العنوان:	أمن وخصوصية البيانات بالحوسبة السحابية: قضايا وتحديات جديدة للمكتبات
المصدر:	مجلة بحوث في علم المكتبات والمعلومات
الناشر:	جامعة القاهرة - كلية الآداب - مركز بحوث نظم وخدمات المعلومات
المؤلف الرئيسي:	يسن، نجلاء
المجلد/العدد:	ع14
محكمة:	نعم
التاريخ الميلادي:	2015
الشهر:	مارس
الصفحات:	275 - 297
رقم MD:	708710
نوع المحتوى:	بحوث ومقالات
اللغة:	Arabic
قواعد المعلومات:	HumanIndex
مواضيع:	تكنولوجيا المعلومات، أمن المعلومات، الحوسبة السحابية، المكتبات والمعلومات
رابط:	http://search.mandumah.com/Record/708710

أمن وخصوصية البيانات بالحوسبة السحابية
قضايا وتحديات جديدة للمكتبات

د. نجلاء يسن
كبير أخصائيين مكتبة جامعة القاهرة
مدرس المكتبات والمعلومات – كلية الآداب – جامعة
مصراتة ليبيا (حاليا)

١/٠ مستخلص

دراسة تناقش التهديدات والمخاطر الأمنية التي قد تواجه المكتبات عند انتقالها إلى بيئة الحوسبة السحابية Cloud Computing (CC)، تهدف إلى الإجابة على تساؤل جوهري حول كيفية السيطرة والحفاظ على بيانات المكتبات في السحابة The Cloud بالرغم من تنازلها عنها لصالح طرف خارجي (موفر الخدمة)؟ وذلك من خلال استعراض الوضع الأمني الحالي للحوسبة السحابية بداية من فهم المزايا والتحديات الأمنية الرئيسية؛ ومرورا بالتعرف على بنية الأمن، والسياسات الواجب اتباعها لحماية البيانات الحساسة، وتحليل المخاطر الأمنية؛ ونهاية بالتعرف على المعايير الأمنية الخاصة بإدارة البيانات، والسياسات الواجب على المكتبة اتباعها لحماية بياناتها قبل الانتقال للتعامل مع هذه التقنية الناشئة.

١/١ تمهيد

مما لا شك فيه أن هجرة المكتبات من بيئة تقنية المعلومات التقليدية إلى بيئة السحابة أو البيئة القائمة على الخدمة والإنترنت يوفر لها العديد من الفرص التي قد ترفع عنها عبئ القلق بشأن تعقيدات إدارة موارد الحوسبة (الخوادم، وقواعد البيانات، والتطبيقات) وكلفة الاستضافة والتوسع في تقنية المعلومات، كما تحول مسئولية دعم وصيانة البنية التحتية، ومراكز البيانات، والبرمجيات، وقضايا التخزينِ وأمن التطبيقات والبيانات والشبكةِ، وترقيات نظمِ التشغيل، وكلفة العتاد وكافة الأنشطة المرتبطة بها إلى أطراف خارجية تقدم خدماتها بناء على الطلب، إلا أنه يطرح أيضا العديد من الأسئلة المتعلقة بأمن خدمات وبيانات المكتبات منها: هل ستظل البيانات التي تم نقلها للاستضافة بالسحابة ملكا للمكتبة أم ستفقد

ملكيتها؟ كيف تؤثر القوانين المحلية للدولة المضيفة على إيواء البيانات؟ ماذا يحدث في حال هجرة المكتبة إلى موفر خدمة جديد في المستقبل أو في حال قطع الخدمة أو خروج موفر السحابة منها؟ ماذا يعني نقل خدمات تقنية المعلومات من بيئة المكتبة إلى طرف خارجي يركز على الإيرادات أكثر من المستخدم؟ كيف تتم السيطرة على عمليات معالجة البيانات وإعداد التقارير والإحصاءات والتي ستفقدها المكتبة؟

٢/١ أهمية الدراسة

تنبع أهمية الدراسة من ازدياد شعبية نموذج الحوسبة السحابية والذي يعد نقلة نوعية جديدة تبشر بآفاق مستقبلية تساعد المكتبات على تغيير فكرتها لاستخدام طاقة الحوسبة، مما دفع بالكثير من موفري خدمة السحابة إلى إنتاج خدمات جديدة أو مطورة للمكتبات مبنية على حلول الاستضافة القائمة على شبكة الإنترنت قليلة الاعتماد على البنية التحتية والعاملين، مثل نظم المكتبة المتكاملة ILS's، ونظم تبادل الإعارة بين المكتبات ILL وغيرها.

مما أوجب معه ضرورة انتباه المكتبات إلى مشكلة فقد السيطرة الأمنية على الأصول والمعلومات الشخصية والحرجة التي تم نقلها من بيئاتها الآمنة إلى أجهزة مؤسسة أخرى تدار مِن قِبل موظفيها وتتاح من خلال شبكتها عبر مناطق جغرافية قد تمتد خلال دول متفرقة، وما يترتب على ذلك من الخضوع لرحمة موفر السحابة بشأن حماية خصوصية البيانات والسيطرة على الخدمات (البنية التحتية، والبرمجيات، أو المنصة)، بالإضافة إلى قوانين الدولة المضيفة بالنسبة للعتاد المستخدم، وخاصة في ظل عدم وجود قيود أمنية ضمن اتفاقيات مستوى الخدمة تحدد العلاقات السابقة بوضوح.

٣/١ تساؤلات الدراسة

تهدف الدراسة الحالية إلى الإجابة على الأسئلة التالية:

- ما المزايا والتحديات الأمنية المترتبة على استخدام المكتبات للحوسبة السحابية والتي يجب الانتباه إليها عند التعامل مع الخدمات المستضافة بها؟
- مما تتكون بنية الأمن بالحوسبة السحابية؟
- كيف يمكن تحليل المخاطر الأمنية للسحابة؟
- ما المعايير الأمنية الخاصة بإدارة البيانات بالسحابة؟ وما السياسات الواجب على المكتبات مراعاتها لحماية خدماتها وبياناتها الحساسة المستضافة بالسحابة التي يتم

استخدامها في نفس الوقت من قبل مستأجرين متعددين هم في الغالب منافسين أو أعداء محتملين لها؟

٤/١ منهج الدراسة

اتبعت الدراسة منهج الوصف التحليلي وذلك من خلال تحديد الواقع الحالي للوضع الأمني للحوسبة السحابية وجمع الحقائق عنه وتحليلها باعتبارها خطوات تمهيدية ضرورية تساعد على حماية المكتبات عند انتقالها مستقبليا إلى استخدام السحابة.

٥/١ أدبيات الموضوع

لم تستطيع الباحثة التوصل إلى دراسات سابقة بشأن موضوع أمن بيانات المكتبات داخل الحوسبة السحابية، الا أنها وجدت العديد من الدراسات التي تناولت موضوع الحوسبة السحابية واستخداماتها في المكتبات بشكل عام أو تناولت أمن السحابة بشكل خاص، وذلك كما يلي:

دراسات كل من (هان ٢٠١٣)[١]، و (روميرو ٢٠١٢)[٢]، و (جالفن، وصن ٢٠١٢)[٣]، و (ليو، وهيوبين ٢٠١٢)[٤] عن الحوسبة السحابية واستخداماتها الحالية في المكتبات، تلك التقنية صاحبة الفضل في تحويل مفهوم تخزين البيانات وإدارة الموارد، نظرا لاعتمادها على تقنيات المحاكاة الافتراضية والبرمجة التي ساعدت على تحقيق مفاهيم تعددية الإيجار والأداء والمرونة، مما حولها إلى منصة تدرجية عالية واعدة تسهل وصول المستخدمين غير الخبراء إلى الأجهزة والبرمجيات عبر الإنترنت، وهدفت هذه الدراسات إلى استكشاف واقع الحوسبة السحابية وفائدتها وسلبياتها لإدارات تقنية المعلومات بالمكتبات، وتأثيرها على نظم المكتبات، وأنواع الخدمات السحابية وكيفية استخدامها في البيئة المهنية وأسباب ضعف هذا الاستخدام، ومعايير تقييم واختيار موفر الخدمة، والمشروعات التي تصلح ولا تصلح للمكتبات بالسحابة.

