استراتيجيـــات اعتماد الحوســـــبة السّحابيـــة

أ . انتصار ميلاد الصل ، أ .بسمة محمد القبي ، أ. زينب أحمد كرواد
كلية تقنية المعلومات ـ جامعة مصراتة

الملخص:

اكتسب التَّـــطور في نظم المعلومات ، الذي حدث في فترة معينة في النصف الثانـــي من القـــرن العشرين ، زخما في الربع الأول من القـــرن الحادي والعشرين ؛ أنتج الزيادة السريعة في كثافة وتنوع طلبات المستخدمين ، بالتوازي مـــع التطـــورات التكنولوجية التغييرات في البرامج ومكونات الأجهزة أدّت هذه التغيرات الكثيرة إلى استخدام منهجيات جديدة في هيكلية المعلومات: (المحاكاة الافتراضية، نموذج الخادم - الزبون - ، الحوسبة الموزعة ، إلخ) ، وتمثـــل الحوسبة السحابية نموذج الخدمـــة الذي ظهر مع تطـــوّر وتكامل التقنيات والمفاهيم الرائـــدة .

مع مراعاة الحلول البديلة لوظيفة التشفير التي يوفرها مقدمو الخدمة، حيث أن الخصوصية مطلوبة بوضوح للبنية التحتية كخدمـــة (IaaS)، والنظام الأساسي كخدمـــة : (PaaS، تتضمن هذه الحلول استخدام خدمات التشفير أو البيانات المشـــفرة للتخزين السحابي المسبق الذي يستضيفه ويديره طرف ثالث ، (ويفضل أن يكون قسما عاما أو مزود خدمة أمان موثوقا به) يتيح التحكم في نماذج هذه الخدمات، ويوافـــق على تنفيذ عمليات التشفير

وتوفر هـــذه الورقة لمستخدمي الحوسبة السحابية بنية مرنـــة ومنخفضة التكاليف وقابلة للتطويـــر ومستقلة عن النظام الأساسي وذات أداء عـــال ، وتهدف هذه الورقة إلى دراسة استراتيجيات اعتماد الحوسبة السحابية من خـــلال اقتراحات الحلول المتعلقة باستخدام الحوسبة السحابية في المؤسسات العامـــة.

الكلمات المفتاحية:

استراتيجيات، الحوسبة السحابية، المؤسسات العامة، حلول، اقتراحات.

:Abstract

The development in information systems, which took place on a certain scale in the second half of the 20th century, gained momentum in the first quarter of the 21st century; The rapid increase in the intensity and diversity of user demands, together with the technological innovations and changes in software and hardware components, made it necessary to use new methodologies in information

architectures. Virtualization, service-oriented architecture, server-client model, distributed computing, etc. cloud computing, a service model that emerged with the development and integration of pioneering technologies and concepts; It offers low-cost, flexible, scalable, platform-independent accessible and high-performance architectures to its users.This paper aims to exmine the strategies for cloud computing adoption through solution suggestions
.regarding the use of cloud computing in the public organizations
Keywords: *Strategies, Cloud Computing, Public Organizations, Solution, .Suggestion*

المقدّمـــــــــــة :

تعتبر الحوسبة السحابية مصطلحا جديدا في عالم الحوسبة [1] ، وهـــي تشير إلى ظهور نموذج جديد للحوسبة [1،2] فقد ظهرت الحوسبة في أوائل التسعينيات، حيث كانت أجهزة الكمبيوتر عالية الأداء مترابطة عبر روابط سريعة لتجميع البيانات، بهدف دعم العمليات الحسابية المعقدة والتطبيقات العلمية.

وتعـــرّف حوسبة الشبكة على أنها :" بنية أساسية للأجهزة والبرامج، حيث توفّـــر وصولاً موثوقا ومتسقا وواســـــع النطاق وغير مكلّف للقدرات الحسابية المتطورة نتجت الحوسبة السحابية عن تقارب الحوسبة الشبكية والبرمجيات كخدمة (SaaS Software as aService)، الذي يمثل نموذجا لتوزيع البرامج، يستضيف فيها مزود الخدمات السحابية التطبيقات ويجعلها متاحة للمستخدمين عبر الإنترنت، ويمثل بشكل أساسي الاتجاه المتزايد نحو النشـــر الخارجي لموارد تكنولوجيا المعلومات، مثل الطاقة الحسابية أو التخزين أوالتطبيقات الأعمال، والحصول عليها كخدمات [3].

وعلى مدار تاريخ علوم الكمبيوتر، تم إجراء العديد من المحاولات لفك ارتباط المستخدمين باحتياجات أجهزة الكمبيوتر، من أدوات مشاركة الوقت المتصورة في الستينيات، وأجهزة الكمبيوتر الشبكية في التسعينات، إلى أنظمة الشبكات التجارية في السنوات الأخيرة [4].

يتطـــور هذا النموذج الجديد من الحوسبة بسرعة ويجذب عددا من العملاء والموردين على حد سواء، حيث يتـــم دعـــم التطور السريع للحوسبة السحابية من خلال تقنيات الحوسبة الناشئة التيتسمح باستخدام البنية التحتية للحوسبة وقدرات التخزين الضخمة بأسعار مناسبة [5]. كما أنه يلغي الحاجة إلى استثمارات ضخمة مستقبلا في البنية التحتية لتكنولوجيا المعلومات.

أصبح هذا حقيقة واقعة بشكل مطرد حيث يتجه عدد من الأكاديميين ورجال الأعمال في هذا المجال من العلوم نحو الحوسبة الممكنة، المتمثلة في الحوسبة السحابية التي تشكل بنية مبتكرة لنظام المعلومات (IS) ، يتـــم تصورها على أنها قد تكون هي مستقبل الحوسبة، وهي قـــوة دافعة تتطلب من مستفيديها إعادة التفكير في فهم أنظمة التشغيل الخاصة بهم، والهندسة المعمارية للخادم العميـــل، والمتصفحات، وقد أعفت الحوسبة السحابية المستخدمين من متطلبات الأجهـــزة ، مع تقليل المتطلبات الإجمالية من جانب العميل والتعقيد فيها [6].

تم استلهام اسم الحوسبة السحابية من رمز السحابة الذي يستخدم غالبا لتمثيل الإنترنت في المخططات الانسيابية والرسومات التخطيطية ، تم الترحيل المتميز إلى السحابة على مدار السنوات الأخيرة مع المستخدمين النهائيين "شيئا فشيئا" للحفاظ على عدد متزايد من البيانات الشخصية، بما في ذلك الإشارات المرجعية والصور وملفات الموسيقى وغير ذلك على الخوادم البعيدة التي ويمكن الوصول إليها عبر الشبكة [7].

