، كما تختص المنصات (Platforms) بتحديث البرامج، وأدوات التشغيل (Telecommunication Standardization Sector Of Itu, 2014)) (خويلدات؛ حدادي ، 2016).

الطبقة الثالثة البنية التحتية كخدمة : (Infrastructure as a Service (IaaS : يتم توفير أجهزة الحاسب الآلي المادية أو الافتراضية والمصادر الأخرى مثل الشبكات، ووسائط التخزين من قِبل مقدم السحابة لدعم العمليات الخاصة؛ بمستفيد السحابة، حيث يكون المستفيد قادراً على نشر، وتشغيل بعض البرامج مثل أنظمة التشغيل والتطبيقات، ولا يقوم المستفيد؛ بإدارة، أو التحكم في البنية التحتية للسحابة، ولكن يمكنه التحكم في أنظمة التشغيل، والتخزين، والتطبيقات المنشورة، وربما سيطرة محدودة على بعض مكونات الشبكات (مثل الجدران النارية)، وبالتالي يعتمد هذا النموذج على توفير الأجهزة، والبنية التحتية، وبدلا من شراء الخوادم، والبرمجيات، والمساحات الخاصة؛ بمركز البيانات، يمكن دفع تكلفة استخدام هذه المصادر كخدمة مستقلة تماماً، ويتم وصف الخدمة عادة على أساس المنفعة الحوسبية، وكم المصادر المستخدمة، ومن أمثلة نموذج IAAS خدمات الأمازون Amazon web services، حيث يستضيف مواقع الانترنت، ويقدم لها الخدمات حسب طلب المستفيد سواء التخزين، أو الخدمات التفاعلية، وإعداد النسخ الاحتياطيةBackup ، وتأمين التعاملات على الموقع، وخصوصاً المالية، ويتماشى هذا كثيرا مع إدارة الوثائق الرقمية، وخدمات موقعPixlr ؛ لتعديل الصور، وإتاحتها، وتخزينها، كما يقوم موقعAvairy لتحرير الصوت والصورة وبه أرشيف صوتي، وموقعJaycut ؛ لإعداد وتحرير الأفلام، ووضع نصوص على الفيديو، و من أشهر خدمات الحوسبة السحابية المقدمة للأفراد هي تخزين البيانات على الإنترنت حيث تكون ملفات المستفيد، و صوره موجودة على السحابة، و يمكنه الوصول إليها من أي مكان، و كل ما تحتاجه اتصال إنترنت و شاشة، التي تتيح إمكانية تخزين الملفات و الصور، و أفضل مثال على ذلك ما

تقدمه شركة آبل(ICloud) من خلال خدمات النسخ الاحتياطي لجميع محتويات الجهاز، واستعادة البيانات و بث الصور.

ويتضح من ذلك أن البنية التحتية كخدمة تكفل هذه الطبقة للمستفيد عدداً أكثر من الامكانات والفرص، حيث يمكنه التحكم في برامج التطبيقات، ونظم التشغيل، والشبكات وخصوصية البيانات، وأمن المعلومات، عن طريق تثبيت برامج الحماية المعنية؛ بهذا الشأن، وبالإضافة إلى ذلك تميز بإعفاء هذه المؤسسات، والأفراد من عناء صيانة، و مراقبة مكونات البنية التحتية من خوادم، وحدات تخزين و شبكة (Hoefer; Sehgal; Bhatt, 2018)(karagiannis, 2021)) (العليمي، 2014).

التعافي من الكوارث (Disaster Recovery ,DR) :

تُعرف المنظمة الدولية للمعايير و المقاييس(ISO) التعافي من الكوارث بأنه: قدره عناصر تكنولوجيا المعلومات والاتصالات في الهيئة علي دعم وظائفها التجارية المهمة إلى مستوي مقبول في غضون فتره زمنية محدده سلفا بعد وقوع كارثة (International Organization for Standardization "ISO", 2017).

و يُعرف أيضاً التعافي من الكوارث بأنه : عمليات وسياسات وإجراءات تتعلق بالإعداد واسترداد واستمرار البنية التحتية للتكنولوجيا الحيوية لعمل المؤسسة بعد وقوع كارثة طبيعية أو من صنع الإنسان كالهجمات السيبرانية، ويُعد التعافي من الكوارث قسماً فرعياً من مخطط استمرارية العمل، حيث أن استمرارية العمل تتناول التخطيط لحفظ جميع جوانب أداء الأعمال في خضم الأحداث التخريبية، وبالتالي فإن التعافي من الكوارث يركز فقط على أنظمة تكنولوجيا المعلومات، و التكنولوجيا التي تدعم وظائف العمل، وتمثل خطة التعافي من الكوارث الجيدة في استعادة النظام عند انقطاع الاتصال بالمواقع الأساسية من خلال مواقع النسخ الاحتياطي في نفس توقيت انقطاع الاتصال بمواقع التخزين الاساسية .

