الحوسبة السحابية

المصطلحات

العميل(Customer) :

كل شخص طبيعي أو جهه تحصل على خدمات تقنية على السحابة.

مستخدم السحابة(Cloud Consumer) :

الجهة التي تطلب وتستخدم المصادر والخدمات المتوفرة على السحابة.

مزود السحابة (Cloud Provider) :

الجهة التي توفر مصادر و خدمات السحابة والأنشطة اللازمة لتوفير هذه الخدمات وضمان ايصالها إلى مستخدم السحابة.

تكنولوجيا الحوسبة السحابية (Cloud Computing Technology) :

نموذج لتمكين الوصول الشبكي من أي مكان وبشكل مناسب وعند الطلب إلى مجموعة مشتركة من مصادر الحوسبة القابلة للإعداد(مثل الشبكات والخوادم ووسائط التخزين والتطبيقات والخدمات)لدى مزود السحابة.

البنية التحتية للسحابة (Cloud Infrastructure)

مجموعة من المكونات المادية والبرمجيات مثل الخوادم ووسائط التخزين والشبكات وبرامج المحاكاة الافتراضية اللازمة لدعم متطلبات الحوسبة السحابية.

اتفاقية مستوى الخدمة السحابية (Cloud Service Level Agreement) :

اتفاقية تعاقدية بين مزود السحابة والشركة يتم فيها تحديد متطلبات الشركة ومستوى الخدمة والضمانات التي يقدمها مزود السحابة بشأن توافرية الخدمات وأداءها ومستويات الدعم لها.

تقييم المخاطر (Risk Assessment) :

قياس وتحديد احتمالية حدوث المخاطر وشدتها وتوقع مقدار تأثيرها على الشركة.

إدارة التغيير (Change Management) :

إدارة وضبط وتوثيق أي تغيير يتم إجراؤه على أي من الخدمات المسندة

الحوسبة السحابية

لمزود السحابة.

ضوابط الوصول/النفاذ (Access Control) :

القواعد والآليات المستخدمة للسماح باستخدام ونفاذ الأشخاص المخولين فقط إلى أصول المعلومات وبما يتوافق وطبيعة مسؤولياتهم.

تصنيف المعلومات (Information Classification)

تحديد مستوى الحساسية المناسب للمعلومات التي يتم إنشاؤها أو تغييرها أو نقلها أو تعديلها أو حفظها على أية وسائل كانت وبأية تقنيات ممكنة، اعتمادا على المخاطر المترتبة عن الاطلاع والاستخدام غير المشروع لتلك المعلومات.

التعافي (Recovery)

مجموعة الاجراءات التي يتم اتخاذها واتباعها لإعادة الأعمال في الشركة الى وضعها الطبيعي وإعادة تشغيل موارد التكنولوجيا المعتمد عليها في تشغيل عمليات الشركة إلى ما كانت عليه قبل وقوع الحدث.

عمليات المسح (Vulnerability Scanning)

آلية تستخدم لتحديد خصائص الانظمة و نقاط الضعف المرتبطة بها.

اختبارات الاختراق (Penetration Testing) :

اختبار يحاول فيها المقيمون المختصون بالبحث عن الثغرات الامنية والتحايل على الخصائص الأمنية لأنظمة المعلومات والضوابط الامنية واستغلالها لمحاولة اختراق تلك الانظمة من خارج او داخل الشركة لمعرفة مدى فعالية الضوابط الأمنية المستخدمة من قبل الشركة لحماية أنظمتها.

زمن التعافي المستهدف (RTO) :

اقصى وقت مسموح به لإعادة تشغيل الخدمة أو العملية بعد حدوث الانقطاع للخدمة.

نقطة الاسترجاع المستهدفة (RPO) :

العمر الأقصى المسموح للبيانات التي قد تفقد عند استعادة الخدمة بعد حدوث انقطاع.

