استقصاء وعي منسوبي إدارات تكنولوجيا المعلومات للانتقال إلى خدمة الحوسبة السحابية
(حالة دراسية: مؤسسات يمنية)

أ. م. د. اروى الارياني
اليمن – جامعة سبأ

الباحثة سماح عبد العزيز العريقي
اليمن – الجامعة اليمنية

المستخلص

قدمت الحوسبة السحابية خدمات كثيرة لقطاع الأعمال، وانتشر استخدامها بشكل كبير. ولكن في نفس الوقت مازالت التهديدات الأمنية تثير مخاوف المؤسسات والشركات خاصة الكبيرة منها وذات النشاط الحرج. هدف البحث إلى استطلاع هذه المخاوف ومعرفة أسبابها وطرق مجابهتها. وذلك بهدف معرفة واستطلاع رأي مدراء وموظفي بعض المؤسسات اليمنية عن الحوسبة السحابية ومدى وعيهم لفوائدها ومخاطرها وكذا مدى جاهزية مؤسساتهم من وجهه نظرهم للانتقال لهذه البيئة الجديدة. أظهر تحليل الاستبيانات أن الأغلبية يعرفوا عن الحوسبة السحابية بقدر مقبول ولكن مخاوفها وتهديداتها مازالت غامضة وغير معروفة لدي الأغلبية. بشكل عام نتوصل إلى أن المؤسسات اليمنية مازالت تحتاج لكثير من الوقت لتوعية موظفيها ذات العلاقة بفوائد ومخاطر الحوسبة السحابية. وفي الأخير تقدمت الباحثتان بمجموعة من التوصيات لعل أهمها ضرورة الاهتمام بالجانب البحثي للحوسبة السحابية بالمؤسسات اليمنية ومدها بالمعلومات الداعمة لها للانتقال السلس إلى بيئة الحوسبة السحابية.

الكلمات المفتاحية: الحوسبة السحابية، منتسبي إدارات تكنولوجيا المعلومات، المؤسسات اليمنية التهديدات الأمنية.

Abstract

Cloud computing offers a lot of benefits to business section. Most of the companies started to move to cloud computing, besides in the same time some companies specially the large ones still concern about the security in cloud computing. This research aims to discover the awareness among the managers and employees of the IT departments in Yemen organizations about the cloud computing and its security problems, as well as the readiness of moving to the new environment. The results of the data analysis presented that most of participates do awareness about the benefits of cloud computing but the security still unrealized. The Yemeni organizations still need a lot of awareness to their employees. Finally, the researchers presented recommendations to help the organizations move smoothly and safely to cloud computing.

1. المقدمة

تقدم لنا التكنولوجيا دائما الجديد ومنها الحوسبة السحابية كخدمة جديدة بهدف تيسير وتسهيل عمل المؤسسات والشركات والأفراد على حد سواء. وتعتمد هذه الخدمات على تسهيل العمل على المستفيدين لتغطية نطاق الاستخدام حتى يشمل مستخدمين من المتخصصين في التكنولوجيا أو غير المتخصصين. ولتحقيق هذا الهدف تعتمد كثير من الخدمات على الانترنت إلى إعطاء ميزة شفافية البنية التحتية بحيث لا تعني للمستخدم مكوناتها أو طرق عملها والاكتفاء بالاستفادة من الخدمة. ولكن ومهما كانت هذه الميزة مهمة وساعدت على توسيع نطاق المستفيدين، إلا أن الكل يركز على الجوانب الأمنية من حيث الحفاظ

على سرية وخصوصية البيانات وأمنية ممتلكات وموارد المؤسسات التي تستخدم تلك الخدمات (Aljoumah, et. al.,2015). قدمت الحوسبة السحابية خدماتها تحت عدة مفاهيم منها مفهوم الدفع عند الاستخدام عوضا عن قبل الاستخدام، مفهوم استئجار البنية التحتية عوضا عن شراءها، مفهوم المشاركة في البنية التحتية عوضا عن امتلاكها ومفهوم تقديم خدمة عوضا عن منتج ولكن هذه المفاهيم شكلت حاجز أمام المستفيد لمعرفة آليات الحفاظ على أمنية وسرية بياناته وممتلكاته على السحب حيث أن هناك طرف جديد يحتكر بعض من هذه الأليات وهو مقدم الخدمة.

2. أهداف الدراسة

تهدف الدراسة إلى معرفة أهم التهديدات التي تواجهه أمن الحوسبة السحابية بهدف تقديم رؤية عن مدى استيعاب المؤسسات اليمنية لمميزات ومخاطر الحوسبة السحابية ومدى استعدادها للتعامل معها وجاهزيتها للانتقال إليها وتسليط الضوء على هذا الجانب المهم.

3. أهمية الدراسة

تعتبر الأمنية دائما من المواضيع التي تؤرق مستخدمي التكنولوجيا خاصة عند ظهورها الأول ولكن تحرص الكثير من المؤسسات على الاستفادة منها ومحاولة التغلب على مشاكلها ومخاطرها. تكمن أهمية هذا البحث من أهمية الأمنية في الحوسبة السحابية التي باتت من التكنولوجيا الحديثة التي تقدم كثير من الخدمات والمميزات وتحرص كثير من المؤسسات على الاستفادة منها ولكن الهواجس الأمنية يمكن أن تكون عائق للاستخدام ومن هنا يأتي أهمية البحث الذي يركز على دراسة وضع معين وهو وضع المؤسسات اليمنية ومعرفة تأثير الهواجس الأمنية على استخدام الحوسبة السحابية. كما تكمن اهمية الدراسة في تعزيز النتاج الفكري العربي المنشور في مجال الحوسبة السحابية.

4. أسئلة الدراسة

- ماهي التهديدات التي تواجهه مستخدمي الحوسبة السحابية؟
- كيف يتم مواجهة هذه التهديدات؟
- ما مدى وعي منتسبي إدارات تكنولوجيا المعلومات في المؤسسات اليمنية لمفهوم الحوسبة السحابية.

5. منهجية الدراسة

تعتمد هذه الدراسة على المنهج الاستكشافي من خلال البحث في الدراسات السابقة التي قدمت استطلاعات وتحليل لجوانب الأمنية في الحوسبة السحابية وتكوين نظرة فاحصة لأهم ثغرات هذه الأمنية من خلال معرفة التهديدات التي تتعرض لها الخدمة على السحب. يعتمد البحث الاستكشافي على مراجعة الدراسات المتاحة وبياناتها بهدف الوصول إلى معرفة الظاهرة أو اكتساب رؤية جديدة من أجل الوصول إلى صياغة أكثر دقة لموضوع الدراسة. ومن ثم سيعتمد البحث على استطلاع الوضع في المؤسسات اليمنية من خلال الاستبيانات لعينة من مدراء وموظفي التكنولوجيا في عدد من المؤسسات اليمنية.

