واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة دراسة حالة

إعداد

مروة رجاء القاضي

طالبة ماجستير بكلية الآداب والعلوم الإنسانية

جامعة الملك عبد العزيز

جدة – المملكة العربية السعودية

marwa.alkadi12@gmail.com

إشراف

د. سوزان أحمد سلطان

كلية الآداب والعلوم الإنسانية

جامعة الملك عبد العزيز

جدة – المملكة العربية السعودية

suzanlegend@gmail.com

المستخلص:

عد الأمن السيبراني من أهم العوامل التي تؤثر على جودة العملية التعليمية واستمرارية الأعمال داخل الجامعات من ناحية عملية وإدارية وبحثية، لذا من المهم اتخاذ الإجراءات الأمنية اللازمة للحفاظ على أمان الحوسبة السحابية، وهدفت الدراسة إلى التعرف على أبرز مواضيع الأمن السيبراني في الحوسبة السحابية، وإيضاح ضوابط الأمن السيبراني للحوسبة السحابية في المملكة العربية السعودية، والاستكشاف الشامل لواقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة، واعتمدت الدراسة على المنهج الوصفي بكل من شقية التحليلي ودراسة الحالة، واستخدام قائمة المراجعة التي تم إعدادها استنادًا على ضوابط الأمن السيبراني للحوسبة السحابية الصادرة من الهيئة الوطنية للأمن السيبراني كأداة لجمع البيانات، واستكمال بياناتها من خلال تحليل محتوى المصادر الأولية الصادرة عن قسم الأمن السيبراني في موقع جامعة طيبة والمقابلة المفتوحة مع عينة الدراسة المتمثلة بمهندسين من

تاريخ استلام البحث: 2024/01/09 تاريخ إجازة البحث: 2024/01/19

قسمs الأمن السيبراني ومهندسين من قسم تقنية المعلومات في جامعة طيبة. وتوصلت الدراسة إلى مجموعة من النتائج أبرزها ضرورة تطبيق الضوابط والمعايير الأمنية للحفاظ على أمن البيانات والمحتوى المخزن في السحابة، وأن وثيقة ضوابط الأمن السيبراني للحوسبة السحابية تسعى إلى تحقيق الأهداف الوطنية للأمن السيبراني عن طريق التركيز على خدمات الحوسبة السحابية من منظور مقدمي الخدمات والمشتركين، وتحسين الاستعداد للمخاطر السيبرانية عبر جميع خدمات الحوسبة السحابية، ووجود درجة تطبيق كبيرة لضوابط الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة. كما أوصت الدراسة بضرورة تقديم خارطة استرشادية وتوجيهية بشأن التدابير والممارسات الأمنية المطلوبة لحماية الأنظمة والشبكات السيبرانية من قبل الهيئة الوطنية للأمن السيبراني وتهدف إلى التطبيق الفعال لكافة الضوابط ذات الصلة، وأوصت أيضًا بتعاون جامعة طيبة مع مقدم خدمات سحابية داخل المملكة العربية السعودية للتأكد من الاستجابة السريعة والامتثال للتشريعات والقوانين الخاصة بالدولة ودعم اقتصادها المحلي، وتحث الدراسة على استكمال المجال البحثي في مجال الأمن السيبراني للحوسبة السحابية من خلال إعداد دراسات لقياس مستوى تنفيذ ضوابط ومعايير الأمن السيبراني للحوسبة السحابية في مؤسسات التعليم العالي.

الكلمات المفتاحية: الأمن السيبراني؛ الحوسبة السحابية؛ الأمن السحابي

1. الإطار المنهجي:

1.1 تمهيد:

يعيش العالم اليوم في عصـــر رقمي يشـــهد تطورات تكنولوجية وابتكارات تقنية مبهرة، وأصـبحت تقنية الحوسـبة السـحابية محورًا مهمًا في تطويرالعمليةالتعليمية. توفر الحوسـبة السـحابية مجموعة من المزايا التي تجعلها أداة قوية في مجال التعليم، كالوصـــول إلى الموارد الحاسـوبية والتطبيقات عبر الإنترنت مما يسـمح للطلاب وأعضـاء هيئة التدريس بالوصـول إلى المحتوى التعليمي ومشـــاركة المعرفة في أي وقت ومن أي مكان وبفضـــل هذا الوصـــول المرن والفوري أصبح التعليم عن بعد ممكنًا مما يسـهم في التغلب على تلك التحديات التي قد تواجه العملية التعليمية. حيث سـاهمت الحوسـبة السـحابية بشـكل كبير في التغلب على التحديات التي فرضـــها فيروس كورونا (COVID-19) على العملية التعليمية. عندما علقت العديد من البلدان الفصـــول الدراســـية واضـــطرت الجامعات إلى التحول إلى نماذج التعليم عن بعد، وبمســـاعدة الحوســـبة الســـحابية تمكن الطلاب من مواصـــلة التعلم من خلال الوصـــول إلى المحتوى التعليمي والأدوات التعليمية عبر الإنترنت، وتمكن أعضـــاء هيئة التدريس من تقديم الموارد التعليمية وإرســـال الواجبات والاختبارات ومراقبة تقدم الطلاب عن بعد عبر الإنترنت. ومع تزايد اعتماد التعليم على الحوســـبة الســـحابية ظهرت تحديات أمنية وهجمات إلكترونية وتهديدات ســـيبرانية جديدة. وللحفاظ على ســـمعة الجامعات وحفظ خصـــوصـــيتها والحماية الأكاديمية والبحثية وللحماية ضـــد التهديدات الســـيبرانية لابد من الالتزام بضـــوابط ومعايير أمنية وتنفيذ تدابير أمنية قوية مثل التشـفير والمصـادقة متعددة العوامل والتحكم في الوصـول لموارد السـحابة وغيرها، للحفاظ على أمن البيانات ومنع التدخلات غير المصـرح بها لاسـتمرارية العملية التعليمية. لذا يجب أن تتخذ المؤسـسـات التعليمية إجراءات اسـتباقية لحماية بياناتها وتطبيقاتها داخل الحوســـبة الســـحابية ويعرض هذا الفصـــل المنهجية العلمية للدراســـة وما تعتمد علية من مناهج وأدوات لتحقيق أهدافها، والدراسات السابقة المتعلقة بها

1.2 مشكلة الدراسة:

تعتبر الحوســـبة الســـحابية من التقنيات المهمة في عصـــرنا الرقمي وتوجهت الكثير من المنظمات والمؤســـســـات لتطبيقها ومواكبة التغيرات، ووفقًا لما جاء في تقرير (IDC) انه من

المحتمل ارتفاع قيمة الحوسبة السحابية في السوق بالمملكة العربية السعودية إلى الضعف بحلول عام 2025 م للاستفادة من فوائد و مميزات الحوسبة السحابية في الأعمال، كما أن اللجنة الوطنية للتحول الرقمي قد اعتمدت سياسة للحوسبة السحابية في 2020 وتهدف السياسة الى تبني خدمات الحوسبة السحابية ورفع الكفاءة والإنفاق وتعزيز الأمن السيبراني والمرونة والموثوقية(منشآت، 2022). ويمكن صياغة مشكلة الدراسة في التساؤل الرئيسي التالي:

ما واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة؟

1.3 أهمية الدراسة:

يعتبر الأمن السيبراني من أهم العوامل التي تؤثر على جودة العملية التعليمية واستمرارية الأعمال داخل الجامعات من ناحية عملية وإدارية وبحثية، لذا من المهم اتخاذ الإجراءات الأمنية اللازمة للحفاظ على أمان الحوسبة السحابية ومن هنا تأتي أهمية الدراسة وذلك لأهمية المجال الموضوعي لعنوانها والاستكشاف الشامل لواقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة، وتعد الدراسة إضافة للمحتوى العربي الذي يسوده ندرة الدراسات في مجال الأمن السيبراني للحوسبة السحابية.

1.4 أهداف الدراسة:

1. التعرف على الحوسبة السحابية واستخداماتها في التعليم
2. التعرف على أبرز مواضيع الأمن السيبراني في الحوسبة السحابية
3. تبيان ضوابط الأمن السيبراني للحوسبة السحابية في المملكة العربية السعودية
4. وصف واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة

1.5 تساؤلات الدراسة:

1. ما هي الحوسبة السحابية وما استخداماتها في التعليم؟
2. ما هي أبرز مواضيع الأمن السيبراني في الحوسبة السحابية؟
3. ما هي ضوابط الأمن السيبراني للحوسبة السحابية في المملكة العربية السعودية؟
4. ما واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة؟

1.6 منهج الدراسة:

لتحقيق أهداف الدراســة تم اختيار المناهج التالية: المنهج الوصــفي بكل من شــقية التحليلي في الجزء النظري وذلك لتوضيح المفاهيم المترابطة مع موضوع الدراسة بالاعتماد على أحدث الدراسات، ودراسة الحالة في الجزء التطبيقي لملائمته لأهداف الدراسة التي تسعى إلى التعرف على واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة.

1.7 مجتمع الدراسة:

تشتمل الدراسة على كل من إدارة الأمن السيبراني وإدارة تقنية المعلومات بجامعة طيبة كمجتمع للدراسة كونها الجهتين المسؤولة عن الحوسبة السحابية وأمنها السيبراني بالجامعة.

