التخزين الآمن للبيانات على الحوسبة السحابية

دراسة تقييمية

د.ناصرأبوزيد محجوب الكشكى

مدرس علوم المكتبات والمعلومات

كليه الآداب_ جامعة سوهاج

المستخلص:

تعد الحوسبة السحابية شكلًا جديداً من التقنية التي تشتمل على خدمات البنية التحتية، وتطوير المنصة أو المضيف، وتوفير البرمجيات، وتقديم التسهيلات للعملاء. وتكتسب هذه الدراسة أهميتها بما يوفره هذا النوع من الحوسبة لمؤسسات المعلومات من حلول خارجية، وخيارات إستراتيجية، يمكن الاعتماد عليها في تنمية هذه المؤسسات وتطويرها. وتسعى هذه الدراسة إلى تحليل المخاوف الأمنية المختلفة التي تعيق الشركات والمكتبات من تبني الحوسبة السحابية، ووضع آلية أو طريقة لتامين البيانات على الحوسبة السحابية، عن طريق تعرُّف المشكلات التى تقف فى طريقها.

الكلمات المفتاحية: *الحوسبة السحابية، مشاكل الحوسبة السحابية، التخزين الآمن للبيانات، حماية البيانات، قوانين حماية البيانات على الحوسبة السحابية.*

Abstract

Safe Storage of Data in Cloud Computing: An Evaluative Study

Cloud computing is a new form of technology which encompasses infrastructure services, platform and server development, provision of software applications and provision of facilities for users. Part of the significance of this study relates to the services and external and strategic solutions that cloud computing makes available for data and information agencies – solutions that can be drawn upon in developing and enhancing those agencies. The study seeks to investigate the different safety issues that hinder the use of cloud computing by companies, organizations and libraries. Based on an identification of obstacles facing cloud computing, the study also

seeks to develop a mechanism for protecting data stored or shared using cloud computing.

Keywords: *cloud computing – issues in cloud computing – safe storage of data – protection of data – data protection regulations for cloud computing*

الاستشهاد المرجعي:

الكشكي،ناصر أبو زيد محبوب(٢٠١٤).التخزين الآمن للبيانات على الحوسبة السحابية : دراسة تقييمية ـ **مجلة التعليم عن بعد والتعليم المفتوح**ـ اتحاد الجامعات العربية. كلية الآداب. جامعة بني سويف.ـ مج٢، ع ٢(يناير ـ مايو)ـ ص ص ٦١ : ١٣٣.

تمهيد :

الحوسبة السحابية شكل جديد من التقنية التي تشتمل على خدمات البنية التحتية، وتطوير المنصة أو المضيف، وتوفير البرمجيات، وتقديم التسهيلات للعملاء. وتعد هذه التقنية من أهم القضايا الساخنة فى الوقت الحالي؛ لما تطرحه من حلول وتحديات فى الوقت نفسه، ولما تقدمه من خدمات لتخزين البيانات بسهولة، وبكمية هائلة للمنظمات، وعلى الجانب الآخر يعد التخزين الآمن للبيانات التحدي الحقيقي لكل من الأفراد والمنظمات؛ حيث تتيح الحوسبة السحابية تخزين البيانات والحفاظ عليها على الخوادم البعيدة، التي تدار من قبل مقدمي الخدمات السحابية Cloud Service Providers (CSP) مثل Yahooو Google ، التى توفر خدمات الوصول السهل للبيانات من أي مكان عن طريق الإنترنت، مع انخفاض التكلفة، وتبادل البيانات بين جميع الأشخاص المعتمدين لديها، ولكن بعد كل ذلك، ينبغي على العملاء أن يثقوا بأن بياناتهم في يد آمنة؛ لذلك فهم بحاجة إلى وسيلة للتحقق من سلامة البيانات؛ للتأكد من أنه لا يوجد أي تعديل، أو يحدث أي فقدان للبيانات. وسعيًا لكسب الثقة بين العملاء ومقدمي الخدمة السحابية، ينبغي على مقدم الخدمة توفير التأمين اللازم لهذه البيانات، إضافة إلى ذلك إدارة الموارد السحابية بكفاءة؛ لتلبية

احتياجات المستخدمين، وتلبية التوقعات من جودة الخدمة Quality of Service (QoS)، مع المرونة وإضافة تطبيقات فى أية لحظة.

وتسعى هذه الدراسة إلى تحليل المخاوف الأمنية المختلفة التي تعيق الشركات والمكتبات من تبني الحوسبة السحابية، ووضع آلية أو طريقة لتأمين البيانات على الحوسبة السحابية.

مشكلة الدراسة:

الحوسبة السحابية تكتسب شعبية؛ بسبب فعاليتها؛ من حيث التكلفة في تقديم الخدمة، وما توفره للمستخدم من راحة كبيرة، عن طريق تحريره من الحاجة لفهم تفاصيل التجهيز، لكن متطلبات أمنية معينة؛ مثل السرية والنزاهة وتوافر البيانات، هي المخاوف الأمنية الرئيسة في اعتماد السحابة. وعلى الرغم من قيام الشركات المقدمة لهذه الخدمة، بتشفير بيانات العملاء قبل أن تُخزّن، فإن أفضل تقنيات التشفير يمكن مهاجمتها، وتعد مشاكل الأمن والموثوقية هواجس وعوائق، تحول دون التوسع في استخدام هذه التقنية في تخزين البيانات، خصوصاً البيانات التي تكتسب صفة الأهمية، بالنسبة لمؤسساتها وللمستفيدين على حد سواء.

أهمية الدراسة وأهدافها:

تكتسب هذه الدراسة أهميتها؛ بما يوفره هذا النوع من الحوسبة لمؤسسات المعلومات من حلول خارجية، وخيارات إستراتيجية، يمكن الاعتماد عليها في تنمية هذه المؤسسات وتطويرها؛ حيث الإدراك والفهم الواعي للقضايا الأمنية، التي تحيط بعملية تخزين البيانات على السحب الحاسوبية، وكذلك سبل مواجهتها والتقليل من أخطارها؛ يعزز ذلك التوسع في استخدام هذه التقنية السحابية من قبل المكتبات ومؤسسات المعلومات؛ حيث لا يمكن الإفادة من الحوسبة السحابية بصورة عامة؛ بسبب الخطر الكامن في تسوية البيانات من النظم التي لا يمكن السيطرة عليها. وتحتاج هذه المنظمات إلى آليات، تتيح لهم استخدام الموارد السحابية، مع مستوى الضمانات المطلوبة لتلبية السرية والثقة، وتسعى الدراسة إلى تحقيق الأهداف الآتية:

- تعرُّف مفهوم الحوسبة السحابية، وخصائصها، وأنواعها.
- تعرف مدى أهمية الحوسبة السحابية في التخزين الآمن للمكتبات ومؤسسات المعلومات.
- تحديد أهم القضايا والتهديدات الأمنية للبيانات المخزنة على الحوسبة السحابية.

- تحليل الفجوة بين المعايير والحلول القائمة للتخزين الآمن للبيانات على الحوسبة السحابية.
- مناقشة عملية الحماية الأمنية للبيانات المخزنة على الحوسبة السحابية.

حدود الدراسة:

تناقش الدراسة موضوع أمن البيانات المخزنة، باستخدام تقنية الحوسبة السحابية، متناولًا القضايا الأمنية للبيانات، وتحدياتها، وسبل التغلب عليها، والتقليل من حدتها.

منهج الدراسة:

تتبع الدراسة المنهج الوصفي التحليلي، الذي يقوم على أساس تحديد خصائص الظاهرة، ووصف طبيعتها، ونوعية العلاقة بين متغيراتها، وأسبابها، واتجاهاتها. وبناء على ذلك، حُصرت الدراسات التي تناولت موضوع السحب الحاسوبية بوجه عام، والدراسات التي تناولت القضايا الأمنية للبيانات المخزنة على السحب الحاسوبية، وسبل حمايتها على وجه الخصوص.

مصطلحات الدراسة:

١-الحوسبة السحابية Cloud computingهي نموذج لمشاركة مجموعة من الموارد الحاسوبية (مثل: الشبكات و الخوادم ووسائط التخزين والتطبيقات والخدمات)، من أي مكان حسب الطلب [١]، أو هي المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة، والتي تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية؛ بهدف التيسير على المستخدم، وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية، كما تشمل قدرات معالجة برمجية وجدولة للمهام، والطباعة عن بعد، ويستطيع المستخدم عند اتصاله بالشبكة التحكم في هذه الموارد، عن طريق واجهة برمجية، بسيطة تُبَسِّطُ وتتجاهل الكثير من التفاصيل والعمليات الداخلية [٢].

٢-التخزين السحابي Cloud storage هو نموذج للتخزين على شبكة الإنترنت، عن طريقه تُخزّن البيانات على خوادم ظاهرية متعددة، بدلًا من استضافتها على خادم محدد، وتكون عادة مقدمة من قبل شركات الاستضافة التي تمتلك مراكز بيانات متقدمة، تقوم بتأجير مساحات خزن سحابية لعملائها، بما يتواءم مع احتياجاتهم [٣].

الدراسات السابقة

في ضوء مراجعة أدبيات موضوع الدراسة في المصادر المطبوعة العربية والأجنبية المتاحة، وقواعد البيانات المتخصصة في مجال المكتبات والمعلومات، هذا بجانب البحث في عدد من محركات البحث، تبين قلة الدراسات العربية فى هذا الموضوع، واكتفاؤها بعرض التعريفات للحوسبة السحابية، ولم يقع الباحث على أية دراسة عربية، تناولت موضع أمن البيانات على الحوسبة السحابية، إضافة إلى قلة في الدراسات الأجنبية فى هذا الموضوع. ونعرض لأهم الدراسات المناظرة أو ذات العلاقة بموضوع الدراسة.

أولاً: الدراسات العربية:

تناولت دراسة رحاب فايز[٤] مفهوم السحب الحاسوبية وتطبيقاتها، كما تناولت إيجابيتها وسلبياتها، وأهم نظم الحوسبة السحابية مفتوحة المصدر، ثم عقدت مقارنة بينها للوقوف على جوانب الاتفاق والاختلاف؛ حيث استخدمت الدراسة لتحقيق أهدافها ثلاثة مناهج:

أولها: المنهج التاريخي؛ للوصف والتسجيل للأحداث التي مرت بها الحوسبة السحابية والمصدر المفتوح،

ثانيها: منهج تحليل النظم؛ لدراسة نظم الحوسبة السحابية مفتوحة المصدر بنظرة شاملة؛ لمعرفة علاقة النظم ببعض.

ثالثها: المنهج المقارن؛ للمقارنة بين نظم الحوسبة السحابية مفتوحة المصدر؛ للوصول إلى الفروق بين النظم.

ومن أبرز النتائج التي توصلت إليها الدراسة، أن نظام Eucalyptus يوفر منصة برامج سحب واسعة الانتشار لمنظمات تكنولوجيا المعلومات والأعمال التجارية التكنولوجية للبنية التحتية كخدمة. وأوصت الدراسة بالتنبيه إلى أن الحوسبة السحابية، مازالت في مراحلها الأولى، وتحتاج إلى أبحاث ودراسات علمية وأكاديمية، تتناول تحديد تعريف لها واستخداماتها المحتملة، كذلك تكثيف الجهود البحثية بين المجتمعات البحثية؛ لتطوير النظم السحابية الفعالة، واختبار كفاءتها.

تناولت دراسة شريهان نشأت المنيري(٥) : مفهوم الحوسبة السحابية وبنيتها التحتية، والعلاقة بين البنية التحتية لتكنولوجيا المعلومات والحوسبة السحابية، كما تناولت هذه الدراسة العملية الإدارية للسحب الحاسوبية، والإيجابيات والسلبيات الناجمة عن استخدام هذه التقنية الجديدة.

وتوصلت الدراسة إلى أن الحوسبة السحابية، من المتوقع أن تحدث ثورة جديدة في العالم قريباً في مجالات مختلفة؛ أهمها المجال التكنولوجي والاقتصادي، مع مؤشرات تدخلها في المجال السياسي أيضاً، وخاصة بعد الإشارة إلى احتمالية أن تصبح هذه

التكنولوجيا الحديثة، الدعامة التكنولوجية الرئيسة في نظام التصويت الإلكتروني الحديث؛ مما يحتم أن نفهم جيداً أبعاد هذه التكنولوجيا الحديثة، ومن هم القائمون عليها، ومخاطرها، وما يحيط بها من تهديدات أمنية؛ للاستعداد التام لاستخدامها، ومواجهة تحدياتها وسلبياتها، وعدم التسرع في استخدامها، دون الاستعداد لها جيداً.

تناولت دراسة أحمد أبوسعدة (٦) تقييم الحوسبة السحابية في مكتبات مصر العامة المطبقة بمختلف مستوياتها. وكذلك تعمل هذه الورقة البحثية على التقدم بمشروع، يشارك فيه الاتحاد العربي للمكتبات، والفهرس العربي الموحد، والحكومات العربية، ودورهم في بناء مجتمع المعرفة. واعتمدت الدراسة منهج دراسة الحالة؛ لتحقيق أهدافها، ورصد الخدمات المتاحة في مكتبات مصر العامة، التي تقدم عن طريق تقنية الحوسبة السحابية.

وتوصلت الدراسة إلى ضرورة تفعيل هذا النوع من التقنيات، في مجتمع المكتبات في العالم العربي، كفرصة لبناء مجتمع المعرفة العربي، كما أوصت بتفعيل الحوسبة السحابية على منظومة المكتبات المصرية، وغيرها من الدول لتقليل التكلفة.