كذلك دراسات الباحثة (٢٠١٥)[٥] و(٢٠١٣)[٦]، و(معوض ٢٠١٢)[٧]، و(زكريا ٢٠١٢)[٨]، و (أبو سعدة ٢٠١٢)[٩] وتناولت موضوع الحوسبة السحابية واستخداماتها في المكتبات سواء بوجه عام من خلال مناقشة بعض القضايا الرئيسية الخاصة بالمفهوم والنشأة والميزات والتحديات والبنية والسمات والمكونات ونماذج النشر والخدمات الرئيسية وموفري الخدمة بالعالم العربي، أو بوجه خاص بالتطبيق على بعض النماذج العربية مثل سحابة قطر الحاسوبية كنموذج على تغيير ممارسات اقتناء الموارد الحاسوبية من المركزية داخل

جدران المكتبات إلى المشاركة في بيئة الحوسبة السحابية، ومنصة شبكة التواصل الاجتماعي الفيسبوك ودورها في مساعدة المكتبات على مشاركة المعرفة بغض النظر عن الحواجز الزمنية والمكانية والشكلية.

هذا بالإضافة إلى دراسات (هيودك وآخرون ٢٠١٣)(١٠)، و(ديلوزير ٢٠١٣)(١١)، و(شي وآخرون ٢٠١١)(١٢) عن أمن الحوسبة السحابية وكيفية تأمين البيانات الحساسة بها باستخدام الحد الأدنى من التشفير مع توفير الخصوصية والأمن جنبا إلى جنب مع قضايا الأداء، وذلك بغرض مساعدة عملاء السحابة على فهم الوضع الأمني الراهن للحوسبة السحابية والعمل على تحسين مستواه، وتجنب الأخطارَ الأمنية الرئيسية المترتبة على انتقال المؤسسات إلى السحابة.

٦/١ مصطلحات الدراسة

- أمن المعلومات Information Security: المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي الأشخاص غير المخولين عبر الاتصالات، وضمان أصالة وصحة هذه الاتصالات(١٣).

- الجهاز الافتراضي Virtual Machine (VM): نسخة معزولة وكاملة الحماية من العتاد المادي لأجهزة الحاسب(١٤).

- الحوسبة السحابية Cloud Computing (CC): وسيلة تعتمد في طريقة عملها على ثلاثة ركائز هي شبكة الإنترنت ومراكز البيانات عن بعد وتقنية المحاكاة الافتراضية، تسمح بتشغيل البرمجيات والتطبيقات وتخزين البيانات ومشاركة موارد الحوسبة كالشبكات، والخوادم، وعرض النطاق الترددي كخدمات تتاح من أماكن بعيدة جغرافيا عن بيئة العميل (المكتبة) الحوسبية (أجهزة الحاسب والخوادم الخاصة به)، كمنفعة عامة غير قاصرة على فئة معينة، بأقل جهد إداري أو تقني، وسرعة في التحميل والتشغيل أو التعامل مع موفر الخدمة، يتم الدفع فيها حسب الاستخدام الفعلي(15).

- المحاكاة الافتراضية Virtualization: عرفتها جمعية صناعة تخزين الشبكات (SNIA) Storage Networking Industry Association بأنها فعل تجريد (إخفاء تفاصيل التنفيذ في البرمجيات والبيانات) وإخفاء أو عزل الوظائف الداخلية لنظام التخزين الكلي/الفرعي أو الخدمة عن التطبيقات وأجهزة الحاسب المضيفة أو موارد الشبكة بغرض تمكين الإدارة المستقلة للتطبيق والشبكة عن التخزين أو البيانات(١٦).

- برنامج مراقبة الأجهزة الافتراضية هايبرفايزور Hypervisor: يعد قلب الجهاز الافتراضي ويحتل مكانه بين موارد الخادم ونظم التشغيل(١٧). وتتمثل وظيفته في تقليد ومَحاكاة أو تمكين تشغيل الوظائف الضرورية للأجهزة الافتراضية، حيث يساعد على تشغيل عدد من أنظمةِ التشغيل معاً كتطبيقات على أجهزة افتراضية مستقلة(١٨).

٧/١ أمن الحوسبة السحابية

يشير أمن الحوسبة السحابية إلى مجموعة واسعة من السياسات والتقنيات والضوابط الخاصة بحماية البيانات، والتطبيقات، والبنية التحتية للسحابة، ويعد أحد الشواغل الرئيسية وأكبر القضايا المفتوحة التي توثر على مصداقيتها وانتقال المكتبات إليها، وذلك نظرا لتشجيع نموذج الحوسبة السحابية للاستخدام المكثف للتطبيقات التي تعمل في مكان ما في البني التحتية للسحابة والقائمة الوصول على شبكة الإنترنت، وتخزين البيانات، وإيصال الخدمات من قبل طرف خارجي (موفر السحابة) يقوم باستضافة البيانات المهمة أو تنفيذ العمليات الحرجة في أماكن غير معلومة، بالإضافة إلى سعة حجم السحابة وتنوعها وتشتتها الجغرافي الذي قد يؤدي إلى تعريض بيانات المكتبات للعديد من المخاطر الأمنية.

ويرتبط الأمن بكامل نظام إدارة السحابة ويعد وظيفة أساسية تمرر عبر كافة طبقاتها المختلفة بداية من طبقة الموارد والشبكة المسئولة عن إدارة الموارد المادية والافتراضية؛ ومرورا بطبقة الخدمات التي تشمل الفئات الرئيسية من الخدمات السحابية كالمنصة كخدمة PaaS والبنية التحتية كخدمة IaaS والتطبيقات كخدمة SaaS والاتصالات كخدمة CaaS، وطبقة الوصول الخاصة بواجهة برمجة التطبيقات API؛ ونهاية بطبقة المستخدم التي تغطي وظائف المستخدم النهائي وشركاء السحابة والإدارة(١٩).

هذا وقد أوجبت قضية أمن الحوسبة السحابية ضرورة وضع عدد من التدابير القانونية والتنظيمية في الحسبان قبل التعاقد مع موفر السحابة ونقل التطبيقات والبيانات إليها، بداية من فهم المزايا والتحديات والتهديدات الأمنية للحوسبة السحابية، وذلك كما يلي:

١/٧/١ المزايا الأمنية للحوسبة السحابية

مما لا شك فيه أن أمن البيانات يقع في أعلى قائمة أولويات المكتبة عند انتقالها إلى بيئة قائمة على السحابة، ومن الممكن إيضاح المزايا الأمنية للحوسبة السحابية من خلال ما يلي:

- ضمان أمن البيانات والذي يبدأ بمجرد تخزينها بالسحابة نظرا لقيام موفري الخدمة

بعمليات النسخ الاحتياطي للبيانات مما يجعلها متوفرة دائما حسب الحاجة ويعمل على حمايتها من الخسارة والفقد والتلف والذي قد يحدث نتيجة تلف خادم المكتبة نظرا لعدم تأثير عطل الخادم في السحابة على البيانات كنتيجة طبيعية لاقتنائها لخوادم بديلة تقوم بعملية النسخ الاحتياطي بطريقة آلية تلقائية منتظمة.

– تقليل الإصابة بالبرمجيات الخبيثة التي قد تغزو الأقراص الصلبة بأجهزة سطح المكتب أو الخوادم الخاصة بالمكتبة، بالإضافة إلى تقليل فرص سرقة العتاد لارتباط المعالجة بالخادم.