الحوسبة السحابية

الفصل الأول :تكنولوجيا الحوسبة السحابية

1.1 تمهيد

تعتبر تكنولوجيا الحوسبة السحابية نموذج لتمكين الوصول الشبكي من أي مكان وبشكل مناسب وعند الطلب إلى مجموعة مشتركة من المصادر المادية (Physical Resources) أو الإفتراضية (Virtual Resources) مثل الشبكات والخوادم ووسائط التخزين والتطبيقات والخدمات التي يمكن توفيرها بسرعة واستخدامها بأقل جهد .
ويتكون هذا النموذج من خمس خصائص أساسية (Essential Characteristics) ،
وثلاثة نماذج خدمة(Service Models) ،
وأربعة نماذج للنشر(Deployment Model).

1.2 الخصائص الأساسية(Essential Characteristics)

- **خدمة ذاتية بناء على الطلب (On-Demand Self-Service)**

خاصية تمكن مستخدم السحابة من طلب خدمات تخزين ومعالجة حسب الحاجة وتلقائيا بهدف التقليل من الحاجة الى التفاعل المباشر مع مزود السحابة.

- **وصول واسع الى الشبكة (Broad Network Access)**

يتضمن الوصول الشبكي من أي مكان إلى مصادر مزود السحابة عن طريق منصات الشركة مثل :الهواتف الجوالة والأجهزة اللوحية وأجهزة الحاسوب المحمولة ومحطات العمل.

- **تجميع المصادر (Resource Pooling)**

يتم تجميع مصادر الحوسبة المختلفة من قبل مزود السحابة لخدمة العديد من مستخدمي السحابة باستخدام نموذج (Multi-tenant model) مع تخصيص مصادر مادية وافتراضية مختلفة بشكل ديناميكي وإعادة تخصيصها وفقا لطلب مستخدم السحابة دون الحاجة لسيطرة مستخدم السحابة أو معرفته للموقع المحدد للمصادر الموفرة له من قبل مزود السحابة مع الاحتفاظ بحقه في تحديد الموقع على مستوى معين(على سبيل المثال البلد أو مركز البيانات)

- **مرونة سريعة (Rapid Elasticity)**

يمكن توفير الإمكانات وقدرات المعالجة على السحابة بشكل مرن وتلقائي وامكانية ضبط حجم المصادر المستخدمة بما يتناسب مع حجم العمل المطلوب من قبل مستخدم السحابة حيث تكون القدرات المتاحة غير محدودة ويمكن تخصيصها في أي وقت من خلال العقود المبرمة بين مستخدم ومزود السحابة.

- **الخدمة المقاسة (Measured Service)**

الحوسبة السحابية

يمكن التحكم تلقائيا في استخدام مصادر السحابة وتحسين ومراقبة استخدامها وتدقيقها وعمل تقارير بخصوص ذلك، وبالتالي توفير الشفافية لكل من مزود ومستخدم السحابة على أن يتحمل المستخدم التكلفة حسب المصادر المطلوبة.

1.3نماذج الخدمة (Service Models)

- **البرمجيات كخدمة Software as a Service (SaaS)**

نموذج لتوزيع البرامج وإتاحتها لمستخدم السحابة عبر الشبكة بحيث تكون التطبيقات مستضافة من قبل مزود السحابة دون الحاجة إلى تنصيب أو تشغيل التطبيقات على أجهزة المستخدم حيث يتمكن من استخدام التطبيقات التي تعمل على البنية التحتية الخاصة بالمزود ويمكن للمستخدم الوصول إلى تلك التطبيقات من خلال أجهزة مختلفة وعن طريق واجهة معينة مثل واجهة متصفح الويب أو البرنامج، وعمل اعدادات محدودة على تلك التطبيقات دون أن يقوم مستخدم السحابة بإدارة أو التحكم في البنية التحتية للسحابة.

- **المنصة كخدمة Platform as a Service (PaaS)**

تقدم المنصة بيئة حوسبة متكاملة بما في ذلك نظام التشغيل وبيئة تنفيذ لغات البرمجة وقواعد البيانات وخوادم الويب لتمكين مستخدم السحابة من تطوير وتشغيل التطبيقات الخاصة به ونشر تطبيقاته على البنية التحتية للسحابة والتحكم بإعداداتها دون أن يقوم المستخدم بإدارة أو التحكم في البنية التحتية للسحابة.