تناولت دراسة نجلاء أحمد يس [٧] بعض القضايا الرئيسة المتعلقة بالحوسبة السحابية، واستخداماتها في المؤسسات الأكاديمية العربية وسحابة قطر نموذجًا، وانتهجت الدراسة منهجين لتحقيق أهدافها:

أولهما: المنهج الوصفي التحليلي، الذي يقوم على أساس تحديد خصائص الظاهرة، ووصف طبيعتها، ونوعية العلاقة بين متغيراتها وأسبابها واتجاهاتها،

ثانيهما: منهج دراسة الحالة الذي يقوم على أساس الاهتمام بحالة بعينها؛ وهي سحابة قطر.

وأبرز ما خلصت إليه الدراسة، أن السحابة نمط من أنماط الحوسبة القابلة للتطوير والمرونة، التي تعتمد على قدرات تقنية المعلومات والإنترنت، كما أن السحب الحاسوبية تمثل مستقبل تقنيات المعلومات للمؤسسات الأكاديمية، وتعد سحابة قطر الحاسوبية تجربة رائدة على المستوى العربي؛ لتطبيق فكر الحوسبة السحابية داخل المؤسسات الأكاديمية العربية.

تناولت دراسة محمد عبد الحميد معوض [٨] تعريف الحوسبة السحابية، وكيف أنها تختلف عن غيرها من أنواع الحوسبة، كما تتناول الورقة كيفية استخدام الحوسبة السحابية من قبل المكتبات، وكذلك المزايا والعيوب لتطبيق هذه التقنية في المكتبات، كما

تقدم شرحاً للمتطلبات التي يلزم النظر فيها، ودراستها قبل الانتقال إلى حلول الحوسبة السحابية، وتوصلت الدراسة إلى أن المكتبات لديها الفرصة لتحسين خدماتها، عن طريق استخدام هذه التقنية الحديثة؛ حيث إن الحوسبة السحابية يمكنها تحقيق فوائد عدة للمكتبات. وأوصت الدراسة بأن تكون المكتبات خالية من إدارة التكنولوجيا؛ حتى تتمكن من التركيز على بناء المجموعات، وتحسين الخدمات والابتكار.

ثانيًا الدراسات الأجنبية:

تناولت دراسة Savita Bhayal [٩] مفهوم الحوسبة السحابية، المستخدم على نطاق واسع من قبل الشركات ومنظمات الأعمال؛ حيث ركزت على تعزيز الإفادة من هذه التقنية الجديدة، عن طريق معالجة القضايا الأمنية التي تهدد البيانات المخزنة باستخدام الحوسبة السحابية، فعرضت لهذه الإشكاليات الأمنية، وانتهجت المنهج الوصفي التحليلي لتحقيق أهدافها، وانتهت إلى إمكانية استخدام تقنيات التشفير التقليدية لحماية هذه البيانات، وتعزيز الخدمات السحابية.

وتناولت دراسة Jyothi Kiran Reddy [١٠] التطور التاريخي للحوسبة السحابية؛ حيث ركزت على تحول الحوسبة الافتراضية إلى مستوي جديد، عن طريق تنفيذ بنية هجين، تجمع

بين الشبكة والحوسبة السحابية. واستخدمت هذه الدراسة المنهج التاريخي؛ لتحقيق أهدافها. وتوصلت إلى أهمية هذا النوع من البنية في الارتقاء بمستويات تقنية الحوسبة السحابية.

تناولت دراسة Ahmed Moneed Azab[١١] الحوسبة السحابية كنموذج جديد للحوسبة، وهدفت إلى التحقق من مدى فعاليتها في التوفير الاقتصادي للمستخدمين النهائيين؛ فاستخدمت المنهج التحليلي لتحقيق هذا الهدف، وتوصلت إلى موقف إيجابي لهذه التقنية تجاه الأبعاد الاقتصادية، ولكن بشروط؛ منها الحماية الأمنية للبيانات، وكان من أثر ذلك وجوب معالجة القضايا الأمنية التي تهدد الحوسبة السحابية، خصوصاً البيانات المخزنة عليها.

تناولت دراسة Pradnyesh Bhisikar [١٢] أمن البيانات، التي تخزن باستخدام الحوسبة السحابية، التي هي بالأساس نظم تخزين موزعة؛ حيث تناولت تأمين الطرق المتعددة لنقل البيانات بين الخوادم والمستفيدين، وانتهت الدراسة إلى اقتراح مخطط موزع، يتسم بالفعالية والمرونة لتأمين البيانات المخزنة وبيانات المستفيدين، وكذلك يحقق التكامل بين ضمان صحة البيانات وأخطاء الترجمة.

الحوسبة السحابية، النشأة والمفهوم:

الحوسبة السحابية نموذج متطور من البنية التحتية الافتراضية، التي توفر خدمات تكنولوجيا المعلومات والاتصالات المشتركة عن طريق الإنترنت، للكثيرمن المستخدمين الخارجيين، عن طريق استخدام الإنترنت أو شبكات خاصة واسعة النطاق، وتوفر الحوسبة السحابية وصول المستخدم إلى جهاز حاسوب، والإفادة من الخدمات (تخزين أي التطبيقات والخوادم والبيانات)، دون الحاجة إلى فهم التقنية أو ملكيتها(١٣).

ويرتبط مصطلح "السحابة" بالانترنت؛ حيث يعتمد على مخطط السحابة الذي كان يستخدم سابقًا لتمثيل شبكات الهاتف والإنترنت، والحوسبة السحابية تقنية قوية يستعملها بتزايد كل من الأفراد والمؤسسات. وقد يطلق مصطلح الحوسبة السحابية علي أشياء مختلفة، ولكنها تعني بشكل عام استخدام مزود خدمة لتخزين البيانات الخاصة وإدارتها على الإنترنت، وتمتاز "الحوسبة السحابية" بسهولة مزامنة البيانات مع كثير من الأجهزة في أي مكان في العالم(١٤) .

ويعود ظهور مصطلح الحوسبة السحابية " Cloud Computing" إلى العام ١٩٩٧، في محاضرة للعالم "رامناث شيلابا" من جامعة تكساس، والتي اقترح فيها أهمية وجود "نمط

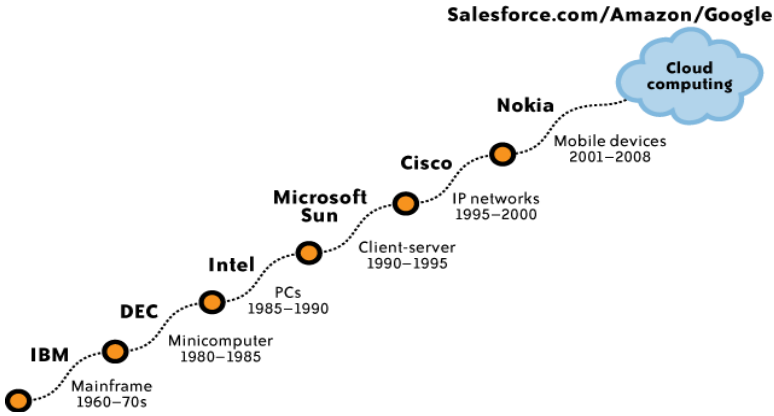
للحوسبة يحده المنطق الاقتصادي بدلًا من المنطق التقني بمفرده< وفي العام ١٩٩٩، حاول "مارك آندرسن" تسويق الحوسبة السحابية مع البنية التحتية كنموذج خدمة. وفي العام ٢٠٠٠، وسعت مايكروسوفت مفهوم البرمجيات كخدمة software-as-a-service" (SaaS):"، عن طريق تطوير خدمات الويب. وفي العام ٢٠٠١، قامت (ABM) بتطوير تقنيات متطورة للحوسبة؛ بغرض تحسين إدارة نظم تقنيات المعلومات المعقدة، وفي العام ٢٠٠٥، قامت "أمازون" باستخدام السحابة في بنيتها التحتية؛ مما أدى إلي توفير خصائص جديدة، تمتاز بالسرعة والسهولة.

وفي العام ٢٠٠٧، قام كل من "Google" (ABM)بمبادرة شراكة مع عدد من الجامعات على مستوى العالم؛ بهدف الدخول في مشروع بحثي كبير لتطوير الحوسبة السحابية.

وتمثل الحوسبة السحابية الثورة التقنية الثالثة بعد الحاسبات الآلية والإنترنتP حيث تعد تطوراً لتقنيات الحوسبة الموزعة "Distributed Computing"، والحوسبة المتوازية "Parallel Computing"، والحوسبة الشبكية " Grid Computing"، وقواعد البيانات الموزعة Distributed "Databases"، والحوسبة الأداتية "Utility Databases"[١٥].

وتعد الحوسبة السحابية والخدمات السحابية خطوة مهمة نحو تطور نماذج الحوسبة، وثورة في تقديم خدمات تكنولوجيا المعلومات، وفي الوقت نفسه تهدد_ حالياً_ وضعية تكنولوجيا المعلومات؛ حيث إنها في المراحل الأولى من التحول التقني، التي من شأنها فرض تغييرات في نهج أمن المعلومات وتطوير التطبيقات، وفى مفاهيم رأس المال ونفقات التشغيل، وفى حجم القوى العاملة ومهاراتهم، وما تتيحه من استئجار عشرات الخوادم، والتي تسلم إليهم بالكامل فى مجرد لحظات أمر يبعث على الدهشة، وبجزء ضئيل من التكلفة التقليدية هو ثورة. إن مجرد فعل الانتقال من الأنظمة القديمة يعطينا الأمل في أن نتمكن من استعادة السيطرة على الفجوات والقضايا [١٦].

وتعد تقنية الحوسبة السحابية آخر موجات عصر المعلومات، والتي بدأت مع أجهزة الحواسيب المركزية و تقدمت إلى متوسطة، والحواسيب الشخصية وهكذا. ونحن ندخل الآن أحدث موجات عصر المعلومات بالحوسبة السحابية. ويوضح الشكل الآتي الموجات الفرعية في عصر المعلومات [١٧]:



شكل رقم (١) يوضح الموجات الفرعية فى عصر المعلومات

و يستند تعريف الحوسبة السحابية إلى خمس سمات؛ هى:

١- الموارد المشتركة: على عكس النماذج الحاسوبية السابقة، والتي تقوم على الموارد المخصصة حتى تكون المرافق مخصصة لمستخدم واحد أو مالك بعينه، ولكن فى الحوسبة السحابية يعتمد على نموذج الأعمال؛ حيث تقسم الموارد، مما يعنى تعدد المستخدمين فى استخدام الموارد نفسها في الشبكة، وفى مستوى المضيف ومستوى التطبيق .

٢- السعة الهائلة: على الرغم من احتواء المنظمات على المئات أو الآلاف من النظم، توفر الحوسبة السحابية النطاق لهذه النظم، إضافة إلى القدرة على عرض النطاق الترددي على نطاق واسع، وتوفير مساحات التخزين .

٣- المرونة: حيث يمكن للمستخدمين، وبشكل سريع، تقليل موارد الحوسبة الخاصة بهم قدر حاجتهم، وكذلك التخلي عن الموارد غير المطلوبة لهم؛ لغرض استخدامات أخرى، إضافة إلى تعديل بياناتهم.

٤- الدفع حسب الطلب: حيث يسدد المستخدمون _فقط_ قيمة الموارد التي يستخدمونها فعلًا، وفقط في الوقت الذي تطلب منهم .

٥- -توفير الموارد الذاتية للمستخدمين، وتحريرهم من فهم هذه التقنية، وما توفره لهم من قدرات التجهيز، والبرمجيات، والتخزين. (١٨)

نموذج النظام (الأطراف المكونة لنظام الحوسبة السحابية):

تتكون بنية النظام الخاص بالحوسبة السحابية من أربعة كيانات، وهي:

- مالك البيانات: وهو _أيضًا_ مستخدم السحابة، ولديه كمية كبيرة من البيانات، يحتاج إلى تخزينها على السحابة.
- مستخدم السحابة: وهو الشخص المخول له الوصول إلى البيانات من قبل مالكها.

- خادم السحابة: الذي يدار من قبل مزودي الخدمات السحابية؛ لتقديم خدمات تخزين البيانات، وتبادلها، ومشاركتها، ولديه مساحة تخزين وموارد.
- المدقق (طرف ثالث): وهو كيان موثوق به في تقييم الأمان؛ بغرض التخزين على السحابة، نيابة عن مالك البيانات، ويعمل بناء على طلب المالك [١٩].