1.8 عينة الدراسة:

تشتمل عينة الدراسة على كل من:

قسم تقنية المعلومات:

1. مدير إدارة الدعم الفني والصيانة: م. محمود عبد العزيز البدر
2. مدير إدارة تطوير الأنظمة: م. عاطف عباد الجابري.

قسم الأمن السيبراني:

م. أحمد العبيري.

1.9 أدوات جمع البيانات:

اعتمدت الباحثة لتحقيق متطلبات الدراسة على كل من:

1. قائمة المراجعة التي تم إعدادها استنادًا على ضوابط الأمن السيبراني للحوسبة السحابية الصادرة من الهيئة الوطنية للأمن السيبراني
2. المقابلة المفتوحة مع عينة الدراسة
3. تحليل محتوى المصادر الأولية الصادرة عن قسم الأمن السيبراني في موقع جامعة طيبة

1.10 حدود الدراسة:

تتحدد الدراسة بالحدود التالية:

- الحدود الزمانية: تم إجراء الدراسة في عام 2023 / 1445

- الحدود المكانية: أجريت الدراسة في جامعة طيبة - المدينة المنورة
- الحدود الموضوعية: واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة: دراسة حالة.
- الحدود اللغوية:

1. اللغة العربية: تمت كتابة البحث باللغة العربية، واعتماده أيضا على بعض الدراسات السابقة باللغة العربية.
2. اللغة الإنجليزية: يعتمد البحث على بعض الدراسات السابقة والمصادر باللغة الإنجليزية

1.11 مصطلحات الدراسة:

تم تعريف المصطلحات التالية إجرائيًا:

- الحوسبة السحابية: هي نموذج يقدم الخدمات الرقمية ويتيح للشركات والأفراد الوصول الشبكي للموارد الحاسوبية القابلة للتوسع واستخدامها من أي مكان وفي أي وقت، مثل الشبكات والتخزين والتطبيقات عن بعد دون الحاجة لامتلاك الأجهزة التشغيلية.
- أمن الحوسبة السحابية: هو مزيج من التقنيات والسياسات والممارسات لتأمين وحماية النظام السحابي استباقيًا والحفاظ على سلامة البيانات والمعلومات التي تم تخزينها أو معالجتها أو نقلها عبر السحابة من أي استخدام غير قانوني أو تهديدات أو الهجمات السيبرانية لضمان استمرارية الأعمال.

1.12 الدراسات السابقة:

يتعلق هذا الجزء بأهم الدراسات ذات العلاقة بموضوع الدراسة الحالية وهي: واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة: دراسة حالة، وعلى حد علم الباحثة لا يوجد دراسات عربية تتعلق بالأمن السيبراني للحوسبة السحابية بالتعليم العالي لذلك سيتم استعراض الدراسات الأجنبية، والتي سيتم ترتيبها زمنيًا من الأحدث إلى الأقدم وتم ترتيب سنوات النشر المتشابهة وفقًا لاسم المؤلف ترتيبًا هجائيًا، وتمتد الفترة الزمنية التي تغطيها الدراسات السابقة ما بين (2009- 2022 م)

الدراسات الأجنبية:

دراسة (Liando et al.,2022) تهدف هذه الدراسة إلى فهم بنية أمن الحوسبة السحابية والعوامل الكامنة وراء اعتماد الأمن السحابي في المؤسسات التعليمية. وقد شملت طريقة البحث منهجًا وصفيًا نوعيًا، كما تم جمع البيانات من خلال فحص المصادر ذات الصلة مثل الكتب والأدبيات والتقارير والسجلات المتعلقة بالموضوع. ومن نتائج الدراسة تأكيد أهمية الحفاظ على أمن البيانات في الحوسبة السحابية، وإيضاح التحديات التي تواجه المؤسسات التعليمية عند تطبيق تقنية الحوسبة السحابية والحاجة إلى تدابير أمنية مناسبة لضمان أمن البيانات، والعوامل المؤثرة على اعتماد أنظمة أمان الحوسبة السحابية في المجال التعليمي. كما تؤكد الدراسة على أهمية معرفة القواعد التي يضعها مقدمين الخدمات السحابية ومعرفة من يمكنه الوصول إلى البيانات. وأوصت الدراسة بأن تختار المؤسسات التعليمية مقدم خدمة سحابية موثوقًا به وتتخذ التدابير الأمنية المناسبة لمنع سرقة البيانات. وتوصي الدراسة أيضًا بأن تستخدم المؤسسات التعليمية معايير ISO 27001 أو COBIT لضمان أمن البيانات.

دراسة (Mary and Rose, 2019) تقدم الدراسة تحليلًا شاملًا لتأثيرات ومخاطر وتحديات الحوسبة السحابية في المجال الأكاديمي، وتقدم نظرة ثاقبة حول كيفية قيام الجامعات بالتخفيف من المخاطر والتحديات الأمنية أثناء اعتماد الحوسبة السحابية. وتركز الدراسة على المخاوف الأمنية والمخاطر المرتبطة باعتماد الحوسبة السحابية في التعليم في البلدان النامية. وتناقش الدراسة الاختلافات بين نماذج السحابة العامة والسحابة الخاصة وكيفية تأثيرها على الأمان والسرية. وشملت طرق البحث مراجعة الأدبيات بين عامي2010-2019م. وأوضحت نتائج الدراسة إلى أن عدد السكان ينمو بشكل كبير ونتيجة لذلك، سيكون هناك نقص في المعلمين المهرة وذوي الخبرة. وأوصت الدراسة بتوفير آليات أمنية مثل أدوات فحص الفيروسات، وطرق مختلفة لحماية كلمة المرور والمصادقة، والتوقيعات الرقمية لضمان سلامة المتعلمين الإلكترونيين واختيار أفضل مزود خدمة لإدارة الأمن بشكل فعال في سحابة التعليم وتوفير التسهيلات عبر الإنترنت ورفع الوعي والتدريب.

دراسة (WENDY and GUNAWAN, 2019) تهدف الدراسة إلى قياس أداء كل من أمن المعلومات والأمن السيبراني للحوسبة السحابية الخاصة في التعليم العالي وتوفير رؤى مفيدة

حولها. وتقييم مستوى نضج أمن المعلومات في الحوسبة السحابية الخاصة في جامعة XYZ. تم تطبيق أساليب البحث الكمية والنوعية كما تم جمع البيانات من خلال 12 استبيانًا تم توزيعها على قسم تكنولوجيا المعلومات بجامعة XYZ ضمن هيكل وظيفي محدد، وتمت الإجابة على11منها ومن ثم تمت معالجة البيانات باستخدام تطبيق Excel. وأظهرت نتائج الدراسة مستوى نضج أمن المعلومات والأمن السيبراني في الحوسبة السحابية الخاصة بجامعة XYZ و تحديد نقاط الضعف في الحوسبة السحابية لدى جامعة XYZ وتقديم توصيات لتحسين الوضع الحالي للجامعة، واستخلصت الدراسة أن مشكلات الأمن السيبراني و أمن المعلومات الحالية للحوسبة السحابية الخاصة تتمثل في تنفيذ سياسة التشفير، وعدم وجود حدود وعمليات تدقيق لمقدمون الخدمات، ونقص في كل من السياسات المرتبطة بالامتثال القانوني و سياسة مراقبة البنية التحتية وإدارة أمن الشبكات والاتصال ومراقبة نظام إدارة أمن المعلومات (ISMS) نفسه. وأوصت الدراسة بتنفيذ إطار لإدارة المخاطر وإجراء عمليات تدقيق أمنية منتظمة، واستخدام مجموعة من أطر آمن المعلومات، مثل ISO 27001:2013 وCOBIT5 لقياس وتحسين أمن المعلومات وأداء الأمن السيبراني.

دراسة (Al-Shqeerat et al.,2017) تهدف هذه الدراسة إلى معالجة التحديات الأمنية الرئيسية لاعتماد الحوسبة السحابية في مؤسسات التعليم العالي وشملت طرق البحث مراجعة الأدبيات وتم جمع البيانات من خلال إجراء الاستطلاع في مؤسسات تعليمية متنوعة لدراسة آراء أصحاب المصلحة حول نقاط الضعف الأمنية السحابية والأساليب المستخدمة للتغلب عليها. ومن نتائج الدراسة أن العديد من المستخدمين ليس لديهم المعرفة الكافية بالمخاطر الأمنية التي تهدد السحابة الخاصة بهم، وان من أكثر التحديات شيوعا هي القضايا الأمنية المرتبطة بالمحاكاة الافتراضية وطريقة التشفير المستخدمة في السحابة، وحاجة المؤسسات التعليمة إلى تحسين الوعي الأمني والاستعداد للتخفيف من المخاطر المتعلقة بأمن الحوسبة السحابية. تم التوصل الى توصية شاملة لتجنب المخاطر الأمنية بشكل فعال عند اعتماد المؤسسات التعليمية للحوسبة السحابية. تتضمن هذه التوصيات توفير برامج توعية وتدريب منتظم لتثقيف أصحاب المصلحة فيما يتعلق بالقضايا الأمنية المرتبطة بالحوسبة السحابية، استخدام آليات التشفير لحماية البيانات وتنفيذ ضوابط وصول قوية، ومراقبة الخدمات السحابية وتدقيقها بانتظام.