أما خطة التعافي من الكوارث فتُعرف في تكنولوجيا المعلومات : بأنها العمليات والسياسات والإجراءات المتعلقة بالتحضير لاستعادة أو استمرار البنية التحتية للتكنولوجيا ذات الأهمية الحاسمة للهيئة (Amazon Web Services "AWS", 2019).

و تزود خطة التعافي من الكوارث نظم تقنية المعلومات بالتوفر التام و حماية البيانات بدون تكبد نفقات البنية التحتية للموقع المادي الثاني، فهي توفر خاصية تجاوز الفشل بالنظام السحابي، وهذه الخاصية تحمي الأعمال من التوقف، وبالإضافة إلى ذلك فإنها تقدم ميزة لوحة تحكم لمراقبة الوقت الحقيقي للتكرار بين الموقع الأساسي والهدف (Alhazmi, O. H ; Malaiya, Y. K, 2012)؛ فما هي الكوارث التي تصيب الوثائق المخزنة بالسحابة ؟

تصنيف الكوارث التي تصيب الوثائق المخزنة بالسحابة:-

تُصنف الكوارث إلى فئتين رئيستين، وهما:

أولاً: الكوارث الطبيعية : مثل الفيضانات، الأعاصير و الزلازل، ومن الصعب جدا منع وقوع الكوارث الطبيعية، ويمكن اتخاذ تدابير مثل التخطيط الجيد الذي يتضمن تدابير لتخفيف أو تجنب وقوع الخسائر، ولا يمكن للمرء التعرف على فقدان البيانات عند حدوث كارثة.

ثانياً: الكوارث البشرية: من صنع الإنسان وتشمل فشل في البنية التحتية والإرهاب الإلكتروني أحد الكوارث التي يصنعها الإنسان والتي يمكن أن تتم لأسباب كثيرة، في هذه الحالة ستكون حماية البيانات المهمة واستعادتها هدفًا رئيساً في خطط التعافي من الكوارث (DRP) بجانب استعادة النظام، و الكوارث البشرية هي :

- **فشل الشبكة** (Network Failure): يتم ربط السحابة والعملاء عن طريق شبكة الإنترنت، وعندما تفشل الشبكة يتم تعطل الأنظمة المتصلة بالسحابة وبالتالي سيتم فقد البيانات، و من ثِم تعاني التطبيقات التي تعمل على السحابة.
- **اقتحام الشبكة** (Network Intrusion) : عندما يتم غزو فيروس للتطبيقات السحابية، فهناك فرصة لحدوث كارثة، من خلال وضع تطبيقات غير صالحة للاستعمال، و يمكن منع حدوث مثل هذه الكوارث من خلال وضع قائمة للمراقبة لمثل هذه التطبيقات الخبيثة.
- **القرصنة أو الاكواد الخبيثة** (Hacking or Malicious Codes): تحدث الكوارث داخل أو خارج الهيئة على الرغم من أنها تمنع القرصنة أو التعليمات البرمجية الضارة من تعديل البيانات إلا أنه يحدث فقد للبيانات.

- **فشل النظام** (System Failure): إذا فشلت البنية التحتية في الهيئة، فسوف تتعطل الأنظمة بالكامل المتصلة في هذه الهيئة، وسوف يؤثر ذلك على أنظمة التشغيل (McLelland,Robert ;etal, 2014).

أهداف خطة التعافي من الكوارث:-

الغرض من تقنية استعادة النظام (خطة التعافي من الكوارث) هو مساعدة المستفيد على جمع المعلومات من أي خادم نسخ احتياطي عندما يفقد الخادم بياناته ولا يستطيع توفير البيانات للمستفيد، و تهدف خطة التعافي من الكوارث للنظام الأساسي إلى مواجهة ثلاثة تحديات:

- استعادة الخدمة.
- تقليل فقد البيانات اثناء انقطاع أو تعطيل الشبكة.
- اكتشاف الفشل (Alhazmi, O. H; Malaiya, Y. K, 2013) .