وصف الاستبيان

ينقسم الاستبيان إلى ثلاث محاور هم قياس معرفة المفاهيم الاساسية للحوسبة السحابية، قياس معرفة التهديدات التي تواجهه مستخدمي الحوسبة السحابية وأخيرا قياس مدى جاهزية هذه المؤسسات من وجهه نظر موظفيها للاستفادة من خدمات السحب. تحت كل محور عدة عبارات مستسقاة من الدراسات السابقة.

يندرج تحت المحور " معرفة المفاهيم الاساسية للحوسبة السحابية " 11 عبارة على النحو التالي:

ما مدى معرفتك بوجود تقنية الحوسبة السحابية، ما مدى معرفتك بالتطبيقات والخدمات التي تقدمها تقنية الحوسبة السحابية، ما مدى معرفتك بتقنية I cloud الموجودة على اجهزة I pad و I phone ، ما مدى معرفتك بالمواقع التي تعتمد على تطبيقات الحوسبة السحابية مثل google chrome ، ما مدى معرفتك أن الحوسبة السحابية تمكنك من استئجار الأجهزة المطلوبة لعملك عوضا عن شراءها، ما مدى معرفتك أن الحوسبة السحابية تمكنك من التعامل مع النظام من أي مكان ومن أي أجهزة، ما مدى معرفتك أن الحوسبة السحابية تخفض من كلفة النظام، ما مدى معرفتك أن الحوسبة السحابية تشركك مع أخرين بنفس المصادر، ما مدى معرفتك أن الحوسبة السحابية توفر مراكز بيانات، ما مدى معرفتك أن الحوسبة السحابية توفر مساحة تخزين، ما مدى معرفتك بوجود مزودي خدمة الحوسبة السحابية. وتنوعت الخيارات بين معرفة جيدة جدا، معرفة جيدة، معرفة بسيطة، لا اعرف.

ويندرج تحت محور " قياس معرفة التهديدات التي تواجهه مستخدمي الحوسبة السحابية " 7 عبارات على النحو التالي:

من التهديدات في الحوسبة السحابية أساءة الاستعمال والأعمال الخبيثة مثل دخول غير المخول لهم نتيجة سهولة اجراءات الدخول، من التهديدات في الحوسبة السحابية أن واجهات التطبيقات بين العميل (المنظمة) ومزود الخدمة غير أمنة، من التهديدات في الحوسبة السحابية وجود الخبيث الداخلي – والخبث الداخلي هو استغلال أن الموظفين لا يملكون الرؤية الواضحة حول سياسات مزودي الخدمة للدخول للنظام من خلالهم للأضرار فيه– ، من التهديدات في الحوسبة السحابية قضايا التكنولوجيا المشتركة حيث يتقاسم عدة جهات نفس الموارد وهذا قد يساعد على عدة اختراقات للأنظمة من خلال هذه الثغرة، من التهديدات في الحوسبة السحابية فقدان أو تسرب البيانات دون عمل نسخ احتياطية والتي تعتبر من مسئولية مزود الخدمة، من التهديدات في الحوسبة السحابية احتمال سرقة الخدمة أو الحساب عادة ما تتم سرقة وثائق التفويض من خلال الخداع والغش واستغلال الثغرات الامنية بالبرامج، من التهديدات في الحوسبة السحابية كثير من المخاطر غير المعروفة . فمثلا نتيجة أن المنظمات المستفيدة اقل ملكية للأجهزة والبرامج وعمليات الصيانة فتظل اجراءات الأمن الداخلي والاتفاقيات الامنية غير معروفة للمنظمة. وتنوعت الاختيارات بين نعم، أحيانا، قليل، لا أعرف.

وأخيرا يندرج تحت المحور الثالث " مدى جاهزية هذه المؤسسات من وجهه نظر موظفيها للاستفادة من خدمات السحب " 6 عبارات على النحو التالي:

لدينا بنية تحتية جيدة، لدينا كادر تقني جيد، أعتقد أن الإدارة العليا يمكن أن تستوعب فوائد الحوسبة السحابية، أعتقد أن مدراء إدارات التكنولوجيا يمكن أن يستوعبوا فوائد الحوسبة السحابية، أعتقد أن

الموظفين يمكن أن يستوعبوا فوائد الحوسبة السحابية، أعتقد أن المؤسسة جاهزة للحوسبة السحابية. وتنوعت الاختيارات بين نعم بشكل كبير، نعم بشكل متوسط، نهائيا، لا أعرف.

6. الدراسات السابقة

تاريخ تطور الحوسبة السحابية

السحابة هي تعبير كان يستخدم في البداية للإشارة إلى الإنترنت، ولكن جاءت فكرة البرامج كخدمات عندما عبر" جون مكارثي "الأستاذ بجامعة ستانفورد عن الفكرة بقوله" قد تنضم الحوسبة لكي تصبح خدمة عامة في يوم من الأيام"، حيث رأى أنه من الممكن أن تؤدي تكنولوجيا مشاركة الوقت Time sharing إلى مستقبل تُباع فيه الطاقة الحاسوبية وحتى التطبيقات الخاصة كخدمة من خلال نموذج تجاري، وبالفعل حظت تلك الفكرة بشعبية كبيرة في أواخر الستينيات، ولكنها تلاشت في منتصف السبعينيات عندما اتضح أن التكنولوجيا الحديثة المتعلقة بمجال تكنولوجيا المعلومات غير قادرة على الحفاظ على هذا النموذج من الحوسبة المستقبلية .ولكن عادت هذه الفكرة مؤخرا لتصبح مصطلحا شائعا cloud computing في مجالات التكنولوجية والمؤسسات وظهرت الحوسبة السحابية التي يتم فيها تقديم المصادر الحاسوبية كخدمات، ويتاح للمستفيدين الوصول إليها عبر شبكة الإنترنت (السحابة)، دون الحاجة إلى المتابعة الفنية للبنية التحتية ولا حتى امتلاكها فعليا للاستفادة من الخدمة (رحاب فايز ، 2013).

مفهوم الحوسبة السحابية

الحوسبة السحابية هي أحد التقنيات، التي يتم فيها تقديم المصادر الحاسوبية كخدمات، ويتاح للمستخدمين إمكانية الوصول إليها عبر شبكة الإنترنت (السحابة) ، من أي مكان وفي أي وقت ودون الحاجة إلى امتلاك المعرفة، أو الخبرة، أو حتى التحكم بالبنية التحتية التي تدعم هذه الخدمات. كما يمكن النظر إلى الحوسبة السحابية على أنها مفهوم عام يشمل البرمجيات كخدمة، وغيرها من التوجهات الحديثة في عالم التقنية التي تشترك في فكرة الاعتماد على شبكة الإنترنت لتلبية الاحتياجات الحوسبة للمستفيدين (رحاب فايز، 2013).