ويتم تمكين الحوسبة السحابية من خلال تقنية المحاكاة الافتراضية؛ وهـــي تقنية تعود إلـــى عام 1967 م ، ولكنها كانت متاحة فقط لعقود على أنظمة الحاسوب المركزي. حيث يقوم الكمبيوتر المضيف بتشغيل تطبيق يعرف باسمHypervisor ، مما يؤدّي إلى إنشاء واحد أو أكثر من الأجوزة الافتراضية، والتي تحاكي أجهزة الكمبيوتر الفعلية ، بحيث ويمكن محاكاة تشغيل، أي : برنامج، من أنظمة التشغيل، إلى تطبيقات المستخدم النهائي [7 ، 8].

تعد الحوسبة السحابية نموذجا يتضمن الاستعانة بمصادر خارجية لموارد الحوسبة مع إمكانية قابلية تطوير الموارد القابلة للاستهلاك، عند التزويد بالطلب بتكاليف قليلة أو غير مسبقة للاستثمار في البنية التحتية لتكنولوجيا المعلومات [9،10]. تقدم الحوسبة السحابية فوائدها من خلال ثلاثة أنـــواع من الخدمة أو نماذج التسليم وهي البنية التحتية كخدمة (Infrastructure as a Server IaaaS) ، والنظام الأساسي كخدمة (Platform as a Server PaaS) ، والبرمجيات كخدمة (SaaS) كما تقدم خدماتها من خلال أربعة نماذج نشر وهي السحابة العامة والسحابة الخاصة وسحابة المجتمع والسحابة المختلطة [10]. ينظر إلى الحوسبة السحابية على أنها واحدة من أكثر التقنيات الواعدة في مجال الحوسبة اليوم، وهي قادرة بطبيعتها على معالجة عدد من المشكلات.

من الخصائص الرئيسية للحوسبة السحابية [11]. المرونـــة ، حيث ويمكن للمستخدمين توفير مـــوارد الحوسبة بسرعة حسب الحاجة، دون تفاعل بشري، ويمكن توفير القدرات بسرعة وبشكل مـــرن ، وفي بعض الحالات تلقائيا ، لتوسيع نطاقها أو زيادتها بسرعـــة. قابلية تطوير البنية التحتية: ويمكن إضافة عقد جديدة أو إسقاطها من الشبكة كما يمكن للخوادم المادية، مع إجراء تعديلات محدودة لإعداد البنية التحتية والبرامج.

ويمكن للبنية السحابية التوسع أفقيا أو عموديا، حسب الطلب. كقدرات متاحة عبر الشبكة، كما يمكن الوصول إليها من خلال الآليات القياسية التي تعزز الاستخدام من قبل المنصات غير المتجانسة (مثـــل : الهواتف المحمولة ، وأجهزة الكمبيوتر المحمولة) [12].

وهناك شعور باستقلالية الموقع ، حيث لا يمتلك العميل عموما أي سيطرة ، أو معرفة بالموقع الدقيـــق للخادم ، ولكن قد يكون قادرا على تحديد الموقع على مستوى أعلى من التجريد (مثل الدولة أو الولاية أو مركز البيانات). تتحســـن الموثوقية من خلال استخدام العديد من المواقع الزائدة عن الحاجة، مما يجعل الحوسبة السحابية مناسبة لاستمرارية الأعمال والتعافي من الأعطال، وحجم التكلفة، وتميل التطبيقات السحابية، بغض النظر عن نموذج التطوير، إلى أن تكون كبيرة قدر الإمكان من أجل الاستفادة من المساحات المتوفرة [13 ، 14 ، 15]، وغالبًا ما توجد عمليات النشر السحابية الكبيرة من محطات الطاقة الرخيصة وفي بنيات منخفضة التكلفة، وذلك لتقليل التكاليف تأتيا لاستدامة من تحسين استخدام الموارد، وأنظمة أكثر كفاءة.

غالبًا ما تحتوي تطبيقات السحابة على تقنيات أمان متقدمة، تتوفر في الغالب بسبب مركزية البيانات والبنية العامة [16] ، وتتيح الطبيعة المجمعة للموارد المتجانسة للسحابية، لمقدمي الخدمات السحابية، تركيز جميع موارد الأمان الخاصة بهم على تأمين بنية السحابية، وفي الوقت نفسه عادة ما تؤدي إمكانيات التشغيل الآلي داخل السحابية ، جنبًا إلى جنب مع مورد الأمان المركز السحابي، إلى إمكانات أمان متقدمة.

استعـــراض الأدبيـــــــــات:

معوقات اعتماد الحوسبة السحابية في المؤسسة.

على الرغم من وجود العديد من الفوائد لاعتماد الحوسبة السحابية، إلا أن هـــناك – أيضا- بعض العوائق الكبيرة التي تحـــول دون اعتمادها [17 ، 18].

الأمـــان والخصوصية : نظرا ؛ لأن الحوسبة السحابية تمثل نموذجا جديدا للحوسبة ، فهناك قدر كبير من عدم اليقين بشأن كيفية تحقيق الأمان على جميع المستويات (مثل الشبكة ، والمضيف ، والتطبيق ، ومستويات البيانات) ، وقـد أدّى ذلك بشكل غير مؤكد إلـى قيام المديرين التنفيذيين للمعلومات على الدوام بالقول إن الأمن هـو مصدر قلقهم الأول في مجال الحوسبة السحابية. تم التشكيك في قدرة الحوسبة السحابية على معالجة لوائح الخصوصية بشكل مناسب. [14]

الاتصال والوصول المفتـوح : تعتمد الإمكانات الكاملة للحوسبة السحابية على توفيـر الوصول عالي السرعة للجميع ، يفتـح هـذا الاتصال ، مثل : توفـر الكهرباء ،.و يعزز الاتصال والوصول المفتوح إلى قوة الحوسبة ، وتوافر المعلومات من خلال السحابية حقبة أخـرى من التصنيع والحاجة إلى المزيد من المنتجات الاستهلاكية المعقدة.

الموثـوقيـة: أصبحت تطبيقات المؤسسة الآن بالغة الأهمية بحيث يجب أن تكون موثوقة لدعم العمليات ، وفي حالة الفشل أو الانقطاع ، يجب أن تسري خطط الطوارئ بسلاسة، وفي حالة الفشل الكارثي، يجب أن تبدأ خطط الاسترداد بأقل قدر من التعطيل . قد تترافق التكاليف الإضافية مع المستوى المطلوب للموثوقية ؛ ومع ذلك ، يمكن للشركة أن تفعل الكثير فقط للتخفيف من المخاطر وتكلفة الفشل . سيكون إنشاء سجل حافل بالموثوقية شرطا أساسيا للتبني على نطاق واسع.