وتمر البيانات على الحوسبة السحابية بست مراحل؛ ففي **المرحلة الأولى:** يتقاسم الكثير من المستخدمين مراكز كبيرة قوية باستخدام محطات وهمية، وفي **المرحلة الثانية:** تُصبح الحواسب المكتبية القائمة بذاتها قوية بما فيه الكفاية؛ لتلبية معظم احتياجات المستخدمين، أما **المرحلة الثالثة:** فيتم فيها توصيل الحواسب المكتبية، والحواسب المحمولة والخوادم مع بعضها بعضًا، عن طريق الشبكات المحلية لمشاركة المصادر وزيادة الأداء، وفي **المرحلة الرابعة:** ربطت الشبكات المحلية بالشبكات المحلية الأخرى؛ لتشكيل شبكة عالمية مثل الإنترنت للإفادة من التطبيقات عن بعد والمصادر الأخرى، وفي **المرحلة الخامسة**، وفرت شبكة الحوسبة قوة حوسبة مشتركة ومساحة تخزين عن طريق نظام الحوسبة الموزع، أما **المرحلة السادسة:** فقد وفرت الحوسبة السحابية المزيد من

الموارد المشتركة على الإنترنت، بطريقة متدرجة وبسيطة. ويوضح الشكل الآتي هذه المراحل [٢٠]:

شكل رقم(٢) مراحل تخزين البيانات على الحوسبة السحابية

خصائص الحوسبة السحابية:

مثلما أحدثت الإنترنت ثورة وديمقراطية فى الوصول إلى المعلومات، فالحوسبة السحابية تفعل الشيء نفسه بالنسبة لتكنولوجيا المعلومات، عن طريق ما تقدمه من نقلة نوعية فى الموارد والخدمات؛ هذه النتائج مهمة لكل من مقدمي الخدمة والمستهلكين، وهى بذلك تمثل التوجه التقني الحديث في عالم الحاسوب وتقنيات المعلومات، ومن أهم خصائص الحوسبة السحابية:

١. ذاتية الخدمة حسب الطلب: حيث يستطيع المستخدم أن يستفيد من إمكانات السحابة الحاسوبية، في الزمان والمكان المناسبين له، دون الحاجة إلى العامل البشري.

٢. الوصول الشبكي واسع النطاق: حيث تمتلك السحابة الحاسوبية إمكانيات متاحة على شبكة الإنترنت، عن طريق معايير وآليات تعزز استخدام منصات المستخدم غير المتجانسة؛ كالهواتف المحمولة، وأقراص وأجهزة الكمبيوتر المحمولة، ومحطات العمل.

٣. تجميع الموارد ودمجها: حيث يعمل مزود الخدمة على تقديم خدمات إلى المستخدمين، عن طريق تجميع إمكانات مادية افتراضية ودمجها؛ منها ما هو مؤجر، ومنها ما يمتلكه.

٤. المرونة السريعة: حيث إن إمكانيات الحوسبة السحابية، يمكن الإفادة منها بشكل تلقائي، عن طريق قبول بعض الشروط، والالتزام بالطلبات.

٥. قياسية الخدمة: حيث إن نظم السحب تتحكم تلقائيًا، وتحدد الاستخدام الأمثل للموارد، عن طريق الإفادة من القدرة على القياس المجرد المناسب لنوع الخدمة؛ على سبيل المثال: التخزين والمعالجة وعرض النطاق الترددي، وحسابات المستخدمين النشطة والإبلاغ عنها [٢١].

٦. تقليل حجم المصروفات على البنية التحتية، والوصول للمعلومات والخدمات المطلوبة بشكل سهل.

٧. سرعة المعالجة الفائقة، عن طريق عدد قليل من الأشخاص القائمين على السحابة، عبر الوصول إلى خوادم فائقة السرعة .

٨. مرونة الوصول من أي مكان وفى أي زمان إلى السحابة، والإفادة من خدماتها.

٩. مرونة الاختيار والانتقال من مزود إلى مزود آخر دون ضرر.

١٠. تقليل تكلفة التدريب.

١١. الطاقة التخزينية غير المحدودة للسحب الحاسوبية، بالاعتماد على خوادم موزعة.

١٢. التحديث التقني المستمر للسحابة بوساطة مزود الخدمة؛ سواء كان ذلك في البنية التحتية، أو الخوادم، أو البرمجيات.

١٣. مرونة التكاملية بين الخدمات المختلفة للسحب الحاسوبية؛ مثل التعاقد في التخزين مع جهة، والبرمجيات مع جهة أخرى.

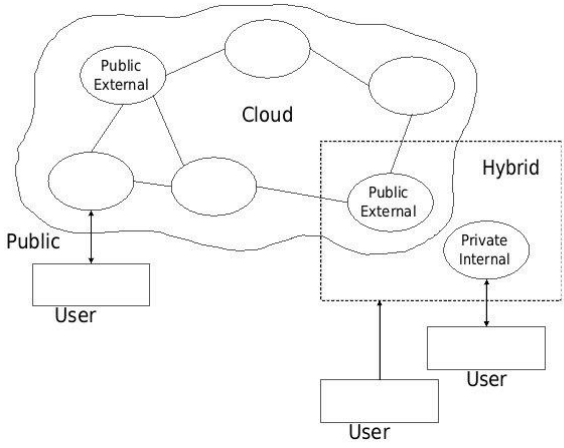
١٤. الأمن النسبي للبيانات المخزنة على السحب الحاسوبية؛ ففي حالة فقدان الأجهزة الشخصية الحاملة للبيانات أو تدميرها، تكون البيانات في مأمن.

١٥. معالجة المخاطر الطارئة؛ حيث انتقلت تلك المهمة لمزود الخدمة[٢٢].

أنواع الحوسبة السحابية:

يمكن أن نقسم الحوسبة السحابية، من حيث نوع الخدمة، على أربعة أنواع رئيسة : -

١. الحوسبة السحابية الخاصة(Private Cloud Computing)
٢. الحوسبة السحابية العامة(Public Cloud Computing)
٣. الحوسبة السحابية بالموبايل أو بالمشغل(Mobile Cloud Computing).
٤. الحوسبة السحابية الهجين (Hybrid Cloud Computing)



شكل رقم (٣) أنواع من الحوسبة السحابية

وفيما يلي توضيح موجز لهذه الأنواع :

١.الحوسبة السحابية الخاصة(Private Cloud Computing)

هي حوسبة سحابية من حيث المفهوم التقني، ولكنها ليست مفتوحة للعامة؛ وإنما مغلقة لعدد محدد من العملاء؛ مثل: حوسبة سحابية لبنك، وحوسبة سحابية لجامعة، وحوسبة سحابية لحكومة؛ حيث إن الحوسبة السحابية الخاصة _عادة_ تكون للمؤسسات الكبيرة ذات الخصوصية .

٢.الحوسبة السحابية العامة (Public Cloud Computing)

هي حوسبة سحابية متاحة للجميع لمن يريد الخدمة المقدمة، وهي في الواقع النموذج العام للحوسبة السحابية، وكل الميزات التي ذكرت في الحوسبة السحابية، وكل العيوب التي ذكرت في الحوسبة السحابية، تنطبق على هذا النوع من الحوسبة السحابية.

٣.الحوسبة السحابية بالموبايل أو بالمشغل(Mobile Cloud Computing)

هذه الحوسبة هي المتوقع تعميمها خلال الأعوام القليلة القادمة؛ حيث تقوم بالخدمة شركات الموبايل نفسها، التي تقدم خدمات المحادثات والإنترنت.

٤. الحوسبة السحابية الهجين(Hybrid Cloud Computing)

يمكن أن تكون هناك في مؤسسة واحدة حوسبة سحابية عامة أو بالموبايل، وحوسبة سحابية خاصة للتطبيقات الحساسة أو كتطبيق مساند، إذا لم تكن الثقة متوافرة من تجاه المؤسسة في الحوسبة السحابية العامة. وتعد الحوسبة السحابية الهجين أفضل المعالجات العملية؛ لتجاوز عيوب الحوسبة السحابية العامة آنفة الذكر؛ حيث يمكن للمؤسسة أو الشركة عمل حوسبة سحابية خاصة؛ كمساندة أو كتأمين إضافي للبيانات الحساسة، إذا تخوفت من الاعتماد الكلي على الخدمة العامة [٢٣].

الشركات التى تقدم خدمات الحوسبة السحابية:

معظم الشركات تقدم خدماتها بأجر، ولكن بعضها يقدم تطبيقات مجانية أو يسهم في ذلك، وفيما يلي أهم الشركات العاملة فى هذا المجال [٢٤]:

١- شركة "Verizon": وتمتلك الكثير من المخدمات. وقد استحوذت شركة Terremark الناشئة في مجال الحوسبة السحابية، بصفقة بلغت ١.٨ مليار دولار. و بذلك أصبحت من أفضل شركات الاتصالات التي تقدم خدمات الحوسبة السحابية، وتتحكم

بالبنية التحتية للحوسبة وموصلات الشبكات بين العميل/ المستخدم والسحابة.

٢- شركة "VMware" :لا تقدم خدمات السحاب بنفسها؛ إنما تصنع برامج؛ مثل "vcloud" الذي يستخدم لإنشاء السحابات. وباستخدام هذه التطبيقات يمكن لكل شركة بناء سحابتها الخاصة؛ مما يسمح لها بسهولة بنقل ضغط العمل بين محطات البيانات والسحابة. ويوجد حتى الآن أكثر من مئة سحابة خاصة، بنيت باستخدام"vcloud" .

٣- شركة "Linode" تتميز بأنها تبني سحابات بتكاليف ثابتة؛ وليس بقدر الاستخدام كما هو الحال في باقي الشركات؛ لذا يفضلها مستخدمو "لينوكس"؛ وتعد البديل المفضل لدى كل من يتخلى عن خدمات "أمازون".

٤- شركة "Salesforce.com"، وقد ارتبط اسمها بالسحابة، وقد كانت واحدة من أكثر السحابات شيوعاً، و يمكنها تشغيل التطبيقات المنزلية، وقد اشترت "Salesforce.com" شركة "Heroku"بمبلغ ٢١٢ مليون دولار وطورتها؛ لتتمكن بوساطة خدماتها، من عرض تطبيقات المبرمجين في السحابة بسهولة بالغة.

٥- شركة "Citrix Systems" تبنت تطبيقات السحابة، وتنافس بقوة شركات كبرى مثل "VMware" وغيرها، واشترت الشركة الناشئة "Cloud.com" وحققت منها أرباحًا تتجاوز 200 مليون دولار؛ مما دفعها للدخول بقوة إلى مجال تطبيقات السحاب مفتوح المصدر، الذي يمكن استخدامه لبناء السحاب، ومن بعدها قدمت تطبيقها مفتوح المصدر "Cloud Stack" إلى منظمة "Apache"، التي تدير عدة مشاريع شهيرة مفتوحة المصدر.

٦- شركة "Red Hat"التى تقدم سحابتها مجانًا، وتعد سحابة "OpenShift"من"Red Hat " اسم معروف بشكل واسع؛ وذلك لأن "أمازون" كانت تستخدمها في مشاريعها، وتتيح هذه السحابة بكل لسهولة لمحبي "لينوكس" إطلاق تطبيقاتهم عبر "أمازون"، وتقدم" Red Hat" برنامجها مجانًا؛ لتستعرض إمكانياتها التقنية التي يمكن أن تنافس"VMware" .

٧- شركة "Google" التي تعمل على عدة أصعدة في مجال الحوسبة السحابيةP فمثلًا محرك "Google App"يسمح للمطورين بتأسيس تطبيقاتهم؛ سواء بلغة "الجافا" أو "البايثون"، وتقدم هذا المحرك من أجل تشغيل "مايكروسوفت أوفيس" على السحاب مقابل أجور، وأصبحت خدمات "Google Cloud Storage" بديلًا تفضله الشركات عن "Amazon S3" لفترة طويلة من الوقت،

والآن أصبح هناك "Google Drive" الذي سينافس بقوة فى خدمات التخزين السحابي أيضًا، وتقدم "CloudPrint"للطباعة عبر السحاب بين أجهزة غير متصلة ببعضها بشكل مباشر بشبكة، إضافة إلى نظام التشغيل"ChromeOS" ، الذي تعمل عليه "جوجل"، والمتوقع أن يكون بالكامل مبنيًا على السحاب، بدلًا من تشغيل التطبيقات من القرص الصلب.

٨- شركة "Microsoft"، التي لم تدرك إلا مؤخرًا فكرة أن الحوسبة السحابية أصبحت جزءًا ضروريًا، تتجه إليه الشركات الكبرى، ولاحقًا الأفراد؛ لما له من مزايا مهمة، وأطلقت "Azure" وهي منصة سحابية، يمكن للمطورين أن يبرمجوا التطبيقات نفسها، التي تعمل على نظم تشغيل "ويندوز"، لتصير تعمل على السحاب، وتقدم منصة "Azure" خدمات الوسائط المتعددة، وبث الفيديو، وبأسعار منافسة.

٩- شركة "Rackspace" التى تقود ائتلاف ضخم لتطبيقات السحاب المجانية، وتستمد قوتها من تطبيق OpenStack المفتوح المصدر لإنشاء السحب. ويعد هذا التطبيق للحوسبة السحابية نظام "أندرويد" للهواتف المحمولة، وتعاونت مع "ناسا" بعدما اخترعت الأخيرة بعض تطبيقات السحاب الجيدة، و اليوم أكثر من ١٦٠ شركة تتعاون في برمجة OpenStack ليبقى مجانيًا.

١٠-شركة "Amazon" تعد أهم شركة تقنية في مجال السحاب. والمميز في هذه الشركة أنها تحافظ على روح الابتكار لديها؛ حيث إنها تعمل دوماً تعمل وكأنها شركة ناشئة في السوق، ودوماً تتطلع لخطوة نحو الأمام.

مشاكل الحوسبة السحابية:

١- **الاعتماد الكلى على الاتصالات والإنترنت:** قد يتعرض النظام أو تتعرض الخدمة لتوقف تامٍّ أو جزئيٍّ؛ بسبب مشاكل في الاتصالات أو الإنترنت.