كما تم تعريف الحوسبة السحابية في الويكيبيديا أنها مصطلح يشير إلى المصادر والأنظمة الحاسوبية المتوفرة تحت الطلب عبر شبكة الانترنت والتي تعمل على 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 وخدمة البريد الإلكتروني والطباعة عن بعد، ويستطيع المستخدم عند اتصاله بالسحابة التحكم في هذه الموارد عن طريق واجهة برمجية بسيطة تبسط الكثير من التفاصيل والعمليات الفنية الداخلية. كما أن هذه الموارد يمكن المشاركة فيها بين عدة عملاء (ويكيبيديا).

يمكن تلخيص أهم مفاهيم الحوسبة السحابية بأنها تقدم خدمة عوضا عن منتج، تأجر الموارد المطلوبة عوضا عن شراءها، مبدأ الدفع عند الاستخدام فقط وأخير المشاركة في هذه الموارد وفقا لنوع السحب المطلوبة.

معمارية الحوسبة السحابية

الحوسبة السحابية قامت بدمج تقنيات الحوسبة المختلفة لتقديم الخدمات إلى المستفيدين بأبسط الطرق. لفهم المسائل الأمنية المتصلة بالحوسبة السحابية، من المهم معرفة المفاهيم التي تساهم في الحوسبة السحابية. لاقى تعريف المعهد الوطني للمعايير والتكنولوجيا (The National Institute of Standards and Technology's (NIST)) الحوسبة السحابية قبول على نطاق واسع ويعتبر هذا التعريف من NIST أن الحوسبة السحابية تعتمد على نموذج ثلاثي لتوفير الخدمات يتكون من: 1- الخصائص الاساسية 2- نماذج الخدمة 3- نماذج النشر (Mazhar, et. al , 2015) ، (Sah, et. al,214).

الخصائص الأساسية: تتبلور الخصائص الأساسية للحوسبة السحابية على عدة مفاهيم منها (Fernandes, et. al, 2014) (Mazhar, et. al,2015):

- عند طلب الخدمة (On-demand self-service): يمكن للمستفيدين طلب الخدمة وإدارتها من السحب دون أي اهتمام بالجوانب الفنية والبنية التحتية.
- الوصول للشبكة (Broad network access): كافة خدمات المستفيدين والتطبيقات والبيانات الموجودة على السحابة يمكن الوصول إليها من قبل المستفيدين من خلال الآليات الموحدة والبروتوكولات. كما توفر خدمات لدعم البيئة غير المتجانسة مثل الهواتف المحمولة واجهزة الكمبيوتر المحمولة ومحطات العمل.
- تجميع الموارد (Resource pooling): تعتبر موارد السحب مشتركة بين العديد من المستفيدين عن طريق تجميع الموارد في بيئة متعددة المستفيدين. وتتسم بالشفافة بشأن موقع هذه الموارد أو المستفيدين المشتركين.
- المرونة السريعة (Rapid elasticity): تعطى الموارد لكل مستفيد بسرعة ومرونة ووفقا لمنوال الدفع عند الاستخدام (pay-as-you-go).
- قياس الخدمة (Measured service): تقدم الموارد للمستفيد بشكل ديناميكي يمكن قياسه ووفقا لمنوال الدفع عند الاستخدام (pay-as-you-go)

وهذه الخصاص الذي عرفها المعهد الوطني للمعايير والتكنولوجيا تم اضافة خاصية مهمة قد لا تكون اساسية من قبل The cloud Security Alliance (CSA) هي خاصية تعدد الاتفاقيات (Multi-tenancy): وهي الخاصية التي تمكن عدة مستفيدين من استخدام مورد من موارد السحابة دون ان يكونوا منتمين لنفس المنظمة ويمكن ان نقول انهم مرتبطين افتراضيا.

نماذج الخدمة: قسم المعهد الوطني للمعايير والتكنولوجيا نماذج الخدمة إلى (Cloud security alliance,2011)، (Aljoumah, et. al,2015):

- البرمجيات كخدمة Software as a Service (SaaS): تقدم البرامج عبر السحابة وتجعلها نموذجا يحتذى به في توزيع البرامج عبر الإنترنت. مع العلم أن الزبائن الذين يدفعون ثمن الاستخدام لا يمتلكون هذه البرامج التي يستخدموها.

- المنصة الحاسوبية كخدمة Platform as a Service (PaaS): لا تعطي المستفيد السيطرة على البنية التحتية للسحب ولكن فقط التحكم على التطبيقات التي نقلها للسحابة.
- البنية التحتية كخدمة Infrastructure as a Service (IaaS): تقدم الموارد على شكل الأنظمة الافتراضية التي يتم الوصول اليها من خلال الانترنت. ويمتلك موفر خدمة الاتصال communications service provider (CSP) السيطرة على الموارد الاساسية.

نماذج النشر: من نماذج النشر

(abu-Sanab, et.al, 2014) , (Huth, et. al, 2011) , (Kumar, et. al, 2011) , (Mazhar, et. al, 2015)