أهمية خطة التعافي من الكوارث:-

تأتي خطة التعافي من الكوارث عندما يتم تنفيذ إجراء تجاوز الفشل للتبديل تلقائيًا إلى موقع النسخ الاحتياطي، و يصبح الموقع النشط الحالي غير متاح، وفي حالة حدوث كارثة يستبعد إجراء تجاوز الفشل للموارد المعطلة، ويعيد توجيه أحمال العمل إلى موقع ثانوي باستخدام مقياس تحميل متخصص، وتأتي أهميتها علي الأخص في :

- الإتاحة التامة : توفر خدمة التعافي من الكوارث خوادم متصلة على مدار الساعة وتطبيقات تجاوز الفشل بدون انقطاع العمليات التقنية من خلال الرجوع لمراكز بيانات الاتصالات المتكاملة لموقع للكوارث.
- **حماية البيانات:** توفر الخدمة الحماية القصوى للبيانات والوثائق المهمة وتخزينها في مراكز البيانات الخاصة، حيث يمكن استرجاعها في أي وقت.
- **نقل البيانات :**تُمكن خدمة من نقل البيانات والتطبيقات بكل سهولة إلى المنظومة السحابية للاتصالات المتكاملة.

- **القدرة**: تأمين الموارد بطريقة كافية لتوسيع نطاقها حسب الحاجة.
- **الأمن**: توفير الأمن المادي لحماية الأصول.
- **البنية الأساسية للشبكة**: بما في ذلك مكونات البرنامج مثل جدران الحماية وموازنات التحميل.
- **الدعم**: إتاحة الفنيين المهرة لأداء أعمال الصيانة، ومعالجة المشكلات.
- **عرض النطاق الترددي**: تخطيط عرض النطاق الترددي المناسب لتحميل الذروة.
- **المرافق**: ضمان البنية التحتية المادية بما في ذلك المعدات والطاقة (Google Cloud, 2021).

متطلبات خطة التعافي من الكوارث:-

قام الاتحاد الأوروبي (European Union,EU) بالضغط علي شركات مقدمي الخدمة السحابية بضرورة وجود خطة لتعافي من الكوارث بالشركات، ثم قامت المنظمة الدولية للمعايير والمقاييس (ISO) بالإسراع في إصدار معيار (ISO/ 19086) ونص المعيار علي ضرورة وجود خطة لتعافي من الكوارث(Bushey ,Jessica ;etal , 2015)، وحددت منظمة الأيزو (ISO)، بعض المتطلبات لتطبيق استراتيجية قوية خاصة بخدمات استمرارية الأعمال والتعافي من الكوارث، من المؤكد أن تحديد العمليات المهمة وأعباء العمل بما يُمكن من الحفاظ على تشغيل وظائف الأعمال المهمة، والتي تمثل الخطوات الأكثر أهمية في هذا الصدد، لابد أن يتطلب تحديد متطلبات خطة التعافي من الكوارث والتي تتمثل في:-

- **زمن التعافي المستهدف** (Recovery Time Objective, RTO) :ويسمي أيضاً بـ هدف وقت التعافي أو هدف وقت استعادة النظام وهو الوقت اللازم لاستعادة النظام إلى مستوى مقبول، وهو اقصى وقت مسموح به لإعادة تشغيل الخدمة أو العملية بعد حدوث الانقطاع، ويُعد زمن التعافي المستهدف (RTO) مقياسًا مقبولًا على نطاق واسع لعملية استعادة النظام المطلوبة إلا أنه يستند بشكل أساسي إلى متطلبات العمل، حيث قد تختلف هذه المتطلبات اختلافًا كبيرًا، لأن بعض الهيئات يمكنها تحمل ساعات من العمليات المفقودة بينما قد يكون البعض الآخر أقل بكثير، ويُعد ذلك مقياساً للوقت

الذي يمكن أن يتحمله للعودة إلى النظام عند حدوث كارثة، وقد تكون دقائق أو ساعات أو أيام، و يشمل أيضًا اكتشاف الأعطال وإعداد الخوادم المطلوبة لمواقع النسخ الاحتياطي لاستخدامها عند انقطاع الخدمة عن المواقع الاساسية، كما يحدد هدف وقت استعادة النظام مقدار التوقف المقبول عند وقوع كارثة وتوقف المواقع الاساسية عن العمل، ولابد أن يتم تحديد هذه القيمة كجزء من اتفاقية مستوى الخدمة (SLA) .

- **نقطة التعافي المستهدفة** (Recovery Point Objective, RPO): وتسمي أيضاً بـ هدف نقطة استعادة النظام، وهي الحد الاقصى المسموح للبيانات التي قد تفقد عند استعادة الخدمة بعد حدوث انقطاع، وتمثل نقطة استعادة النظام المستهدفة الميزة الرئيسة للخدمات السحابية في توفر الخدمة عند حدوث كارثة.