٢- **الاعتماد الكلى على مقدم الخدمة:** لابد أن نتنبه إلى أننا أصبحنا نعتمد اعتماداً كليًا فى هذه الخدمة على طرف ثانٍ؛ فأنت أصبحت تُملَك ـــ على سبيل المثال ـــ معلوماتك الحساسة لطرف آخر.

٣- **الهجوم العدائي على البيانات:** إن وجود الخدمة في بيئة الإنترنت، يجعل هذه الخدمة معرضه للهجوم، بوساطة الهاكرز أو غيرهم؛ مما يعرض الخدمة؛ سواء كانت تخزين بيانات أو برمجيات أو غيرها، للاختراقات الأمنية.

٤- **ابتزاز مزود الخدمة:** قد يطلب مزود الخدمة، بعد الاعتماد الكلي عليه، زيادة في الأجر، أو تغييراً في التعاقد، أو مبالغ غير مناسبة على الصيانة أو التحسينات السنوية.

٥- **إهمال مقدم الخدمة:** قد لا يستجيب مقدم الخدمة لتساؤلات المستخدم، أو طلباته بالسرعة المطلوبة، أو قد يجيب إجابات ضعيفة على التساؤل.

٦- **الدراسة الدقيقة لاختيار مزود الخدمة :**هناك متطلبات علمية إضافية لمقارنة مزودي الخدمة، من حيث القدرات المهنية والكفاءة، ومن حيث الالتزام الأخلاقي. ومازال الكثير يفتقد الخبرة الكافية للقيام بهذا الدور؛ لحداثة تجارب الحوسبة السحابة.

٧- **ضعف التجارب القضائية في منازعات الحوسبة السحابة:** بسبب لحداثة تعاقدات الحوسبة السحابة ومشاكلها، فإن كثيراً من القضاة والمحامين، قد يتجنبون الحكم بالسرعة المطلوبة [٢٥].

الحوسبة الإلكترونية من منظور المكتبات:

الحوسبة السحابية Cloud Computing تقنية جديدة، تناسب التعامل مع المعلومات، وتلبي احتياجات مجتمع المعرفة، قد أعطي ظهورها الفرصة للمكتبات لتحقيق الاقتصاد في وظائفها، والتخفف من عبء التعامل مع الممارسات التقنية المعقدة، المرتبطة بإدارة الوصول إلى الدوريات الالكترونية، واستضافة المكتبة الرقمية ونظم المكتبة المتكاملة؛ حيث وفرت لها الابتعاد عن امتلاك الخادم وتشغيله والتطبيقات والتحول، عوضاً عن ذلك إلى الحصول على

وظائف مماثلة عبر شبكة الإنترنت، بطريقة أسرع من مثيلتها المحلية، دون الحاجة إلى القلق بشأن الإصدارات المناسبة من المنصات، أو البنية التحتية، أو تحديد المساحة المتوافرة على الخادم(٢٦).

ويرى الكثير من المكتبيين أن أخصائي المكتبات، قد أفادوا بالفعل من تطبيقات الحوسبة السحابية، ربما حتى قبل انتشار هذا المفهوم لدى مستخدمي الحاسب الآلي والإنترنت؛ فالكثير من المكتبات تعتمد علي برامج مثبتة علي خوادم بعيدة؛ للقيام بكافة العمليات المكتبية؛ من فهرسة، وتصنيف، وتقديم الخدمات للمستفيدين، بدون الحاجة لوجود تلك البرامج على الحاسبات الموجودة في المكتبة، إلا أننا هنا نحاول أن نتناول أهم التطبيقات الجديدة التي ظهرت بعد انتشار مفهوم الحوسبة السحابية، وما الخدمات التي يمكن أن تستفيد منها المكتبات؛ ومن أمثلة هذه الخدمات "Dura Cloud"، وهي خدمة استضافة، تركز بشكل رئيس علي تقديم خدماتها للمكتبات، وتستخدم هذه الخدمة حاسبات أو "سيرفرات" بعيدة خاصة بها لتقديم خدمات محلية للمكتبات المشتركة بالخدمة؛ مما يوفر على تلك المكتبات مصاريف صيانة الأجهزة الخاصة بها، وتركز هذه الخدمة علي تقديم خدمات حفظ المجموعات الرقمية والوصول إليها، ولا تقتصر علي ذلك فقط بل

أيضاً تتيح إمكانية مشاركة المجموعات التاريخية والإنسانية والعلمية المهمة مع المكتبات الأخرى، ويوجد الكثير من المكتبات التي تعتمد على هذه الخدمة [٢٧].

السحب الحاسوبية وتخزين البيانات Data Storage:

تساعد الحوسبة السحابية على التقليل من تهديدات حفظ البيانات الرقمية وتخزينها (النص الكامل أو التسجيلات الببليوجرافية أو البرامج التعليمية...)، ومنها: فشل المكونات، والتقادم، والأخطاء البشرية، والكوارث الطبيعية، والهجمات أو الأخطاء الإدارية، والحد من ارتفاع التكلفة؛ حيث تقوم المكتبة بالدفع مقابل مساحة التخزين التي تتطلبها البيانات المراد تخزينها بالسحابة [٢٨]. وفيما يلي نتناول قضايا تأمين البيانات المخزنة على السحب الحاسوبية:

أمن بيانات الحوسبة السحابية:

من أهم المشكلات التي تواجه هذه التقنية، مشكلة الأمان بالنسبة للبيانات المخزنة؛ حيث إن هذه التقنية تتيح للمستخدم الدخول إلى النظام والتعامل معه، مما يشكل تحدّيًا، يتعلق بعملية الحماية للملفات والبيانات الكائنة علي السحابة. ويثير موضوع أمن معلومات السحب الإلكترونية الكثير من الجدل؛ فهناك من يري أن المعلومات

لا تكون آمنة إلا عند إدارتها في شبكة داخلية، فى حين يرى آخرون أن السحب الإلكترونية تستطيع توفير الأمن اللازم؛ لضمان حفظ المعلومات وسلامتها.

ويمكن القول إن مشاكل أمن المعلومات في السحب الإلكترونية، تأتى من جهتين؛ هما: موفر الخدمة والعميل، لكن يعوّل على موفر الخدمة بشكل أكبر؛ حيث إنه هو الملزم بتوفير بنية تحتية قوية وأدوات ومستودعات تخزين آمنة [٢٩].

ويمكن تعريف أمن البيانات بأنه مجموعة واسعة من السياسات، والتقنيات، والضوابط لحماية البيانات المنتشرة، والتطبيقات، والبنية التحتية المرتبطة بها، والمكونة للحوسبة السحابية، أو بصورة أخرى هي تكامل واندماج أغلب مجالات أمن المعلومات؛ مثل: أمن الشبكات، وأمن الأنظمة، وأمن التطبيقات، وغيرها في مجال جديد، يعتمد كل جزء فيه على الجزء الآخر في تناغم تام. وتنقسم التحديات الأمنية المتعلقة بالحوسبة السحابية على قسمين؛ هما:

- المصاعب و التحديات الأمنية التي تواجه مزود خدمة الحوسبة السحابية.
- المصاعب و التحديات الأمنية التي تواجه مستخدم خدمة الحوسبة السحابية [٣٠].

وتمثل قضية الأمن النسبي لخدمات الحوسبة السحابية مسألة مستمرة، و قد تؤجل العمل بها؛ حيث تتمثل القضايا المعيقة لتبني الحوسبة السحابية بصورة أساسية، في القلق الذي يساور المستخدمين حول الإدارة الخارجية للخدمات القائمة على الأمن؛ فالسمة المسيطرة على الخدمات القائمة على الحوسبة السحابية، أنها تحفز الإدارة الخارجية للخدمات المتوفرة، مما يخلق حافزاً ضخماً بين مزودي خدمات الحوسبة السحابية، في خلق أولوية لبناء إدارة قوية للخدمات الآمنة وصيانتها.

وقد تأسّس الكثير من المنظمات؛ بهدف توفير المعايير اللازمة لمستقبل أفضل، في مجال تقديم خدمات الحوسبة السحابية. ومن تلك المنظمات ــ على سبيل المثال ــ "تحالف الأمن السحابي" (Cloud Security Alliance)، التي تعد منظمة غير ربحية، تأسست لتعزيز قضية استخدام أفضل الممارسات لتوفير الضمان الأمني ضمن مجال الحوسبة السحابية [٣١].

وتكمن أهمية الحوسبة السحابية في تمكين الشركات من الإفادة من مستويات غير معهودة من المرونة، على امتداد البنية التحتية للتقنية المعلوماتية، بيد أن هناك الكثير من التحديات الجدية التي تواجهها الشركات، بعد انتقالها إلى الحوسبة السحابية، هذا ما أكدته دراسة استطلاعية عالمية مهمة، أجرتها مؤخراً شركة

"ترينـد مايكرو"، المزود الرائد عالميًا بحلول لحماية بيئة الحوسبة السحابية؛ إذ أظهرت الدراسة ارتفاع عدد الشركات التي عانت مشكلات في أمن بياناتها المخزنة في السحابة، من 43% في العام 2011 إلى 46 % في العام 2012، واستطلعت الدراسة آراء 1400 من المديرين المعنيين باتخاذ القرارات المتصلة بالتقنية المعلوماتية، في الولايات المتحدة والمملكة المتحدة، وألمانيا، والهند، وكندا، واليابان، والبرازيل. وأظهرت الدراسة أن الشركات الهندية، واجهت أكبر عدد من مشكلات أمن المعلومات في بيئة الحوسبة السحابية، مقارنة بنظيراتها بالبلدان الأخرى؛ حيث وصلت النسبة عندها إلى (67%)، تلتها البرازيل (55 %)، كما تصدرت الشركات الهندية القائمة (12%) من حيث نسبة ازدياد حالات هفوات أمن المعلومات في بيئة الحوسبة السحابية في العام ٢٠١١، تلتها اليابان (7 %) ثم كندا (6 %). ووفقًا للدراسة الاستطلاعية الموسّعة، فإن اليابان هي الأقل نزوعًا نحو الانتقال إلى بيئة الحوسبة السحابية، مقارنة بالبلدان الأخرى التي شملتها الدراسة، كما أنها الأقل استخدامًا للبنية التحتية، لسطوح المكتب الافتراضية، وبيئة الحوسبة السحابية الخاصة والعامة.

وتشير أرقام المؤسسات الاستشارية العالمية إلى أن معدّل الانتقال الضعيف إلى بيئة الحوسبة السحابية، ارتفع عالميًا من 55% في العام 2011 إلى 59 % في العام 2012؛ الأمر الذي قد يفسر مخاوف أمن المعلومات التي أثارها المستطلعة آراؤهم، لاسيما في بلدين مثل الهند وكندا اللذين شهدا أكبر زيادة في معدّل الانتقال إلى بيئة الحوسبة السحابية؛ إذ ارتفع معدّل الانتقال إليها في الهند من 38 % في العام 2011 إلى 49 % في عام 2012، بينما ارتفع في كندا من 42% في عام 2011 إلى 51 % في العام ٢٠١٢. ومن أبرز نتائج الدراسة الاستطلاعية:

- أكثر من نصف (53 %) من صناع القرار المستطلعة آراؤهم، قالوا إن مخاوفهم إزاء أمن البيانات، هي ما يحول دون الانتقال إلى بيئة الحوسبة السحابية. ويتماشى ذلك مع قول 40 % من المستطلعة آراؤهم إن أيًا من مزوِّدي الخدمات السحابية الحاليين، لم يحقق لهم متطلباتهم بشأن أمن التقنية المعلوماتية بالشكل الأمثل.
- قال 53 % من المستطلَعة آراؤهم إنهم سيفكرون جدّيًا في الانتقال إلى بيئة الحوسبة السحابية، في حال اتخذ مزوِّدو الخدمة السحابية تدابير مباشرة بشأن أمن البيانات، أو في حال كانوا هم

أنفسهم على درايةٍ بكيفية حماية المعلومات المؤسسية المخزنة في بيئة الحوسبة السحابية[٣٢] .

عملية حماية البيانات:

وهذا العنصر يقوم على علاقة تشاركية بين المستخدم ومقدم الخدمة؛ حيث إن لكل منهم دوراً مهمًا جدًا فيها، فمن جهة المستخدم عند القيام بأي عملية يجب عليه التأكد من جودة اتصاله بالإنترنت، وأنه قام فعلًا بتخزين الملف على الشبكة، وأن معلومات حسابه لا يعلمها أحد سواه، ومن جهة مقدم الخدمة، فإنه يحرص دائمًا على حفظ معلومات المستخدم، وعدم تسريبها، أو تدميرها؛ ومن ثمة فقدانها. [٣٣]

كما أن حماية البيانات قضية أمنية حيوية بالنسبة لمعظم المنظمات؛ حيث تعد هذه القضية من العوامل الأساسية في اتخاذ قرار الانتقال إلي استخدام تقنية الحوسبة السحابية من عدمه؛ ومن ثمة يعمل مزودو الخدمة على توافر سياسة أمنية لحماية البيانات، وكذلك سياسة لآليات الإنقاذ. وهنا تتضمن العملية الأمنية الخاصة بالبيانات معظم التطبيقات والبيانات العابرة بين السحابة والمستخدم، التي يمكن بثها عبر الإنترنت أو عن طريق وسائل الإعلام المتنقلة، بالإضافة إلى البيانات التي تخزن على الخوادم الخاصة بمزودي الخدمة، والمتضمنة للمعلومات التعريفية أو هوية المستخدم

كنموذج الإدارة، وبيانات المراجعة الخاصة بالخدمة كنموذج المراجعة، والبيانات المؤقتة التي تنشأ خلال العملية التشغيلية، وغيرها من التطبيقات الأخرى.