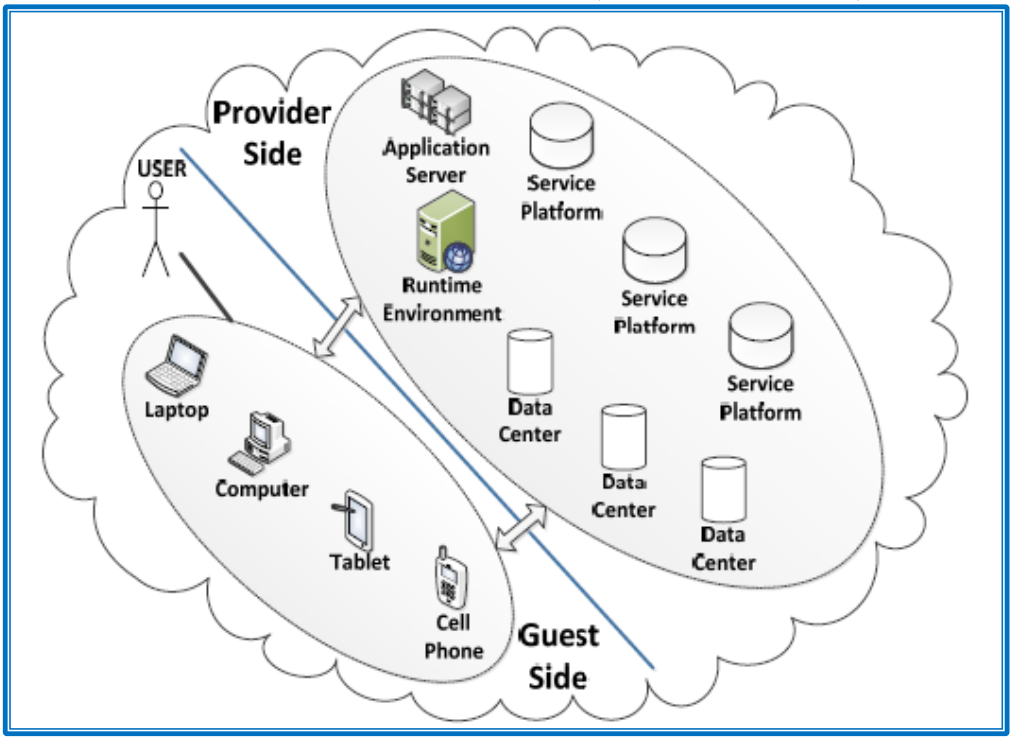
- السحب الخاصة (Private cloud): هي سحب خاصة لاستخدام جهة معينة، توفر مراقبة كاملة للبيانات، تضمن الأمن وجودة البيانات. قد تُدار من قبل منظمة أو طرف ثالث ويمكن النفاذ لها من العمل أو المنزل أو أي مكان بعيدا عن مكان العمل.
- السحب العامة (Public cloud): متاحة لعامة الجمهور أو لقطاع معين وهي مبنية على أساس تجاري وعادة ما تكون مملوكة من قبل شركات بيع الخدمات السحابية. هذا ما يسمح للمستخدم بتطوير العمل على برمجية معينة أو استغلال مورد معين من خدمة في السحاب عن طريق مبدأ الاستئجار مع تكلفة مادية ضئيلة جدا بالمقارنة مع النفقات الكبيرة المرتبطة عادة بامتلاك تلك الخدمات.
- السحب المجتمعية (Community cloud): يتم تقاسم البنية التحتية السحابية من قبل العديد من المنظمات والذين عادة ما يتمتعون بالمتطلبات والاهتمامات نفسها ومجال العمل المشابه، والنفاذ للسحابة ممكن أن يتم من مقر الشركة/الشركات التي تتشارك هذه الخدمة أو من خلال طرف ثالث حسب الطلب.
- السحب الخليطة (Hybrid cloud): البنية التحتية السحابية لها تكون مركبة من اثنين أو أكثر من السحب (الخاصة، والمجتمعية، أو العامة) والتي ترتبط بمعايير موحدة أو تكنولوجيا خاصة تمكنها من السماح للبيانات و/أو التطبيقات لكي يتم نقلها من سحابة إلى أخرى.

كيانات الحوسبة السحابية Cloud computing entities

عرف (Barron,2013) كيانات الحوسبة السحابية على النحو التالي:

- مزودي السحب (Cloud Providers): وهي تشمل مزودي خدمة الانترنت، شركات الاتصالات، عمليات الاعمال، مراكز البيانات والانظمة والخدمات المختلفة المقدمة للمستهلك.
- سماسرة خدمة السحب (Cloud Service Brokers): تشمل مستشاري التكنولوجيا، الخدمات الاحترافية في المنظمات، التي تساعد المستفيد لاختيار أفضل حلول في الحوسبة السحابية. وهو الذي يقوم في المفاوضات بين مزود الخدمة والمستفيد.
- بائع السحب (Cloud Resellers): يعتبر أهم عامل في تسويق السحب حيث يقوم مزود الخدمة باختيار شركة استشارية او بائع لعرض منتجاتها والخدمات المقدمة في السحب.

ويوضح الشكل التالي ما يوجد بكل من طرفي الحوسبة السحابية وهما العميل ومزود الخدمة.



المخطط من (Barron,2013)

مزود الخدمة في الحوسبة السحابية

من أهم ما استجد في الحوسبة السحابية هو وجود ما يعرف بـ مزود الخدمة، ألقت دراسة الباحثان (Alshammari, et. al, 2013) الضوء على هذا الجانب من خلال التساؤلات التالية: أين موقع البيانات على السحب؟ هل هو قانوني أن تنتقل بيانات العميل إلى مراكز بيانات في دولة أخرى؟ كم ستبقى البيانات على السحب؟ من يتحكم بسياسات إدارة هذه البيانات؟ هل يمكن نسخ البيانات من قبل مزود الخدمة؟ أو تدميرها أو جعل الدخول لها غير ممكن؟ هل يحتفظ مزود الخدمة بالبيانات لأغراض خاصة فيه؟ وضحوا الباحثين (Alshammari, et. al, 2013) أن اغلب خدمات السحب لا تعطي مكانا جغرافيا محددا لمستخدمي التطبيقات وحتى لا يحق لهم طلب ذلك، ولكن بعض الجهات الحكومية تشترط أن تكون على علم بمكان تطبيقاتها وقد تشترط أيضا أن تكون ضمن نطاق جغرافي تتوافق القوانين واللوائح فيه مع ما هو متفق عليه في بلدانهم. من حق المستفيدين أن يكونوا على علم أن نسخ من بياناتهم موزعة في مواقع متعددة حتى تكون موجودة في حالة حدوث أي تعطل لأحد هذه المواقع، وهذا مما يجب على موفر الخدمة تقديمه. كما وضحوا (Alshammari, et. al ,2013) أن عدم وجود معايير محددة لخدمات السحب، انما خاضعة لاتفاقية مزود الخدمة، يجعل من هذه وضوح الاتفاقية الأرضية الضرورية لمعرفة مسئوليات مزود الخدمة.

مميزات وعيوب الحوسبة السحابية

توفر الحوسبة السحابية تكاليف كبيرة على مستخدميها نتيجة عدم الاضطرار إلى شراء أجهزة خاصة وكذلك تكاليف صيانتها الدورية كما توفر الحوسبة السحابية دخولاً آمناً على البيانات والمعلومات المخزنة

عليها بشرط توفر الدليل على أن المستخدم له الحق في الاطلاع على هذه البيانات واستخدامها. تعتبر الحوسبة السحابية وسيلة ممتازة للحفاظ على البيانات والمعلومات خشية الفقدان. ومن المميزات أيضاً ضمان عمل الحوسبة السحابية بشكل دائم وفى هذه النقطة تحديداً يأتي دور موفري الخدمة الذين يتعهدون بتوفير خدمة آمنة وجيدة المستوى و بدون انقطاع (Migrating Applications,2013) , (Apostu)