قابليـة التشغيـل البينـي : تعـد قابلية التشغيل البيني وإمكانية نقل المعلومات بين السحابة الخاصة والعامة من العناصر التمكينية الحاسمة للتبني الواسع للحوسبة السحابية من قبل المؤسسة ، وقد حققت العديد من الشركات تقدما كبيرا نحو توحيد عملياتها وبياناتها وأنظمتها من خلال تنفيذ أنظمة تخطيط مـوارد المؤسسات (ERP).

القيمـة الاقتصاديـة : يعتمد نمو الحوسبة السحابية على عائـد الاستثمار الذي يتحقـق . يبدو بديهيًا أنـه من خلال مشاركة الموارد لتخفيف القيـم الاقتصادية، والدفع فقط مقابل ما يتم استخدامه،وتقليص الاستثمار الرأسمالي المسبق في تطوير حلول تكنولوجيا المعلومات (IT) ، ستكون القيمة الاقتصادية موجودة. ستكون هناك حاجة للموازنة بعناية بين جميع التكاليف والفوائد المرتبطة بالحوسبة السحابية على المدى القصير والطويل ، يمكن أن تشمل التكاليف المخفية الدعم والتعافي من الكوارث وتعديلات التطبيقات والتأمين على فقدان البيانات.

التغييرات في تنظيـــــم تقنية المعلومات:

ستتأثـــــر مؤسسة تكنولوجيا المعلومات بالحوســـبة السحابية ، كما كان الحال مع التحولات التكنولوجية الأخـــرى ، فهناك بُعدين للتّحول في التكنولوجيا.

الأول : هـــــو اكتساب مجموعات المهارات الجديدة لنشـــر التكنولوجيا فـــي سياق حل مشكلة العمل .

الثانـــي : هو كيفية تغيير[1] تخطيط موارد المؤسســـة (Enterprise Resource Planning ERP) : حيث يشير إلى نوع من البرامج التي تستخدمها المؤسسات لإدارة أنشطة الأعمال اليومية مثل : المحاسبة والمشتريات وإدارة المشاريع وإدارةالمخاطر والامتثال وعمليات سلسلة توريد التكنولوجيا لدور تكنولوجيا المعلومات. خلال حقبة[1] COBOL، نادرا ما تتم برمجة المستخدمين ، وتباينت توقعات واجهة المستخدم، وكانت قابلية تكيف الحل منخفضة .

وعلى الرغم من المشكلات السياسية بسبب الحدود العالمية في عالم الحوسبة السحابية، إلا أن هناك تباينًا من حيث مكان تواجد البيانات المادية ، وأين تتم المعالجة؟ ومن أين يتم الوصول إلىالبيانات؟. وبالنظر إلى هذا التباين وقواعد وأنظمة الخصوصية المختلفة، تصبح السياسة حسب التعريف عنصرا في اعتماد الحوسبة السحابية، والتي تعد فعالة متعددة الاختصاصات.

الثقة والتحديات في اعتماد الحوسبة السحابية.

تم الإبلاغ عن مزايا عديدة للحوسبة السحابية للأعمال والعملاء الذين تحولوا إلى الخدمات القائمة على السحابية مثل : الموثوقية، وإمكانية الوصول، وخفض التكلفة والقدرة على توسيع نطاق الخدمات بسهولة ، والمرونة ، وتقليل معدلات الفشل [19]. ومع ذلك ، هناك عدد من المخاوف المرتبطة بالحوسبة السحابية [20].

ومن أهم التحديات التي تواجهها قضايا الأمان[21]، حيث كشفت الدراسات الحديثة أن قضايا الخصوصية والأمان والثقة تنشأ نتيجة للتعامل مع موارد الحوسبة من قبل أطراف ثالثة يمكن الوصول إليها عبر شبكة [22] وفي هذا الاقتراح، سيتم التحقيق في ثقة الأمان بشكل أكبر في محاولة لتطوير نموذج الثقة الذي يمكن استخدامه من قبل العملاء عند اختيار مزود الخدمة، ويعتبر أغلب أهل الاختصاص

---

[1] COBOL (Common Business-Oriented Language) لغة الأعمال الشائعة الموجهة) هيلغة برمجة عالية المستوى لتطبيقات الأعمال. كانت أول لغة شائعة مصممة لتكون حيادية لنظام التشغيل ولاتزال مستخدمة في العديد من التطبيقات المالية والتجارية اليوم.

أن الأمان هو مصدر قلق في الحوسبة السحابية المتعلقة بأشياء أخرى غير المصداقية والتفويض والمسؤولية ؛ كما أنها تتعلق بحماية البيانات والتعافي من الكوارث واستمرارية الأعمال [23]. وتهتم طبيعة الحوسبة السحابية بالتخلي عن السيطرة المباشرة على العديد من جوانب الأمان والخصوصية [24]. نتيجة لذلك، تتردد العديد من المؤسسات في استضافة بياناتها الداخلية على أجهزة كمبيوتر خارجية عن أجهزتها والتي قد يتم استضافتها بشكل مشترك مع تطبيقات الشركات الأخرى.

ويواجه اعتماد الحوسبة السحابية تحديات كثيرة ، ومن هذه التحديات: التحديات الأمنيـــــة ، والتحديات القانونية ، وتحديات الامتثال ، والتحديات التنظيمية [25 ، 20] .

وهذه التحديات ترتبط بمسألة الثقة بين العملاء والموردين ، لأن الحوسبة السحابية تدعو المؤسسات إلى الوثوق بالموردين من خلال إدارة موارد وبيانات تقنية المعلومات الخاصة بهم ، والثقة عامل حاسم في اعتماد الحوسبة السحابية، سيركز هـــذا المقترح بشكل خاص على تحديد التحديات التي تواجه المنظمات عند السعي لاعتماد الحوسبة السحابية ، من بين جميع التحديات ،

علاوة على ذلك، تمكن مقدم والخدمة من الوصول إلى جميع البيانات السحابية بشكل متعمد أو استخدامها عن طريق الخطأ لأغراض غير معتمدة [26،29] من خلال القيام بذلك ، تمنح المؤسسات مستوى عال من الثقة بمزود السحابية [27،28]. حيث ينظر إلى الثقة على أنها مصدر قلق رئيسي للمستهلكين النهائيين والعملاء من المؤسسات والمنظمين ، ويعد الافتقار إلى الثقة من العوائق الرئيسية لاعتماد خدمات الحوسبة السحابية ، حيث يشك المستخدمون فيما يحدث لبياناتهم عندما يتم نقلها إلى السحابية [30،31].