الخدمات الأمنية:

تتضمن الخدمات الأساسية لتأمين البيانات وحمايتها، التأكد من (ضمان السرية والسلامة، والإتاحة: Confidentiality, Integrity and, Availability CIA) للبيانات؛ حيث أصبحت قضية أمن البيانات أكثر تعقيداً؛ بسبب الخصائص الجوهرية لتقنية الحوسبة السحابية. ويمكن تناول الخدمات الأمنية الأساسية، على النحو الآتي:

أولًا: ضمان سرية البيانات:

هي خدمة أمنية أساسية لحماية البيانات في الحوسبة السحابية. وأهمية هذه الخدمة تكمن فى خصائص الحوسبة السحابية، التي من شأنها تزيد من خطر خرق البيانات، وتخزين البيانات عن بعد، كما تفتقر الشبكة إلى إطار واضح ومحدد، فى ظل تعدد نظم الإبحار والتبادل الواسع للبنية التحتية، بالإضافة إلى ذلك فإن الحوسبة السحابية تدمج الكثير من التقنيات الحالية والمستقبلية؛ ومن ثمة حتماً سوف تتعرض السحب الحاسوبية إلى

مخاطر أمنية؛ بسبب عيوب في تصميم النظام وفي التطبيق. وهذا يفرض تحديًا ملحًا لتوفير ضمانات أمنية مرضية من حيث السرية. وهذه التحديات يمكن أن تأخذ وجهين؛ هما:

الأمن مقابل الاستخدام، واتزان النظام مقابل الديناميكية، والطريقة الأكثر استخدامًا هي تشفير كافة البيانات المهمة عند تخزينها، وتحمي هذه الخدمة البيانات من الكشف عنها إلى أطراف غير شرعيين، وتعد سرية البيانات في الحوسبة السحابية من الخدمات الأمنية الأساسية، على الرغم من أن هناك أنواعًا من البيانات قد تحتاج إلى متطلبات أخرى، مختلفة في شروطها، وسرية البيانات قد تشمل جميع أنواع البيانات، التي يتعامل بها على تقنية الحوسبة السحابية.

ثانيًا: حماية سلامة البيانات (Integrity):

تحمي هذه الخدمة البيانات من التعديلات الخبيثة التي يحدثها العابثون بها، وتمثل هذه الخدمة أهمية كبيرة لدى المستخدمين للسحب الحاسوبية؛ حيث إن هناك بيانات لها حجية قانونية، وأي عبث بها يفقدها أهميتها، وتتضمن هذه الخدمة عمليات مراجعة وتدقيق للبيانات؛ لضمان أن تكون جميع البيانات أصلية، وتطبق هذه الخدمة على جميع أنواع البيانات.

ولا بد من حماية عمليتي نقل المعلومات وتخزينها؛ لمنع أي تغيير للمحتوى بشكل متعمد أو غير متعمد. وتكمن أهمية ذلك في الحفاظ على محتوى مفيد وموثوق به، وفي الغالب تكون الأخطاء البشرية وعمليات العبث المقصودة، هي السبب في تلف أو تشويه للبيانات؛ وينتج عن ذلك أن تصبح البيانات عديمة الجدوى، وغير آمنة للاستخدام، ولتلافي تشويه البيانات أو تلفها، يُمكن استخدام تقنيات؛ مثل: البصمة الإلكترونية للرسالة (digest message)، والتشفير (encryption)، ومن المفيد أيضًا استخدام برمجيات مضادة للفيروسات (software anti-virus)؛ لحماية أجهزة التخزين من انتهاكات الفيروسات التي تتسبب في تلف البيانات أو تشويها، ومن المهم أيضًا الاحتفاظ بِنُسَخ احتياطية (backup) لاسترداد البيانات المفقودة، في حال تعرضها للضرر، أو في حال تعطُّل الشبكة أثناء عملية النقل.

ثالثًا: ضمان إتاحة البيانات:

تعمل هذه الخدمة على ضمان إتاحة البيانات المخزنة على السحب الحاسوبية، عند كل طلب استرجاع مقدم من مستخدم السحابة الشرعي. وتشكل هذه الخدمة أهمية خاصة للبيانات الموجودة على خوادم السحابة، وكذلك تؤكد انجاز الخدمات المقدمة للمستخدمين وتحقيقها، وفقًا لاتفاقيات مستوى الخدمة،

وتكتسب خدمة إتاحة البيانات أهمية خاصة في حالات تخزين البيانات لأجل طويل؛ بسبب ازدياد احتمال تدمير البيانات وفقدانها، من على خوادم السحب الحاسوبية.

رابعًا: نظام إدارة الهوية (Privacy):

وهو نظام معلوماتى، يهدف إلي التحقق من هوية المستخدم، والتأكد من أنه الصاحب الحقيقي الشرعي للحساب. ولزيادة الحماية، يمكن أن يكون موجوداً بشكل أفضل من طرف العميل، في مؤسسة تعمل على السحب الحاسوبية.

وكي يحافظ على خصوصية الرسالة الإلكترونية، يجب ألا يتمكّن من الاطلاع عليها إلا الأطراف المعنية المسموح لها بذلك. وللحفاظ على الخصوصية لا بُدّ من التحكم بعملية الولوج، وأكثر طرق التحكم انتشاراً هي: استخدام كلمات المرور (passwords)، والجدار الناري (firewall)، إضافة إلى شهادات الترخيص. وهنا تجدُر الإشارة إلى أمر بالغ الأهمية؛ وهو أن على المستخدِم الحفاظ على سرية كلمة المرور؛ لأنها تشكل خط الدفاع الأول في وجه الولوج غير المُرخّص، وبهذه الطرق يُمكن منع حدوث الجرائم المتعلقة بانتهاك الخصوصية؛ مثل: التنصّت (eavesdropping)، واستعراض معلومات معيّنة بدون ترخيص[٣٤].

خامسًا: الأنظمة والتوافق:

قد يتم الامتثال المحدد من قبل الأنظمة للقوانين واللوائح، خصوصًا بالنسبة للبيانات التي تمتلك صفة "الحساسة"؛ حيث يجب على المستخدمين مراجعة هذه القوانين واللوائح بدقة، قبل تقرير نقل البيانات على السحابة.

سادسًا: خدمة المراجعة والتدقيق:

توفر هذه الخدمة وسيلة للمستخدمين لرصد السحابة الحاسوبية، وتمكينهم من الوصول إلى البيانات الخاصة بهم، كذلك التأكد من استجابة السحابة والامتثال لطلبات استرجاع البيانات؛ أي أن هذه الخدمة تعمل على تأكيد الشفافية الجديرة بالثقة للوصول للبيانات.

سابعًا: الأمن المادي:

ويأتي من جانب مقدم الخدمة؛ حيث يجب عليه التأكد من جودة الشبكة والتطبيقات والخوادم التي يستعملها، وعدم وجود أي ثغرات أمنية بها، ويمكنه عمل ذلك عن طريق اختبار الاختراق (Penetration test)، الذي يفحص جميع الأجهزة والأنظمة ومتعلقاتها؛ بهدف اكتشاف ما بها من ثغرات أمنية، يمكن أن يستغلها أي مخترق؛ من أجل الحصول على معلومات.

ثامنًا: أمن التطبيقات:

السحب الحاسوبية تقوم بتوفير أدوات معالجة البيانات والأدوات البرمجية، التي تساعد المستخدم على تطوير أي كود برمجي وتجربته. لذلك ينبغي أن تكون هذه الأدوات _دائمًا_ على قدر عالٍ من الكفاءة؛ حيث يجب أن يتميز أداؤها بالسلاسة وعدم حفظ البيانات غير المهمة؛ حيث يمكن لهذه الأدوات أن تكون أداة في تسريب أي بيانات مهمة للمستخدم.

تاسعًا: التحقق من هوية الأطراف الأخرى(Peer Authentication):

يجب التأكد من هوية الأطراف المعنية بعملية تبادل البيانات؛ إذ يجب على كلا الطرفين معرفة هوية الآخر؛ لتجنب أي شكل من أشكال الخداع (مثل: عمليات التزوير، وانتحال الشخصيات). وهناك بعض الحلول والإجراءات للتحقق من هوية الأطراف المتصلة؛ مثل: كلمات المرور (passwords)، والتواقيع الرقمية (digital signatures)، والشهادات الرقمية (certificates digital) التي يُصدرها طرف ثالث، ويُمكن _أيضًا_ تعزيز الأمن، بالاعتماد على بعض المميزات المحسوسة؛ مثل: بصمة الإصبع (print finger)، والصوت، إضافةً إلى الصورة.

التشفير وأهميته في حماية البيانات:

استخدم الإنسان التشفير منذ نحو ألفي عام قبل الميلاد؛ لحماية رسائله السرية، وبلغ هذا الاستخدام ذروته في فترات الحروب؛ خوفًا من وقوع الرسائل الحساسة في أيدي العدو. وقام "يوليوس قيصر" بتطوير خوارزميته المعيارية المعروفة باسم شفرة قيصر (Caesar Cipher)، التي كانت نصًا مشفّرًا (Cipher text)؛ لتأمين اتصالاته ومراسلاته مع قادة جيوشه، وظهرت فيما بعد الكثير من الآلات التي تقوم بعمليات التشفير.

ويُعرّف التشفير بأنه عملية تحويل المعلومات إلى شفرات غير مفهومة (تبدو غير ذات معنى)؛ لمنع الأشخاص غير المُرخّص لهم من الاطلاع على المعلومات أو فهمها. ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفّرَة _ ومن المعلوم أن الإنترنت تشكّل في هذه الأيام الوسطَ الأضخم لنقل المعلومات_ ولا بد من نقل المعلومات الحساسة (مثل الحرَكات المالية) بصيغة مشفّرة، إن أُريدَ الحفاظ على سلامتها وتأمينها من عبث المتطفلين والمخربين واللصوص، وتُستخدَم المفاتيح في تشفير (encryption) الرسالة وفك تشفيرها (decryption)، وتستنِد هذه المفاتيح إلى صِيَغ رياضية معقّدة (خوارزميات).

وتعتمد قوة التشفير وفعاليته على عاملين أساسيين: الخوارزمية، وطول المفتاح (مقدّرًا بالبت (bits))، ومن ناحية أخرى فإن فك التشفير هو عملية إعادة تحويل البيانات إلى صيغتها الأصلية؛ وذلك باستخدام المفتاح المناسب لفك الشيفرة.

ومن أبرز المؤسسات التي أسهمت في هذا المجال، المعهد الوطني للمعايير والتكنولوجيا (National Institute of Standards and Technology -NIST)، المعروف سابقًا باسم المكتب الوطني الأمريكي للمعايير (U.S. National Bureau of Standards)؛ إذ طوّر هذا المعهد في العام ١٩٧٣ معيارًا، أطلق عليه معيار تشفير البيانات (Data Encryption DES -Standard). ويستنِد هذا المعيار إلى خوارزمية لوسيفَر (algorithm Lucifer)، التي تستخدِم مفتاح تشفير بطول ٥٦ بت (bit)، وتشترط أن يكون لكل من المرسِل والمستقبِل المفتاح السري ذاته. وقد استخدمت الحكومة هذا المعيار الرسمي في العام ١٩٧٦، واعتمدته البنوك لتشغيل آلات الصراف الآلي (ATM)، وبعد عام واحد من تطبيق معيار تشفير البيانات (DES)، طَوّر ثلاثة أساتذة جامعيون نظامَ تشفير آخر، أطلقوا عليه اسم (RSA)، ويستخدم هذا النظام زوجًا من المفاتيح (مفتاح عام (public key)، ومفتاح خاص (private key))، عوضًا عن استخدام مفتاح

واحد فقط. وعلى الرغم من أن هذا النظام كان ملائماً جداً لأجهزة الكمبيوتر المعقّدة، فإنه قد اخترق فيما بعد، وبقيت الحال على ذلك حتى قام "فيل زيمرمان" في العام ١٩٨٦ بتطوير برنامج تشفير يعتمد نظام (RSA)، ولكنه يتميز باستخدام مفتاح بطول ١٢٨ بت، ويُدعى برنامج الخصوصية المتفوّقة (Pretty Good Privacy-PGP). ويتوفر من هذا البرنامج نسخة تجارية، و نُسخة مجانية، وهو من أكثر برامج التشفير انتشاراً في وقتنا الحالي [٣٥].

أنواع الهجمات العدائية على السحب الحاسوبية:

ينقل المستخدمون تطبيقاتهم من داخل حدود مؤسساتهم إلى سحابة مفتوحة. وبهذا يفقدون السيطرة المادية على البيانات الخاصة بهم، وتتعرض بياناتهم إلى جميع أنواع الهجمات. ويمكن تقسيم هذه الهجمات على نوعين؛ هما:

أولًا: هجمات داخلية Insiders:

وهي الهجمات التي تكون من داخل النظام؛ حيث قد يقوم بعض العاملين الذين لديهم صلاحيات الوصول للبيانات على السحابة، بممارسة هذه الهجمات العدائية داخل السحابة؛ بدافع الفوائد الاقتصادية؛ كإعلام المستخدمين الآخرين للسحابة بكلمات مرور ومعلومات المصادقة الخاصة بمستخدمين آخرين،

وكذلك التحكم في الآليات الافتراضية، والدخول إلى جميع الاتصالات الخاصة بالمستخدمين للسحابة، واستغلال صلاحياتهم في الوصول.