دراسة (Tout et al.,2009) تهدف الدراسة إلى تقديم لمحة عن الحوسبة السحابية وفوائدها المتوقعة لمؤسسات التعليم العالي. وتوضح الدراسة المخاطر المرتبطة بالحوسبة السحابية، مثل المخاوف الأمنية وخصوصية وأمن البيانات. تم جمع البيانات من خلال مراجعة الأدبيات. أظهرت نتائج الدارسة العديد من فوائد الحوسبة السحابية لمؤسسات التعليم العالي مثل توفير التكاليف والمرونة وقابلية التوسع وتحسين التعاون، كما أن هناك العديد من المخاوف بشأن اعتماد الحوسبة السحابية مثل آمن الحوسبة السحابية. وأن الحوسبة السحابية قد يكون لها إمكانيات كبيرة في تحسين تطبيقات تكنولوجيا المعلومات والبنية التحتية في مؤسسات التعليم العالي. وأوصت الدراسة بالاتصال الوثيق مع منظمات معايير الصناعة مثل المعهد الوطني للمعايير والتكنولوجيا (NIST)، وأن تتبع المؤسسات التعلمية نهجًا استراتيجيًا دقيقًا لاعتماد السحابة، وأن تقيّم المؤسسات التعليمية الاحتياجات الفعلية لأعمالهم والنظر في اعتماد نهج هجين حيث يجمع بين الحلول القائمة على السحابة والحلول المحلية، وتحليل التكلفة والعائد، والتأكد من إجراء تقييم شامل لمقدمي الخدمات السحابية قبل اتخاذ القرارات.

2. الحوسبة السحابية

2.1 تمهيد:

توفر الحوسبة السحابية وصولًا عالميا وتعد تقنية ثورية في مجال التعليم لقدراتها العالية في التخزين والمرونة ومشاركة الموارد لذا فإن إضافة قدرات الحوسبة السحابية للجامعات أمرًا بالغ الأهمية في عصرنا الحالي لتعزيز التعلم التفاعلي الفعال والوصول الفوري والمرن إلى المحتوى التعليمي والتطبيقات عبر الإنترنت وتعزيز التكامل العالمي للتعليم ونستعرض في هذا الفصل مفهوم الحوسبة السحابية، وخصائصها، وأنواع النشر، ونماذج الحوسبة السحابية، واستخداماتها في التعليم وفوائدها لكلٍ من أعضاء هيئة التدريس والطلاب.

2.2 مفهوم الحوسبة السحابية:

عرفت هيئة الاتصالات والفضاء والتقنية الحوسبة السحابية على أنها نموذج يتيح الوصول الشبكي السهل وحسب الطلب إلى مجموعة مشتركة من الموارد الحاسوبية القابلة للتكوين، على سبيل المثال الخوادم والشبكات والتخزين والخدمات البرمجية والتطبيقات التي يمكن توفيرها وإطلاقها بشكل سريع بأقل جهد إداري أو تفاعل بشري مع مقدم الخدمة (هيئة الاتصالات

والفضاء والتقنية، 2022). وعرف تحالف أمن الحوسبة السحابية على أن الحوسبة السحابية هي نموذج تشغيلي جديد ومجموعة من التقنيات لإدارة التجمعات المشتركة لموارد الحوسبة. وهي تقنية لديها القدرة على تعزيز التعاون وخفة الحركة والتوسع والتوافر، وتوفر الحوسبة السحابية فرصاً لخفض التكلفة وفعالية بالأداء. يتصور نموذج السحابة عالماً يمكن فيه تنظيم المكونات وتوفيرها وتنفيذها وإيقاف تشغيلها بسرعة، وتوسيع نطاقها أو خفضها لتوفير نموذج شبيه بالمرافق عند الطلب للتخصيص والاستهلاك (Mogull et al.,2021). وتعد الحوسبة السحابية نموذجًا لتمكين الوصول إلى الشبكة في كل مكان وبشكل ملائم وعند الطلب إلى مجموعة مشتركة من موارد الحوسبة القابلة للتكوين (مثل الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها وإصدارها بسرعة وبأقل جهد إداري أو تفاعل مع مزود الخدمة (NIST,2011).

2.3 الخصائص الرئيسية للحوسبة السحابية؟

وتخلص الباحثة الخصائص الأساسية للحوسبة السحابية

1. الخدمة الذاتية حسب الطلب: يمكن للمستهلك توفير إمكانات الحوسبة من جانب واحد وتقديم الخدمات الحاسوبية من جانب واحد، حسب الحاجة تلقائيًا دون الحاجة إلى تفاعل بشري مع كل مقدم خدمة (Mogull et al.,2021).
2. الوصول الشبكي الواسع: توفر الخدمات من خلال الشبكة مع إمكانيات الوصول بالوسائل والطرق القياسية التي تتيح للمشترك استخدام الخدمة عبر منصات مختلفة مثل الحواسب المحمولة والهواتف الذكية والحواسب المكتبية (هيئة الاتصالات والفضاء والتقنية ،2022).
3. تجميع الموارد: يتم تجميع موارد الحوسبة لخدمة العديد من المشتركين عن طريق استخدام نموذج متعدد المستأجرين، مع تخصيص موارد مادية وافتراضية مختلفة وإعادة تخصيصها ديناميكيًا وفقًا لطلب المشترك. هناك نسبة من استقلالية الموقع حيث إن العميل بشكل عام ليس لديه سيطرة أو معرفة بالموقع الدقيق للموارد المقدمة، ولكن قد يكون قادرًا على تحديد الموقع على مستوى أعلى، على سبيل المثال: الدولة أو الولاية أو مركز البيانات. وتتضمن الأمثلة على الموارد مساحات التخزين والذاكرة والمعالجة والحواسب الافتراضية وسعة نطاق الشبكة. (NIST,2011)

4. المرونة والسرعة: توفير الخدمات السحابية بسرعة ومرونة مما يتيح توسيع وتخفيض نطاق الموارد المستخدمة بسرعة، وبشكل تلقائي في بعض الحالات، أما بالنسبة للمشتركين غالبا ما تتاح الخدمات وتقدم بشكل غير محدود ويمكن شراؤها في أي وقت بكميات غير محدودة (هيئة الاتصالات والفضاء والتقنية ،2022). على سبيل المثال، يتم إضافة خوادم افتراضية مع زيادة الطلب، ومن ثم إغلاقها عند انخفاض الطلب (Mogull et al.,2021).
5. قياس الخدمة: تستخدم الموارد الحاسوبية عن طريق الاستفادة من قدرات القياس عند مستوى محدد من التجريد بما يتناسب مع أنواع الخدمات المقدمة مثل التخزين وسعة النطاق والمعالجة وحسابات المستخدمين النشطة. حيث يمكن حساب معدل استخدام الموارد والتحكم فيها والإبلاغ عنها مما يوفر الشفافية لكل من مقدم الخدمة والمشترك (هيئة الاتصالات والفضاء والتقنية ،2022)

2.4 نماذج الخدمة:

1- البرمجيات كخدمة (SaaS):

تشمل الخدمات المقدمة للمستهلكين استخدام التطبيقات التي تعمل على الأنظمة الأساسية السحابية والبنية التحتية لمقدم الخدمات السحابية. يمكن الوصول إلى التطبيق من مجموعة متنوعة من أجهزة المشتركين من خلال واجهة البرمجيات التي تعتمد على خوادم client thin والمشابهة لمتصفح الويب (على سبيل المثال، البريد الإلكتروني المستند إلى الويب). لا يمكن للمشترك إدارة أو التحكم في البنية التحتية السحابية الأساسية مثل الشبكات، أو الخوادم، أو أنظمة التشغيل، أو التخزين أو حتى وظائف التطبيقات الفردية، باستثناء إعدادات تكوين التطبيقات المحددة الخاصة بالمستخدم. ومن الأمثلة على ذلك: التطبيقات الحكومية، الكمبيوتر الافتراضي، خدمات الإنترنت، نظام إدارة علاقات العملاء CRM، نظام تخطيط موارد المؤسسات ERP، برامج الاتصال: البريد الإلكتروني والرسائل الفورية.

2- المنصات كخدمة (PaaS)

تشمل الخدمات المقدمة للمستهلكين نشر التطبيقات على المنصات السحابية وتطبيقات البنية التحتية التي تم تطويرها من قبل المستهلكين أو شراؤها من مزودي الخدمة السحابية، والتي يتم

تطويرها باستخدام لغات البرمجة والأدوات التي يدعمها مزود الخدمة السحابية، لا يمكن للمشترك إدارة أو التحكم في البنية التحتية السحابية الأساسية، كالشبكات، أو الخوادم، أو أنظمة التشغيل، أو التخزين، ولكن يمكن للمشترك التحكم في التطبيقات المنشورة وربما تكوين بيئة استضافة التطبيقات. ومن الأمثلة على ذلك: تطوير التطبيقات، قواعد البيانات ونظم إدارة قواعد البيانات DBMS، البرامج الوسيطة لـ MQ Web، وWebSphere، وما إلى ذلك، أدوات الاختبار وأدوات المطور، خدمة دليل المستخدم Services Directory.