- **البنية التحتية كخدمة Infrastructure as a Service (IaaS)**

يتم توفير أجهزة الحاسوب المادية أو الافتراضية والمصادر الأخرى مثل الشبكات ووسائط التخزين من قبل مزود السحابة لدعم العمليات الخاصة بمستخدم السحابة حيث يكون المستخدم قادر على نشر وتشغيل بعض البرامج مثل أنظمة التشغيل والتطبيقات، ولا يقوم المستخدم بإدارة أو التحكم في البنية التحتية للسحابة، ولكن يمكنه التحكم في أنظمة التشغيل والتخزين والتطبيقات المنشورة، وربما سيطرة محدودة على بعض مكونات الشبكات(مثل الجدران النارية.)

1.4نماذج النشر(Deployment Models)

- **السحابة العامة (Public Cloud)**

يتم توفير البنية التحتية للسحابة للاستخدام المفتوح العام وقد تكون مملوكة أو تدار أو تشغل من قبل مؤسسة تجارية أو أكاديمية أو حكومية أو مجموعة منها وتكون البنية التحتية للسحابة موجودة في مقر تابع لمزود السحابة .ومن الممكن أن تخزن البيانات التابعة لمستخدم السحابة في مواقع غير معروفة له ومن الممكن ألا يتم استرجاعها بسهولة وقد تخزن البيانات الخاصة بمستخدم السحابة مع بيانات مستخدم آخر على نفس السحابة.

- **السحابة المجتمعية (Community Cloud)**

يتم توفير البنية التحتية للسحابة للاستخدام الحصري من قبل مجتمع معين من مستخدمي السحابة من الشركات التي تتشارك بنفس الاهتمامات مثل مهماتها ومتطلباتها الأمنية وسياساتها واعتبارات الامتثال لديها .وقد تكون مملوكة أو تدار أو تشغل من قبل واحدة أو أكثر من الشركات في ذلك المجتمع أو طرف ثالث أو مزيج منها، وهي أكثر تكلفة من السحابة العامة حيث يتم توزيع التكلفة على عدد من مستخدمي السحابة مقابل مستوى أعلى من الالتزام والخصوصية والأمن وقد تكون موجودة داخل أو خارج مواقع تلك الشركات، وقد تخزن البيانات الخاصة بكل شركة مع البيانات الخاصة بمنافسيها على نفس السحابة المجتمعية.

- **السحابة الخاصة(Private Cloud)**

يتم توفير البنية التحتية للسحابة للاستخدام الحصري من قبل مجموعة من مستخدمي السحابة قد تكون مملوكة أو تدار أو تشغلها المجموعة أو طرف ثالث أو كلاهما .وقد تكون البنية التحتية للسحابة داخل مقر المجموعة (On-premises) أو خارج مقرالمجموعة(Off-premises)، وتعتبر السحابة الخاصة من اقل نماذج النشر خطورة الا أن الخدمات المقدمة من خلالها قد لا تكون مرنة كما هي في السحابة العامة.

- **السحابة الهجينة (Hybrid Cloud)**

تتكون البنية التحتية للسحابة من اثنين أو أكثر من نماذج النشر سواء كانت السحابة خاصة أو مجتمعية أو عامة وتعتبر كيان مستقل ولكنها مرتبطة معا بتقنية موحدة تمكن البيانات والتطبيقات من الانتقال فيما بينها، وقد ينشأ عن ذلك مخاطر بسبب دمج أكثر من نموذج للنشر وهنا يقع على عاتق مستخدم السحابة مسؤولية تصنيف المعلومات ليتم تخزينها على
نموذج النشر الخاص بها، ويبين الجدول رقم (A) ادناه مقارنة بين نماذج النشر المختلفة.