وفي نفس الوقت هناك عدة عيوب أو مخاوف، مثل مخاوف انقطاع الخدمة أو توقفها لفترة وتحدث هذه المشاكل أحيانا رغم جودة وفعالية الصيانة. ومن العيوب التي يجب على مستخدمي السحب معرفتها أنهم يقوموا بتسليم بيانات وممتلكات شركاتهم لطرف آخر هو موفر الخدمة، وعليه يتوجب على المستفيدين اختيار موفري الخدمة الموثوق فيهم ودراسة اتفاقية الخدمة جيدا. كما أن وضع بيانات الشركة على السحب قد تكون عرضة للاختراق والقرصنة للبيانات الحساسة والمهمة. ورغم ميزة مفهوم استئجار الموارد إلا أنه يجعل الشركات الصغيرة معتمدة كليا على هذه الموارد والتي لا تمتلكها فعليا. وللوهلة الأولى تبدو خدمة الحوسبة السحابية أرخص بكثير من غيرها إلا أن معرفة ما إذا كانت الشركة المستفيدة تستفيد من كافة مميزات التطبيقات التي تستأجرها أم لا قد يجعلها تبدوا غير متوافقة مع الثمن حيث أن هذه التطبيقات تحت سيطرة موفر الخدمة. كما يعاب على خدمة الحوسبة السحابية فقدان الخصوصية نوعا ما (Apostu, et. al, 2013). وبإيجاز، يبدو مقنعا أن من الضروري على الحوسبة السحابية الاهتمام بتحديد معايير واجراءات الأمن والخصوصية للبيانات وكذلك خدمة الاسترداد وهذا قد يساعد على زيادة ثقة الجمهور في السحابة، ولكن دون هذه التنظيمية اللازمة ومعايير الخدمة فأن بيئة خدمات السحب ستظل "غامضة" (Sichao,2012).

أمنية الحوسبة السحابية

أخذت أمنية الحوسبة اهتمام كبير من كثير من الباحثين الذين قاموا برصد الثغرات والتهديدات وكيفية مواجهتها (Zhou, et. al, 2010).

قام الباحثون (Mazhar, et. al, 2015) في هذه الدراسة بعمل استطلاع (مسح) لمعرفة تفاصيل القضايا الأمنية التي تنشا بسبب طبيعة الحوسبة السحابية. قدمت الدراسة أحدث الحلول لمواجهة القضايا الأمنية. وعلاوة على ذلك قام الباحثون بإعطاء رأى مختصر لأهم الثغرات الأمنية في الحوسبة السحابية بما فيها تلك التي على الهواتف النقالة كما سلطوا الضوء على القضايا المفتوحة واتجاهات البحوث المستقبلية. وقد توصلوا الباحثون من خلال الاستطلاع إلى أنه وعلى الرغم من المزايا التي تقدمها الحوسبة السحابية، إلا أن هناك مخاوف أمنية لدي المستفيدون والتي قد تعيق سرعة معدل اعتماد الحوسبة السحابية. على جميع المستفيدين سواء كانوا أفراد أو منظمات ان يدركوا جيدا للتهديدات الامنية الموجودة في السحابة وسبل مواجهتها، وعليهم اتخاذ التدابير التي ستساعد على القيام بتحليل التكاليف والمنافع للتحول الى السحابة بطريقة ناجحة وأمنة. أظهر هذا الاستطلاع أيضا أن المخاوف الأمنية التي تنشا بسبب المشاركة الافتراضية الموجودة ضمن طبيعة نموذج الحوسبة السحابية تستدعي اتخاذ اجراءات اضافية لضمان الأمنية. كما ناقش الباحثون في هذه الدراسة الحوسبة السحابية على الهواتف النقالة وذلك

بسبب زيادة استخدامها. هدفت الدراسة من خلال تسليط الضوء على هذه القضايا إلى تحفيز البحوث والدوائر الاكاديمية للتركيز على هذا الموضوع.

في دراسة Padhy مع أخرون (Padhy, et. al, 2011) قام الباحثون بعدة أبحاث لتحليل تحديات الحوسبة السحابية وتقديم أفضل الممارسات لمزودي الخدمات. وتم مناقشة القضايا الأمنية في بيئة الحوسبة السحابية منها (الوصول الى التطبيقات والخدمات – نقل البيانات – حماية الآلة الافتراضية – حماية الشبكة – حماية الخصوصية – تكامل البيانات – موقع واتاحة البيانات والسياسات الأمنية وإدارة الحزم). وقد ظهرت عدة تحديات قام الباحثون بدراستها منها (اتفاقية مزودي الخدمة – إدارة أمنية حوسبة البيانات – تشفير البيانات – قابلية تبادل المعدات والموارد – التحكم بالوصول – إدارة الطاقة – دعم المزودات – خدمة والإتاحة – المعايير العامة للسحب – إدارة المنصة). وقد هدفت هذه الدراسة إلى فهم تحديات الحوسبة السحابية وسبل مواجهتها.

في هذه الدراسة (Barron, et. al, 2013) قام الباحثون بعدة تحقيقات عن الواقع الحياتي لبعض شركات السحب التي تعرضت لهجوم واختراقات. تتضمن أمينة الحوسبة السحابية عدة قضايا وعدة خوارزميات تعمل على منع الهجوم المختلف وحماية هذه الأنظمة السحابية. وقد قام الباحثون بتطوير تكنولوجيات جديدة لتحسن الأمنية. كما عمل الباحثون على أخذ عدة حالات منها هجوم الشركات بواسطة (الهندسة الاجتماعية – تعليق توقيع XML– حقن Malware– معالجة البيانات – سرقة الحسابات – الشبكة المحلية اللاسلكية– حالة انقطاع الخدمة). وقام الباحثون بدراسة حلول ووضع خوارزميات لمزودي الخدمة تساعدهم على منع هذه الهجوم واكتشافها في المستقبل.

تهديدات أمنية الحوسبة السحابية

رصد تقرير منظمة أمنية السحب (Cloud Security Alliance (CSA),2011 الذي جاء تحت عنوان" Top Threats to Cloud Computing" والذي صدر في مارس 2010 كثير من التهديدات الأمنية في الحوسبة السحابية. وجاء هذا التقرير لمساعدة المنظمات المهتمة بالانتقال إلى خدمات الحوسبة السحابية في اتخاذ القرار مع إدراك حجم المخاطر والتهديدات التي قد تواجهها. من التهديدات المرصودة في التقرير ما يلي:

التهديد 1: أساءه الاستعمال والأعمال الخبيثة (Abuse & Nefarious)

الوصف: أن اجراءات التسجيل البسيطة والسهلة نسبيا للوصول الى خدمات السحابة سهلت على مرسلي الرسائل غير المرغوب فيها، والمتطفلين وغيرهم من المتسللين الاستفادة منها لشن هجمات مختلفة. وأمثلة على هذه الهجمات الهجوم على كلمة المرور الرئيسية (password)، تسكين البيانات الخبيثة (key cracking)، اخفاء الخدمة عن المستفيدين (DDOS)، شن هجوم ديناميكية، بناء جداول قوس قزح (rainbow tables) والتي تستخدم لاستعادة أرقام المرور، التحكم عن بعد بـ القيادة/المراقبة (botnet)، حل مشاكل اللـ CAPTCHA التي تكشف هوية المهاجم إذا كان نوع من أنواع البرمجيات الخبيثة. ويستهدف هذا التهديد مستوى البنية التحتية كخدمة PaaS والمنصة الحاسوبية كخدمة IaaS.