منهـــج البحث:

تتمثل التوصيات ومقترحات الحلول لشبكة الاتحاد الأوروبي وكالة أمن المعلومات (ENISA) لإنشاء سحابات عامة آمنة وفقا للوضع الحالي في أوروبا والسيناريوهات المتوقعة فيما يتعلق باعتماد الحوسبة السحابية في الدول الأوروبية كما يلي :

- تدعم الدول الأعضاء (MS) والمفوضية الأوروبية (EC) تطوير استراتيجية الاتحاد الأوروبي لضمان اعتماد السحابية العامة.
- تقوم المفوضية الأوروبية والدول الأعضاء بتطوير نموذج أعمال لضمان استدامة الحلول السحابية العامة والقدرة على تحمل تكاليفها .

ـ تشجع الدول الأعضاء و مقدمو الخدمات السحابية على تطوير إطار عمل للتخفيف من مشكلة "فقدان السيطرة" .

ـ تشجع الدول الأعضاء و مقدم والخدمات السحابية تطوير حلول السحابية العامة التي تتوافق مع اللوائح الخاصة بالاتحاد الأوروبي والبلد .

ـ يدعم مستوى خدمة من المفوضية الأوروبية والدول الأعضاء تطوير إطار عمل الاتفاقية (اتفاقيات مستوى الخدمة (SLA) .

ـ تشجع المفوضية الأوروبية و الدول الأعضاء اعتماد تدابير الأمان الأساسية لنماذج نشر السحابة العامة والخاصة .

ـ تضع المفوضية الأوروبية والدول الأعضاء لتشجيع الأكاديميين وموفري الخدمات السحابيةعلى البحث في أمان السحابية العامة.

ـ تدعم المفوضية الأوروبية و الدول الأعضاء زيادة خصوصية البيانات في السحابية.

النتائج والمناقشـــــــــــة :

فيما يلي شرح لهذه الاقتراحات والاحتياطات الواجب اتخاذها:

الاقتراح الأول ـ استراتيجية السحابية العامة للاتحاد الأوروبي :

اعتماد الحوسبة السحابية في القطاع العام غير متجانس للغاية في أوروبا، حيث عملية التبني بطيئة ؛ يعتمد ذلك على العديد من الأسباب مثل الأمان والسيطرة وحماية البيانات والجهل. على الرغم من أن التشريعات الأمنية الحالية أو المقترحة تغطي بعض متطلبات أمنالمعلومات، إلا أن إدراك كيفية عمل خدمات تكنولوجيا المعلومات ومعرفة ما هي تعديلاتالتدابير الأمنية سيؤدي اعتماد السحابية إلى تأثير كبير على استخدام الحوسبة السحابية. تشيرالدراسات إلى أن التبني المنهجي للسحابية العامة أكثر تقدما في البلدان التي لديها استراتيجية وطنية لمعالجة اعتماد الحوسبة السحابية. علاوة على ذلك، فإن العديد من الخبراء مقتنعون بأن تطوير استراتيجية الاتحاد الأوروبي التي تركـــز بشكل منفرد على الاستراتيجيات الوطنية للقطاع العام ، والحوسبة السحابية العامة ستعزز اعتماد السحابية العامة.

الإجـــــراءات و التدابيـــــر:

1ـ تصميم استراتيجية مفصلة على مبادئ عالية المستوى تغطي المسائل الفنية والقانونية وقضايا الشركات.

2- التوفير الضخم للخدمات السحابية الآمنـــــة ، مع وضع في اعتبار خطة عمل خطوة بخطوة، وتحقيـــق برنامج يخطط من خلال تحديد مخرجات ومعالم ذات مغزى.

3- تشجيع نشر السحابية وتشجيع المنظمات ؛ تعزيز استخدام السياسات القائمة على المعرفة والقائمة على المخاطر والحلول السحابية العامة الخارجية من أجل "البيانات المفتوحة" في القطاع العام.

4- ربط الاستراتيجية الوطنية للحوسبة السحابية بمشاريع ومبادرات لزيادة كفاءة تقنيات المعلومات والاتصالات واتفاق مراكز البيانات في القطاع العام.

5- تقييم خيارات بنية السحابية العامة (مفتوحة، خاصة، مجتمعية ، ومختلطة) بناء على نوع الخدمات ومتطلباتها ، مثل الخصوصية والأمان والتحكم.

6- على الدول الأعضاء تأمين استراتيجية وطنية لضمان امتثالها للقوانين واللوائح ومتطلبات الوكالة الوطنية بشأن الأمان وحماية البيانات ، وكذلك، مع مراعاة سرية البيانات والأمان وحماية المعلومات والأصول والبنى التحتيـــــة ، إلخ ، ضمان امتثالها للقوانين واللوائح الوطنية التابعة للاتحاد الأوروبي.

7- تطـــوير (كتالوجات) - (منشور مصور يحتوي على قائمة أو عرض لمنتج ، ويتضمن عادة معلومات وصفية لهذا المنتج) - الخدمات العامة : تقييـــم كتالوجات المنتجات السحابية والتطبيقات والخدمات،بالإضافة إلى الخيارات التي تصنف المنصات العامة المستهدفة، وملفات تعريف الاستخدام، وأفضل الممارسات.

الاقتراح الثاني ــ نمـــوذج أعمال يضمـــن الاستدامـــة:

تستخدم اليوم البنية السحابية الخاصة بشكل شائع في السحابية العامة للاتحاد الأوروبي. ويرجـــع انخفاض استخدام بنية السحابية العامة إلى نقاط الضعف التنظيمية وعدم نضج حلول السحابية العامة. هناك ثلاثة تحديات رئيسية يطرحها عدم النضج المتكرر لسوق الحوسبة السحابية العامة:

1- على الرغم من وجود العديد من مزودي خدمات الحوسبة السحابية في السوق، فإن معظمهم في مستوى الدخول الأولي وبالتالي لا يمكنهم ضمان مستوى الاستقرار الذي ينبغي أن تتمتع به الشركة القادرة على التعاون مع الجمهور،

2- تم تصميم العديد من الحلول في سياق عمل محدد، وبالتالي فإن العديد من حلول السحابية العامة في السوق لا يمكنها تلبية الاحتياجات المحددة للجمهور.