3- البنية التحتية كخدمة (IaaS)

تشتمل الخدمات المقدمة للمستهلكين المعالجة والشبكات والتخزين وموارد الحوسبة الأساسية الأخرى. يتمتع المشتركون بحرية تحديد البرامج التي سيتم نشرها وتشغيلها، والتي يمكن أن تشمل أنظمة التشغيل والتطبيقات. لا يمكن للمشترك إدارة أو التحكم في البنية التحتية السحابية الأساسية، ولكن يمكن للمشترك التحكم في نظام التشغيل والتخزين والتطبيقات المنشورة، وقد يكون لديه تحكم محدود في بعض مكونات الشبكة مثل أنظمة الأمان. ومن الأمثلة على ذلك: أجهزة الكمبيوتر المركزية، منشآت تكنولوجيا المعلومات (خدمات استضافة)، أجهزة افتراضية (هيئة الاتصالات والفضاء والتقنية، 2022).

2.5 نماذج النشر:

1. منصة الحوسبة السحابية العامة:

يتم توفير البنية التحتية لمنصة الحوسبة السحابية للاستخدام العام من قبل كيانات مختلفة ويمكن امتلاكها وإدارتها وتشغيلها من قبل الشركات، أو المؤسسات الأكاديمية، أو الحكومات، أو جميعها. وتقع داخل مقرات مقدمي الخدمات السحابية، وغالبا ما توفرها جهات عالمية مثل AWSوAzure Microsoft و Cloud Googleبالإضافة إلى جهات محلية مثل شركات تقنية المعلومات وشركات الاتصالات ويضمن موفرو الخدمات السحابية اتفاقيات مستوى الخدمة (SLAs)عندما تكون الخدمات متاحة ويديرون عملية النسخ للبيانات. يوفر هذا النموذج فوريًا آلية التركيب والتشغيل التي يمكنها تسريع الجدول الزمني لنشر حلول جديدة (هيئة الاتصالات والفضاء والتقنية، 2022). توفر السحابة العامة على الشركات التكلفة العالية لشراء وإدارة البنية التحتية للأجهزة والتطبيقات المحلية وصيانتها - ويكون موفر السحابة مسؤولاً عن إدارة النظام وصيانته، وتتميز بنظام أساسي قابل للتطوير اللانهائي تقريبا. حيث تمكن موظفين

الشركة من استخدام نفس التطبيقات في جميع الفروع ومن أي مكتب طالما لديه إمكانية الوصول إلى الإنترنت. أثارت السحابة العامة مخاوف أمنية، ولكن إذا تم تنفيذها بشكل صحيح، يمكن أن تكون السحابات العامة آمنة مثل السحابات الخاصة، وأكثر فعالية إذا استخدم مقدمين الخدمات أساليب الأمان مثل أنظمة كشف التسلل ومنعه (IDPS)(Azure، n.d)

2. منصة الحوسبة السحابية الخاصة:

يتم توفير البنية التحتية لمنصة الحوسبة السحابية بشكل مخصص وتستخدم من قبل مؤسسة واحدة تضم مستخدمين متعددين مثل الإدارات والأقسام ووحدات الأعمال، وقد تكون مملوكة ومدارة ومشغلة من قبل تلك المؤسسة أو طرف ثالث أو كليهما. وقد يكون الموقع المادي لها داخل المقر الرئيسي للمؤسسة أو خارجه. هذا النموذج لا يوفر ضمانات من حيث اتفاقية مستوى الخدمة والتوفر، وتدير المؤسسة عملية نسخ البيانات بنفسها، وغالبًا ما يستغرق تطوير الحلول على السحابة الخاصة وقتًا طويلًا نظرًا لأن جميع عمليات النشر والاختبارات يجب أن تتم داخل المؤسسة (هيئة الاتصالات والفضاء والتقنية، 2022).

3. منصة الحوسبة السحابية المشتركة:

يتم توفير البنية التحتية لمنصة الحوسبة السحابية بشكل مخصص وتستخدم من قبل مجموعة محددة من المستهلكين الذين ينتمون إلى مؤسسات ذات اهتمامات مشتركة ومتوافقة، وقد تكون مملوكة ومدارة ومشغلة من قبل مؤسسة أو أكثر من مؤسسات المجموعة أو طرف ثالث أو كليهما. وقد يكون الموقع المادي لها داخل المقر الرئيسي للمؤسسة أو خارجه. ويضمن مقدم الخدمة في هذا النموذج اتفاقيات من حيث مستوى الخدمة والتوفر، ويدير عملية نسخ البيانات، ويوفر آليات التركيب والتشغيل التي يمكنها تسريع الجدول الزمني لنشر الحلول الجديدة. أحد النماذج الشائعة للقطاع العام لمنصة الحوسبة السحابية المشتركة هي تلك المملوكة للحكومة، غالبًا ما تسمى الحوسبة السحابية الحكومية Gov-Cloud أو Cloud-G. عادةً ما تكون المنصة مملوكة بالكامل للحكومة ويتم تعيينها كمنصة حوسبة سحابية حكومية. ويتم استخدامها حصريًا من قبل الجهات الحكومية، ويمكن أن تتولى جهة حكومية تنفيذ عملياتها، أو طرف ثالث أو كليهما. وعادة ما يكون موقعها المادي داخل الدولة، بغرض حماية البيانات (هيئة الاتصالات والفضاء والتقنية، 2022).

4. منصة الحوسبة السحابية الهجينة:

هي عبارة عن مزيج من اثنين أو أكثر من البنى التحتية السحابية المختلفة (عامة أو خاصة أو مشتركة) التي تحافظ على بنيات متميزة، ولكنها مرتبطة معًا من خلال تقنيات قياسية أو مملوكة ملكية فردية لتمكين النقل المتوازن للبيانات والتطبيقات. على سبيل المثال، يمكن تحويل منصة سحابية خاصة إلى منصة عامة لموازنة الحمل بين منصات الحوسبة السحابية ذات الصلة (هيئة الاتصالات والفضاء والتقنية، 2022).

2.6 فوائد الحوسبة السحابية في التعليم:

2.6.1 الفوائد للطلاب(Al-shqeerat et al., 2017):

1- تقدم الحوسبة السحابية خدمات للطلاب ذوي القدرات الجديدة التي لا تقدمها الطرق التقليدية في الوقت الحاضر، ويمكن للطالب تخزين كل ما يرغب به مثل الجداول الزمنية والملاحظات الصفية والتقارير وأي ملفات أخرى، ونسخ الملفات احتياطيًا على السحابة واستعادتها عند الحاجة.
2- يتمكن الطلاب من الوصول إلى الكتب المدرسية الإلكترونية والمواد التعليمية عالية الجودة. وهذا يحل مشكلة إحجام الطلاب عن شراء الكتب المدرسية بسبب ارتفاع الأسعار، كما تحل المواد التعليمية السحابية مشكلة العديد من المؤسسات التي تستخدم الكتب المدرسية القديمة، مما يتيح للطلاب الوصول إلى أحدث مصادر التعلم.
3- تتيح التطبيقات المخبرية عبر الإنترنت والموارد الإضافية أداء المهام المعملية باستخدام أجهزة شخصية منخفضة التكلفة ومن أي مكان، ولذلك لم يعد الطلاب بحاجة إلى شراء أجهزة عالية التكلفة أو تثبيت برامج خاصة.
4- يتيح الطلاب الوصل إلى النظام بسهولة وفي أي وقت لحضور الدورات وإجراء اختبارات عبر الإنترنت وتحميل الواجبات والمشاريع بأقل وقت وجهد ممكن.
5- التعاون بين الطلاب في نفس الوقت كفريق عمل واحد أو بين عضو هيئة التدريس والطالب.

2.6.2 الفو ائد لأعضاء هيئة التدريس(Al-shqeerat et al., 2017):

1- توفر تقنية الحوسبة السحابية للمعلمين منصة بسيطة ومرنة لإعداد الدورات التعليمية والعروض التقديمية والمقالات والمؤتمرات وغيرها
2- التغلب على نقص المهارات لدى بعض أعضاء هيئة التدريس من خلال عقد ورش عمل عن بعد لتبادل الخبرات.
3- إتاحة الفرصة لأعضاء هيئة التدريس للعمل من المنزل واستخدام أجهزتهم الخاصة لتحضير الاختبارات عبر الإنترنت وإنجاز المهام.
4- تبادل الموارد التعليمية وتجنب تكرر الجهود والتعاون مع مدربين أخرين
5- التغذية الراجعة من خلال الحصول على آراء الطلاب حول العملية التعليمية.
6- تمكن الباحثين من المناقشة والوصول إلى مصادر الحوسبة العالمية وقدرات تخزين كافية.