وعلى الرغم من توافر الثقة بين المستخدمين ومزودي الخدمة في أغلب الأحيان، فإن بعض العاملين على السحابة، يقومون بأداء سلوكيات غير سوية؛ كالآتي:

- إخفاء ما يفسد البيانات؛ سواء كانت آليات يعتمدها مزود الخدمة أو غيرها؛ للحفاظ على سمعة السحابة ومزود الخدمة.
- الإهمال في الحفظ، أو تعمد حذف بعض البيانات، التي نادراً ما تسترجع؛ وذلك لتوفير الموارد.
- محاولة الحصول على أكبر قدر من المعلومات كلما أمكن، عن طريق التصنت، ومراقبة مسارات الشبكة.
- التواطؤ مع عدد قليل من المستخدمين الضارين؛ من أجل حصاد البيانات التفصيلية المفيدة للغاية.

ويجب على مستخدمي السحابة المراجعة الشاملة لجميع نقاط الضعف المحتملة، وحماية أصولها بشكل مقصود أو غير مقصود من الاختراق الأمني، كما يجب على مستخدمي السحابة_ بشكل خاص_ أن يعوا ويدركوا أنواع الخدمات الأمنية التي يوفرها مزود الخدمة،

ومدي كفاءتها، والكيفية التي تطبق بها، كما يجب أن تكون آليات التحقق متاحة لمستخدمي السحابة؛ للتحقق من الخدمات الأمنية المقدمة من قبل مزودي الخدمة، حيث بالنسبة للبيانات ذات القيمة العالية، فإن مستخدمي السحابة قد يطبقوا آليات حماية خاصة بهم؛ مثل الحماية التشفيرية؛ سواء كان مزود الخدمة لدية حماية من هذا النوع أم لا[٣٦].

ثانيًا: الهجمات الخارجية Outsider :

يفقد المستخدمون سيطرتهم على البيانات بمجرد نقلها إلى السحابة؛ حيث تكون الحوسبة السحابية عرضة لهجمات عدائية خارجية عن طريق الإنترنت، فالحوسبة السحابية لا تدقق في نوعية المستخدمين؛ فعلي سبيل المثال يستطيع أي مستخدم عن طريق تسجيل بيانات البطاقة الائتمانية أن يستفيد من خدمات السحابة؛ ومن ثم يمكن القيام بهجمات عدائية تؤثر سلبًا فى السحابة؛ كإسقاط شبكة الاتصالات، وكذلك إطلاق هجمات؛ كصيد معلومات الاعتماد للمستخدمين الشرعيين، والتلاعب في مسارات الشبكة. وتمثل الهجمات الخارجية الشكل القاسي للهجمات؛ حيث تستفيد من تدفق نظام المعلومات بين المستخدم والسحابة، كما يمكن للمهاجمين الخارجيين مراقبة الأجهزة الافتراضية وتهديد أمنها،

كما يمكنهم السيطرة على كامل النظام عن طريق أجهزة مراقبة افتراضية.

وتقع مسؤولية معالجة الهجمات الخارجية على مزودي الخدمات السحابية؛ حيث يجب أن يكون لديهم بنية تحتية مؤمنة بشكل جيد؛ كعزل تطبيقات المستخدمين على السحابة، وتصحيح العيوب في الوقت المناسب، وإخطار مستخدمي السحابة بأي مخاطر أمنية تكتشف، كما يجب أن يلتزم مستخدمو السحابة بتوجيهات الأمن عند استخدام الخدمات السحابية؛ بهدف تقليل إمكانية الاختراق الأمني، كما يجب أن تكون هناك آلية تفاوض بين مزودي السحابة والمستخدمين؛ للاتفاق على آليات الحفظ الاحتياطي؛ لتعزيز العملية الأمنية الخاصة ببياناتهم(٣٧).

مواجهة التحديات التي تعيق انتشار الحوسبة السحابية:

إن البيئة السحابية تنطوي على تحديات كثيرة وفجوات أمنية عدة، لا يمكن للحلول الأمنية التقليدية مواجهتها، فكما ذكر سابقًا فإن الأمن يشكل الهاجس الأول بين التحديات أو المسائل المقلقة عند الحديث عن الحوسبة السحابية. ولذلك طورت "أتريند مايكروب" حزمة من الحلول الأمنية المتكاملة والمتقدمة Trend Micro Secure Cloud؛ لتوفير الحماية الكفيلة بإزالة مثل هذه المخاوف؛ إذ تحد هذه الحزمة الجديدة من المخاطر الأمنية،

والمخاوف المتصلة بالخصوصية والتوافقية عند نشر المعلومات في بيئة الحوسبة السحابية، فاليوم بعد أن أخذت تتحدد معالم الحوسبة السحابية، وبدأت مؤسسات المعلومات بتخزين كميات هائلة من بياناتها المؤسسية في البيئة السحابية، صار لزامًا تطوير الحلول الأمنية الكفيلة بحماية البيانات، وتعزيز معايير التحكم بها. (٣٨).

ويجب الموازنة بين الفوائد المالية، التي توفرها خدمات الحوسبة السحابية للحكومات، وقطاع الأعمال، والمواطنين والمستهلكين، وبين المخاطر التي قد تنطوي عليها هذه الخدمات بالنسبة لخصوصية الفرد أو بياناته الشخصية. فهل يعرف المستهلكون كيف يمكن أن تُستغل هذه البيانات؟ أو هل يدركون المخاطر الممكنة التي تحيط بأمن البيانات؟ وما القيمة الحقيقية للبيانات الشخصية، التي يُشار إليها على أنها ÷نفط جديد× من المنظور التجاري؟ وهل ينبغي أن تكون للمستهلكين حقوق اقتصادية مقابل المتاجرة ببياناتهم؟

وفقًا لدراسة استقصائية، أجرتها مؤسسة أبحاث "Special Eurobarometer" لمواقف الأفراد في ٢٠١١، كانت نسبة ٧٤% ممن شملتهم الدراسة يرون أن إفشاء المعلومات على الخط، يمثل جزءًا متزايدًا من حياتهم اليومية، وأعربت الغالبية عن مخاوفها

بشأن تسجيل سلوكهم عن طريق الهواتف المتنقلة، وبطاقات الدفع والإنترنت المتنقلة، ولكن نسبة ٥٨% رأت أنه لا يوجد بديل لإفشاء المعلومات الشخصية، إذا كانوا يريدون الحصول على منتجات وخـدمـات.

ويستعرض تقرير اتجاهات الإصلاح في الاتصالات للعام ٢٠١٣ الأطر الحالية لحماية الخصوصية، والبيانات في الاتحاد الأوروبي، وكذلك في مجموعة متنوعة من البلدان تمثل العالم المتقدم والعالم النامي. وقد سارت بلدان كثيرة ممن طبقت أو تنظر في تطبيق نظام لحماية البيانات على منوال النموذج الأوروبي، الذي يوضح بطريقة مفيدة المشكلات التي تواجه قطاع الأعمال والاقتصاد؛ نتيجة لعدم وجود قوانين واضحة ومتوافقة، يجري تنفيذها بيسر عبر الحدود الدولية.

فعلى المستوى الإقليمي، صدر÷التوجيه الأوروبي لحماية البيانات×،(الذي يُشار إليه اختصاراً بأنه ÷التوجيه الأوروبي×) في ١٩٩٥، و ينص هذا التوجيه _عموماً_ على فرض التزامات خاصة بحماية البيانات على الشركات المتحكمة فيها، في حين تخضع الجهات المعنية بتجهيز البيانات لشروط معينة خاصة بالأمن، بيد أن التعاريف المختلفة المستعملة في البلدان الأوروبية المختلفة،

بالإضافة إلى أن التصنيف غير الواضح للجهات المعنية بتقديم خدمات الحوسبة السحابية، يؤدي إلى الالتباس والغموض.

وكثيراً ما يكون العملاء هم المسئولون عن تحمل العبء الكامل للالتزامات الخاصة بحماية البيانات والامتثال لها، على الرغم من تحكمهم الضئيل في الإجراءات التي تتخذها الجهة المعنية بتقديم أو حركة البيانات، ويكون عملاء خدمات الحوسبة السحابية مطالبين بممارسة اليقظة الواجبة، فيما يتعلق باختيار مقدِّم الخدمة، الذي يعرض ضمانات كافية بشأن كل من الموثوقية والكفاءة والأمن، بما يتوافق مع القوانين ذات الصلة [٣٩].

وينص ÷التوجيه الأوروبي× على أن البيانات الشخصية، لا يجب نقلها إلى بلدان خارج المنطقة الاقتصادية الأوروبية، التي يُرى أنها لا تطبق تدابير كافية لحماية البيانات. وقد أنشأت مؤسسة Amazon، على سبيل المثال، موقعًا أوروبيًا للحوسبة السحابية، يوفر للمستهلكين الثقة بأن البيانات، لن تُنقل عبر الحدود بالشكل الذي يعد انتهاكًا للتوجيه الأوروبي، كذلك تحظى خطة المرفأ الآمن الأمريكية بالقبول على أنها كافية لأغراض نقل بيانات شخصية معينة، بشرط خضوعها لبعض الاستثناءات الملحوظة ولليقظة الواجبة.

ومع ذلك، يجري التعامل عادة مع الحوسبة السحابية بدون موقع ثابت، وليس من المحتمل أن تكون الجهات المعنية بتقديم الخدمة موجودة فقط في بلدان محددة، وقد لا يستطيع العميل التأكد من الموقع الحقيقي لتجهيز البيانات أو تخزينها. وتواجه الهيئات التنظيمية المشكلة نفسها؛ مما يجعل من الصعب إنفاذ القيود الخاصة بتدفق البيانات عبر الحدود.

القوانين التي تُطبق في الحوسبة السحابية:

لا يوجد تشريع خاص مُلزِم عالميًا، يغطي جميع بلدان العالم، وكثير منها ينظِّم التدفق الدولي للبيانات كآلية لحماية خصوصية الأفراد وإنفاذ السياسات الوطنية. ويستهدف التوجيه الذي أصدره الاتحاد الأوروبي، بشأن الخصوصية الإلكترونية، شركات تقديم شبكات الاتصالات العمومية والدولية، التي ينبغي أن يكون النفاذ فيها إلى البيانات الشخصية بتفويض شخصي للأغراض المصرح بها قانونًا، أو أنه ينبغي أن يكون تخزين البيانات الشخصية أو نقلها محميًا ضد الإتلاف العرضي أو غير القانوني، أو الضياع أو التغيير العرضي، وضد التخزين أو المعالجة أو النفاذ أو الإفشاء غير المُصرح به أو غير القانوني، وينص التعريف الواسع للبيانات

الشخصية على أنها أي معلومات خاصة بشخص طبيعي غير محدد أو لا يمكن تحديده.

وفي ٢٥ من يناير ٢٠١٢، نشرت المفوضية الأوروبية التغييرات المقترح إدخالها على التوجيه الأوروبي لحماية البيانات، في محاولة لتوفيق الإطار التشريعي المتفتت والقديم المطبق على حماية البيانات، وتتضمن التغييرات المقترحة ما يلي [٤٠] :

- يكون من سلطة السلطات التنظيمية الوطنية اتخاذ إجراءات ضد الشركات العاملة في الدول الأعضاء الأخرى في ظروف معينة، ويجوز لها فرض غرامات تصل إلى مليون يورو أو ٢% من حجم الأعمال السنوية للشركة في بعض الحالات.
- توسيع تعريف البيانات الشخصية؛ بحيث يغطي أية معلومات متصلة بصاحب البيانات، وتشترط القواعد التنظيمية الحصول على موافقة صريحة من الفرد بالسماح بحجب البيانات.
- تطبق القواعد التنظيمية فيما يتجاوز الاتحاد الأوروبي؛ بحيث تشمل كيانات الاتحاد الأوروبي، التي تمتلك بيانات شخصية، ذات صلة بمواطني الاتحاد الأوروبي.

• يُشترط أن تقوم الهيئات المعنية بالإبلاغ بدون أي تأخير أي خرق للبيانات، وأن يتم ذلك في غضون ٢٤ ساعة من وقوع الخرق.

• يُشترط أن تقوم الشركات المتحكمة في البيانات بتقييم أثر حماية البيانات، وتعيين مسئولين عن حماية البيانات، وإبلاغ الأطراف الأخرى بأية خروقات.

• يكون للأفراد حق جديد، هو ÷الحق في النسيان في ظروف معينة، ولا يكونون مطالبين بعد الآن بدفع مقابل للنفاذ إلى بياناتهم.

• تخضع عمليات النقل الدولي للبيانات لإطار تنظيمي أكثر تفصيلًا، ينص على ضمانات يجب تطبيقها، وعلى أن تقوم السلطات بإجراء فحوص مسبقة، وزيادة تقييد قدرة الشركات المتحكمة في البيانات على إبطال هذه الضمانات.

ومع ذلك، أثارت طبيعة الإصلاحات المقترحة المثيرة للجدل الكثير من الجدل والنقاش، وهذا يعني أن تنفيذها قد يتأخر كـثـيـــراً.

وفي الوقت نفسه ، في المملكة المتحدة على سبيل المثال ضيّقت المحاكم معنى البيانات الشخصية، ذاكرة أن البيانات يجب

أن تكون مما يتصل بالسيرة الذاتية بمعناها الحقيقي، ويجب أن تركز على الفرد، وليس على أي شخص آخر، أو معاملة أخرى، أو حدث آخر.