– يوفر تواجد خوادم السحابة في مواقع جغرافية متباينة المزيد من المرونة في خيارات الأمن بالنسبة لموفر الخدمة، كما يضمن عدم انهيارها في حال حدوث مشكلة بأحدها وذلك بضمان استمرارية العمل على غيره، كما يساعد على إضافة المزيد من الأجهزة عند الحاجة وإمكانية دمجها في السحابة وزيادة عامل الأمن(٢٠).

– يساعد فصل البيانات والتطبيقات على عدد مختلف من الأجهزة الافتراضية إلى منع وصول المستخدمين إلى ما لا ينبغي لهم الوصول إليه.

- عدم تأثر التطبيقات أو المستندات المفتوحة في حال تعطل جهاز الحاسب الشخصي نظرا لارتباطها بالسحابة وليس بسطح المكتب.

– عدم تأثر الأجهزة الافتراضية منفصلة الكيانات في حالة إصابة الجهاز المادي بالبرمجيات الخبيثة نظرا لإمكانية عزل الفيروسات أو مشاكل الجهاز المادي عن هذه الكيانات.

– إمكانية استرداد حالة عمل الجهاز السابقة بالكامل نظرا للنسخ الاحتياطي الذي يتم على فترات منتظمة(٢١). وسهولة استعادة البيئة الافتراضية عن نظيرتها المادية، مما يساعد في حال حدوث مشكلة على الجهاز المضيف على نسخ الأجهزة الافتراضية بأكملها على جهاز مضيف آخر، فيعمل على متابعة العمل بالحد الأدنى من وقت التوقف(٢٢).

٢/٧/١ التحديات الأمنية للحوسبة السحابية

وتمثل عدد من القضايا المهمة التي ينبغي على المكتبات الانتباه إليها قبل انتقالها إلى السحابة، ومنها:

١/٢/٧/١ أمن تخزين وخصوصية البيانات

ويختص بحماية البيانات من حيث السرية والتوافر والسلامة، والتزام موفر الخدمة بحماية

بيانات المكتبة والتي قد يؤدي عدم الاهتمام بها إلى التعدي على الملكية الفكرية وإفشاء الأسرار التجارية أو المعلومات الشخصية نتيجة لتعددية التخزين والإيجار، وذلك كما يلي:

- خصوصية تخزين بيانات المكتبة: حيث يستند مفهوم الحوسبة السحابية على تخزين البيانات عن بعد أو الاستعانة بمصادر خارجية لتخزينها مما يجعل من الثقة المتناهية في موفر السحابة والاتفاق معه على أمن وسلامة البيانات الخيار الأوحد أمام المكتبة.

- خصوصية بيانات المكتبة أثناء فترة التشغيل: أي عدم السماح بعرض أو تغيير البيانات بواسطة الآخرين أثناء فترة التشغيل (تحميل ذاكرة النظام).

- خصوصية بيانات المكتبة عند نقلها خلال الشبكة: وتشمل أمن نقل البيانات بالسحابة بحيث إن لا يتم عرضها أو تغييرها من قبل الأشخاص غير المخول لهم ذلك.

- مالك البيانات المخزنة وحقوق المكتبة نحو استخراج البيانات الخاصة بها للاستخدامات الأخرى أو في حال ترك الخدمة تماما(٢٣).

- سياسة الوصول حيث يمكن لعدد من المستخدمين الوصول إلى البيانات على نفس السحابة نظرا لسمة تعددية الإيجار مما يجعل أمن البيانات أكثر عرضة للخطر ويضع الأمر كله على قوة موفر السحابة في فرض السيطرة على سياسة الوصول.

- تصنيف البيانات ونقلها حيث تمثل إشكالية حفظ بيانات المكتبة على حده عن غيرها وطريقة تشفير هذه البيانات وكيفية إرسالها عبر الشبكة بأمان أمر يسترعى الانتباه.

- استرداد البيانات ومدى اتخاذ إجراءات النسخ الاحتياطي بشكل منتظم لتلافي الكوارث ومنها الكوارث الطبيعية(٢٤).

- سلامة البيانات: حيث يخلق استخدام خدمات الحوسبة السحابية خطرا على سلامة نظام المعلومات بسبب فقد الخبرة التقنية أو الاعتماد على موفر خارجي أو الاستعانة بمصادر خارجية، كما يؤدي إلى صعوبة تتبع البيانات على المدى الطويل(٢٥).

- تسرب البيانات: فعند الانتقال إلى السحابة يحدث تغييرين لبيانات العملاء، أولهما تخزين البيانات بعيدا عن أجهزة المكتبة، وثانيهما نقل البيانات من بيئة مستأجر واحد (المكتبة) إلى بيئة متعددة الإيجار (26).

- البيانات المتبقية Residual Data/ مغناطيسية البياناتData Remanence: أي بقايا البيانات التي يستمر تواجدها برغم محاولات إزالتها نتيجة لبعض الخصائص الفيزيائية التي تسمح بإعادة بنائها بعد حذفها، مما يتطلب المحو الأمن لها في نهاية دورة حياتها التي يسيطر عليها طرف خارجي وخاصة عند ترحيلها إلى بيئة سحابية جديدة(٢٧). وتعد تقنية

التخلص النهائي من البيانات بما في ذلك المراجع وملفات النسخ الاحتياطي المخفية والتدمير الكامل لها وعدم الاكتفاء بحذفها مطلب ضروري ينبغي مراعاته عند التعامل مع السحابة(٢٨).

– فقد السيطرة المباشرة على المعلومات والبيانات: بانتقالها من بيئة المكتبة الآمنة إلى مشاركتها في بيئة خارجية/بيئة السحابة.

– تكرار البيانات: ويعد مطلب ضروري لتجنب فقد البيانات وضمان سلامة ذات المهام الحرجة منها ومدى توافرها.

– موقع البيانات: والذي يتم الاحتفاظ به سرا بمنأى عن المكتبة مما قد يخلق حاجزا بينها وبين موفر السحابة، ويسمح بوصول طرف خارجي إلى المعلومات الخاصة به(٢٩).

– السلامة على المدى الطويل: أي إتاحة البيانات أو استردادها لوضعها في تطبيق بديل في حال إفلاس موفر السحابة أو انسحابه.

٢/٢/٧/١ تهديدات الأمن التقليدية.

وتتمثل في الممارسات الأمنية التقليدية مثل حماية أمن المرافق المادية، والشبكات، ونظام الحاسب، وتطبيقات البرمجيات من الاختراق والهجوم والذي قد يصبح أسهل بالانتقال إلى السحابة(٣٠)، مما يوجب على موفر السحابة توفير الإجراءات الأمنية اللازمة لمواجهتها.

٣/٢/٧/١ تحكم طرف خارجي في البيانات.

مما يتطلب من المكتبة مراعاة ما يلي:

– الآثار القانونية المترتبة على التحكم في البيانات والتطبيقات من قبل طرف خارجي، وما يترتب عليه من نقص في الشفافية، مما يفرض على بعض المؤسسات بناء السحابة الخاصة تجنبا لهذه القضايا(٣١).

– تقييم كفاءة موفر السحابة(٣٢): ومكانته بين غيره وطرق التشفير التي يقدمها وأساليب الحماية للأجهزة المادية التي تخزن عليها البيانات والنسخ الاحتياطي لبيانات المكتبة وجدران الحماية، وفي حال استخدام سحابة المجتمع يجب الانتباه إلى الحواجز التي تقدم للحفاظ على المعلومات الخاصة بكل عميل منفصلة عن غيره، والأحكام والشروط القياسية التي يوفرها للإجابة على هذه الأسئلة.

– خطورة سيطرة موفر السحابة دون غيره على البنية التحتية مما يعطيه الحق في تغيير مواصفاتها تبعا لاتفاقيته التي يوقعها مع المكتبة.