ويتم احتساب نقطة استعادة النظام المستهدفة (RPO) :عن طريق تحديد الحد الأقصى للبيانات المفقودة خلال فترة زمنية محددة في حالة توقف الخدمة عند حدوث كارثة، وتُعد نقطة استعادة النظام المستهدفة (RPO) ضرورية وقرارًا عامًا للأعمال بالنسبة لبعض الهيئات، حيث لا تسمح بعض الهيئات على الإطلاق بفقدان أي بيانات، أي أن نقطة استعادة النظام المستهدفة تساوي صفر (RPO = 0)، ويتطلب ذلك استخدام النسخ المتماثل المتزامن المستمر، بينما بالنسبة للهيئات الأخرى قد يتراوح فقدان البيانات المقبول من بضع ثوانٍ إلى ساعات أو حتى أيام، وعادةً ما تخضع نقطة الاسترجاع المستهدفة (RPO) للطريقة التي تحفظ بها والنسخ الاحتياطي للبيانات، ولابد أن يتم تحديد هذه القيمة كجزء من اتفاقية مستوى الخدمة (SLA).

ويختلف هذا المقياس استنادًا إلى طرق استخدام البيانات، ويمكن أن تحتوي بيانات المستفيد التي يتم تعديلها بشكل متكرر على نقطة استعادة النظام المستهدفة (RPO) بعد بضع دقائق، وفي المقابل يمكن أن يكون للبيانات الأقل أهمية والمعدلة بشكل متكرر معدل عائد مؤقت لعدة ساعات (يصف هذا المقياس طول الفترة الزمنية فقط ولا يتناول مقدار أو جودة البيانات المفقودة) (International Organization for Standardization "ISO",2017) .

ويتضح من ذلك أن خدمات استمرارية الأعمال والتعافي من الكوارث توفر حلاً يقوم من خلاله مقدم الخدمة بإدارة متطلبات التعافي من الكوارث في مؤسسة ما، حيث يضمن من خلال الاتفاق مع المؤسسة توفير نسخ احتياطية وإجراءات استعادة البيانات وتوفير الأدلة والمواجهات

واستعادة النظام في حالات الكوارث، وذلك بموجب اتفاقيات مستوى الخدمة (SLAs)، وبعد هذه الخطوات يمكن تطوير خطة لخدمات استمرارية الأعمال والتعافي من الكوارث واختبارها في بيئة المحاكاة بالشركات السحابية (Public Records Office Victoria, 2012).

التخطيط للتعافي الكوارث:-

قامت بعض شركات مقدمي خدمات السحابة (CPS) بإصدار بعض الآليات التي يتم تنفيذها لضمان النسخ الاحتياطي للبيانات عند استخدام تقنية استعادة النظام بعد عطل فادح، وعند الرغبة في عمل نسخة احتياطية من البيانات، ويمكن اتباع بعض الآليات لضمان النسخ الاحتياطي للبيانات من المصادر التالية:

- التعاقد مع الشركات المتخصصة في تقديم خدمات التعافي من الكوارث.
- اتفاقية متبادلة مع مؤسسة أخرى لتبادل مرافق مركز البيانات في حالة وقوع كارثة (Microsoft Azure , 2021).

وبالتالي قامت شركات عالمية بإصدار خدمة التعافي من الكوارث علي النحو التالي :

التعافي من الكوارث كخدمة (Disaster Recovery As A Service):-

التعافي من الكوارث كخدمة (DRaaS) تم الترويج لها من قِبل مقدمي الخدمات السحابية، وهي خدمة مقدمة لإدارة دعم الفشل في حالة وقوع كارثة، وتقوم بعمل نسخة احتياطية، وإمكانية تشغيل التطبيقات على الخدمة المقدمة من خلال استعادة النظام بعد عطل فادح من خلال نسخة احتياطية للموقع الأساسي، كما تقوم خدمة التعافي من الكوارث من تكرار الخوادم الأساسية، والبنية التحتية لمركز البيانات في السحابة.