وفي فرنسا تتولى إنفاذ ÷قانون معالجة البيانات، وملفات البيانات والحريات الفردية المـُعدّل اللجنة الوطنية لأجهزة الحاسوب والحريات التي تعمل بشكل استباقي، وقد نشرت اللجنة توجيهًا بشأن المعالجة القانونية للبيانات الشخصية، يفرض على الشركات المتحكمة في البيانات شرط الإبلاغ والتعاون، كما يفرض عليها شروطًا بالمحافظة على أمن البيانات الشخصية، ويفرض عليها في ظروف معينة حصول الهيئة على موافقة مسبقة بشأن معالجة البيانات.

وفي ألمانيا يتم الحصول على البيانات الشخصية مباشرة من صاحب البيانات، ما لم يشترط القانون الحصول عليها لأغراض تجارية حقيقية، أو إذا كان الحصول عليها يتطلب بذل جهد غير تناسبي، ولا يوجد ما يدل على أن صاحب البيانات سوف يتأثر، وعلاوة على ذلك، يركز القانون الفيدرالي لحماية البيانات بصفة خاصة على تصميم أنظمة لحماية البيانات لتقييد معالجة البيانات

الشخصية إلى أقل قدر ممكن، عن طريق جعل صاحب البيانات مجهولًا أو استعمال اسم مستعار.

وفي الولايات المتحدة، تغير التشريع بدرجة كبيرة في أعقاب الهجمات التي وقعت في ١١من سبتمبر ٢٠١١، باستحداث قانون المواطنة الأمريكي، الذي يسمح بتقاسم البيانات الشخصية الخاصة بأي فرد، مُشتبه في ضلوعه في أنشطة إرهابية أو في غسيل أموال. وقد نتجت عن ذلك، إمكانية توسيع نطاق النفاذ إلى المعلومات الشخصية وتقاسمها.

وقد اعترفت المحكمة العليا الأمريكية استناداً إلى الدستور الأمريكي بالحق في الخصوصية، على الرغم من أن الدستور الأمريكي لا ينص صراحة على مثل هذا الحق. ويوجد في كثير من الولايات قواعد لحماية الخصوصية داخل حدود ولايتها القضائية. وولاية كاليفورنيا هي فقط التي وسّعت الحق في حماية البيانات من التدخل الحكومي وجعلته التزاماً على القطاع الخاص.

وفي كندا، ينص ميثاق الحقوق والحريات على حق الفرد في أن يكون ÷في مأمن من التفتيش أو الحجز بدون مبرر، وقد وسّعت المحاكم نطاق هذا الحق ليشمل حماية حق الفرد في توقع درجة معقولة من الخصوصية. وفي قضية حديثة، استحدثت محكمة

الاستئناف في "أونتاريو" قانونًا عامًا، عن الأضرار المترتبة على انتهاك الخصوصية، والقوانين الكندية لا تقيد النقل الدولي للبيانات الشخصية، ولكن أي عملية نقل تبقى ضمن مسؤولية الطرف الذي يفشي البيانات.

وطبقت البرازيل تشريعًا خاصًا لحماية البيانات، على الرغم من أن الدستور البرازيلي، لا ينص على حقوق أساسية في شأن الخصوصية وسرية المراسلات. كذلك ينص القانون المدني على أنه يجوز للفرد أن يطلب حمايته من أي تهديد تتعرض له حقوقه الشخصية، وعلى عدم إمكانية انتهاك حياة الفرد الشخصية. كما يتضمن قانون حماية المستهلك قواعد واسعة لحماية البيانات، من بينها حق المستهلكين في النفاذ إلى البيانات، وتصحيح أية بيانات شخصية مسجلة.

ولا يوجد في جنوب إفريقيا أي تشريع خاص بحماية البيانات، وإن كان الحق في الخصوصية منصوصًا عليه في الدستور، كما يتضمن قانون حماية المستهلك للعام ٢٠٠٨، وقانون الاتصالات والمعاملات الإلكترونية للعام ٢٠٠٢، نصوصًا خاصة بالمعلومات الشخصية، والامتثال للقانون الأخير طوعي، ويجب تسجيل الامتثال للقانون في اتفاق مع صاحب البيانات. ومعروض على البرلمان في الوقت الحاضر مشروع قانون جديد لحماية المعلومات الشخصية.

ولا يوجد في المملكة العربية السعودية أي تشريع خاص بحماية البيانات، على الرغم من أن الحق في الخصوصية مقرّر في عدد من القوانين، وعلى وجه الخصوص، ينص قانون الإدارة الأساسي على مبدأ أساسي؛ مؤداه أن جميع المراسلات والاتصالات بين الأطراف، ينبغي أن تكون سرية تماماً، وينبغي عدم إفشائها.

وفي حالة عدم انطباق أي تشريع، تطبق المحاكم مبادئ الشريعة الإسلامية، التي تنص على التعويض عن الأضرار المترتبة على إفشاء معلومات شخصية بطريق الخطأ، إذا ترتب عليه تعرض الفرد للخسارة أو الضرر.

ولا يوجد في الإمارات العربية المتحدة أي تشريع خاص بحماية البيانات، على الرغم من أن الحق في الخصوصية منصوص عليه في الدستور وفي مختلف القوانين. إذ ينص الدستور على أن يتمتع الفرد بحرية الاتصال بواسطة البريد، أو البرق، أو بأي وسيلة اتصال أخرى، وتكون سرية الاتصالات مكفولة وفقًا للقانون وبالإضافة إلى ذلك، ينص قانون العقوبات على حقوق معينة في شأن الخصوصية وحماية البيانات الشخصية.

ولا ينص الدستور في الهند على أية حقوق خاصة في شأن الخصوصية، على الرغم من أن المحكمة العليا قررت إضافة الخصوصية إلى الحق في الحياة والحرية الشخصية. وينظم قانون

تكنولوجيا المعلومات للعام ٢٠٠٠ جمع البيانات الشخصية ومعالجتها؛ حيث ينص على أن الشركات يجب أن تطبق ممارسات الأمن المعقولة أثناء معالجة البيانات الشخصية، وأنه يجب في حالة الحصول على هذه البيانات بموجب عقد، عدم إفشائها دون موافقة صاحبها.

وتشارك اليابان، بوصفها عضواً في مجلس التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC)، في النهج الذي يطبقه المجلس إزاء الخصوصية، وينظم قانون حماية البيانات الشخصية جمع البيانات الشخصية واستعمالها في اليابان. ويغطي القانون أي شكل من أشكال البيانات، ولكنه ينطبق فقط على الحالات التي تمس خمسة آلاف فرد أو أكثر. ويفرض القانون التزامات خاصة بالقبول، والأمن، وتوفير المعلومات، بالإضافة إلى اشتراطات إضافية خاصة بالإشراف على الموظفين والأطراف الأخرى، الذين يتعاملون مع البيانات الشخصية.[٤١]

وتقوم الكثير من الجهات؛ كالجامعات، والمنظمات الحكومية، بتخصيص جزء من تمويلها في إجراء الأبحاث العلمية حول موضوع الحوسبة السحابية، ومن أمثلة تلك المعاهد الأكاديمية: جامعة ملبورن (أستراليا)، وجورجيا تيك، ويال، ووين ستيت، وفيرجينيا تيك، وجامعة ويسكونسن-ماديسون، وكارنيجي مالون، وإم آي تي،

وجامعة إنديانا، وجامعة ماساتشوسيتس، وجامعة ميري لاند، وآي آي تي بومباي، وجامعة نورث كارولينا ستيت، وجامعة بردو، وجامعة كاليفورنيا، وجامعة واشنطون، وجامعة فيرجينيا، وجامعة أوتاه، وجامعة مينيسوتا، وغيرها.

ومن أمثلة المشروعات المشتركة فيما بين الجهات الحكومية، الأكاديمية المتخصصة، والباعة التعاونية مبادرة آي بي إم/ جوجل الأكاديمية للحوسبة السحابية (IBM/Google Academic Cloud Computing Initiative)؛ حيث قامت آي بي إم بالتعاون مع جوجل في أكتوبر ٢٠٠٧، بإعلان إنشاء مشروع على مستوى الكثير من الجامعات، والمصمم لزيادة معرفة الطالب الفنية ودعمها؛ بهدف مواجهة تحديات الحوسبة السحابية، أما في إبريل ٢٠٠٩ انضمت مؤسسة العلوم القومية (National Science Foundation) للمبادرة، ورصدت جوائز بما يقدر ٥ مليون دولار أمريكي كمنحٍ لأربعة عشر معهدًا أكاديميًا متخصصًا، وفي يوليو ٢٠٠٨، أعلنت كلٌ من هوليت باكارد (إتش بى)، وإنتل، وياهوو إنشاء مركز عالمي متعدد البيانات، صمم على شكل سرير اختباري مفتوح المصدر، أُطلق عليه اسم أوبن سيروس(Open Cirrus) ، والذي صُمِمَ بهدف تشجيع الأبحاث في كل سمات الحوسبة السحابية، بالإضافة إلى إدارة مركز البيانات والخدمات. ويتمثل

شركاء أوبن سيروس في كلٍ منNSF ، وجامعة إلينوي (UIUC)، ومعهد كارلسر وهو للتقنية، وهيئة تنمية الاتصالات المعلوماتية (إنفوكووم) بسنغافورة (IDA)، ومعهد أبحاث الإلكترونيات والاتصالات في كوريا(ETRI) ، والمعهد الماليزي للأنظمة الإلكترونية الدقيقة(MIMOS) ، ومعهد برمجة النظام في الأكاديمية الروسية للعلوم (ISPRAS) . هذا، وفي سبتمبر ٢٠١٠، انضم المزيد من الباحثين لمشروع أوبن سيروس لأبحاث الحوسبة السحابية، التابع لكلٍ من إتش بي / إنتل/ ياهوو، وكان الباحثون الجدد كالآتي: معهد الصين لأبحاث الهواتف المحمولة (CMRI)، ومركز جاليسيا للحوسبة العملاقة في أسبانيا (CESGA)، ومركز جورجيا تيك للأبحاث التجريبية في أنظمة الحاسوب (CERCS) وتشينا تيلي كوم [٤٢].

أما في يوليو ٢٠١٠، فقد أعلنت معامل إتش بي لابس إنديا عن تقنية جديدةٍ قائمةٍ على السحابة، صممت لتسهيل أخذ المحتوى، وجعله ممكن الحركة والتنقل، حتى من أجهزة النهاية المنخفضة، حيث تسلط تلك المنشأة الإدارية الأضواء على كفاءات الأمن العالية، والسحابة عالية المرونة القائمة على الملكية الفكرية، التي طورت في معامل إتش بي. وهنا يتمثل الهدف من تلك المنشأة في تقليص المخاوف من أمن السحابة، كما تُعَدُ معامل إتش بي في

بريستول ثاني أكبر موقع لمركز أبحاث، ويعد مسئولًا الآن عن إجراء الأبحاث في مجالات الحوسبة السحابية والأمن.

هذا وتُعَدُ لجنة IEEE الفنية لخدمات الحوسبة في جمعية حاسوب IEEE الراعي لمؤتمر IEEE الدولي حول الحوسبة السحابية، أما في ٢٣من مارس ٢٠١١، فقد شكل كلٌ من: جوجل، وميكروسوفت، وياهوو، ,هوليت-باكارد، وفيرايزون للاتصالات وتيليكوم الألمانية(Deutsche Telecom) ، بالإضافة إلى ١٧ شركةً أخرى منظمةً غير ربحيةً، يُطلق عليها مؤسسة الشبكة المفتوحة(Open Networking Foundation) ، والتي ركزت على توفير الدعم لمبادرة سحابية جديدة، يُطلق عليها الشبكة معرفة البرمجيات(Software-Defined Networking) ؛ حيث كان الغرض من المبادرة نشر الابتكارات والإبداعات عبر تغييرات برمجية بسيطة في شبكات الاتصالات، والشبكات اللاسلكية، ومراكز المعلومات ومناطق الشبكات الأخرى [٤٣].

الخلاصـــة:

على الرغم من أن الحوسبة السحابية أثرت بالفعل فى الحياة اليومية، فإن الكثير من المستخدمين ما زالوا يشكون بشأن أمنها؛ وبذلك يكون أهم عوامل نجاحها هو خلق الثقة والأمن، ويتم ذلك خلال تخزين البيانات عن طريق المحافظة على الخصوصية، ووضع بروتوكول التدقيق دون معرفة محتويات بيانات المستخدم، والتحقق من هوية المستخدمين أو الأنظمة؛ ومن ثم تحديد الامتيازات التي تعطى للمستخدمين الشرعيين (الخدمة الذاتية)، ويمكن للمستخدمين تغيير كلمة المرور الخاصة بهم، والمحافظة على المعلومات وتحديثها.

ومن أهم النتائج التى توصلت إليها الدراسة:

١- هناك اتجاه عالمي نحو استخدام الحوسبة السحابية فى المؤسسات؛ لما توفره من خدمات وقدرات عالية، وسعة تخزينية، وانخفاض فى التكلفة.

٢- تعد النواحي التأمينية فى الحوسبة السحابية الجانب الأضعف فى هذه التقنية.

٣- هناك الكثير من التحديات الأمنية فى خدمات الحوسبة السحابية؛ منها:-

-عدم الفهم الواضح لمفهوم الحوسبة السحابية من قبل العملاء.