التهديد 2: واجهات التطبيقات غير أمنة (Insecure Interfaces & APIs)

التوصيف: تعتبر وجهات التطبيقات التي يتفاعلوا المستخدمين مع الخدمات من خلالها ثغرة، يمكن من خلالها توقع هجوم. وعلى موفر الخدمة ضمان أمنية هذه الواجهات وبنفس الوقت على المستفيد التنبه للمخاطر الأمنية عند الاستخدام من خلال إدارة ومراقبة الخدمة. أمثلة على تلك التهديدات تبعية الـ API، محدودية الرصد/امكانيات التسجيل، عدم مرونة التحكم بالوصول، وصول مجهول، يمكن اعادة استخدام المميزة/كلمات مرور، مصادقة النصوص و/أو نقل المحتويات من التصاريح. ويستهدف هذا التهديد مستوى البنية التحتية كخدمة IaaS، والبرمجيات كخدمة SaaS والمنصة الحاسوبية كخدمةPaaS

التهديد 3: الخبيث الداخلي (Malicious Insiders)

التوصيف: الخبيث الداخلي يشكل خطرا كبير في بيئة الحوسبة السحابية، حيث يستغل المهاجمين أن المستخدمين لا يملكوا رؤية واضحة حول سياسات واجراءات موفر الخدمة وعليها تعتبر هذه ثغرة للاستهداف والهجوم. على سبيل المثال دخول الموظفين والمستخدمين للخدمة والمراقبة والامتثال لمعايير الممارسات عادة لا تكون شفافة للمستفيدين (تحجب عليهم بهدف تسهيل العمل) فيتمكن المهاجم من استغلال هذا والحصول على الدخول غير المصرح به الى داخل المنظمات وممتلكاتها. بعض هذه التهديدات قد تشمل الاضرار تماما بالجانب المالي وتسبب فقدان الانتاجية. ويستهدف هذا التهديد مستوى البنية التحتية كخدمة IaaS والمنصة الحاسوبية كخدمة PaaS والبرمجيات كخدمة SaaS.

تهديد 4: قضايا التكنولوجية المشتركة (Shared Technology Issues)

الوصف: يقوم مستوى البنية التحتية كخدمة IaaS في الحوسبة السحابية على مفهوم التشاركية بالبنية الأساسية (مثل أقسام القرص، وحدة المعالجة المركزية، وحدات معالجة الرسومات (GPU)، الخ) ولكن غالبا ما تكون هذه الموارد غير مصممة لاستيعاب بنية متعددة المستأجر (multi-tenant). ومثل هذا العيب سمح لأنظمة التشغيل المستضافة الحصول على مستويات غير مرخص بها من تحكم وتأثير على المنصة (platform). ويستهدف هذا التهديد مستوى البنية التحتية IaaS.

التهديد 5: فقدان أو تسرب البيانات (Data Loss or Leakage)

التوصيف: من التهديدات التي تتعرض لها الحوسبة السحابية أيضا احتمالات حذف البيانات او تعديلها بدون عمل نسخة احتياطية، وفك ربط السجل من السياق الأوسع، فقدان مفتاح الترميز والوصول غير المصرح به للبيانات الحساسة والحرجة، احتمالية زيادة حجم في البيانات في الحوسبة السحابية بسبب البنية. ويستهدف هذا التهديد مستوى البنية التحتية كخدمة IaaS، والبرمجيات كخدمة SaaS، والمنصة الحاسوبية كخدمة PaaS .

التهديد 6: الاستيلاء على الحساب أو الخدمة (Account or Service Hijacking)

التوصيف: عادة ما تتم استغلال الثغرات الأمنية بالبرامج لسرقة وثائق التفويض من خلال هجمات تعتمد على الخداع والغش. ويستهدف هذا التهديد مستوى البنية التحتية كخدمة IaaS، والبرمجيات كخدمة PaaS، والمنصة الحاسوبية كخدمة SaaS

التهديد 7: المخاطر غير المعروفة (Unknown Risk Profile)

التوصيف: خدمات الحوسبة السحابية تعنى ان المنظمات المستفيدة اقل ملكية للأجهزة والبرامج وعمليات الصيانة. وعلى الرغم من ان هذا يوفر مزايا هامة خاصة من حيث الكلفة، إلا أنه ينبغي للمنظمات أن تكون على علم بقضايا كثيرة مثل إجراءات الأمن الداخلي، اتفاقيات الأمنية، الولوج للسحابة وغيرها مالم فأنها قد تتعرض لهجمات مختلفة تستهدف مستوى البنية التحتية كخدمة IaaS، والبرمجيات كخدمة SaaS، والمنصة الحاسوبية كخدمة PaaS.

كما رصد (Security for Cloud Computing) التهديدات في الحوسبة السحابية على النحو التالي: فقدان قوة الحكم أو التحكم (Loss of governance)، ضبابية المسؤولية (Responsibility ambiguity)، المصادقة والترخيص (Authentication and Authorization)، فشل العزل (Isolation failure)، المخاطر القانونية (Compliance and legal risks)، معالجة الحوادث الأمنية (Handling of security incidents)، إدارة ضعف الواجهات (Management interface vulnerability)، حماية التطبيق (Application Protection)، حماية البيانات (Data protection)، الخبيث الداخلي (Malicious behavior of insiders)، فشل العمل من مقدم الخدمة (Business failure of the provider)، عدم توفر الخدمات (Service unavailability)، التقيد بالمورد (lock-in Vendor)، فقدان أمنية واكتمال البيانات (Insecure or incomplete data deletion)، الرؤية والمراجعة (Visibility and Audit).