- الشهادات الأمنية للسحابة والتي ينحصر أغلبها في تغطية أمن مركز البيانات وموقع التخزين دون التعرض لانتقال البيانات عبر الويب وما يمكن أن يقابل ذلك من أخطار عند مغادرتها لمركز البيانات نظرا لعدم وجود تشفير آمن لها، كما ينبغي التأكد من مدى إتباع موفر الخدمة لمعايير الأمن المعتمدة مثل معيار ISO/IEC 27001 والذي يركز على متطلبات نظم إدارة أمن المعلومات، ومعيار SAS70/SSAE16 والذي يركز على فحص ضوابط وإجراءات خدمة المنظمة(٣٣).

٤/٢/٧/١ أمن الأجهزة الافتراضية

من الممكن أن تسبب المحاكاة الافتراضية عدد من المشكلات الخاصة بالسحابة، لذا ينبغي تقييم المخاطر الافتراضية من جهة المزايا والعيوب ومستوى الأمان قبل الانتقال من تخزين البيانات في مراكز البيانات الخاصة بالمكتبة والتي تتميز بالخصوصية والأمان إلى مراكز بيانات السحابة حيث يتم فقد السيطرة المباشرة عليها، وذلك من حيث:

- المخاطر الأمنية للمحاكاة الافتراضية والتي تعد الأكثر شيوعا في البيئات الافتراضية وتشمل الهجرة الحيوية، ومهارات الإدارة والتدريب، وعناصر التحكم في الوصول(٣٤).

- مخاطر العزلة: والتي تعد واحدة من أكبر التحديات التي تواجه قضايا الأمن حيث يؤدي اشتراك الأجهزة الافتراضية في نفس العتاد والموارد بالرغم عزلها عن بعضها البعض إلى السماح للكيانات الخبيثة بتسريب البيانات والهجوم عبر الأجهزة الافتراضية.

- كسر العزلة: أي ضمان عدم تأثير أحد الأجهزة الافتراضية على غيره الذي يعمل معه على نفس الجهاز المضيف من جهة أو إدارة جهاز افتراضي لآخر من جهة أخرى أو حتى إمكانية وصول جهاز افتراضي إلى الجهاز المضيف نفسه من جهة ثالثة، ويمكن كسر العزلة من قبل المستخدمين الذين يتم منحهم صلاحيات فائقة الوصول لأجهزتهم الافتراضية(٣٥).

- رفض الخدمة: حيث يتم مشاركة الموارد في البيئة الافتراضية كوحدة المعالجة المركزية والذاكرة والقرص الصلب وشبكة الاتصالات بين الأجهزة الافتراضية والجهاز المضيف، مما قد يؤدي إلى فرض أحد الأجهزة الافتراضية للسيطرة على موارد الجهاز المضيف، ويجعل النظام يرفض طلبات تشغيل الأجهزة الضيوف الأخرى نظرا لعدم توفر موارد متاحة.

- فصل البيانات: والتي عادة ما تكون مشتركة في بيئة السحابة جنبا إلى جنب مع

بيانات العملاء الآخرين، وربما يمثل التشفير وسيلة فعالة ولكن ليس علاجا للجميع.

– استغلال نقاط الضعف والثغرات الأمنية لبرنامج مراقبة الأجهزة الافتراضية الهايبرفايزر Hypervisor والذي يعد العنصر الرئيسي في برمجيات المحاكاة الافتراضية، وضعف ضوابط العزلة للتحكم مما يسمح بتسرب بيانات العملاء الحساسة من البنى التحتية الافتراضية ويؤثر على سرية السحابة ونزاهتها.

– إعتماد الأجهزة الافتراضية على برنامج Rootkit (مجموعة من الأدوات/البرمجيات التي تمكن مستوى الإدارة من الوصول إلى حاسب أو شبكة حاسبات) مما قد يهدد برنامج مراقبة الأجهزة الافتراضية Hypervisor، كما يمكن أن يتحكم في الجهاز المادي بأكمله.

– العودة إلى مشكلة اللقطات Snapshots: وهي آلية تسمح بالتقاط صورة للجهاز عند نقطة معينة والعودة إلى استخدام هذه اللقطة في حالة الضرورة، مما قد يسبب مشاكل أمنية مثل استخدام السياسات الأمنية القديمة، وإعادة تمكين/تعطيل الحسابات السابقة وكلمات السر (٣٦).

– تحديد الجهاز الافتراضي VM: أي عدم وجود ضوابط لتحديد الأجهزة الافتراضية التي يتم استخدامها لتنفيذ عملية معينة أو لتخزين الملفات.

– الهجمات عبر الجهاز الافتراضي VM: بما فيها محاولات تقدير معدلات الحركة لسرقة مفاتيح التشفير وزيادة فرص توظيف الهجمات على الجهاز الافتراضي VM(٣٧).

٥/٢/٧/١ الواجهات

تركز على كافة القضايا المتعلقة بالمستخدم والإدارة وواجهات البرمجة لاستخدام ومراقبة السحابة، وتشمل ما يلي:

– واجهة برمجة التطبيقات API: واجهة برمجة ضرورية للبنية التحتية كخدمة IAAS، والمنصة كخدمة PaaS، للوصول إلى الموارد الافتراضية والنظم والتي يجب أن يتم حمايتها منعا للاستخدام غير الشرعي.

– الواجهة الإدارية: تمكن التحكم في الموارد عن بعد من إدارة الأجهزة الافتراضية VM في البنية التحتية كخدمة IAAS، وتطوير المنصة كخدمة PaaS (الترميز، والنشر، والاختبار) والأدوات (التحكم في وصول المستخدم، والتكوين/التهيئة) في التطبيقات كخدمة SaaS(٣٨).

– واجهة المستخدم النهائية: لاستكشاف توافر الموارد والأدوات (الخدمة نفسها)، مما يعني ضرورة اتخاذ تدابير تأمين هذه البيئة.

– المصادقة والتفويض: أي الآليات اللازمة لتمكين وصول المستخدمين إلى بياناتهم

الخاصة بشكل صحيح(٣٩). حيث تجلب معالجة البيانات الحساسة خارج المكتبة مستوى من الخطر ويجعلها عرضة لعدد كبير من الهجمات ينتج عن الاستعانة بمصادر خارجية تتجاوز السيطرة المادية والشخصية(٤٠).

٦/٢/٧/١ الحوكمة

ويقصد بها القضايا المتصلة بفقد الضوابط الإدارية والأمنية في السحابة، وتتناول ما يلي:

- مراقبة الأمن: نظرا لما يؤديه فقد الحكم على الآليات والسياسات الأمنية وشروط الاستخدام من صعوبة تقييم المكتبة لأوجه الضعف والاختراق.
- مراقبة البيانات: حيث يعني نقل البيانات إلى السحابة فقد السيطرة عليها نظرا للتكرار، والموقع، وأنظمة الملفات.
- الإغلاق: نظرا لاعتماد المكتبة على موفر خدمة محدد بدون اعتماد معايير راسخة مما يعرضها للهجرة منه أو إنهاء الخدمة معه(٤١).

٧/٢/٧/١ المتطلبات القانونية

وتتعلق بالجوانب القضائية والقانونية، مثل بيانات المواقع المتعددة وإدارة الصلاحيات، وتشمل:

- موقع البيانات: وتأثيره على بيانات المكتبة عند تنفيذ الإجراءات القانونية بالأحكام القضائية للدولة المضيفة بشكل مباشر أو غير مباشر.
- اكتشاف البيانات: والذي ينتج عن مصادرة الأجهزة بما تحتويه من بيانات لأجراء التحقيقات في حال تنفيذ الإجراءات القانونية على عميل محدد.
- سمعة موفر الخدمة: والتي يجب التأكد منها بالاستفسار عن مكانته في سوق السحابة وما يمكن أن يواجه البيانات المخزنة في حال توقفه، حيث يعد اطلاعه على البيانات أحد أنواع التهديدات المحتملة للسرية، والتوافر وسلامة بيانات وعمليات المكتبة.
- التشريعات: وتشمل المخاوف القانونية المتعلقة بالمفاهيم الجديدة التي أدخلتها الحوسبة السحابية(٤٢).