3- لا يوجد سوى عدد قليل من الحلول المتوفرة في السوق اليوم والتي يمكن أن تأخذ في الاعتبار المسؤولية الخاصة للجمهور عن حماية البيانات،

نتيجة لذلك، لا يزال هناك عدد قليل نسبيا من حلول الحوسبة السحابية العامة في السوق المناسبة للاستخدام من قبل الحكومة. ومع ذلك، فإن إنشاء السحابية الخاصة يمكن أن يكون مكلفا للتشغيل ونقل الخدمات الحالية.، ومن الصعب تطوير نموذج تكلفة قادر على توفير التكلفة الحقيقية.

ولزيـــــادة اعتماد السحابية، تحتاج السلطات المختصة التابعة للمفوضية الأوروبية والدول الأعضاء، بالتعاون مع موفـــري السحابية ، إلى تطوير عمل تجاري، والحل هـــو التحرك نحو استخدام نموذج مناسب يضمن الكفاءة.

كما أن التحرك نحو استخدام بنية سحابية مناسبة ومفتوحة / مجتمعية ، سيقلل من تكاليف الاستثمار لزيادة توافرالبيانات والخدمات و موثوقية الخدمة وأمانها.

الإجـــــراءات و التدابيـــــر: هناك حاجة إلى إطار تنظيمي لضمان اعتماد البنية التحتية متعددة المستأجرين وتقاسم الخدمات بين الدول الأعضاء. يجب أن يعالج هذا الإطار قضية البيانات وموقع الخدمة. كما يجب أن يعالج إطار العمل - أيضا - كمشكلات التي تطرح عند تبديل مزود السحابية أو إنهاء الخدمة السحابية. هنا، يجب التأكيد على المصطلحات والتوافقات التي يجب أن تكون في اتفاقية مستوى الخدمة (SLA) ، و قابلية تطبيق هذه الشروط والتراضي.

ثانيا : يجب ضمان مستقل من طرف ثالث يمكن أن يسهم في الثقة بيـــن المزود والعملاء ، حتى تتمكن الشركات الصغيرة والمتوسطة الأوروبية والمنظمات الأخرى من الاستفادة بشكل أكبر منخدمات الحوسبة السحابية. الفكرة الرئيسية هي إنشاء إطار عمل يمكن من خلالله للوكالاتالحكومية اعتماد بائعي السحابية وتقديم شكل من أشكال خدمة الضمان النشطة والفعالة من قبلطرف ثالث. وبهذه الطريقة، يمكن للطرف الآخر تولي العمليات السحابية دون انقطاع ويمكن لموفر السحابية (أ) أن يتقدم إلى الموفر (ب) خدمات للمستخدم. يجب أن يحتوي هذا البرنامج على الوضع الحالي لمعاملات بيانات المستخدمين.

ثالثا : يحتاج مقدمو الخدمات السحابية العامة إلى زيادة سمعتهم ومصداقيتهم. وبشكل أكثر تحديدا، يجب أن تدعم بنية السحابية المجتمعية المفتوحة ما يلي :

- لائحة الاتحاد الأوروبي بشأن استخدام البنى التحتية متعددة المستأجرين لخدمات الحكومة الإلكترونية.
- إطار عمل للمصادقة على تقييم كفاءة المزود العام (على سبيل المثال ، برنامج الشهادات الطوعية الذي يوفر إجراءات تدقيق شفافة.

ـ إطار النيابات العامة لجميع الهيئات الحكومية التي تحتاج إلى تقديم خدمات الحوسبة السحابية.
ـ إطار قانوني للتعامل مع قضايا المصادر الخارجية.
ـ وصف الإجراءات القياسية للتطبيق وترحيل البيانات.
ـ إطار عمل للتحكم في موقع البيانات ومعالجة البيانات بشكل عام.

المقترح الثالث ــ إطار عمل لتقليل فقدان السيـــطرة:

يعتبـــر فقدان التحكم في البيانات والموارد كأحد أهـــم العقبات التي تواجه السحابية العامة مشـــكلة" فقدان السيـــطرة " ليست مجرد مسألة تقنية؛ إنها أيضا مسألة وعي وشفافية وتنظيم وعقود بينالمزودين والعملاء. على سبيل المثال ، عندما تقوم وكالة حكومية بنقل البيانات والتطبيقاتالمملوكة لها إلى السحابية ، فقد تكون قلقة بشأن إمكانية وصول مزود السحابية إلى بياناته ومعالجتها، بسبب نقص الشفافية في إجراءات مزود الخدمات السحابية (على سبيل المثال ،الإجراءات القياسية لتلف البيانات) ، وغياب أحكام الاتصال المشتركة ولوائح الاتحاد الأوروبي .

وجانب آخـــر من جوانب فقدان السيطـــرة مسألة الاعتماد على المزود ، على سبيل المثال : في حالة عطل مقدم الخدمة ، قد تنشأ مخاوف بشأن مصير البيانات والتطبيقات. يجب أن يكون من الممكن دائمًا نقل البيانات والتطبيقات من مـــزود إلى مزود خدمة سحابية آخـــر، بدون قيود التكلفة والوقت التي تفرضها تبعية الموفر . ويجب الإعلان عن كل هذه الأحكام وفهمها في اتفاقية مستوى الخدمة.

الإجـــراءات : يجب أن تعمل المفوضية الأوروبية والسلطات المختصة في الدول الأعضاءبالتنسيق مع مقدمي الخدمات السحابية والعملاء العموميين؛ على تقليل " فقدان السيطرة" من خـــلال معالجة الإدارة والمراقبة والتحكم عن كثب في تبعية المزود ومعالجة البيانات. والخطوات الواجب اتخاذها في هذا الصدد هـــي :

1. تحديد إطار عمل للمراقبة والتدقيق لمستويات الخدمة العامة في السحابية الحكومية.
2. وصف الإجراءات القياسية لمعالجة البيانات،
3. تحديد الإجراءات المعيارية لنقل البيانات والخدمات.

المقترح الرابـــع : إطار تنظيمـــي لحلّ مشكلة المحلية (Locality):

عادة ما يقوم موفرو الخدمات السحابية بتخزين البيانات في مراكز البيانات الخاصة بهم ، والتي يمكن أن توجد في العديد من البلدان المختلفة. غالبا ما ينظر إلى إمكانية وجود بيانات وموارد خارج الدولة على أنها عائق أمام اعتماد السحابية العامة

بسبب مشكلات خصوصية البيانات قد يؤدي تعريف الإطار التنظيمي لموقع البيانات إلى تقليل اعتراضات المستخدمين العامين على بنية السحابية ، ولكن الشاغل الأكثر أهمية لحماية البيانات هو أمان البيانات بدلا من موقعها . لتحقيق ذلك، تمت الإشارة إلى الحلول التقنيـــة (مثل: استخدام التشفير)

ومع ذلك ، فإن الخطر لا يقتصر فقط على اتخاذ تدابير فنية؛ إذ عادة ، ما تحظر السلطات القضائية المحلية حيازة البيانات المملوكة ملكية عامة في الخارج فقط .