وتصرح شركات مقدمي الخدمات السحابية بانها خدمة منخفضة التكلفة بالمقارنة مع خدمة التعافي من الكوارث التقليدية، وتتميز بالمرونة في التكرار ماديا أو عمليا، كما توفر الخدمة استعادة التطبيقات العاملة مثل خادم SQL، ولديها خيارات مسبقة لبيئات الاستعادة الافتراضية بما في ذلك الأمن والاتصال بالشبكة وفشل الخادم عند النسخ المتماثل باستمرار بين الخوادم، وتأتي بنية التعافي من الكوارث كخدمة (DRaaS) بثلاثة نماذج، وهي:

- من السحابة (From Cloud): عندما يكون التطبيق أو البيانات الأساسية في السحابة، ويكون موقع النسخ الاحتياطي أو استعادة النظام من مركز بيانات خاص.
- في السحابة (In cloud): عندما يكون كلاً من الموقع الأساسي وموقع الاستعادة في السحابة.
- إلى سحابة (To cloud): عندما يكون التطبيق في مركز البيانات الأساسي، ويكون موقع النسخ الاحتياطي أو استعادة النظام في السحابة، لاختبار عمليات استعادة النظام يتم استخدام صناديق الحماية، ويتم اختبارها؛ دون تعطيل تشغيل التطبيق، ويتم الوصول إليها من قِبل مسؤولي النظام فقط.

والتعافي من الكوارث كخدمة (DRaaS) عبارة عن خدمات معبأة مسبقًا توفر حلولاً لبيئة قياسية سحابية يمكن شراؤها لكل استخدام؛ بمعدلات متفاوتة استنادًا إلى نقطة التعافي المستهدفة (RPO)، وزمن استعادة النظام (التعافي) المستهدف (RTO)، وعادةً ما تكون قيم RTO و RPO أصغر (أي يجب أن يتعافى التطبيق بشكل أسرع عند المقاطعة)، وكلما تكون القيمة أصغر كلما كثرت التكلفة (National Archives And Records Administration ,2021).

وأصبحت هناك شركات تقدم هذه الخدمة كما تستعين بها الشركات المقدمة لخدمة الحوسبة السحابية، مثل شركة Transdev وشركة Malibu Boats، وشركة CGS وشركة Ward ,Greg, Cassandra Backup (2018)

سياسة وضع خطة التعافي من الكوارث:-

تتكون سياسة وضع خطة لمواجهة الكوارث والتعافي منها، من الآتي:-

- عند صياغة خطة التعافي السريع وبناءها، يجب أن تقوم الهيئة أو المؤسسة بتحليل للسيناريوهات ومعالجة مختلف أنواع سيناريوهات الطوارئ الأخرى مثل حالات انقطاع الخدمة عن النظام الرئيس التي قد تنتج عن أخطاء في النظام أو خلل في الأجهزة أو أخطاء تشغيلية أو حوادث أمنية.
- قد تتصاعد التأثيرات الناتجة عن حوادث تقنية المعلومات إذا تم التعامل معها بطريقة غير ملائمة إلى مواقف لها تأثيرات كبيرة على عمليات الهيئة ومستفيديها، ويجب أن تقوم

الهيئة بتقييم خطة التعافي وإجراءات الاستجابة للحوادث مرة كل سنة على الأقل، وتحديثها عندما تحدث تغييرات في العمليات والأنظمة وشبكات الأعمال.

- لتعزيز إجراءات التعافي المتعلقة بالأعطال واسعة النطاق والمخاطر، ينبغي على الهيئة تنفيذ عمليات النسخ الاحتياطي، والقدرة على التعافي السريع على مستوى النظام الفردي أو على مستوى المجموعات، ويجب الأخذ بعين الاعتبار الترابط بين الأنظمة الحساسة في رسم خطة التعافي وإجراء اختبارات الطوارئ (Khoshkholghi , etal , 2014)(Olivieri ,Anthony , 2019)
- يجب على الهيئة تحديد أولويات تعافي النظام، واستئناف الأعمال، ووضع أهداف التعافي والاستعادة المحددة؛ بما في ذلك موضوعية زمن الاسترجاع المستهدف (RTO) لأنظمة وتطبيقات تقنية المعلومات، وهي المدة الزمنية من نقطة الانقطاع، والتي يجب استعادة النظام خلالها، بالإضافة إلي نقطة التعافي المستهدفة (RPO)، والتي تمثل مقدار مقبول من البيانات المفقودة لنظام تقنية المعلومات في حالة حدوث كارثة (ARMA International, 2022) .
- يجب على الهيئة إجراء عمليات التعافي في موقع منفصل جغرافياً عن الموقع الأساسي حتى يمكن استعادة الأنظمة الحساسة، واستئناف العمليات التجارية في حالة حدوث عطل في الموقع الأساسي.
- تعتمد سرعة التعافي المطلوبة على مدى أهمية استئناف العمليات التشغيلية، ونوع الخدمات، وما إذا كانت هناك طرقاً بديلة، ووسائل معالجة للحفاظ على استمرارية وتقديم الخدمة الكافية، وقد ترغب الهيئة في التعرف علي الاستراتيجيات والتقنيات لتعزيز قدرة التعافي لديها.
- تعتمد المرونة والقوة في النظم الحيوية التي يتم إسنادها إلى مقدمي الخدمة السحابية الخارجيين بدرجة كبيرة على استقرار وتوافر روابط الشبكة العابرة للحدود، لتقليل التأثير على العمليات التشغيلية في حالة حدوث كوارث على سبيل المثال(حدوث زلزال).
- يجب على الهيئة التأكد من تركيز عمليات الشبكة العابرة للحدود، مع استراتيجيات أخرى مثل مشاركة مقدمي خدمة الشبكة المختلفة، ومسارات الشبكة البديلة التي يتم تأسيسها للتعافي من