2.7 استخدامات الحوسبة السحابية في التعليم (mary and Rose,2019)

1- الممارسات التعليمية: وهي أبرز الاستخدامات الأساسية وتعني الدمج بين الفصول الحضورية في مقر الجامعة والفصول الدراسية عبر الإنترنت والتعليم عن بعد.
2- انخفاض النفقات: تقوم مؤسسات التعليم العالي بالدفع مقابل حزم برامج لاستخدامها عبر الإنترنت من خلال مواقع متنوعة بدلًا من شراء تراخيص فردية لأجهزة قليلة وتكاليف متعددة
3- زيادة في العمل التعاوني: يتاح للطلاب وأعضاء هيئة التدريس استرداد المعلومات من أنظمتهم الخاصة دون الحاجة إلى برامج أو موارد أو أجهزة. وتعزز مزامنة الخدمات السحابية التعاون وتوزيع المهام، وزيادة جودة المعلومات والعملية التعليمية.
4- النسخ الاحتياطي للمعلومات: غالبا ما يعمل مقدمين الخدمات السحابية على تخزين نسخ متعددة من البيانات المحفوظة في العديد من الخوادم. لذلك يضمن هذا التكرار حفظ البيانات من الضياع والوصول الفوري إلى الملفات مع ضمانات النسخ الاحتياطي.

5- الدعم في الإدارة المالية وإدارة الموارد البشرية: تتيح الجامعات لأعضاء هيئة التدريس إدارة المعلومات المالية الخاصة بهم عن طريق الإنترنت. مما ينتج عنه تحسين فعالية الجامعة ورفع كفاءة الإدارة وتعزيز إدارة المعلومات الخاصة بالموظفين في الوقت المناسب لجميع الأطراف ذات الصلة.

6- تعزيز الاعتماد الجامعي: إرسال التقييمات الحساسة والسرية مثل امتحانات اختبارات تحديد المستوى والقبول ودرجات الطلاب واستطلاعات الأداء الأكاديمي لعضو هيئة التدريس فوراً إلى المستخدمين المصرح لهم.

7- تعزيز مرونة المعلم: تتيح الحوسبة السحابية لأعضاء هيئة التدريس حرية العمل خارج الجامعة ومراجعة المناهج وإدارة الفصول الدراسية والدورات وإرسال الدرجات بكل سهولة عبر الإنترنت، وزيادة الإنتاجية في أداء المهام بما يتناسب مع أوقاتهم.

3. الأمن السيبراني

3.1 تمهيد:

إن سرعة التطورات التكنولوجية والتقدم التقني المبهر يفتح أبوابًا عديدة للابتكار وتسهيل الحياة اليومية، ولكن يفتح أيضًا أبوابًا أمام الهجمات الإلكترونية والتهديدات السيبرانية. لذا تتناول هذه الجزئية تعريف الأمن السيبراني، وتعريف الأمن السحابي، وما أهمية أمن الحوسبة السحابية، وماهي مميزات وفوائد استخدام سحابة أمنة، وكيف يتم توزيع المسؤوليات الأمنية داخل الحوسبة السحابية، وما واجبات مقدم الخدمة وماهي حقوق المشتركين، بالإضافة للمخاطر والتهديدات الأمنية وأبرز القضايا الأمنية، ثم تعرض كيفية تحديد مستوى الأمن المطلوب وماهي معايير الحوسبة السحابية وضوابطها وختامًا تعرض ضوابط الأمن السيبراني للحوسبة السحابية في المملكة العربية السعودية.

3.2 مفهوم الامن السيبراني:

حسب ما نص عليه تنظيم الهيئة الوطنية للأمن السيبراني الصادر بالأمر الملكي رقم (٦٨٠١) وتاريخ (١١/٢/١٤٣٩هـ)، فإن الأمن السيبراني هو"حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات. وما تقدمه من خدمات وما تحتويه من بيانات من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير

مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات، والأمن الرقمي، ونحو ذلك" (NCA,2020). وهو مجموعة من الوسائل التنظيمية والتقنية والإدارية والتشغيلية الرامية لمنع الاستخدام غير المصرح به والغير القانوني وسوء استخدام واسترجاع المعلومات الإلكترونية وأنظمة المعلومات والاتصالات، ومن أهداف الأمن السيبراني ضمان توافر واستمرارية عمل المعلومات وتعزيز حماية وسرية وخصوصية البيانات الخاصة بالمؤسسات الوطنية والأفراد (الجنفاوي، 2021)

3.3 مفهوم أمن الحوسبة السحابية:

هو مجموعة واسعة من السياسات والتقنيات والضوابط لحماية البيانات المنتشرة والتطبيقات والبنية التحتية المرتبطة بها والمكونة للحوسبة السحابية أو بصورة أخرى هي تكامل واندماج أغلب مجالات أمن المعلومات مثل أمن الشبكات وأمن الأنظمة وأمن التطبيقات وغيرها في مجال جديد يعتمد كل جزء فيه على الجزء الآخر في تناغم تام (علي،2020).

3.4 أهمية أمان الحوسبة السحابية:

زاد انتقال المؤسسات الحديثة إلى البيئات المعتمدة على الحوسبة السحابية ونماذجها IaaS أو Paas أو SaaS. يمكن أن تنشأ في تلك الطبيعة الديناميكية العديد من التحديات الأمنية. ولكن مع ذلك تمنح هذه النماذج المؤسسات القدرة على رفع الكفاءة والأداء وإنجاز العديد من المهام التي تستغرق وقتًا طويلًا. لذا مع استمرار المؤسسات في الترحيل إلى السحابة، أصبح من الضروري فهم متطلبات الأمان للحفاظ على البيانات آمنة. يلتزم معظم مقدمين الخدمات السحابية بأفضل الممارسات الأمنية ويتخذون تدابير استباقية لحماية وسلامة خوادمهم. ومع ذلك، تحتاج المؤسسات إلى أخذ الاعتبارات الخاصة بها عند حماية البيانات والتطبيقات وجميع ما يتعلق بالحوسبة السحابية. مع استمرار تطور البيئة الرقمية، أصبحت التهديدات الأمنية أكثر خطورة. تستهدف هذه التهديدات على وجه التحديد مقدمين الحوسبة السحابية بسبب افتقار المؤسسات بشكل عام إلى الرؤية فيما يتعلق بالوصول إلى البيانات وحركتها. بدون اتخاذ خطوات استباقية لتحسين أمان السحابة، قد تواجه المؤسسات مخاطر كبيرة تتعلق بالحوكمة والامتثال عند إدارتها لمعلومات العملاء، لذلك يجب أن يكون الأمان السحابي موضوعًا مهمًا للمناقشة مهما كان حجم المؤسسة لضرورة حماية البيانات والقدرة على الدفاع ضد الهجمات

السيبرانية والحفاظ على استمرارية الأعمال. فإن الاعتماد الناجح القائم على السحابة يعتمد على تدابير مضادة وقوية للدفاع ضد الهجمات السيبرانية الحديثة. سواء كانت المؤسسة تعمل في بيئة سحابية خاصة أو عامة أو مختلطة، فإن الحلول الامنية السحابية واعتماد أفضل الممارسات ضروري لضمان استمرارية الأعمال (IBM, n.d).

3.5 مزايا الحوسبة الأمنة في البيئة التعليمية :

يعد تطبيق التدابير الأمنية وأفضل الممارسات مهمًا جدًا في التعليم كونه يؤثر على استمرارية أمن بيانات الطلاب وأعضاء هيئة التدريس وجميع العاملين لمنع سرقة بياناتهم وتزويرها وغير ذلك. لذلك فإن الحفاظ على أمان الحوسبة السحابية مهم جدًا، ونذكر فيما يلي مزايا استخدام الحوسبة السحابية الأمنية، والتي تتمثل في الآتي(Liando et al.,2022):

1- مرونة عالية وسعة تخزين غير محدودة، يمكن استخدامها حسب الحاجة.

2- فعالية من حيث التكلفة و الوقت.

3- الأمان الكامل، وقدرات تشفير خاصة من خلالها تتم حماية جميع أجزاء البيانات بواسطة طبقات متعددة من الأمان. ولذا يحافظ أمان الحوسبة السحابية على سرية البيانات حتى في حال استخدام وسائط التخزين اليدوية.

4- نسخ احتياطي للبيانات، وبهذه الطريقة يتم حفظ البيانات المخزنة دون حدوث أي مشكلة ولن تفقد البيانات نظرًا لوجود نسخ أخرى يمكن استخدامها.

3.6 فوائد أمن الحوسبة السحابية (Liando et al.,2022)**:**

1- الدفاع ضد هجمات DDoS:

هو هجوم إلكتروني يتضمن إغراق الإنترنت بحركة مرور وهمية يتم إنشاؤها من خلال خادم أو نظام أو شبكة. وللدفاع ضد تلك الهجمات، توفر الخدمات السحابية نطاقًا ترددًا عمقًا وضخم، ويمكن لإمكانيات أمان السحابة إعادة توجيه حركة مرور الإنترنت، وتوفير النسخ الاحتياطي.

2- مستوً عالٍ من التوافر:

القدرة على العمل لمدة تصل إلى 24 ساعة، والمراقبة المستمرة وإعداد التقارير. تعد هذه الفائدة في غاية الأهمية لضمان توفر موقع الجامعة وتطبيقاتها على مدار 24 ساعة يوميًا حسب حاجة المستخدمين.

3. سرعة النشر:

عند استخدام الخدمات السحابية يتم تنشيطها بمجرد امتلاكها ويتم التنويه بما يجب حمايته لذا الأمان السحابي أفضل من الأمان التقليدي الذي يتطلب تركيب معدات الشبكة وأدوات الأمان وقواعد وسياسات معقدة للتصميم والتنفيذ والاختبار.