ثانيا: لا يتعلق الأمر فقط بموقع البيانات، بل يتعلق - أيضا - بالإطار القانوني الذي يقع ضمنه مزود الخدمات السحابية

وتجدر الإشارة إلى أنه بالنسبة للبلدان الأصغر حجما، فإن نقل البيانات للخارج له تكاليف باهظة وسيكون من الصعب - أيضا - بإنشاء مراكز البيانات والنسخ الاحتياطي الخاصة بهم. يجب أن يأخذ الإطار التنظيمي هذا في الاعتبار ويقدم حلولا للتغلب على هذه الإشكاليات.

الإجـــــراءات: لتعريف إطار العمل الجديد، ينبغي للمفوضية الأوروبية والسلطات المختصة في الدول الأعضاء، بالتعاون مع موفري الخدمات السحابية والعملاء العموميين، العمل على:

1. وصف الإجراءات اللازمة لزيادة وعي المؤسسات العامة ومقدمي الخدمات السحابية حولتشريعات الاتحاد الأوروبي الحالية بشأن هذا الموضوع.

2 - تشجيع تطوير الحلول التكنولوجية بما يتماشى مع التشريعات الحالية.

3. تقييم وتصنيف المتطلبات العامة المتعلقة بملكية البيانات وخصوصية البيانات حسب نوع البيانات المتاحة.

4. تحسين تشريعات الاتحاد الأوروبي الحالية بشأن ملكية البيانات والموارد، مع التركيز على الاستعانة بمصادر خارجية.

5. تحسين تشريعات الاتحاد الأوروبي الحالية بشأن خصوصية البيانات مع التركيز علىالاستعانة بمصادر خارجية.

المقترح الخامـــس : حلول السحابيـــة العامـــة التي تتوافق مع قانـــون الاتحاد الأوروبي والقانون الوطني .

يجب اتخاذ إجراءات لتشجيع تطوير الأنظمة والخدمات التي تتوافق مع لوائح الاتحاد الأوروبي والتشريعات الخاصة بكل بلد، من أجل تهدئة شكوك السلطات العامة حول الحلول التكنولوجية التي يقدمها مقدمو الخدمات.

الإجـــــراءات: يجب أن تحاول المفوضية الأوروبية والدول الأعضاء السلطات والهيئات العامة والهيئات المعيارية وقطاع البحث والتطوير بالتعاون مع مقدمي الخدمات السحابية، تشجيع تطوير الحلول التكنولوجية بما يتماشى مع تشريعات الاتحاد الأوروبي والتشريعات الوطنية.

الخطوات الواجب اتخاذها ستكون:

1. إنشاء إطار اعتماد شهادة تضمن أن كل حل سحابي يتوافق مع التشريعات ذات الصلة (القانون الوطني ، أو قانون الاتحاد الأوروبي)،

2 - الترويج لتعريف العقود الموحدة لتشمل التوافق القانوني،

3. زيـــادة وعي الاتحاد الأوروبي و الدول المعنية باللوائح .

4. تعزيز التعليم حول القضايا السحابية لدول الاتحاد الأوروبي.

المقترح الســـادس ــ إطار مشترك للاتفاق على مستوى الخدمة (SLA):

سيكون تطوير إطار عمل مشترك لاتفاقيات مستوى الخدمة القياسية بمثابة إجـــراء لزيادة تطوير السحابية العامة من خلال وجود إطار اتفاقية مستوى الخدمة. ويمكن معالجة التغييرات التي تواجهها المؤسسات الحكومية، مثل : تعريف العقود ، والشكوك حول حلول السحابية العامة.

بدأ هذا العمل في استراتيجية الحوسبة السحابية للاتحاد الأوروبي وبدعم من الشبكة الأوروبية ووكالة أمن المعلومات (ENISA).

1. يجب أن تتضمن التأكيدات والضمانات التي يقدمها مقدمو الخدمات السحابية للجهات الحكومية، اختبارات اختراق محددة لدعم متطلبات الأمان والخصوصية، كما يجب التحقق منها وتقييمها من خلال أنشطة التدقيق من قبل أطراف ثالثة مستقلة يمكن أن تستفيد من التحقق منصحة التعليقات من قبل مدققي الطرف الثالث لتجنب ازدواجية التدقيق.

2. ينبغي التأكد من الوفاء بالالتزام بالرد والإبلاغ عن الحادث وأن مقدمي الخدمات يستجيبون على الفور للحوادث، وشروط العقد، التي تهدف إلى الإبلاغ عن الحوادث التي تبدو خطيرة والتي قد تؤثر على توافر الخدمات، للسلطات ذات الصلة و / أو المستخدمين العموميين، وللتعافي السريع من الهجمات والأخطاء، يجب تنفيذها.

3. الاستجابة للحوادث والإبلاغ عنها ضروريان بشكل خاص للخدمات العامة التي تتمتع بمستوى ما من الأهمية من حيث نوع الخدمة أو حساسية البيانات، في هذه

الحالات، من المفيد فصل اتفاقيات مستوى الخدمة من حيث الاستجابة والجداول الزمنية للإبلاغ.

4. يجب تضمين عقوبات جزائية لتقييد مستوى الخدمة في العقد في هذا الصدد، يبدو أنه من الجدير بالذكر أنه يجب إنشاء عقد خدمة مشابة أو نظام تدوين لتوحيد المستخدمين حول الانتهاكات السابقة ضد التصنيفات الموحدة المماثلة.

الاقتراح السـابع : الإجراءات الأمنيـة للحوسبة السحابية العامة.

يعد تحديد المناهج والأساليب القياسية لإصدار الشهادات الأمنية للخدمات والموفرين أمرا مهما للاستخدام الموثوق به لبنى السحابية ، وذلك من أجل ضمان أمن المؤسسات العامة، ومن الضروري تطوير نموذج يتكـوّن من مستويات التطور التي يجب على موفري الخدمات السحابية الامتثال لها من خلال الشهادة والتي تحدد بوضوح المتطلبات على كل مستوى أمان.