الكوارث (Ryan, James, 2014)(*Official website of the Department of Homeland Security, 2022)* (Computer Business Research, 2022)

الخاتمة:

أولاً النتائج :

تناولت الدراسة خدمة التعافي من الكوارث بالحوسبة السحابية، وقد توصلت الدراسة إلي النتائج التالية: -

- أصبحت الأرشيفات تستفيد من طبقات الحوسبة السحابية الثلاث وهي طبقة البرمجيات (SaaS) وطبقة المنصة (PaaS) وطبقة البنية التحتية (IaaS).
- تعتبر فكرة الخدمة السحابية الأرشيفية جذابة للغاية؛ نظرًا لحقيقة أن منشئي الوثائق والسجلات عادة ما يكونون من المؤسسات غير الأرشيفية والتي قد تفتقر إلى البنية الأساسية والقدرات التقنية ومعرفة الموظفين الكافية للحفاظ على الوثائق والسجلات الموقعة إلكترونيًا على المدى الطويل.
- يجب على الهيئات تحديد العواقب المحتملة التي يمكن أن تسبب الكوارث وتقييم تأثيرها.
- يجب أن يصل كلا من "هدف نقطة التعافي" "وهدف زمن التعافي" إلى الصفر تقريبا خلال دقائق معدودة.
- يجب أن تتميز خدمة التعافي من الكوارث بمعايير عالمية خاصةً معيار الأيزو ISO 19086.

التوصيات:

بعد استعراض نتائج الدراسة توصي الدراسة بالآتي:

- يجب أن يتعلم اختصاصيو الوثائق والأرشيف التواصل مع متخصصي تكنولوجيا المعلومات وغيرهم من المهنيين، وإنشاء شراكات جديدة ومن ثِم تطوير أدوار ومهام جديدة للإخصائيين والمتخصصين، يجب أن تكون هناك مسؤولية مشتركة، ومواجهة التحديات التي تواجه حفظ الوثائق والسجلات والمساءلة الناشئة عن تقنيات المعلومات والاتصالات.

- أثناء انقطاع الخدمة عن النظام، يجب على الهيئة الامتناع عن اعتماد تدابير التعافي غير المجدية، وغير المجربة على إجراءات التعافي المحددة مسبقاً، والتي تم التدرب عليها والموافقة عليها من قِبل الإدارة، تنطوي تدابير التعافي المخصصة على مخاطر تشغيلية عالية حيث لم يتم التحقق من فعاليتها من خلال الاختبارات الصارمة والتحقق من صحتها.
- يجب على الهيئة الاختبار والتحقق على الأقل سنوياً من فعالية متطلبات التعافي، وقدرة الموظفين على تنفيذ إجراءات الطوارئ والتعافي الضرورية.
- يجب تغطية سيناريوهات مختلفة، بما في ذلك إيقاف التشغيل الكلي أو تعطل الموقع الرئيس بالإضافة إلى فشل مكونات النظام الفردي أو على مستوى المجموعات، في اختبارات التعافي بعد الكوارث.
- يجب على الهيئة اختبار عمليات التعافي من خلال الاعتماد على الأنظمة المختلفة، وينبغي إجراء اختبار التعافي الثنائي أو متعدد الأطراف حيث ترتبط الشبكات والأنظمة بمقدمي خدمات ومقدمين محددين.
- يجب على الهيئة إشراك مستفيدي الأعمال في تصميم وتنفيذ حالات اختبار شاملة، للتحقق من أن الأنظمة المتعافية تعمل بشكل صحيح، ويجب مشاركة الأنظمة الموجودة في الخارج في اختبارات التعافي بعد الكوارث التي يجريها مقدمو الخدمة.