4. استخدام الذكاء الاصطناعي:

وتتمثل مهمة الذكاء الاصطناعي في مراقبة الأحداث والإبلاغ عن الأنشطة الغير طبيعية، كما يعد استخدام الذكاء الاصطناعي بحد ذاته أسرع مقارنة بالخدمات التقليدية، التي تتطلب الكثير من الأشياء مثل التصحيحات المنتظمة وتحديثات البرامج الثابتة وغيرها. بينما تتم جميع التحديثات على الفور في الحوسبة السحابية. مما يحمي من انقطاع الخدمة لمليارات الحالات التشغيلية.

5. تقليل التكاليف:

تقليل تكاليف التشغيل بالإضافة إلى سهولة الوصول والأمان.

3.7 نطاق ومسؤوليات أمان السحابة:

- البرمجيات كخدمة (saas): تقع مسؤولية الأمان على مقدم الخدمات السحابية بالكامل تقريبًا ويمكن لمستخدم السحابة فقط الوصول إلى استخدامات التطبيق وإدارته، ولن يتمكن المستخدم من تغيير كيفية عمل التطبيق. على سبيل المثال، يكون مقدم SaaS مسؤولاً عن أمان المحيط والتسجيل والتدقيق والمراقبة وأمن التطبيق، بينما يكون المستخدم قادرًا فقط على إدارة التفويضات والاستحقاقات.

- المنصات كخدمة (paas): تقع مسؤولية الأمان للنظام الأساسي على مقدم الخدمات السحابية، ويكون المستخدم مسؤولاً عن كل ما يفعله على النظام الأساسي، بما في ذلك كيفية تكوين أي ميزات أمان يتم توفيرها. على سبيل المثال، عند استخدام قاعدة البيانات كخدمة، يدير مقدم الخدمات السحابية الأمان الأساسي والتكوين الأساسي والتصحيح، بينما يكون المستخدم السحابي مسؤولًا عن كل شيء آخر، بما في ذلك ميزات أمان قاعدة البيانات التي يجب استخدامها وإدارة الحساب وحتى طرق المصادقة.

- البنية التحتية كخدمة(Iaas): تمامًا مثل PaaS تقع مسؤولية الأمان الأساسي على مقدم الخدمات السحابية، ويكون مستخدم السحابة مسؤولًا عن كل شيء يتم بناءه فوق البنية التحتية. وهذا يضع مسؤولية أكبر على عاتق المستخدم. على سبيل المثال، قد يراقب مقدم IaaS ما يحيط به من الهجمات، ولكن المشترك هو المسؤول الوحيد عن كيفية تعريفه لأمن الشبكة الافتراضية وتطبيقه بناءً على الأدوات المتاحة داخل الخدمة(Mogull et al.,2021).

ويوضح الشكل التالي مسؤوليات الأمان داخل الحوسبة السحابية:

الشكل رقم (١) *يمثل مسؤوليات الأمان داخل الحوسبة السحابية.*

يرتبط نموذج المسؤولية المشتركة بتوصيتين:

1- يجب أن يوثق مقدمين الخدمات السحابية ضوابط الأمان الداخلية بوضوح حتى يتمكن المشتركين في السحابة من اتخاذ قرارات مستنيرة، كما يجب على مقدم الخدمة الالتزام بتصميم وتنفيذ هذه الضوابط بشكل صحيح.
2- بالنسبة لأي مشروع سحابي معين، يجب على المشترك السحابي إنشاء مصفوفة مسؤولية لتوثيق من يقوم بتنفيذ الضوابط وكيف يتم تنفيذها، كما يجب أن يتوافق مع أي معايير امتثال ضرورية.

3.8 واجبات مقدم خدمة الحوسبة السحابية:

يجب على مقدمين خدمات الحوسبة السحابية تقديم العديد من الواجبات والمسؤوليات للمشتركين، ومن أهمها (علي، 2020):

1. حماية البيانات: ويجب حماية البيانات وفصلها ومنع اختلاطها بين المستخدمين. وأن يتم تخزين البيانات بشكل آمن، ويجب أن تكون البيانات قابلة للنقل بشكل آمن من مكان إلى آخر، كما يجب أيضًا تشفير البيانات وفقًا لأفضل تقنيات التشفير.
2. الفصل بين الواجبات: يجب أن يكون هناك فصل صحيح وكامل للواجبات والوظائف (مثل الرقابة والمراقبة والتدقيق) سواء مع مقدم الخدمة أو المستخدم أو طرف ثالث متعاقد مع المزود أو المستخدم الذي لديه أذونات مهمة لأداء مهامه، ويجب الفصل بينهم وتنفيذ أنظمة متكاملة لضمان عدم تسرب البيانات.
3. إدارة الهوية: توفير إدارة الهوية والتحكم في الوصول إلى مصادر المعلومات وموارد الخدمة حسب احتياجات المستخدم، على أن تقبل هذه الأنظمة التكامل ويمكن دمجها وتطويرها مع نظام إدارة هوية المستخدم سواء التقليدي أو المقدم من مزود خدمة آخر (يعرف بعمليات الاتحاد).
4. الأمن المادي: يجب على مقدم الخدمة التأكد من أن المعدات والأجهزة آمنة بما فيه الكفاية وانعدام إمكانية الوصول إليها وأن تكون مقيدة بأنظمة الوصول المتكاملة والموثقة التي يمكن الرجوع إليها إذا لزم الأمر.
5. التوفر: يضمن مزود الخدمة حصول المستخدم على توفر الخدمة، أو بمعنى آخر القدرة على الوصول إلى الأنظمة والبيانات والتطبيقات الخاصة بهم بشكل منتظم ودون انقطاع طوال فترة الخدمة.
6. أمن التطبيقات والأنظمة: يجب على مقدم الخدمة التأكد من أمن التطبيقات والأنظمة المقدمة ضمن الخدمات عن طريق تنفيذ الاختبار وتطبيق الإجراءات والسياسات وأنظمة الحماية متعددة الطبقات.
7. السرية: يجب على مقدم الخدمة ضمان السرية التامة لجميع أنواع البيانات للمستخدم، ولا يسمح بالوصول إلى هذه البيانات من قبل أي شخص آخر غير الأشخاص المصرح لهم من قبل المستخدم.

3.9 حقوق مشتركو خدمة الحوسبة السحابية :

تلخص Gartner حقوق المستخدم ومسؤولياته على النحو التالي (علي، 2020):

1. حق الحفاظ على ملكية البيانات الخاصة واستخدامها والتحكم فيها
2. الحق في الحصول على اتفاقية مستوى الخدمة والتي تتضمن الالتزامات المادية والتقنية والإجراءات العامة.
3. حق إعلام المستخدم واتخاذ خيارات حرة فيما يتعلق بالتعديلات التي تؤثر على عمليات المستخدم.
4. الحق في معرفة متطلبات الخدمة مسبقًا أو القيود التقنية.
5. الحق في المعرفة المسبقة بالمتطلبات القانونية للدولة التي يعمل بها مقدم الخدمة.
6. الحق في معرفة سياسات العمليات الأمنية و الإجراءات التي يعتمدها مقدم الخدمة

3.10 المخاطر الأمنية المتعلقة بالحوسبة السحابية:

1. المخاطر الأمنية التي يواجهها مقدمين الخدمات السحابية، مثل تلك المرتبطة بخدمات البنية التحتية كخدمة (Iaas) أو البرمجيات كخدمة (SaaS) أو خدمات المنصة (Paas).
2. المخاطر التي يواجهها المشتركين (وهم العملاء الذين يختارون استضافة جزء أو كل تطبيقاتهم أو بياناتهم الخاصة على السحابة عند استخدام الخدمات السحابية).

وعلى الرغم من أن أمن الحوسبة السحابية يعد مسؤولية مشتركة بين مقدم الخدمة والمستخدم، إلا أنه يجب على مقدمي الخدمة التأكد من أن البنية التحتية التكنولوجية الخاصة بهم في مكان آمن وأن بيانات وتطبيقات عملائهم محمية من أي تهديدات إلكترونية. ومن ناحية أخرى، يجب على المشتركين أن يفهموا بعناية حقوقهم والتزاماتهم ومسؤولياتهم وأن يتخذوا الخطوات اللازمة لحماية الوصول إلى تطبيقاتهم وبياناتهم من خلال الممارسات الأمنية (آل حيان، 2019).

3.11 التهديدات الأمنية الرئيسية التي تتعرض لها الحوسبة السحابية (بخات واخرون،2020/2022):

1. اختراق البيانات (Data Breach): حدث أمني سيبراني يتم عندما يصل شخص غير مصرح له إلى معلومات حساسة، أو سرية، أو محمية لعرضها، أو استخدامها، أو سرقتها.