لا يمكن تنفيذ نموذج اعتماد الخدمات السحابية إلا من قبل إدارة مركزية مخصصة. يجب أن يكون المستخدمون والمقدمون العموميون أحرارا في اختيار مستوى الأمان المطلوب والمقدم للخدمات العامة ، ويجب أن يترك للإدارات ذات الصلة خيار تنفيذ الأفضل من بين الحلول المالية الأكثر فاعلية وغير المكلفة ، وستكون مجموعة محددة من إجراءات الأمان التي تركز على نشر السحابية العامة كوسيلة لزيادة الموثوقية في سلسلة التـوريد السحابية.

الإجـراءات: الإجراءات الموصى بها لزيادة الأمن وحماية المعلومات في الخدمات السحابية العامة:

1. لدعم عملية التقييم المسبق قبل شـراء الخدمة.
2. إنشاء مجموعة من الإجراءات الأمنية الأساسية التي تركز على السحابية العامة (ينبغي أنتشمل هذه الإجراءات مجالات مثل إدارة الأمان ، وإدارة الهوية، وخدمات النسخ الاحتياطيللبيانات، والتوافر، وما إلى ذلك) ،
3. تضمين مستويات تأثير المخاطر في كل مجال لتقديم نموذج متطور / متقدم؛ تمكين إطارالتدقيق (و / أو التصديق) على إجراءات أمن المعلومات.
4. وضع العلامات الأمنية لتعزيز الأنظمة.

المقترح الثامـــن : إطـــار عمل لإصدار الشهادات.

بالنظر إلى إطار الإدارة العامة، يصبـــح من الواضح أن المشكلة وهـــي أن الاعتراض ليس منتشرا في المؤسسات العامة، وتفضل الوكالات الحكومية الامتثال للمعايير دون الحاجة إلى موافقة مدقق حسابات خارجي

حاليا، كجزء من استراتيجية الاتحاد الأوروبي السحابية، أطلقت المفوضية الأوروبية أنشطة تدعم الشهادات في الشبكة السحابية ، والأهـــم من ذلك هو إنشاء إطار تعريف لجميع مقدمي الخدمات ليتم اعتمادهم. وتعتبر وكالة أمن المعلومات ENISA جزء من المجموعة التي تم اختيارها لتكون مسؤولة عن هذا الإجراء وتدعم بشكل كامل المفوضيةالأوروبية. بدأ هذا العمل في استراتيجية الاتحاد الأوروبي السحابية و بدعم من الشبكة الأوروبية ووكالة أمن المعلومات (ENISA)

الإجـــــــراءات:

1- تعتبر طريقة الحصول على شهادة للمنصة السحابية العامة والخدمات عملية صعبة ومثيرة للجدل. قد يكون الدافع الرئيسي لتحقيق الهدف هو دمـــج الالتزام في الإطار التنظيمي للاتحادالأوروبـــي أو مخطط الاعتماد التطوعي الأوروبي.

2- يجب استكشاف التنمية العالمية والمعايير التي تحركها الصناعة ، وكذلك المتطلبات العامة في البلدان الأخرى.

3. مـــن الضروري دعـــم إنشاء " كتالوجات خدمة وطنية للمنتجات /التطبيقات السحابية التي تمت تجربتها مسبقا ". يقلل هـــذا الأسلوب من تكلفة الخدمة من خلال تطبيق نموذج " تأكد مرة واحدة، قم بالتثبيت عدة مرات".

4. يمكن دمج هذا الإجراء مع توصيات الإجراءات الوقائية السابقة، وإنشاء نظام اعتمادأوروبي لجميع مقدمي الخدمات، الراغبين في تقديم خدمات الحوسبة السحابية للقطاع العام. فيمجال أمن المعلومات، يعد الإطار الفوقي الذي يتضمن ضوابط أمان لكل مجال ويتم تصنيفها إلى مستويات من التطور نقطة انطلاق جيدة.

الاقتراح التاســـع ـــ تعزيز البحث حول أمن السحابة العامة:

من المهم تعزيـــز البحث السحابي العام من خلال الاستفادة من برامج البحث الحالية لدعم تطوير تقنيات السحابية المتوافقة مع متطلبات الحكومة ، حيث يجب توجيه البحث نحو رفع مستوى تأثير المخاطر للحلول السحابية للمرافق.

أقرت المفوضية الأوروبية وسلطات البحث والتطويـــر في الدول الأعضاء والأكاديميين؛ بضرورة دعم مقدمو الخدمات السحابية برامج البحث الوطنية

والأوروبية الحالية والمستقبلية وأن يدمجوا أعمالهم الخاصة بشأن الجوانب الأمنية للحوسبة السحابية في القطاع العام في ببرامجهم البحثية، ويمكن أن تتناول موضوعات البحث هذه : إدارة دورة حياة الخدمة السحابية، والتحكم في سلسلة التوريد السحابية، وإدارة الأحداث ، وتحليل المخاطر السيبرانية ، و نمذجة التهديدات السيبرانية والتشفير، وحماية البيانات، و قياسات الخصوصية السحابية، والمساءلة والشفافية لحماية البيانات وأمن المعلومات في الأنظمة السحابية.

اتخذت المفوضية الأوروبية والسلطات المختصة في الدول الأعضاء إجراءات على مقدمي الخدمات السحابية اتخاذ الإجراءات التالية مع العملاء الحكوميين وصناعة البحث والتطوير والتعاون الأكاديمي:

1. تحديد الأولويات لأهداف البحث المختلفة.
2. التواصل مع برامج البحث الأمني الحالية على مستوى الاتحاد الأوروبي والمستوى الوطني.(Horizon 2020 مثل)
3. العمل مع المؤسسات والمنظمات المناسبة (على سبيل المثال، Framework programوالمجموعات الاستشارية، ومنصات التكنولوجيا ، إلخ) لتحديد برنامج الدراسة المناسب.

المقتـــرح العاشـــر : تعزيز خصوصيـــــة البيانات.

حماية البيانات هي قضية مهمة بسبب حساسية المعلومات التي تتم معالجتها داخل السحابية العامة. يجب ضمان الخدمات السحابية للمفوضية الأوروبية والدول الأعضاء للامتثال لقوانين حماية البيانات في الاتحاد الأوروبي. لضمان الخصوصية في الخدمات السحابية، واستخدمت التشفير بواسطة مزود السحابية والوصول الموثوق من قبل المستخدمين كحل سهل

ومع ذلك، لا يـــزال تنفيذ حلول التشفير في الخدمات السحابية في مستوى منخفض من التطور.