٣/٧/١ بنية الأمن بالحوسبة السحابية

يعد تصميم بنية الأمن بالحوسبة السحابية بطريقة تضمن حماية كافة مواردها (العاملون، البنية التحتية، الشبكات، أنظمة تقنية المعلومات، التطبيقات، البيانات، وغيرها) مع ضمان عزل المستخدمين بشكل آمن في كامل مستويات السحابة (التطبيقات، الخوادم،

الشبكات، التخزين، وغيرها) من الأمور المهمة لضمان السيطرة على السحابة سواء أكانت عامة أو خاصة، وذلك كما يلي(٤٣):

أ) أمن مراكز البيانات

تشكل مراكز البيانات الأساس التقني للحوسبة السحابية حيث تضمن لموفر السحابة تأمين خدماته بما يتناسب مع التقنيات الراهنة، لذا يتوجب اتباع إجراءات الوقاية الأمنية التالية عند التعامل معها:

- المراقبة الدائمة للوصول باستخدام أنظمةِ مراقبة الفيديو، وأجهزة استشعار الحركة، وأنظمة الإنذار؛ وتوفير فريق أمني مدرب.
- تصميم كافة مكونات التجهيز الأساسية مثل التيار الكهربائي، والتبريد والاتصال بالإنترنت بطريقة تسمح بتمديدها.
- وضع مراكز البيانات في منطقة آمنة تتيح الحماية الكافية لها ضد الأضرار الطبيعية، كالعواصف والفيضانات، والدخول غير المصرح به.
- توفير النسخ الاحتياطي الدائم، ومواجهة زيادة الأحمال على مركز البيانات لمواجهة طلبات العملاء عالية المستوي من جهة أو المساعدة عند القيام بالعمل كبديل في حال فشل مركز بيانات آخر عن أداء مهامه من جهة أخرى.
- وضع مراكز البيانات في أماكن بعيدة عن بعضها البعض بما فيه الكفاية لحمايتها والسيطرة عليها في حالة حدوث أضرار كالحريق، أو المياه أو الهواء أو الكوارث الطبيعية.

ب) أمن الخوادم

تمثل الخوادم بيئة مهمة لأداء العمليات بالسحابة، مما يستوجب التعامل مع أنظمة التشغيل التي يتم نشرها كأصغر وحدة هجوم على هذه الخوادم، والانتباه إلى ضرورة تنصيب البرمجيات الأساسية فقط وتعطيل البرمجيات الزائدة أو إلغاء تثبيتها من البداية.

ج) أمن الشبكات

ينبغي على موفر السحابة اتخاذ التدابير الأمنية الفعالة لحماية الشبكة من الهجمات التي يمكن ان تتعرض لها، ومنها تدابير أمن تقنية المعلومات المعتادة مثل الحماية من الفيروسات، والحماية من البريد المزعج، والجدران النارية، كما يتوجب الاهتمام بتشفير كافة الاتصالات بين موفر الخدمة ومستخدمها من جهة وبين موفري الخدمة وبعضهم البعض من جهة أخرى، وفي حال إيصال الخدمة من خلال أطراف ثالثة يجب تشفير الاتصال فيما بينهم أيضا.

ج) أمن التطبيقات والمنصة

توفر المنصة كخدمة PaaS لعملائها كل ما يتصل بقاعدة البيانات، والتدرجية، والوصول وكيفية التحكم به، وغير ذلك مما يساعدهم على تطوير برمجياتهم الخاصة بشكل آمن، لذا يجب الوضع في الاعتبار عدد من الأمور الأمنية في كل مرحلة من مراحل التطوير وضرورة اختبارها والموافقة عليها من قبل مدير أمن موفر الخدمة شرط نشرها.

د) أمن البيانات

تتكون دورة حياة البيانات داخل السحابة من عمليات تخزين البيانات، واستخدامها، وتوزيعها، وتدميرها. مما يلزم موفر الخدمة بتدعيم كافة مراحل هذه الدورة مع توفير آليات أمنية مناسبة لها، والقيام بعمليات النسخ، وتحديد مصير البيانات عند انتهاء العلاقة التعاقدية بين المكتبة وموفر السحابة أو انقضاء الفترة الزمنية المحددة بينهما، بحيث يتم حذف جميع إصدارات بيانات المكتبة كاملة من كافة وسائط التخزين بشكل تلقائي بما في ذلك الملفات المؤقتة وأجزاء الملفات.

٤/٧/١ تحليل المخاطر الأمنية للحوسبة السحابية

يمكن تحليل المخاطر الأمنية للحوسبة السحابية من منظور المكتبة وموفر الخدمة والحكومات، على النحو التالي(٤٤):

أ) مخاطر أمنية تواجه المكتبة.

يمكن تلخيص المخاطر الأمنية التي من الممكن أن تواجهها المكتبة في بيئة الحوسبة السحابية فيما يلي:

١) وقت التوقف لبيئة السحابة والذي يؤدي لخفض ثقة المكتبة.

٢) تسرب بيانات المكتبة.

٣) كيفية مواجهة صلاحيات موفر السحابة والشواغل الأمنية مثل القضاء على الأخطاء والتعويض عن الضرر وهجرة البيانات وغيرها.

ب) مخاطر أمنية تواجه موفر الخدمة، وتشمل ما يلي:

١) ضمان التشغيل الآمن طويل الأمد من مركز البيانات بالسحابة وعزل الأخطاء للوصول إلى أقل حد من تأثير المخاطر الأمنية التي يواجهها موفر الخدمة.

٢) مكافحة القرصنة على الشبكة.

٣) الإدارة الآمنة لطلبات العملاء المختلفة.

ج) مخاطر أمنية تواجه الحكومات.

١) تعزيز الحماية الأمنية على النطاق الشامل لمراكز البيانات.

٢) الإدارة الآمنة لموفري خدمة السحابة المتعددين والمختلفين.

٣) تقييم وترتيب مستوى الأمن لموفري السحابة وعملائها، ونشر التنبيهات الاستباقية للبرمجيات الخبيثة.

٥/٧/١ طرق حماية البيانات بالحوسبة السحابية

يمكن التغلب على مشاكل الأمن بالسحابة بواسطة مراعاة عدد من المجالات الأمنية الرئيسية عند نشر أي خدمة على أجهزة طرف خارجي، وذلك كما يلي(٤٥):

أ) تشفير الاتصال.

يقصد بالتشفير معظم الممارسات الموظفة لتأمين البيانات الحساسة، والمطلوبة من قبل لوائح المكتبة والدولة(٤٦)، ويعد الطريقة الوحيدة لتجنب اعتراض البيانات والتطفل عليها أثناء انتقالها بين شبكة المكتبة والتطبيق الخارجي، وتتوافر حاليا العديد من التقنيات السهلة التنفيذ التي تقوم بذلك، مثل بروتوكول نقل النص الفائق الآمن (HTTPS) لتشفير المواقع.

ب) مصادقة الاتصال.

أحد الأمور المهمة التي تساعد على ضمان وصول المستخدمين المخول لهم فقط إلى الخدمات الخارجية، وتوجد العديد من التقنيات التي تحقق ذلك، مثل Openam.

ج) الجدران النارية/ جدران الحماية الافتراضية.

وتساعد على اتخاذ خطوات لضمان قبول اتصال الخادم الافتراضي بالتطبيق المطلوب فقط، حيث إن السماح بالوصول إلى البرمجيات التي لا علاقة لها بالتطبيق يزيد من فرص وصول القراصنة إليه.

د) الجدران النارية/ جدران الحماية المادية.