مواجهة تهديدات أمنية الحوسبة السحابية

رصد (Security for Cloud Computing) عشر خطوات لمواجهة هذه التهديدات على النحو التالي:

- **ضمان الادارة الفعالة للأخطار والتهديدات:** بالطبع فأن كافة المنظمات لديها سياساتها لضمان أمنية تطبيقاتها وأنظمتها على الإنترنت وهي نفس السياسات عند الانتقال لخدمة السحب ويضاف إليها معرفة أن المسئولية هنا مقسمة بين موفر الخدمة والمستفيد وعليه يجب معرفة ذلك بوضوح، وأيضا إدراك أن التصميم الفيزيائي والسيطرة على العمليات هي بالحقيقة بيد موفر الخدمة وأخيرا أن هناك واجهات للتعامل بين المستفيد وموفر الخدمة يجب أن تكون أمنة.
- **مراجعة الحسابات والعمليات التنفيذية:** يجب فهم بيئة الرقابة الداخلية من مقدم الخدمة السحابية، بما في ذلك المخاطر والضوابط الاخرى والبيئة وقضايا التحكم وكذلك الوصول الى مراجعة حسابات الشركات بما في ذلك سير العمل وحجمه واخيرا التأكيد على إدارة ومراقبة مرافق خدمات السحب وكيفية تامين هذه المرافق.
- **إدارة المستخدمين والصلاحيات والهويات:** لضمان حماية البيانات والمعلومات يجب الارتكاز على نقطتين هامتين هما ضمان عزل تطبيقات وبيانات العملاء في بيئات متعددة المستأجرين وتوفير الحماية لأصول العملاء من الوصول غير المصرح به وهذا من مسئولية مزود الخدمة.
- **ضمان حماية البيانات:** من المعروف أن البيانات هي اساس كافة الأعمال والتطبيقات، والحوسبة السحابية لا تخرج عن هذا المفهوم ولكن لها مستجداتها من حيث توزع هذه البيانات والتطبيقات

ودخول طرف جديد بالمسئولية هو موفر الخدمة. تقع المسئولية أكثر على المستفيد من الخدمة على مستوى البنية التحتية كخدمة IaaS وعلى المستوى البرمجيات كخدمة SaaS تقع المسئولية أكثر على موفر الخدمة وأخيرا على المستوى المنصة الحاسوبية كخدمة PaaS تتشارك المسئولية بين المستفيد وموفر الخدمة.

- **تطبيق سياسات الخصوصية:** على المؤسسات المسؤولة عن تحديد سياسات التصدي للتهديدات المتعلقة بالخصوصية وحماية البيانات، نشر الوعي داخل المنظمة بين المستخدمين لصد هجوم الخبث الداخلي. كما أن من مسؤوليتها أيضا عن ضمان تقيد والتزام موفر الخدمة على السحابة بسياسات الخصوصية.
- **تقييم الاحكام المتعلقة بأمن تطبيقات السحب:** على المستفيدين من الخدمة السحابية الوعي بأن نشر بياناتهم وتطبيقاتهم على السحابة، فأنهم يفقدون بعض من السيطرة والتحكم بسبب وجود الطرف الجديد وهو موفر الخدمة.
- **ضمان أمن شبكة السحابة والاتصالات:** أن مراجعة الحسابات ينبغي أن تتم بواسطة موظفين ذوي مهارات مناسبة والذي عادة ما ينتمون الى منظمة مستقلة لمراجعة الحسابات. التدقيق في التدابير الأمنية يجب ان تتم على اساس معايير الرقابة الامنية. يحتاج العملاء الى التحقق من أن مجموعات من الضوابط تلبي الاحتياجات الأمنية كاملة.
- **تقييم الضوابط الامنية في البنية الاساسية المادية وكافة ملحقاتها:** يجب ان يقدم موفر السحابة نظام آمن للتزويد وادارة هويات فريدة للمستخدمين والخدمات.
- **إدارة وفهم اتفاقية خدمة السحب:** حيث أن اتفاقية الخدمة تتضمن مسئولية منظمتين هما المستفيد من الخدمة وموفر الخدمة وعليه يجب أن تكون الاتفاقية واضحة ومحددة لمسئولية كل جهة.
- **فهم المتطلبات الأمنية في عمليات الخروج:** بقدر ما يجب ان يكون العميل قادر على ضمان الانتقال السلس للسحابة من دون خسارة أو اختراق البيانات فأنه يجب أن تكون عملية الخروج من السحابة أمن أيضا وان تسمح للعميل استرداد البيانات في شكل نسخ احتياطية بأمنية مناسبة، كما يجب الاحتفاظ بها لفترات متفق عليها قبل حذف السجلات والأحداث المرتبطة بها حتى تكتمل عملية الخروج بشكل آمن.

جاهزية الانتقال الآمن من المنصات الحالية إلى منصة الحوسبة السحابية

وضح (Sichao,2012) في بحثه أن الخطوة الأولى يجب أن تكون تقييم استخدام التطبيقات وعبء العمل الحالي، وبعدها دراسة وضع العمل وتطوير النهج التقني، يليها اعتماد نهج مرن ونموذج التكامل وأخيرا والأهم دراسة وتقييم الاتفاقية وإدارة متطلبات الأمان والخصوصية.

7. تحليل البيانات

تم توزيع عدد 24 استبيان كان عدد الذكور (19) والأناث (5) وتم توزيعها على الجهات التالية (وزارة العدل – مؤسسة التأمينات – البنك المركزي– بنك التسليف التعاوني والزراعي) على مدراء وموظفي تكنولوجيا المعلومات.

أظهر محور البيانات الأساسية للحوسبة السحابية أن هناك معرفة لا بأس عن الحوسبة السحابية فيها في أوساط منتسبي إدارات التكنولوجيا. إلا أن معرفة التطبيقات الخاصة بالحوسبة السحابية لاقت معرفة أقل. رغم أن الأغلبية يدركوا أن الحوسبة السحابية ستمكنهم من التعامل مع أنظمتهم من أي مكان إلا أن مفهوم استئجار البنية التحتية غير معروفة لدي البعض. ومن هذه الضبابية عن مفهوم استئجار البنية التحتية لم يتم استيعاب فكرة أن الحوسبة السحابية قد تقلص من تكلفة صيانة الأنظمة. مفهوم المشاركة المعتمد عليه الحوسبة السحابية أظهر أنه معروف لدي أغلبية العينة وكذا توفير مخازن البيانات ومساحات التخزين. بينما معرفة أن دور مزود للخدمة لم يبدوا معروف لدي البعض.

نستطيع أن نوضح أن المفاهيم الأساسية لدي العينة تبدوا جيدة نوعا ما، حيث أن المعرفة بالحوسبة السحابية مرتفعة ولكن خصائصها ومميزاتها مازالت ضبابية لدي الأغلبية. بيانات محور قياس معرفة التهديدات التي قد تتعرض لها الأنظمة المعتمدة على الحوسبة السحابية أظهرت أن معرفة واستيعاب هذه المخاطر مازالت غير واضحة لدي البعض وغير معروفة تماما لدي البعض. توزعت الإجابات على عبارات هذا المحور ما بين معرفة هذه المخاطر والاعتراف بوجودها، والبعض يقلل من أهميتها وهناك نسبة من المستهدفين أظهرت جهلها بهذا التهديدات تماما.

إذا ربطنا بين إجابات المحور الأول وهو فهم المفاهيم الأساسية للحوسبة السحابية والتي ندر فيها الأجوبة بعبارة " لا أعرف"، وبين بعض الإجابات في المحور الخاص بفهم التهديدات حيث أجاب البعض بـ "لا أعرف"، نستنتج أن معرفة أهمية الحوسبة السحابية مرتفع لدي العينة وبنفس الوقت هناك جهل عن التهديدات والمخاطر.