2. تحديث الاعدادات السيئة للتحكم في الوصول (Misconfiguration and Inadequate Change Control): أخطاء التكوين عندما لا يتم إعداد أصول الحوسبة بشكل صحيح، فإنها غالبًا ما تكون عرضة للأنشطة الضارة والقرصنة
3. انعدام هيكلية واستراتيجية أمن الحوسبة السحابية (Lack of Cloud Security Architecture and Strategy): تطبيق بنية الأمن السيبراني المناسبة للبيئات السحابية (على سبيل المثال، الوعي بتقنيات المحاكاة الافتراضية والفهم الشامل لأفضل ممارسات أمان الحوسبة السحابية)
4. الهوية ومؤهلات الوصول وإدارة المفاتيح الغير كافية (Insufficient Identity, Credential, Access and Key Management): تشتمل أنظمة إدارة الهوية وبيانات الاعتماد والوصول على أدوات وسياسات تتيح للمؤسسات بإدارة ومراقبة وتأمين الوصول إلى الموارد القيمة (على سبيل المثال: على مستوى إدارة السحابة).
5. اختراق الحساب (Account Hijacking): يعد اختراق الحساب بمثابة تهديد يسمح للمتسللين بالوصول إلى الحسابات التي تحتوي على مكونات حساسة للغاية وإساءة استخدامها
6. التهديدات الداخلية (Insider Threat): يعرّف فريق الاستجابة لحوادث الكمبيوتر (CERT) التهديد الداخلي بأنه فرد لديه أذونات التهديد الداخلي والذي قد يصل عن قصد أو عن غير قصد إلى بيانات المؤسسة ويستخدم أذوناته بشكل غير قانوني للوصول إلى الموارد، مما قد يكون له تأثير سلبي على المؤسسة.
7. واجهات برمجة التطبيقات غير الآمنة (Insecure Interfaces and APIs): يوفر مقدمين الحوسبة السحابية مجموعة من واجهات مستخدم البرامج (UIs) وواجهات برمجة التطبيقات (API) التي تتيح للمشتركين إدارة الخدمات السحابية والتفاعل معها. يعتمد أمان وتوافر خدمات الحوسبة السحابية العامة على أمان واجهة برمجة التطبيق هذه
8. ضعف مستوى التحكم (Weak Control Plane): وهذا يعني أن الشخص المسؤول لا يتمتع بالتحكم الكامل في منطق وأمان وإثبات بنية البيانات.
9. فشل البنية الأساسية وبنية التطبيق (Megastructure and Applistructure Failures): ويشير إلى الفشل أو الفجوة التي يمكن أن تحدث بين البنية الأساسية وبنية التطبيق،

وغالبًا ما تنتج مثل هذه المشكلات عن ضعف التنفيذ لواجهة برمجة التطبيقات (API) والتي إما أن تكون غير آمنة أو تعرض الكثير من المعلومات عن العملاء والخدمات المركزية.

10. محدودية رؤية الاستخدام السحابي (Limited Cloud Usage Visibility): تشير الرؤية المحدودة لاستخدام السحابة إلى عدم قدرة المؤسسة على تصور وتحليل ما إذا كان استخدام الخدمات السحابية آمنًا أم ضارًا.
11. إساءة استخدام الخدمات السحابية (Abuse and Nefarious Cloud Services): يمكن للجهات الخبيثة الاستفادة من موارد الحوسبة السحابية لاستهداف الشركات أو المستخدمين أو مقدمي الخدمات السحابية الآخرين، على سبيل المثال استخدام عمليات استخراج البيانات.

3.12 تهديدات أمان السحابة الحديثة والتنبؤات واستراتيجيات التخفيف:

في ظل التقدم التقني من المحتمل أن تصبح الحوسبة السحابية عالمية ونتيجة لذلك يأتي زيادة خطر التهديدات السيبرانية التي قد تعرض الأنظمة والبيانات والشبكات الحساسة للمخاطر. فيما يلي تنبؤات لأهم التهديدات الأمنية السحابية التي يجب الحذر منها، بالإضافة إلى بعض إستراتيجيات التخفيف التي يمكن استخدامها لحماية البيئة السحابية(Chaudhary,2023):

3.12.1 اختراق البيانات السحابية:

أظهر تقرير أجرته شركتي Statista Incorporated مع Surfshark أنه في الربع الثالث من عام 2022، تم الكشف عن 15 مليون سجل بيانات في جميع أنحاء العالم بسبب اختراق البيانات، بزيادة قدرها 37٪ مقارنة بالربع السابق. وفي الربع الأخير من عام 2022 تم اكتشاف قدراً كبيراً من سجلات البيانات المكشوفة قرابة 125 مليون مجموعة بيانات. لذلك فأن خروقات البيانات تعد من أهم التهديدات التي تواجه الحوسبة السحابية حاليًا. من المتوقع أن يستمر خلال عام 2023 استخدام السحابة كوسيلة للوصول إلى المعلومات الحساسة. يمكن أن يشمل ذلك بيانات العملاء وسجلاتهم المالية وذكاء الأعمال الخاص بهم.

- سبب الفشل الأمني: فشل التشفير، فشل التحكم في الوصول، وفشل التسجيل
- استراتيجية التخفيف: تنفيذ آليات قوية لتشفير البيانات، إدارة التحكم في الوصول، مراقبة التدابير ومراجعتها بشكل مستمر

3.12.2 التهيئة الخاطئة للسحابة:

في فبراير 2022، كشف خطأ في التكوين في Google Cloud Storage عن المعلومات الشخصية لأكثر من 23 مليون مستخدم لمتاجر التجزئة الرياضية. في مارس 2022، كشفت حاوية تخزين تم تكوينها بشكل خاطئ في Microsoft Azure عن البيانات المالية ومعلومات التعريف الشخصية (PII) لأكثر من 5 ملايين مستخدم للتطبيقات الصحية. في أبريل 2022، أدى خطأ في التكوين في Amazon Web Services (AWS) إلى تسرب 533 مليون سجل مستخدم لفيسبوك، وفي مايو 2022، كشف خلل في التكوين السحابي لماكدونالدز عن معلومات الموظفين، بما في ذلك أرقام الضمان الاجتماعي وتفاصيل الحساب المصرفي قرابة 12000 موظف في جميع أنحاء أمريكا الشمالية. ونتيجة لذلك، فإن جزءًا كبيرًا من حوادث الأمان السحابية يكون سببها التكوينات الخاطئة، والأخطاء البسيطة مثل الفشل في تكوين عناصر التحكم في الوصول بشكل صحيح أو ترك كلمات المرور الافتراضية في مكانها يمكن أن تجعل الموارد السحابية عرضة للهجوم، ونظرًا لأن الأنظمة السحابية أصبحت أكثر تعقيدًا، فمن المتوقع أن يصبح التكوين الخاطئ تحديًا أكبر في عام 2023.

- سبب الفشل الأمني: تهيئة الأمان الخاطئة، تصميم غير آمن ضمن أخطاء التكوين
- استراتيجية التخفيف: اعتماد نهج استباقي لمراجعات التكوين المنتظمة، يجب إجراء فحوصات الثغرات الأمنية ومراجعات التكوين بانتظام في فترة زمنية محددة

3.12.3 هجمات Cloud Ransomware:

كشف تقرير Statista أن 236.1 مليون هجمة فدية حدثت على مستوى العالم في النصف الأول من عام 2022. زادت هجمات برامج الفدية العالمية بنسبة 18% بين الربعين الأول والثاني من عام 2022. أثرت برامج الفدية وحدها على 71% من الشركات في جميع أنحاء العالم في عام 2022. ونتيجة لذلك، استهدفت هجمات برامج الفدية البيئات السحابية على مدى السنوات القليلة الماضية. ومن المتوقع أن تستمر هذه الهجمات في التزايد خلال عام 2023، حيث يستفيد المتسللون من تكتيكات جديدة لاختراق البيانات المستندة إلى السحابة وتشفيرها.

- سبب الفشل الأمني: عدم كفاية التسجيل والمراقبة، مشاكل التخلص من البيانات وتخزين البيانات غير الآمن
- استراتيجية التخفيف: خطة استجابة شاملة للحوادث وCSOC، تنفيذ إستراتيجية نسخ احتياطي قوية وخطوات لاستعادة البيانات بالاختبار المناسب.

3.12.4 البرمجيات الخبيثة والسحابة البوت نت:

وفقًا لشركة CrowdStrike Intelligence، زاد استغلال السحابة في عام 2022 بنسبة 95%، ومع تضاعف عدد الجهات التي تنتهك أمن السحابة، شكلت شبكات الروبوت والبرامج الضارة تهديدًا مستمرًا لأمن السحابة. ومن المتوقع أن تستمر هذه التهديدات في التزايد خلال عام 2023، حيث يستخدم المتسللون أساليب أكثر تطوراً مثل البرامج الضارة الخالية من الملفات لتجنب اكتشافها.

- سبب الفشل الأمني: المكونات المعرضة للخطر والتي عفا عليها الزمن
- استراتيجية التخفيف: تطبيق أدوات متقدمة للكشف عن التهديدات والتخفيف من حدتها، وتقنيات مثل التحليل التفاعلي والتعلم الآلي لتحديد التهديدات ومنعها في الوقت المناسب

3.12.5 التهديدات الداخلية:

في مايو 2022، سرق باحث في شركة Yahoo، كيان سانغ، معلومات سرية عن منتج AdLearn الخاص بشركة Yahoo. وتضمنت البيانات المسربة 570 ألف ملف تحتوي على المعلومات الهندسية الخاصة بالواجهة الخلفية وكود المصدر والخوارزميات السرية وغيرها من الملكية الفكرية. وفي أبريل 2023 أعلن المدعي العام الأمريكي ميريك جارلاند أن مكتب التحقيقات الفيدرالي اعتقل عضوًا في الحرس الوطني الجوي بولاية ماساتشوستس بتهمة تسريب وثائق سرية للغاية ونشرها على الإنترنت. ولذلك، تظل التهديدات الداخلية مصدر قلق لأمن السحابة في عام 2023.