وتعرف جدران الحماية المادية أيضا بالأبواب، والأقفال، والمفاتيح، والجدران، وحراس الأمن، وتعد السيطرة الفعلية عليها الطريق الأسهل للاستيلاء على أي جهاز حاسب وبالتالي يعد الدفاع الأكثر فعالية ضد الدخلاء هو نظام الأمن للأجهزة المادية لمركز البيانات والذي يجب أن يتبع المعايير الدولية لأمن الأجهزة المادية.

هـ) الفصل الافتراضي.

أي مراعاة الفصل الحقيقي للأجهزة الافتراضية في البيئة الافتراضية بحيث لا يصل

جهازين افتراضيين يعملان على نفس الخادم بطريق الخطأ إلى موارد بعضهما البعض.

و) تشفير البيانات الساكنة.

أي تشفير البيانات الحساسة المخزنة على القرص الصلب بحيث إن لا يتم قراءتها في حالة الحدث غير المحتمل (نجاح محاولة الدخول عنوة إلى التطبيق).

٦/٧/١ معايير التحقق من أمن الحوسبة السحابية

تساعد الخطوات التالية على التحقق من أمن السحابة المقدم من قبل موفري خدماتها وذلك كما يلي(٤٧):

- فهم السحابة: بعمق بغرض التعرف على كيفية نقل ومعالجة البيانات بها وذلك بإدراك طبيعة بنيتها التي قد تؤثر على أمن البيانات المرسلة إليها.

- شفافية الطلب: بالتأكد من تقديم موفر السحابة لمعلومات مفصلة عن بنيتها الأمنية واستعداده لقبول التدقيق الأمني الذي قد يتمثل في هيئة مستقلة أو حكومية.

- تعزيز الأمن الداخلي: وذلك بالتأكد من احتواء ممارسات وتقنيات الأمن الداخلي لموفر السحابة على جدران نارية وضوابط وصول مستخدم قوية تناسب الإجراءات الأمنية السحابية.

- النظر في الآثار القانونية: المترتبة على الانتقال للحوسبة السحابية من خلال التعرف على القوانين واللوائح التي تؤثر على ما يتم إرساله إلى السحابة.

- إيلاء الاهتمام: لأي تطور أو تغيير في تقنيات وممارسات السحابة الذي قد تؤثر على أمن البيانات الخاصة بالمكتبة.

٧/٧/١ السياسات الأمنية الواجب على المكتبة مراعاتها لحماية بياناتها بالحوسبة السحابية

ينبغي على المكتبة الوضع في الحسبان الاعتبارات الأمنية التالية لحماية بياناتها قبل انتقالها إلى السحابة، وذلك كما يلي:

أ) تحديث السياسات الداخلية للمكتبة.

قبل المضي قدما مع السحابة، ينبغي على المكتبة القيام بتحديث أو صقل أو حذف السياسات وإجراءات التشغيل الحالية أو إعداد غيرها وذلك لتلبية متطلبات التشغيل الجديدة تحسبا لبيئة السحابة. كما ينبغي أن يكون هناك نموذج يتضمن السياسات الخاصة بالأمن وإدارة التطبيقات والبنية التحتية وإدارة المخاطر والتقييم المستمر لحلول الحوسبة السحابية، وفقا لعدة معايير كالمهمة والأهمية والسرية والتوافر.

ب) إدارة المخاطر.

والتي توضحها إجابات الأسئلة التالية:

- ما سياسات وإجراءات إدارة أمن المعلومات لموفر الخدمة؟ وهل يضمن توافقها مع متطلبات المكتبة؟
- كيف تتم عمليات تقييم المخاطر؟
- ما مستوى اتفاقيات الخدمة المستخدمة؟
- من يتحمل المسئولية في حالة حدوث اختراق أمني؟ وكيف سيتم إخطار المكتبة؟ وإلى أي مدى ستكون مشاركة موفر الخدمة؟ وما مدى خبرته في التعامل مع الحالات المثيلة؟
- ما قدرة موفر السحابة على استعادة بيانات وخدمات المكتبة في حالة الكوارث؟ وما الفترة الزمنية التي تستغرقها عملية الاسترجاع؟

ج) القوانين والمعايير.

ينبغي على المكتبة الرجوع إلى مستشار قانوني لأمن المعلومات قبل توقيع اتفاق مستوى الخدمة مع موفر السحابة بشأن معالجة البيانات والمعلومات الحساسة ووصول المستخدمين وبيانات الموقع وبيانات العزل والنسخ الاحتياطي والشفاء الذاتي وخطط الاستجابة للحوادث وخطط التعافي من الكوارث والتعامل مع الثغرات الأمنية والاختراق والذي يعتبر الضمان القانوني لحق المكتبة عند اللجوء إلى القضاء، هذا بالإضافة إلى الاهتمام بما يلي:

- تحديد الاحتياجات القانونية الداخلية والخارجية.
- تصنيف البيانات وفقا لنوعيتها ودرجة حساسيتها قبل تحديد البيانات التي يمكن أن تنتقل بأمان إلى السحابة.
- اختيار موفر السحابة المعروف عنه الشفافيةِ في الكَشْف عن ممارساتِه الأمنيةِ وإجراءات الاستضافة واتفاقيات الاستخدام الخاصة به والذي يمكن أن يلبي الاحتياجات الخاصة بالمكتبة بغض النظر عن السعر من حيث السمعة ، والشفافية، والمراجعة والأمور المادية.
- وضع حدود لصلاحيات موفر الخدمة وما يمكنه القيام به مع بيانات المكتبة وما يحظر عليه القيام به دون موافقتها.
- الموقع الجغرافي الذي تخزن وتعالج به البيانات الخاصة بالمكتبة.
- طريقة التعامل مع الأمور القضائية كالاستدعاء وغيره.
- النظام القضائي الذي يخضع له هذا الموقع، ومدى انصياع موفر السحابة لقوانين

ومعايير هذا النظام القضائي.

– وجود تعارض بين القوانين الحكومية للدولة التي تتبعها المكتبة ودولة موفر الخدمة.

– وجود بنود في العقد الخاص بموفر الخدمة تعفيه من تحمل مسؤولية الأعطال وتسرب المعلومات.

د) اختيار موفر خدمة السحابة.

يجب عند اختيار المكتبة لموفر خدمة السحابة الاتفاق معه على ما يلي :

- اقتراح موفر الخدمة نهج للانتقال إلى السحابة على مراحل والتحقق من الصحة عند انتهاء كل مرحلة.

- التعرف على تكاليف كل مرحلة انتقالية بالإضافة إلى الكلفة الإجمالية لجميع المراحل.

- التعرف على تكاليف التشغيل للسنوات القليلة القادمة.

- التأكد من تقديمه مزيجا من حلول الاستخدام/ التطبيقات/ التخزين، بالإضافة إلى حساب التكلفة بناء على عدد المستخدمين مع محدودية التخزين/التطبيقات حتى تتمكن المكتبة من اتخاذ الخيار المناسب.

-عدد سنوات الخبرة في مجال الحوسبة السحابية(٤٨)

– مدى فهم موفر الخدمة من خارج تخصص المكتبات لاحتياجات المكتبة.

هـ) التخزين والمحاكاة الافتراضية.

– كيف يقوم موفر الخدمة بتخزين بيانات المكتبة؟

– كيف يتم حماية البيانات الخاصة بالمكتبة عن بيانات غيرها من العملاء؟

– من المخول من قبل موفر الخدمة بالوصول إلى أو تعديل البيانات الخاصة بالمكتبة؟

– هل يتم نسخ البيانات عبر مواقع فيزيائية مختلفة؟

– كيف تتم عملية النسخ الاحتياطي للبيانات؟

– هل يتم التخلص من البيانات المحذوفة بالفعل في حال قيام المكتبة بحذفها؟

– ما طريقة فصل البيانات الخاصة بالمكتبة وما خطط التشفير التي يتبعها موفر السحابة؟

– من يشارك المكتبة البنية التحتية الأساسية للجهاز الافتراضي؟

– كيف يتم تنفيذ الأمن عبر الجهاز الافتراضي؟

– من يستطيع تهيئة الجهاز الافتراضي وتعديل قواعد جدار الحماية وغيرها من المعايير الأمنية؟

من يدير إعدادات الأمان والتحكم في الوصول للتطبيقات القائمة على السحابة؟

و) سياسات مركز البيانات.