-الاعتماد الخارجي على تأمين البيانات.

-نقص صلاحيات العميل في السيطرة على بياناته.

-الاختراقات الأمنية للبيانات؛ سواء الداخلية أو الخارجية.

-يحدث فقد فى البيانات؛ نتيجة استخدام تطبيقات ضعيفة، وبعض العيوب التقنية فى المنصة.

٤- عدم وضوح المسؤوليات القانونية بين مقدمي الخدمات والعملاء، وعدم توحيد لوائح الملكية الفكرية والخصوصية والمراقبة.

التوصيات:

هل يُعد هذا الخليط من القواعد التنظيمية مناسبًا للغرض في الحوسبة السحابية؟ الإجابة الموجزة على هذا التساؤل هي بالنفي. وقد وُضِعت القواعد التنظيمية الوطنية فيما يتعلق باحترام حماية الخصوصية والبيانات منذ ما بين ٢٠ و٣٠ سنة، ولم تكن تتوقع ظهور نظام إيكولوجي رقمي عالمي، وهكذا، فقدت القواعد التنظيمية الحالية أهميتها، ولمواجهة التحديات التي أثارها النظام الإيكولوجي للحوسبة السحابية، يوصي تقرير اتجاهات الإصلاح في الاتصالات للعام ٢٠١٣بالخطوات التي يمكن أن يتخذها صانعو السياسات والهيئات التنظيمية، ونلقي الضوء فيما يلي على بعض هذه الخطوات [٤٤]:

تيسير محو الأمية السحابية: ينبغي للهيئات التنظيمية، أن تساعد المستهلكين في تحديد اختياراتهم، عن عِلْم بشأن المعلومات الشخصية التي يضعونها في الحوسبة السحابية، عن طريق زيادة إلمامهم بالقيمة التجارية لبياناتهم واستعمالاتها المحتملة. فالمواطنون بحاجة إلى معرفة لمن يشتكون، في حالة إساءة استعمال معلوماتهم.

النهوض بالخبرات: ينبغي لصانعي السياسات والهيئات التنظيمية، أن يواكبوا أحدث التطورات التقنية والاجتماعية في الحوسبة السحابية، وتوجيه نظر جميع أصحاب المصلحة، كي يكونوا في موقف يسمح لهم بوضع القوانين ذات الصلة وإنفاذها.

اتباع القوانين المناسبة للغرض: ينبغي لصانعي السياسات على المستويين الدولي والوطني العمل معاً؛ من أجل وضع قوانين فعالة، ومناسبة ومرنة وقابلة للتنفيذ؛ لحماية التوقعات المعقولة من جانب المواطنين، فيما يتعلق بالخصوصية. ويجب أيضاً أن تتنقل مسؤولية وضع التنظيم الذاتي إلى الجهات صاحبة المصلحة.

استعراض القوانين القائمة: ينبغي لصانعي السياسات، أن يستعرضوا القوانين المعمول بها على المستوى الدولي؛ لتيسير الاستخدام الوطني والدولي لخدمات الحوسبة السحابية، وسوف ييسر وضع معايير مشتركة وتحديد متطلبات إمكانية التشغيل البيني

تدفق المعلومات عبر الحدود، مع توافر الحماية المناسبة للأمن والخصوصية.

ومن هذا المنطلق، تدعو هذه الدراسة إلى مزيد من الأبحاث فى هذا المجال البكر، والإفادة من نتائج الأبحاث فى المكتبات ومراكز المعلومات، وتخصيص الدراسات لتقييم البنية التحتية لتقنية الحوسبة السحابية، وتحليل الخوادم وأنواعها، وتعرّف أنواع المضيف والمزايا التى يطرحها للعملاء.

المراجع:

(1) Jerry Archer. Cloud Security Alliance (CSA) security guidance for critical areas of focus in cloud computing V3.0. (2011) [Cited 03-23-2013] Available at: https//cloudsecurityalliance.org/guidance.v3.0.pdf

(٢) ويكيبيديا. حوسبة سحابية.(تاريخ الاطلاع:٢٠١٣/٩/٢٣) متاح على: *http://ar.wikipedia.org/wiki/%D8%AD%D9%88%D8%B3%D8%A8%D8%A9_%D8%B3%D8%AD%D8%A7%D8%A8%D9%8A%D8%A9#.D9.86.D9.82.D8.AF_.D8.A7.D9.84.D9.85.D8.B5.D8.B7.D9.84.D8.AD*

(٣) المرجع السابق نفسه.

(٤) رحاب فايز أحمد. نظم الحوسبة السحابية مفتوحة المصدر: دراسة تحليلية مقارنة. المجلة العراقية لتكنولوجيا المعلومات، مج٥، ع٢، ٢٠١٣، ص ص ١٧- ٤١.

(٥) شريهان نشأت المنيري. الحوسبة السحابية.- المركز العربي لأبحاث الفضاء الالكتروني، ديسمبر ٢٠١١
(تاريخ الاطلاع٢٠١٣/٨/٢٣) متاح على :
http://accronline.com/article_detail.aspx?id=2422

(٦) أحمد أمين أبو سعده. الحوسبة السحابية، حلم المكتبات ودور الحكومات._ الدوحة: في المؤتمر الثالث والعشرين للاتحاد العربي للمكتبات والمعلومات، نوفمبر ٢٠١٢، ص ص ٩٤٦-٩٧٢.

(٧) نجلاء أحمد يس.الحوسبة السحابية في المؤسسات الأكاديمية العربية: سحابة قطر الحاسوبية نموزجاً.- مجلة الاتجاهات الحديثة في المكتبات والمعلومات، مج ٢٠، ع ٤٠، يوليو ٢٠١٣. ص ص ٢١١-٢٣٧.

(٨) محمد عبد الحميد معوض.الحوسبة السحابية وتطبيقاتها في بيئة المكتبات. في مؤتمر دور تكنولوجيا المعلومات والاتصالات في التعليم والبحث العلمي : نحو تفعيل الحوسبة السحابية في مصر وتطبيقاتها._ مركز المؤتمرات جامعة القاهرة، ١٥ يوليو ٢٠١٢، ص ص ١- ٣٧.

(9) Bhayal, Savita. A study of security in cloud computing. [Cited 03-23-2013] Available at: *www.arab-afli.org/shared/.../AFLI23-2012_Ahmed.pdf*

(10) Reddy, Jyothi Kiran. Hybrid cloud: Joining the grid and cloud computing networks. [Cited 03-23-2013] Available at: http://gradworks.umi.com/15/04/1504527.html

(11) Azab, Ahmed Moneed. New System Security Mechanisms for the Cloud Computing Infrastructure. . [Cited 03-23-2013] Available at: *http://proquest.umi.com/pqdweb?did=2587884771&sid=1&Fmt=2&cl ientId=93083&RQT=309&VName=PQD*

(12) Pradnyesh Bhisikar. Security in Data Storage and Transmission in Cloud Computing. [Cited 03-23-2013] Available at: http://scholar.google.co.in/citations?user=iK-gsIkAAAAJ&hl=en

(13) Noemi Antedomenico. *Optimizing Security* of *Cloud Computing within* the *DoD*.p7. [Cited 03-23-2013] Available at: *https://www.hsdl.org/?view&did=11290.*

(١٤) جيمس، كيلي تارالا . استخدام الحوسبة السحابية بشكل آمن. (تاريخ الاطلاع ٢٠١٣/٩/٥) متاح فى :
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_aa.pdf

(١٥) نجلاء أحمد يس. مرجع سابق. ص ٢١٥

(16) Vic (J.R.) Winkler .Securing the Cloud: Cloud Computer Security Techniques and Tactics. - NEW YORK: Elsevier,2011.P 2

(17) Tim Mather .Cloud Security and Privacy._ Beijing: O'Reilly,2009.p8

(18) Kan Yang · Data storage auditing service in cloud computing: Challenges, methods and opportunities. [Cited 03-23-2013] Available at:
https://ece.uwaterloo.ca/~kan.yang/

(19) Shucheng Yu, Wenjing Lou, and Kui Ren. Data Security in Cloud Computing. [Cited 03-23-2013] Available at:
http://www.forbesmiddleeast.com/news/read/articleid/2621#.VEbe5iKUf6c

(٢٠) بوركو فورهت. أساسيات الحوسبة السحابية(تاريخ الاطلاع ٢٠١٣/١١/١٤-٢) متاح في:
http://itwadi.com/node/2693?page=show

(21) Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing.- National Institute of Standards and Technology Special Publication 800-145, 7 pages . [Cited ٠٨-23-2013] Available at:
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

(22)Christopher Olive. Cloud Computing Characteristics Are Key.- General Physics Corporation, ٢٠١٣. [Cited 03-٢-2013] Available at:
http://www.trainingindustry.com/media/3956976/gp%20cloud%20computing%20characteristics%20are%20key.pdf

(23)) Lenk, A., Klems,. What's inside the Cloud? An architectural map of the Cloud landscape. In *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing* (May 23 - 23, 2009). International Conference on Software

Engineering. IEEE Computer Society, Washington, DC, 23-31. Online [Cited 11-23-2013] Available at: http://dx.doi.org/10.1109/CLOUD.2009.5071529

(٢٤) محمد حبش.أهم عشر شركات في الحوسبة السحابية(تاريخ الاطلاع ٢٠١٣/٧/١٢) متاح فى:
http://www.tech-wd.com/wd/2012/06/17/the-most-important-companies-in-the-computing-cloud/

(25) Kuyoro S. O, Ibikunle F, Awodele O. Cloud Computing Security Issues and Challenges International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011. Online. [Cited 03-11-2013] Available at: http://www.cscjournals.org/manuscript/Journals/IJCN/volume3/Issue5/IJCN-176.pdf.

(٢٦) نجلاء أحمد يس. الحوسبة السحابية للمكتبات: حلول وتطبيقات.- القاهرة: للعربي للنشر التوزيع،٢٠١٤.- ص ٩٨.

(٢٧)أحمد ماهر خفاجة .الحوسبة السحابية وتطبيقاتها في مجال المكتبات Cybrarians -.Journal.-ع ٢٢ (يونيو ٢٠١٠) .- (تاريخ الاطلاع ٢١/٤/٢١٠٢)متاح في:
http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=445:2011-08-10-01-36-53&catid=158:2009-05-20-09-59-42&Itemid=63

(28) Shucheng Yu, Wenjing Lou, and Kui Ren. Data Security in Cloud Computing. [Cited 11-03-2013] Available at: http://www.forbesmiddleeast.com/news/read/articleid/2621#.VEbe5iKUf6c

(29)Shucheng Yu, Wenjing Lou, and Kui Ren. Data Security in Cloud Computing. [Cited 11-12-2013] Available at: http://www.forbesmiddleeast.com/news/read/articleid/2621#.VEbe5iKUf6c

(٣٠)ويكيبيديا. مرجع سابق.

(31) Cloud Security Alliance: CSA. [Cited 12-11-2013] Available at https://cloudsecurityalliance.org/about/

(٣٢) أمن الحَوْسَبَة السحابيّة مازال يشغل الشركات حول العالم. (تاريخ الاطلاع ٢١/٤/٢١٠٢)متاح في:
http://www.forbesmiddleeast.com/news/read/articleid/2621#.VEbe5iKUf6c

(٣٣)محمد شوقي شلتوت. الحوسبة السحابية Cloud computing بين الفهم والتطبيق (تاريخ الاطلاع ٢١/٤/٢١٠٢) متاح في:
http://emag.mans.edu.eg/index.php?page=news&task=show&id=365

(34) Shucheng Yu, Wenjing Lou, and Kui Ren. Data Security in Cloud Computing. [Cited 12-23-2013] Available at: http://www.forbesmiddleeast.com/news/read/articleid/2621#.VEbe5iKUf6c

(35) Steve pate , Tushar Tambay. Security Cloud using encryption and key management to solve today's cloud security challenges . [Cited 03-23-2013] Available at: *https://www.eiseverywhere.com/file_uploads/974dc3f1fc021f4f6caa02b20a11b031_Pate_Monday_0940_SNWS11.pdf*

(36) Duncan, A.; Creese, S.; Goldsmith, M.; Quinton, J.S. "Cloud Computing: Insider Attacks on Virtual Machines during Migration", , 2013 12th IEEE International Conference on, On page(s): 493 – 500 . [Cited 12-12-2013] Available at: *http://ieeexplore.ieee.org/xpl/abstractCitations.jsp?tp=&arnumber=6296060&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6296060*

(37)Damien Riquet, Gilles Grimaud, Micha¨el Hauspie. Large-scale coordinated attacks : Impact on the cloud security .- Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012 . [Cited 03-23-2013] Available at *https://hal.archives-ouvertes.fr/hal-00723739/PDF/4684a558.pdf*

(٣٨) شريهان نشأت المنيري. مرجع سابق.

(٣٩) الاتحاد الدولي للاتصالات. حماية البيانات والخصوصية في الحوسبة السحابية: لمن تنتمي الحوسبة السحابية عموماً؟(تاريخ الاطلاع ٢٠١٣/٤/٢) متاح فى : *https://itunews.itu.int/Ar/Note.aspx?Note=3726*

(٤٠) المرجع السابق نفسه

(٤١) المرجع السابق نفسه

(٤٢) ويكيبيديا. مرجع سابق.

(٤٣) المرجع السابق نفسه

(٤٤) الاتحاد الدولي للاتصالات. مرجع سابق