قائمة المراجع :

1. إبراهيم، إسلام جمال صابر. الحوسبة السحابية للوثائق الإلكترونية من واقع مشروع انتربارس (INTERpares) أطروحة دكتوراة .- قسم المكتبات والوثائق وتقنية المعلومات : كلية الآداب، جامعة القاهرة، 2021، ص13-15.
2. الاتحاد الدولي للاتصالات.(2017). النفاذ إلى الحوسبة السحابية :تحديات وفرص للبلدان النامية. مكتب تنمية الاتصالات، ص10.
3. خويلدات، صالح؛ حدادي، عبد اللطيف. (2016). دور تطبيقات الحوسبة الرقمية المبتكرة في تحسين أداء الموارد البشرية في المؤسسة التطبيق السحابي (GOTOmeetin) لإدارة الاجتماعات نموذجا).- الجزائر: مجلة الاجتهاد للدراسات القانونية والاقتصادية، ع10، ديسمبر 2016، ص 238-239.
4. عبد العزيز، أماني محمد.(2012). مسارات الوثائق الرقمية :موضوعات في الحفظ الرقمي.- البحث الدولي المعني بالوثائق الصحيحة الدائمة في مشروع النظم الإلكترونية (Interpares) .- مسودة، يونيو، 2012، ص14-15.
5. العليمي، ثروت العليمي المرسي. (2014). سبل الإفادة من تطبيقات الحوسبة السحابية في تقديم خدمات المعلومات بدولة الإمارات العربية المتحدة، ص6.

المراجع الأجنبية :

6. Alhazmi, O. H ; Malaiya, Y. K.(2012). "*Assessing Disaster Recovery Alternatives: On-site, Colocation or Cloud*".- IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW), pg 19-20.
7. Alhazmi, O. H; Malaiya, Y. K.(2013)." *Evaluating disaster recovery plans using the cloud. Reliability and Maintainability Symposium (RAMS*)".- IEEE Proceedings-Annual, pg 1-6.
8. Amazon Web Services (AWS).(2019). Affordable Enterprise-Grade Disaster Recovery Using AWS: White Paper .- Cloud Endure Ltd,pg1-6.

9. ARMA International. Generally Accepted Recordkeeping Principles.- available at " http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles" last visited 3/1/2022.

10. Bera, Sova Pal.(2016). "*Cloud Computing In Brief* ".- IOSR Journal Of Computer Engineering (IOSR-JCE) , Volume 18, Issue 6, Ver. V (Nov.-Dec. 2016), Pg 101.

11. Bushey ,Jessica ;etal .(2015) Trust in Cloud Service Contracts .- InterPARES Trust Project, v1.0 ,pg 8-10

12. Bushey ,Jessica;etal.(2015). " Cloud Service Contracts: An Issue of Trust / Les contrats de" . pg 128-153.

13. Caraman, M. C; etal.(2012). Continuous Disaster Tolerance in the IaaS clouds.- 13th IEEE International Conference on Optimization of Electrical and Electronic Equipment (OPTIM), pg 1226-1232.

14. Computer Business Research. Disaster recovery. Available at : "http://www.computerbusinessresearch.com/Home/enterprise-architecture/disaster-recovery " last visited 2/4/2022.

15. Computer Business Research. Disaster recovery. Available at : "http://www.computerbusinessresearch.com/Home/enterprise-architecture/disaster-recovery " last visited 2/1/2022.

16. David S, Ferriero. Guidance on Managing Records in Cloud Computing Environments.- available at :" https://www.archives.gov/records-mgmt/bulletins/ 2010/2010-05.html " last visited 20/12/2021.

17. Duranti ,Luciana ; Rogers, Corinne.(2012). Trust In Digital Records: An Increasingly Cloudy Legal Area.- Computer Law & Security Review 2 8 , Pg 529.