جدول (A) مقارنة بين نماذج النشر المختلفة

نموذج النشر	مدير البنية التحتية للسحابة	مالك البنية التحتية للسحابة	موقع البنية التحتية للسحابة	يمكن الوصول إليها وإستخدامها من قبل
العامة(Public)	مزود السحابة	مزود السحابة	خارج مقر مستخدم السحابة	أي مستخدم للسحابة
الخاصة(Private) المجتمعية(Community)	مستخدم أو مزود للسحابة	مستخدم أو مزود للسحابة	خارج أو داخل مقر مستخدم السحابة	جهات موثوقة
الهجينة(Hybrid)	مستخدم أو مزود للسحابة	مستخدم أو مزود للسحابة	خارج أو داخل مقر مستخدم السحابة	جهات موثوقة وغير موثوقة

1.5الجهات الفعالة في السحابة(Cloud Actors)

تتمثل الجهات التي تتشارك في العمليات و/أو المهام المتعلقة بالحوسبة السحابية سواء كانت شركات أو اشخاص بشكل فعال في السحابة بما يلي:

1- **مستخدم السحابة(Cloud Consumer)**

2- **مزود السحابة(Cloud Provider)**

3- **وسيط السحابة(Cloud Broker)**

يعمل كوسيط بين مستخدم ومزود السحابة ويساعد مستخدمي السحابة في اختيار وادارة خدمات الحوسبة السحابية المختلفة والمقدمة من قبل المزود بالإضافة الى توفير خدمات اضافية للمستخدم .وتشمل الخدمات المقدمة من خلال وسيط السحابة ما يلي:

- **الوساطة (Intermediation)**

الحوسبة السحابية

يقوم الوسيط على تعزيز خدمة معينة من خلال تحسينها وتوفيرخدمات ذات قيمة مضافة للمستخدمين، ويمكن أن يكون التحسين متمثل بإدارة الوصول إلى خدمات الحوسبة السحابية، وإدارة الهوية، وتعزيز الأمن، وما إلى ذلك.

- **التجميع (Aggregation)**

يقوم الوسيط على جمع ودمج خدمات متعددة في خدمة واحدة أو أكثر من الخدمات الجديدة وتوفيرها لمستخدم السحابة، كما يوفر الوسيط البيانات وتكامل الخدمات ويضمن حركة البيانات الآمنة بين مستخدم ومزودي السحابة.

- **الموازنة (Arbitrage)**

تشبه خدمة التجميع إلا أن الخدمات المجمعة ليست ثابتة حيث أن الوسيط لديه المرونة في اختيار الخدمات من أكثر من مزود للسحابة.

4- . **مدقق السحابة (Cloud Auditor)**

يقوم مدقق السحابة بمراقبة أداء الخدمات السحابية والضوابط الأمنية التي تنفذ على السحابة للتحقق من الامتثال للسياسات الأمنية الخاصة بالحوسبة السحابية.

5- . **ناقل السحابة (Cloud Carrier)**

يقوم ناقل السحابة بنقل الخدمات السحابية والبيانات بين مستخدمي ومزودي السحابة على أن يتحمل مزود السحابة مسؤولية إعداد اتفاقية مستوى الخدمة السحابية مع ناقل السحابة لضمان ايصال البيانات والخدمات الى مستخدم السحابة ضمن المستوى المتفق عليه.

1.5.1 العلاقة بين الجهات الفعالة في الحوسبة السحابية

- يمكن لمستخدم السحابة طلب خدمات الحوسبة السحابية من مزود السحابة مباشرة أو عن طريق وسيط السحابة وفي حال تم التعامل مع وسيط السحابة فعلى مستخدم السحابة الأخذ بعين الاعتبار أن وسيط السحابة ينطبق عليه ما ينطبق على مزود السحابة في حال تم التعاقد معه.
- يقوم مدقق السحابة بإجراء عمليات تدقيق مستقلة عن الجهات الفعالة الأخرى وجمع المعلومات اللازمة لذلك.
- هناك أدوار محددة لكل من مزود ومستخدم السحابة عند استخدام نماذج الخدمة المختلفة كما هو مبين في الجدول (B)

الحوسبة السحابية

جدول (B) الأدوار المختلفة لكل من مزود ومستخدم السحابة عند استخدام نماذج الخدمة الثلاث