الإجـــــــراءات: أصبحت تقنيات إنفاذ حماية البيانات قضية أساسية وأساليب خاضعة للرقابة والتشفير مثل:

1. يجب أن تؤخذ في الاعتبار السياسات الحديثة بشأن إدارة المعلومات الشخصية من قبل المنظمة، والتي يتم التعبير عنها بوضوح وتتضمن المعلومات التي تم الحصول عليها من المستخدمين الأجانب.

2. لا تضمن نماذج البنية التحتية كخدمة (IaaS)، والنظام الأساسي كخدمة (PaaS) ، وكذلك التشفير في السحابية الخاصة الخصوصية، وأمن البيانات في السحابية الخاصة ؛ يجب أن يتم تنفيذها بوسائل أخـــرى مثل : التحكم في الوصول بدلاً من تقنيات التشفير.

3. عند تقديم خدمات البرمجيات كخدمة (SaaS)، يجب تحديد تقنيات التشفير مسبقًا، وليس عند الطلب، في عقد المزود مع العميل.

الهوامـــــــــش :

[1] Compeau DR, Meister DB, Higgins CA. From Prediction to Explanation: Reconceptualizing and Extending the Perceived Characteristics of Innovating. Journal of the Association for .Information Systems 2007(8):409–39

[2] Dillon T, Wu C, Chang E. Cloud Computing: Issues and Challenges. In: Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on: IEEE Computer .Society; 2010, p. 27–33

[3] for Success: Gregg DG, Walczak S. Dressing Your Online Auction Business An Experiment Comparing Two eBay Businesses. MIS .Quarterly 2008(32):653–70

[4] compatibility beliefs Karahanna E, Agarwal R, Angst CM. Reconceptualizing in technology acceptance research. MIS .Quarterly 2006(Vol. 30 No. 4):781–804

[5] Lawkobkit M, Speece M. Integrating Focal Determinants of Service Fairness into Post-Acceptance Model of IS Continuance in Cloud Computing. In: 2012 IEEE/ACIS 11th International Conference .on Computer and Information Science; 2012, p. 49–55

[6] innovation Sonnenwald DH, Maglaughlin KL, Whitton MC (eds.). Using diffusion theory to guide collaboration technology evaluation: work in progress. Enabling Technologies: Infrastructure for Collaborative Enterprises, 2001. WET ICE 2001. Proceedings. .Tenth IEEE International Workshops on; 2001 Tan X, Kim Y. Cloud Computing

[7] for Education: A Case of Using Google Docs in MBA Group Projects. In: 2011 International Conference on Business Computing and Global Informatization; 2011, .p. 641–644

[8] Tjikongo R, Uys W. The viability of Cloud Computing Adoption in SMME's in Namibia. In: IST-Africa 2013 Conference .Proceedings; 2013, p. 1–11

[9] Computing: Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China.
Heidelberg: Springer Berlin; 2009:347–358
[10] and Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research Development Trend. In Second International Conference on Future Networks(ICFN'10), Sanya, Hainan, China. Washington, DC,
USA: IEEE Computer Society; 2010:93–97.CrossRefGoogle Scholar
[11] .of focus in Cloud Security Alliance: Security guidance for critical areas Cloud Computing V3.0.. 2011
[12] Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing,
.China. Heidelberg: Springer Verlag Berlin; 2009
[13] Centre for the Protection of National Infrastructure:
.Information Security Briefing 01/2010 Cloud Computing. 2010 Khalid A: Cloud
[14] Computing: applying issues in Small
Business. International Conference on Signal Acquisition and
.Processing (ICSAP'10) 2010, 278–28 Rosado DG, Gómez R, Mellado D,
[15] Fernández-Medina E:
Security analysis in the migration to cloud environments. Future
.Internet 2012, 4(2):469–487
[16] Mather T, Kumaraswamy S, Latif S: Cloud Security and
.Privacy. Sebastopol, CA: O'Reilly Media, Inc.; 2009
[17] interoperability of Li W, Ping L: Trust model to enhance Security and Cloud environment. In Proceedings of the 1st International conference on Cloud Computing. Beijing, China:
.Springer Berlin Heidelberg; 2009:69–79 Rittinghouse JW, Ransome JF: Security
[18] in the Cloud. In Cloud
Computing. Implementation, Management, and Security, CRC Press;
.2009 Kitchenham B: Procedures for perfoming systematic review, [18]
software engineering group. Australia: Department of Computer
Scinece Keele University, United Kingdom and Empirical Software
.Engineering, National ICT Australia Ltd; 2004
[20] systematic literature Kitchenham B, Charters S: Guidelines for performing reviews in software engineering. Version 2.3 University of keele (software engineering group, school of computer science and mathematics) and Durham. UK: Department of Conputer
.Science; 2007
[21] Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M:
Lessons from applying the systematic literature review process within
.the software engineering domain. J Syst Softw2007, 80(4):571–583
[22] threats and Dahbur K, Mohammad B, Tarakji AB: A survey of risks, vulnerabilities in Cloud Computing. In Proceedings of the

2011 International conference on intelligent semantic Web-services and applications. Jordan: Amman; 2011:1–6
[23] Ertaul L, Singhal S, Gökay S: Security challenges in Cloud Computing. In Proceedings of the 2010 International conference on Security and Management SAM'10. Las Vegas, US: CSREA Press; .2010:36–42 Grobauer B, Walloschek T, Stocker E: Understanding Cloud
[24] .Computing vulnerabilities. IEEE Security Privacy 2011, 9(2):50–57
[25] delivery Subashini S, Kavitha V: A survey on Security issues in service models of Cloud Computing. J Netw Comput Appl 2011, .11–1:)1(43 10.1016/j.jnca.2010.07.006 Jensen M, Schwenk J, Gruschka N, Iacono
[26] LL: On technical Security issues in Cloud Computing. In IEEE International conference .on Cloud Computing (CLOUD'09). :611 116; 2009:109–116
[27] Computing: Onwubiko C: Security issues to Cloud Computing. In Cloud principles, systems & applications. Edited by: .Antonopoulos N, Gillam L. Springer-Verlag: 2010; 2010
[28] Morsy MA, Grundy J, Müller I: An analysis of the Cloud Computing Security problem. In Proceedings of APSEC 2010 Cloud .Workshop. Sydney, Australia: APSEC; 2010
[29] Jansen WA: Cloud Hooks: Security and Privacy Issues in Cloud Computing. In Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI. Washington, DC, .USA: IEEE Computer Society; 2011:1–10
[30] Zissis D, Lekkas D: Addressing Cloud Computing Security .issues. Futur Gener Comput Syst2012, 28(3):583–592 Jansen W, Grance T:
[31] public Cloud Computing. Guidelines on Security and privacy in Gaithersburg, MD: NIST, Special Publication .800–144; 2011