18. Google Cloud . Google Cloud Platform Terms of Service.- available at :" https://cloud.google.com/terms/" last visited 5/11/2021.
19. Governance & Standards Division.(2017). Cloud Governance Framework :Governance & Standard Division,Pg9-10.
20. Hoefer,c.; karagiannis, G. taxonomy of cloud computing services.- available at (http://doc.utwente.nl/75374/1/1569336959.pdf) ,last visited 3/8/2021.
21. International Organization for Standardization (ISO).(2017). ISO/IEC 19086-3: Information technology — Cloud computing — Service level agreement (SLA) framework — Part 3: Core conformance requirements.- ISO/IEC,pg 11-15.
22. International Organization for Standardization (ISO).(2017). ISO/IEC 19086-3: Information technology — Cloud computing — Service level agreement (SLA) framework — Part 3: Core conformance requirements ,pg 11-15.
23. InterPARES Trust Project.(2016). 10-Contract Terms with Cloud Service Providers.-,pg9.
24. Khoshkholghi, Mohammad Ali; etal .(2014). Disaster Recovery in Cloud Computing: A Survey.- Computer and Information Science; Vol. 7, No. 4; 2014,pg 1-16.
25. McLelland,Robert ;etal.(2014). "*Agreements between Cloud Service Providers and their Clients: A Review of Contract Terms*" ,pg1-13.
26. Mell, Peter ;Grance ,Timothy .(2011). The NIST Definition Of Cloud Computing.- Recommendations Of The National Institute Of Standards And Technology, September 2011,Pg3.

27. Mell, Peter ;Grance ,Timothy .(2011). The NIST Definition Of Cloud Computing.- Recommendations Of The National Institute Of Standards And Technology, September 2011,Pg3.

28. Microsoft Azure . Disaster recovery .- available at :" https://azure.microsoft.com/en-us/solutions/disaster-recovery/#references" last visited 14/11/2021.

29. National Archives And Records Administration. Government Of The United States Of America. Frequently Asked Questions About Managing Federal Records In Cloud Computing Environments .- available at : " Http://Www.Archives.Gov/Records-Mgmt/Faqs/Cloud.Html" last visited 25/10/2021.

30. *Official website of the Department of Homeland Security. Business Continuity Plan.- available at :"* https://www.ready.gov/business-continuity-plan " last visited 2/1/2022.

31. Olivieri ,Anthony .(2019).Azure Government for State & Local Government: Driving Innovation in State & Local Government.- Microsoft Azure,pg 1-2.

32. Public Records Office Victoria.(2012). Cloud Computing: Implications for Records Management .- Australia: State of Victoria, V.1.0, pg 9-17.

33. Rabai ,Latifa Ben Arfa;Jouini ,Mouna .(2015). Design Challenges Of Cloud Computing.- IGI Global..Pg 12.

34. Ryan, James.(2014). "*The Uncertain Future: Privacy and Security in Cloud Computing*".- Santa Clara Law Review 54, no. 2 , pg 497-525.

35. Sehgal ,Naresh Kuma; Bhatt, Pramod Chandra .(2018). Cloud Computing :Concepts and Practices.- Switzerland: Springer ,pg 2.

36. Telecommunication Standardization Sector Of Itu.(2014). Information Technology – Cloud Computing – Overview And Vocabulary.- Series Y: Global Information Infrastructure, Internet Protocol Aspects And Next-Generation Networks Cloud Computing, Recommendation Itu-T Y.3500 ,Pg6-7.

37. Telecommunication Standardization Sector Of Itu.(2014). Information Technology – Cloud Computing – Overview And Vocabulary.- Series Y: Global Information Infrastructure, Internet Protocol Aspects And Next-Generation Networks Cloud Computing, Recommendation Itu-T Y.3500 ,pg 12.

38. The International Council On Archives (ICA) ; International Research On Permanent Authentic Records In Electronic Systems Project (Interpares).(2012) . Digital Records Pathways: Topics In Digital Preservation: Module 8 Cloud Computing Primer ,DRAFT ,July 2012, Pg 8.

39. Ward ,Greg .(2018). Top Manufacturer Of Performance Sports Boats Recovers From It Disaster Within Minutes .- Malibu Boats; Cloudendure Ltd, Pg 1-2.

Arab International Journal of Information Technology & Data
Vol. 2, No. 4 October - December 2022

Cloud computing concept and disaster recovery service

Eslam Gamal Saber Ibrahim
Department of Information Sciences
Faculty of Arts - -Beni Suef University – Egypt
Gamaleslam685@art.bsu.edu.eg

Abstract:

This study aims to identify cloud computing and its concept in relation to records and archives specialists ,and its models and layers, in addition to addressing the classifications of disasters that affect electronic records stored in the cloud, with the presentation of the specifications of the disaster recovery plan that must be available in order to reach the disaster recovery service in cloud computing, and this study recommends the necessity of The records and archive specialist communicates with information technology specialists and other professionals, and establishes new partnerships, and then develops new roles and tasks for specialists and specialists, and accountability arising from information and communication technologies.

Keywords:

Cloud computing; The Cloud; Disaster Recovery; Records and Archive Specialists