- هل تعرف المكتبة الموقع الفيزيائي لمركز بيانات السحابة (الخوادم والبيانات)؟
- هل يستطيع موفر السحابة تهجير بيانات وخدمات المكتبة بطريقة تناسبها؟
- هل الموقع الفيزيائي مجهز للتعامل مع الكوارث وتغطية البيانات؟
- ما مستوى توفر الدعم الذي يمكن الاعتماد عليه طوال أيام الأسبوع ٧ X ٢٤ ؟

ز) القابلية للانتقال.

- ما استراتيجية الخروج التي ستتبعها المكتبة في حال اتخاذ قرار بتغيير موفر السحابة أو الرجوع إلى بيئة مقر العمل التقنية ؟
- ما الحل إذا ما خرج موفر الخدمة من العمل بالسحابة؟
- هل تستطيع المكتبة الحصول على البيانات الخاصة بها في حالة الفشل أو الرغبة في الانتقال؟
- ما التنسيق المستخدم في تخزين البيانات وهل يسمح بعملية استيراد وتصدير البيانات بسهولة؟

٨/١ نتائج الدراسة

✓ الحوسبة السحابية نموذج يمكن النفاذ عبر الشبكة إلى مجموعة من موارد الحوسبة المشتركة كالخوادم والشبكات والتخزين والتطبيقات والخدمات، وتسليمها بناءً على الطلب بأقل جهد إداري أو تدخل من جانب موفر الخدمة بغض النظر عن المكان والزمان. ويتألف هذا النموذج من الخدمة والطلب، والتسليم عبر الشبكة وتجميع الموارد والمرونة والخدمة الذاتية، ويتكون من عائلة كل شيء كخدمة Every Thing as a Services (البرمجيات كخدمة (SaaS) والمنصة كخدمة (PaaS) والبنية التحتية كخدمة (IaaS) والاتصال كخدمة (CaaS) والشبكات كخدمة (NaaS) وغيرها) ، ويحتوي على عدد مختلف من نماذج النشر (السحابة العامة Public cloud ، والسحابة الخاصة Private cloud ، والسحابة الهجينة Hybrid cloud..).

✓ تعد قضية أمن البيانات من أكثر الأسباب الجوهرية وراء خوف المكتبات من الانتقال إلى السحابة حيث تعد محور قلق نظرا لانتقال التحكم الأمني بالبيانات بمجرد دخولها السحابة من يد المستخدم إلى يد موفر خدمة متخصص في الحوسبة القائمة على الإنترنت ، مما يتطلب معه دمج الأمن في كل جانب من جوانب منصات السحابة لزيادة ثقة

المستخدمين بسلامة تخزين البيانات.

✓ ليس بالضرورة أن تهتم المكتبات بكيفية تطبيق تقنية الحوسبة السحابية أو طريقة إدارة الأمور بها ولكن جل ما يجب الاهتمام به هو طريقة الوصول إلى البيانات ومستوى الأمن اللازم لحمايتها والذي يعد مصدر القلق الرئيسي بالسحابة نظرا لوجود بعض البيانات الخاصة بالمستخدمين والتي لا يمكن أن تعطى لمراكز بيانات الطرف الخارجي (موفر الخدمة).

✓ يؤدي عمق تحليل وتقييم مخاطر الإخفاقات الأمنية للخصوصية والسرية والنزاهة والسيطرة التي يمكن أن تحدث لموفر السحابة تبعا لمستوى حساسية المعلومات إلى تجنب المكتبة لكثير من المشكلات وتوفر عليها الكثير من التكاليف الداخلية والخارجية عند انتقالها إلى بيئة الحوسبة السحابية.

✓ يجب وضع موقع استضافة السحابة ضمن سياق المخاوفِ الأمنية للمكتبة، نظرا لقيام بعض موفري الخدمة باستئجار مراكز البياناتُ في مواقعِ منخفضة التكلفة غير آمنة مما يعني الاستضافة في دول أجنبيةِ وخضوع التطبيقِات والبيانات لقوانينِ وسياساتِ الدولة المضيّفِة.

✓ يمكن حماية البيانات بالسحابة عن طريق إتباع عدد من الأمور مثل تشفير ومصادقة الاتصال، والاهتمام بالجدران النارية الافتراضية وجدران الحماية المادية، والفصل الافتراضي للبيانات، وتشفير البيانات الساكنة.

✓ يجب على المكتبة الاهتمام بإستراتيجية الخروج من السحابة مثل اهتمامها بإستراتيجية الدخول إليها وذلك في حال فك الارتباط مع البائع أو موفر الخدمة أو دمج الخدمة مع خدمة مؤسسة أخرى مع التأكيد على كيفية استرداد البيانات من البائع، وخاصة في حالة إيقافه عن العمل بالسحابة.

✓ يمكن التغلب على المشاكل الأمنية باستخدام الحوسبة السحابية كامتداد للشبكات الداخلية الموجودة بالمكتبة، مع اعتماد تدابير الحماية والاحتياطات الأمنية الوقائية المتبعة محلياً.

✓ تختلف الاحتياطات الأمنية التي يجب على المكتبة مراعاتها باختلاف مستوى السحابة من الأقل إلى الأعلى بداية من البرمجيات كخدمة SaaS إلى المنصة كخدمة PaaS إلى البنية التحتية كخدمة IaaS، حيث يتطلب كل نموذج من هذه النماذج معالجة أمنية مختلفة من موفر الخدمة من حيث المعايير والمعالجات والنظم أمنية.

9/١ مراجع الدراسة

1. Yan Han. "IaaS cloud computing services for libraries: cloud storage and virtual machines", OCLC Systems & Services, 29, 2, (2013) :87 – 100. Retrieved by Emerald Group Publishing Limited
2. Nuria Lloret Romero. "Cloud computing" in library automation: benefits and drawbacks. The Bottom Line: Managing library Finances. 25 , 3, (2012): 110-114. Retrieved from Emerald Group Publishing Limited.
3. Denis Galvin , and Mang Sun. Avoiding the death zone: choosing and running a library project in the cloud. Library Hi Tech,30, 3, (2012): 418-427. Retrieved from Emerald Group Publishing Limited.
4. Weiling Liu, and Huibin (Heather) Cai. Embracing the shift to cloud computing: knowledge and skills for systems librarians. OCLC Systems & Services: International digital library Perspectives, 29, 1,(2013) : 22-29. Retrieved from Emerald Group Publishing Limited.

٥. نجلاء أحمد يس. "خدمات منصة شبكة التواصل الاجتماعي الفيسبوك Facebook Social Networking Platform Services ودورها في مساعدة المكتبات الأكاديمية العربية على مشاركة المعرفة : دراسة تجريبية على مكتبة جامعة القاهرة." الاتجاهات الحديثة في المكتبات والمعلومات، ع ٤٢ (يناير ٢٠١٥).

٦. ـــ. "الحوسبة السحابية في المؤسسات الأكاديمية العربية: سحابة قطر الحاسوبية Qatar Cloud Computing Qloud نموذجا." الاتجاهات الحديثة في المكتبات والمعلومات، ع ٣٩ (يوليو ٢٠١٣) :٢١١ – ٢٣٧ .

٧. محمد عبدالحميد معوض. الحوسبة السحابية وتطبيقاتها في بيئة المكتبات. في "دور تكنولوجيا المعلومات والاتصالات في التعميم والبحث العلمي : نحو تفعيل الحوسبة السحابية في مصر وتطبيقاتها". جريدة اقتصاد مصر وجامعة النهضة. القاهرة. مركز المؤتمرات جامعة القاهرة. ١٥ يوليو ٢٠١٢.