المحور الأخير وهو قياس الجاهزية للانتقال للحوسبة السحابية، نجد أن الأغلبية لديهم قناعة أن مؤسساتهم لديها البنية التحتية الجيدة وكذا الكادر الفني الجديد حيث حصل على أعلى نسبة موافقة.

ومن تحليل ملاحظات العينة في الاستبيان أهم تحدي في الحوسبة هو الأمن، لا يوجد قوانين ولوائح وإجراءات في اليمن تسمح باستخدام تقنية الحوسبة، اغلب الجهات لا زالت تؤمن بفكرة وجود البيانات في اجهزة مزودات يستطيعون رؤيتها، تعتبر السحابة الإلكترونية هامة جدا لحفظ ومعالجة البيانات بسهولة وإدارة الأعمال في جميع الظروف والأماكن. ومن خلال الملاحظات المدونة نهاية الاستبيانات، يعتبر التشفير من وجهة نظر العينة أحد أهم وسائل المتاحة للتغلب على التهديدات والمخاطر، كما افاد البعض أن الجانب المادي مهم جدا في استخدام تقنيات جديدة لان تغير التقنيات يحتاج الى موارد مالية كبيرة وهذا مالا يستوعبه الكثير من المؤسسات نظرا لسياسة التوفير من الصعب ان تكون المؤسسة جاهزة لاستخدام الحوسبة السحابية في هذه الفترة الحالية.

8. الخلاصة

نستطيع أن نستنتج من تحليل البيانات أن بذور المعرفة بالحوسبة السحابية موجودة بشكل جيد ومبشر. ولكن هناك جهل لدي الأغلبية عن التهديدات التي تتعرض لها الأنظمة على السحابة. وبشكل عام يتفق الأغلبية أن الجاهزية لمؤسساتهم مازالت ضعيفة أو بتعبير أدق يتشككوا في هذه الجاهزية. تقودنا هذه الخلاصة إلى التوصل لحقيقة غياب التأهيل والتطوير النظري والعملي للكادر الفني بالمؤسسات اليمنية في أخر المستجدات التكنولوجية. كما أن التوعية بالمخاطر أيضا لا يأخذ حيز من اهتمام الإدارات العليا رغم أن غياب هذا الجانب قد يؤثر بشكل كبير على أمنية الأنظمة في حالة انتقال المؤسسة إلى الحوسبة السحابية دون اعتماد توعية وتنبيه للموظفين لهذا المخاطر ودورهم في صد بعض من هذه الهجمات بالتعامل الصحيح عند الدخول للأنظمة الحاسوبية أو التعامل معها.

9. التوصيات

تتقدم الباحثتان بعدة توصيات للجهات المعنية في تكنولوجيا المعلومات، منها هذه التوصيات: –

1. لا تزال الحوسبة السحابية في مراحلها الأولى، خاصة في اليمن ولذا هناك حاجة إلى أبحاث ودراسات علمية وأكاديمية، تتناول الوضع الأمني في الحوسبة السحابية في المؤسسات اليمنية بشكل أعمق.
2. استمرارية الدورات التدريبية والتوعية لكافة الموظفين في إدارات التكنولوجيا والموظفين بالإدارات ذات الصلة.
3. رفع الوعي الأمني من ناحية التعامل مع الأنظمة بشكل خاص أو خصوصية عمل المؤسسة بشكل عام.
4. دراسة وتقييم الواضع الراهن وتحديد مطالب الانتقال للحوسبة السحابية بهدف رفع الكفاءة وتقليص الكلفة قبل الانتقال الفعلي للحوسبة السحابية.

المراجع

1. رحاب فايز احمد سيد (2013) " نظم الحوسبة السحابية مفتوحة المصدر :دراسة تحليلية مقارنة"، المجلة العراقية لتكنولوجيا المعلومات " المجلد الخامس – العدد الثاني – لسنة 2013.
2. ويكيبيديا
https://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
3. Abu-Shanab, E. ; Qasem H. (2014) "**Cloud computing Adoption: Brand Equity impact on Users' choice**" , Saba Journal of Information Technology and Networking vol.2 no. 1
4. Aljoumah, E. ; Al-Mousawi, F. , Ahmad, I, ; Al-Shammri, M. ; Al-Jady, Z. (2015) SLA in Cloud Computing Architectures: A Comprehensive Study , International Journal of Grid Distribution Computing Vol. 8, No.5, (2015), pp.7-32

5. Alshammari, H. ; Bach, C. (2013) "Administration Security Issue in Cloud Computing" International Journal of Information Technology Convergence and Services (IJITCS) Vol.3, No.4, August 2013.
6. Apostu, A.; Puican, F. ; Ularu G.; SUCIU, G.; Todoran, G.(2013) "Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud" , Recent Advances in Applied Computer Science and Digital Services
7. Barron C. ; Yu, H. ; Zhan, J. (2013) "Cloud Computing Security Case Studies and Research" Proceedings of the World Congress on Engineering 2013 Vol II, WCE 2013, July 3 - 5, 2013, London, U.K.
8. Cloud security alliance, security guidelines for critical areas of focus in cloud computing v3.0, 2011.
9. Fernandes, D. ; Soares, L.; Gomes,J.; Freire, M.; Inácio, P.(2014) "Security issues in cloud environments: a survey", Int. J. Inform. Sec. 13 (2) (2014) 113–170.
10. Huth, A. ; Cebul, J. (2011) "**The Basics of Cloud Computing**",Carnegie Mellon University, Produced for US-CERT, a government organization
11. Kumar, G.; Chelikani, A. (2011) **"Analysis of Security Issues in Cloud based E-Learning**", Master's thesis in Informatics , 2011MAGI23.
12. Mazhar Ali; Samee Khan; Athanasios Vasilakos (2015) " Security in cloud computing: Opportunities and challenges" Information Sciences 305 (2015) 357–383, ELSEVIER
13. Migrating Applications to Public Cloud Services: Roadmap for Success (2013), the Cloud Standards Customer Council
14. Padhy. R. ; Patra, M. ; Satapathy, S. (2011) "Cloud Computing: Security Issues and Research Challenges" IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011
15. Sah, S. ; Shakya, S. ; Dhungana, H. (2014)A security management for cloud based applications and services with diameter-AAA, in: IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, pp. 6–11.
16. Security for Cloud Computing: 10 Steps to Ensure Success white paper at the Cloud Standards Customer Council
17. Sichao Wang (2012) "Are enterprises really ready to move into the cloud? " available via https://cloudsecurityalliance.org/wp
18. Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and privacy in cloud computing: A survey. In Semantics Knowledge and Grid (SKG)", 2010 Sixth International Conference on (pp. 105-112). IEEE.