نموذج الخدمة	أنشطة مستخدم السحابة (Cloud Consumer Activities)	أنشطة مزود السحابة (Cloud Provider Activities)
البرمجيات كخدمة (SaaS)	استخدام التطبيقات المتوفرة على السحابة لإجراء العمليات الخاصة بنطاق عمله.	يثبت ويدير ويحافظ على ويدعم التطبيقات المتوفرة لديه والخاصة بمستخدم السحابة على البنية التحتية للسحابة لديه
المنصة كخدمة (PaaS)	تطوير واختبار ونشر وادارة التطبيقات المستضافة على منصة السحابة.	تخصيص وإدارة البنية التحتية للسحابة وتوفير أدوات التطوير والنشر والإدارة لمستخدمي السحابة.
البنية التحتية كخدمة (IaaS)	-إنشاء/تثبيت وإدارة ومراقبة خدمات البنية التحتية للسحابة الخاصة به. - التحكم في الأجهزة الافتراضية(Virtual Machines)التي يتم استخدامها على السحابة من حيث أنظمة التشغيل والتخزين والتطبيقات التي تم نشرها على مستوى تلك الأجهزة.	تقديم وإدارة المعالجة المادية والتخزين والشبكات وبيئة الاستضافة والبنية التحتية للسحابة لمستخدمي السحابة.

الفصل الثالث: المعايير الخاصة بالحوسبة السحابية

نظرا للتحديات التي تواجهها الشركات والتي قد تعيق تبنيها لتكنولوجيا الحوسبة السحابية ومن أجل تمكين الشركات من استخدام هذه التكنولوجيا بطريقة آمنة تقلل من تعرضها للمخاطر الناجمة عن ذلك؛ على الشركات اتخاذ كافة التدابير اللازمة لحمايتها من تلك المخاطر من خلال استخدام المعايير الأمنية الشائعة في جميع أنحاء العالم التي تدعم تكنولوجيا الحوسبة السحابية والتي يمكن من خلالها المحافظة على سرية وأمن البيانات عند الإستعانة بمزود السحابة، وتقدم هذه المعايير العديد من الفوائد ومنها:

- تعزيز توافقية أنظمة الشركة مع أي أنظمة أخرى مما يجعل الانتقال من مزود سحابة إلى آخر أبسط.
- ضمان اتباع الشركات ومزودي السحابة أفضل الممارسات بهذا الخصوص
- تعتبر المعايير وسيلة فعالة تمكن الشركات من المقارنة بين مزودي السحابة لاختيار المزود الأنسب.
- يتيح استخدام المعايير مسارا أسهل للامتثال التنظيمي.

وهناك العديد من المعايير الخاصة بـأمن تكنولوجيا الحوسبة السحابية والتي تم نشرها مؤخرا، بما في ذلك ISO/IEC 27017 و ISO/IEC27018، التي توفر إرشادات أكثر تفصيلا لكل من الشركات ومزودي السحابة. بالإضافة إلى ذلك، هناك عدد من المعايير العامة لتكنولوجيا المعلومات التي يمكن تطبيقها عند استخدام تكنولوجيا الحوسبة السحابية حيث أن هذه المعايير ليست محددة للحوسبة السحابية بشكل خاص، ولكنها عامة بحيث يمكن تطبيقها على بيئة الحوسبة السحابية لذا ينبغي على الشركة ومزود السحابة إعطاء الأهمية لهذه المعايير حيث تقدم هذه المعايير توجيهات وتوصيات وبشكل تفصيلي لكل من الشركة والمزود ونخص بالذكر المعايير التالية مصنفة حسب عدة مواضيع كما هو بالجدول (C):