٨. محمود شريف زكريا. الحوسبة السحابية وبناء مجتمع المعرفة: رؤية استشراقية. في المؤتمر الثالث والعشرين للاتحاد العربي للمكتبات والمعلومات(اعلم). "الحكومة والمجتمع والتكامل في بناء المجتمعات المعرفية العربية." الدوحة (قطر)، ١٨-٢٠ نوفمبر ٢٠١٢. ١٩٦٨-١٩٨٢

٩. أحمد أمين أبو سعده. الحوسبة السحابية Cloud Computing حلم المكتبات ودور

الحكومات. في المؤتمر الثالث والعشرين للاتحاد العربي للمكتبات والمعلومات (اعلم). "الحكومة والمجتمع والتكامل في بناء المجتمعات المعرفية العربية." الدوحة (قطر)، ١٨-٢٠ نوفمبر ٢٠١٢. ٩٤٦-٩٧٢

10. Aleksandar Hudic, et al . "Data confidentiality using fragmentation in cloud computing." International Journal of Pervasive Computing and Communications. 9,1, (2013): 37-51. Retrieved from Emerald Group Publishing Limited.
11. Eric P. Delozier. "Anonymity and authenticity in the cloud: issues and applications." OCLC Systems & Services: International digital library Perspectives. 29, 2, (2013): 65-77. Retrieved from Emerald Group Publishing Limited.
12. Jianhua Che, et al. Study on the security models and strategies of cloud computing. 2011 International Conference on Power Electronics and Engineering Application. Procedia Engineering 23 (2011): 586 – 593. Retrieved from science Direct.
13. علوطي لمين. "تحديات الأمن الإلكتروني في المؤسسة." أبحاث اقتصادية وإدارية، ٦ (ديسمبر ٢٠٠٩): ١٦٢.
14. Christophe Pelletingeas. "Performance Evaluation of Virtualization With Cloud Computing." M.S. Edinburgh Napier University, 2010 , 16. http://www.soc.napier.ac.uk/~bill/chris_p.pdf (Accessed 17 January 2015)
15. نجلاء أحمد يس. الحوسبة السحابية للمكتبات: حلول وتطبيقات (القاهرة : دار العربي للنشر والتوزيع، ٢٠١٤). ٢٢-٢٣.
16. Cloud Computing Virtualization Specialist Complete Certification Kit: Study Guide Book and Online Course. (UK: The Art of Service,2009), 159.
17. Boa Ho Man , Goh Hao Yu Gerald, and Tan Wei Hao Benjamin. "Cloud Computing." , 8. Chap. 1 in A Fresh Graduate's Guide to Software Development Tools and Technologies. (Singapore: Current and Past Students School of Computing National University, 2011).
18. H. Frank Cervone. "Managing Digital Libraries: The View From 30,000 Feet an overview of virtual and cloud computing." OCLC Systems & Services: International digital library perspectives , 26, 3,(2010):163.
19. Kangchan Lee. "Security Threats in Cloud Computing Environments." International Journal of Security and Its Applications , 6, 4, (October, 2012):25.
20. Anthony T. Velte, Toby J. Velte, and Robert Elsenpeter. Cloud Computing: A Practical Approach. (United States: McGraw-Hill Companies, 2010),8

21. Cloud Computing Virtualization, 13.
22. "Ibid, 14".
23. Matthew R. Goldner. "Winds of Change: Libraries and Cloud Computing." BFP 34, (Dezember 2010): 274. Retrieved from Walter De Gruyter
24. Savita Bhayal. "A study of Security in Cloud Computing." M.S. Department of Computer Engineering and Computer Science. California State University, 2011, 17. Retrieved from Dissertations & Theses: Full Text.
25. ACP. Banque de France. Autorité de contrôle prudential. Analysis et syntheses. The risks associated with cloud computing. 16 (July 2013), 14.
26. Farzad Sabahi. "Secure Virtualization for Cloud Environment Using Hypervisor-Based Technology." International Journal of Machine Learning and Computing 2, No. 1, (February 2012): 43.
27. "Ibid".
28. Nelson Gonzalez et al. "A quantitative analysis of current security concerns and solutions for cloud computing." Journal of Cloud Computing: Advances, Systems and Applications , (2012):3 Retrieved by Springer.
29. Alexa Huth, and James Cebula. The Basics of Cloud Computing. Us-Cert. United States Computer Emergency Readiness Team. Carnegie Mellon University, 2011, 4.
30. Jianhua Che et al. Study on the Security Models and Strategies of Cloud Computing. in "2011 International Conference on Power Electronics and Engineering Application." Procedia Engineering 591, (2011): 587. Retrieved from Science direct.
31. Richard Chow, et al. Controlling Data in the Cloud: Outsourcing Computation Without Outsourcing Control. CCSW 2009: The ACM Cloud Computing Security Workshop, 13 November 2009, Hyatt Regency Chicago, Chicago, IL, 2. http://www.parc.com/content/attachments/ControllingDataInTheCloud-CCSW-09.pdf (Accessed 28 January 2015)
32. Wayne Jansen, and Timothy Grance. Guidelines on Security and Privacy in Public Cloud Computing. (NIST) National Institute of Standards and Technology, 2011,35. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf (Accessed 20 November 2013)
33. Carl Grant. "The Future of Library Systems: Library Services Platforms." ISO Information Standards Quarterly .24, 4 (Fall 2012) :6-7.
34. Mariana Carroll, Paula Kotzé, and Alta Van Der Merwe. Secure Virtualization Benefits, Risks and Controls . in "Closer 2011 -International Conference on Cloud Computing and Services Science."Noordwijkerhout: The Netherlands, 6-9 May, 2011, 4. http://researchspace.csir.co.za/dspace/bitstream/10204/5054/1/Kotze1_2011.pdf (Accessed 7 February 2015)
35. Hanqian Wu et al. Network Security for Virtual Machine in Cloud Computing.

National Natural Science Foundation of China,19. http://csis.bits-pilani.ac.in/faculty/murali/netsec-11/seminar/refs/sreeraj1.pdf (Accessed 20 March 2015).

36. "Ibid".

37. Gonzalez. A quantitative analysis of current security concerns and solutions for cloud computing , 3.

38. "Ibid,2 "

39. Handbook of Cloud Computing /Edited by Borko Furht, and Armando Escalante. (New York :Springer Science+Business Media, 2010) , 24.

40. Michael Hugos, and Derek Hulitzky. Business in the Cloud: What Every Business Needs to Know About Cloud Computing. (Hoboken, New Jersey: John Wiley & Sons, Inc, 2011), 67-68.

41. Gonzalez. A quantitative analysis of current security concerns and solutions for cloud computing , 3.

42. "Ibid,4 "

٤٣. Federal Office for Information Security . White Paper. Security Recommendations for Cloud Computing Providers (Minimum information security requirements),23-35.avaliable at www.bsi.bund.de/grundschutz.

44. Che, Study on the Security Models and Strategies of Cloud Computing, 590.

45. Richard Holland. Ten Steps to Successful Cloud Migration. Eagle Genomics Ltd, 2011, 3-4. http://www.eaglegenomics.com/download-files/whitepaper/CloudWhitePaper.pdf (Accessed 20 November 2014)

46. Gonzalez. A quantitative analysis of current security concerns and solutions for cloud computing ,3 .

47. Anthony Bisong, and Syed (Shawon) M. Rahman. "An overview of the Security Concerns in Enterprise Cloud Computing." International Journal of Network Security & Its Applications (IJNSA), 3, 1, (January 2011): 38. http://arxiv.org/ftp/arxiv/papers/1101/1101.5613.pdf (Accessed 13 October 201٥)

48. Denis Galvi ,and Mang Sun. "Avoiding the Death Zone: Choosing and Running A Library Project in the Cloud." Library Hi Tech 30, 3, (2012): 422. Retrieved from Emerald Group Publishing Limited