الحوسبة السحابية

الموضوع	المعايير
الحوكمة وإدارة المخاطر والامتثال	▪ COBIT ▪ ISO/IEC 20000 ▪ SSAE 16 or ITIL depending on type of workload ISO/IEC 27001 and ISO/IEC 27002 ▪ ISO/IEC 27017 & ISO/IEC 27018 ▪ ISO/IEC 38500 – IT Governance ▪ Cloud Security Alliance (CSA) Cloud Controls Matrix ▪ National Institute of Standards and Technology (NIST) ▪ Cybersecurity Framework (CSF)
العمليات التشغيلية والتجارية	▪ SSAE 16 ▪ ISO/IEC 27000
إدارة الادوار	▪ LDAP, SAML 2.0, OAuth 2.0, WS-Federation, OpenID Connect, SCIM ▪ XACML ▪ PKCS, X.509, OpenPG
حماية البيانات والمعلومات	▪ ISO/IEC 27018
سياسات الخصوصية	▪ ISO/IEC 27033 or FIPS199/200 standards
أمن وحماية الشبكات	▪ ISO/IEC 27002 ▪ ISO/IEC 27017 & ISO/IEC 27018
الضوابط الامنية على البنية التحتية شروط الأمان في إتفاقية مستوى الخدمة	▪ ISO/IEC 19086 ▪ ISO/IEC 27004:2009, TM Forum TR 178, NIST Special Publication 800-55, CIS Consensus Security Metrics V1.1.0, and ENISA Procure Secure ▪ CWE list ▪ CSA STAR registry ▪ PCI DSS ▪ FedRAMP program
عمليات الإنهاء	▪ ISO/IEC 19086

المراجع

الحوسبة السحابية

.1ABS Cloud Computing Implementation Guide 1.1 For The Financial Industry in Singapore, The Association of Banks in Singapore, 2 Aug 2018.

2. Banking on Cloud (A discussion paper by the BBA and Pinsent Masons), BBA Cloud Working Group, 5 December 2016.

3. NIST Cloud Computing Standards Roadmap, NIST Cloud Computing Standards Roadmap Working Group, NIST Cloud Computing Program, July 2013.

4. NIST Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards & Technology Gaithersburg, MD, United States , 2011

5. Australian Government Cloud Computing Policy Smarter ICT Investment, Australian Government, Department of Finance, Version 3.0, October 2014

6. International Standard ISO/IEC 17788 First edition 2014-10-15, ISO/IEC 17789, 2014

7. Cloud Security Policy for Government Agencies, Qatar National Information Assurance, 2014

8. Practical Guide to Cloud Computing Version 2.0, Cloud Standard Customer Council, April, 2015

9. Cloud Security Standards "What to Expect & What to Negotiate Version 2.0", Cloud Standard Customer Council, 2016.

10. Security for Cloud Computing Ten Steps to Ensure Success Version 2.0 March, Cloud Standards Customer Council, 2017

11. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance

.12PCI DSS Cloud Computing Guidelines, Cloud Special Interest Group PCI Security Standards Council, February 2013

13. Best Practices for Security in Cloud Adoption by Indian Banks, Members of The Open Group Security Forum, March 2015

14. How Cloud is Being Used in the Financial Sector: Survey Report, CSA, March 2015

15. Towards a Generic Value Network for Cloud Computing, Markus Böhm*, Galina Koleva, Stefanie Leimeister, Christoph Riedl, and Helmut Krcmar, 2010

16. Secure Use of Cloud Computing in the Finance Sector / Good practices and recommendations, European Union Agency for Network and Information Security, December 2015.

17. A Reference Guide to Cloud Computing Dimensions: Infrastructure as a Service Classification Framework, Jonas Repschlaeger, Stefan Wind, Ruediger Zarnekow, Klaus Turowski, 2012

18. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, CSA, December 2009

19. Cloud Computing-Software as Service, Gurudatt Kulkarni, Jayant Gambhir, Rajnikant Palwe, March, 2012

20. FG 16/5 - Guidance for firms outsourcing to the 'cloud' and other third- party IT services, FCA, July 2016.

21. Framework for Risk Management in Outsourcing Arrangements by Financial Institutions, State Bank of Pakistan, 2017

22. Circulaire Cloud Computing, De Nederlandsche Bank, 2012

23. Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives/ISACA, 2009

24. Outsourcing in Financial Services, Basel Committee on Banking Supervision, February 2005

.25 Guidelines on Outsourcing, Monetary Authority of Singapore, 27 JUL 2016

26. Guidelines on Business Continuity Planning, Monetary Authority of Singapore, June 2003

27. Public Consultation on Guidance on Outsourcing, Response to Feedback Received, July 2016

28. سبل الإفادة من تطبيقات الحوسبة السحابية في ت قديم خدمات المعلومات بدولة الإمارات العربية المتحدة، 3/2014 كلية الدراسات الإسلامية والعربية بدبي،