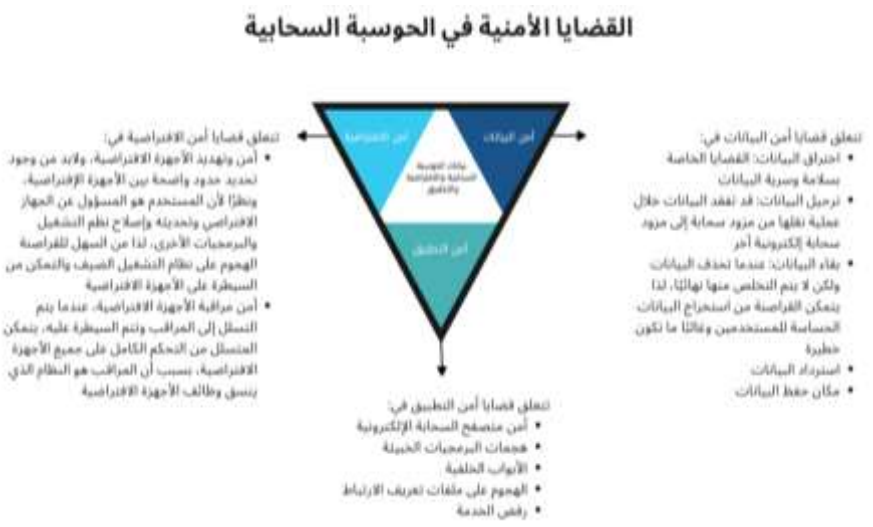
- سبب الفشل الأمني: التحكم بالوصول المكسور، المصادقة معطلة، إلغاء التسلسل غير الآمن
- استراتيجية التخفيف: تطبيق ضوابط وصول صارمة، الحد من الامتيازات على أساس وظائف الوظيفة، مراقبة نشاط المستخدم عبر الأنظمة السحابية، يمكن أن يساعد إجراء برامج تدريب وتوعية منتظمة للموظفين على تحديد الأنشطة المشبوهة والإبلاغ عنها.

3.13 القضايا الأمنية في الحوسبة السحابية(أحمد،2018):

1- قضايا نماذج الحوسبة السحابية:

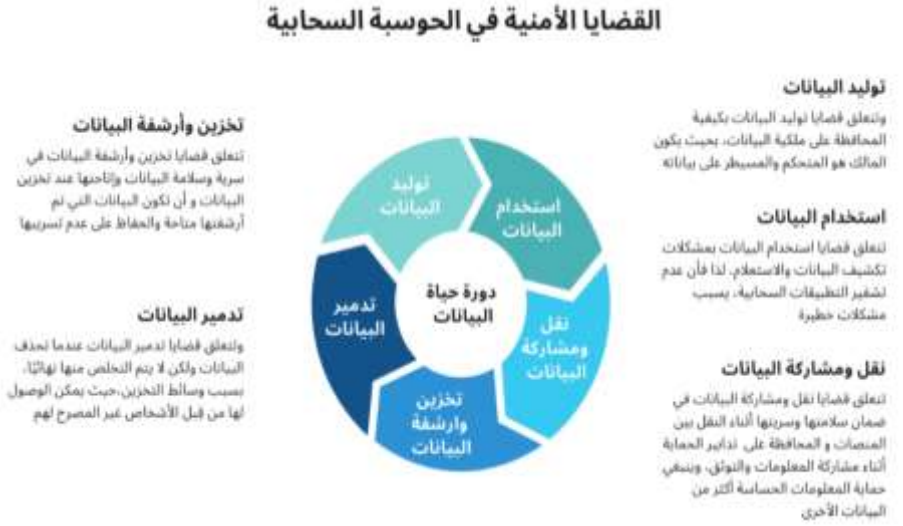
الشكل رقم (٢) *قضايا نماذج الحوسبة السحابية*

2- قضايا بيانات الحوسبة السحابية والافتراضية والتطبيق:



الشكل رقم (٣) *قضايا بيانات الحوسبة السحابية والافتراضية والتطبيق*

3- قضايا دورة حياة البيانات :



الشكل رقم (٤) *قضايا دورة حياة البيانات.*

3.14 آلية تحديد مستوى الأمن المطلوب:

يعتمد تحديد مستوى الأمن المطلوب للخدمات السحابية على عدة عوامل، أبرزها (آل حيان، 2019):

1- أهمية المؤسسة المستهدفة، ويحدد هذا العامل طبيعة القواعد واللوائح والتشريعات المطبقة على المؤسسة. على سبيل المثال، عند تصميم الخدمات السحابية للقطاعات الحكومية أو الرعاية الصحية أو المصرفية، يجب أن يكون مستوى الأمان مرتفعًا. وعندما يتم إنشاء خدمة سحابية للألعاب عبر الإنترنت أو الشبكات الاجتماعية، قد يكون مستوى الأمان معتدلاً.

2- حساسية البيانات: يؤثر مستوى حساسية البيانات على طبيعة المتطلبات الأمنية اللازمة لحماية البيانات. على سبيل المثال، عندما تتعلق البيانات بالمدفوعات المصرفية، أو المعاملات الحكومية، أو المطالبات القضائية، أو الطبية، يجب تطبيق معايير وضوابط صارمة. غالبا ما تفرض ضوابط الأمان هذه تشفيراً للبيانات على

قواعد البيانات حيث تم تخزينها وتستخدم إجراءات أمان عالية المستوى للتحكم في الوصول الإلكتروني عبر قنوات الشبكة وللتحكم في الدخول والخروج إلى مركز البيانات حيث يتم تخزين البيانات. ومن ناحية أخرى، فإن الضوابط الأمنية هذه ليست صارمة عندما يتعلق الأمر ببيانات وسائل التواصل الاجتماعي في شكل نصوص، وصور، ومقاطع فيديو، وتغريدات. والسبب هو أن هذه البيانات عامة بطبيعتها لأن مستخدمي شبكات التواصل الاجتماعي سبق لهم القبول والموافقة على شروط الخدمة، والتي تتضمن أن تكون البيانات عامة وليست خاصة، لذلك يتم تخزين البيانات في قاعدة البيانات ولن يتم تشفير المواقع فيها.

3- مستوى تحمل المخاطر. وتكمن أهمية هذا العامل من أنه يرتبط عكسيًا بالسمعة العامة للمؤسسة ورضا المستفيدين منها. على سبيل المثال، تنظر بعض المؤسسات إلى الخروقات الأمنية على أنها مزعجة لدرجة أنها قد تضر بعلاقاتها العامة مع الآخرين، وخاصة المستفيد من تعرض خدماتها للاختراق. ولتجنب مثل هذه العواقب، تسعى بعض المؤسسات إلى تنفيذ ضوابط أمنية صارمة. فمن ناحية قد تكون هناك علاقة قوية بين مستوى تحمل المخاطر وحجم المنظمة المستفيدة وأصولها الحديثة أو القديمة. تعطي المؤسسات الكبرى الأولوية لتطبيق الضوابط الأمنية على سرعة الوصول إلى العملاء؛ للحفاظ على سمعتها لدى العملاء وأصحاب المصلحة. ومن ناحية أخرى، زادت المؤسسات الصغيرة الجديدة أيضًا من القدرة على تحمل المخاطر، حيث إن الوصول إلى العملاء بسرعة وبتكلفة أقل أكثر أهمية من إنفاق مبالغ كبيرة على الأمن.

4- توقعات المستفيدين: غالبًا ما تحدد تصورات المستفيد المستقبلي للسحابة مستوى وعمق المتطلبات الأمنية للخدمات السحابية. ويتأثر هذا المنظور بعدة عوامل، أبرزها: الخوف من اختراق البيانات، والتكاليف المالية، والمرونة والأدوات التي توفرها السحابة. يجب على مقدمي الخدمات الاستعداد مبكرًا لتحديد وفهم توقعات المستفيدين بشكل كامل وتقديم مجموعة متنوعة من الحلول السحابية التي تناسب طبيعة احتياجات المستفيدين. على سبيل المثال، قد تخطط إحدى المؤسسات لوضع

تطبيقاتها وبياناتها بالكامل على سحابة عامة، حيث تتم مشاركة موارد السحابة بين عدة مستلمين. قد تواجه المؤسسة أحد عملاء السحابة المهمين الذين يرفضون وضع بياناتهم على السحابة العامة. وفي هذه الحالة، يمكن للمؤسسات تنفيذ حلول بديلة تتمثل في السحابة الهجينة لتحقيق رغبات العملاء، وبالتالي زيادة العوائد المالية من خلال الاحتفاظ بالعملاء.

5- مستوى نضج الخدمات السحابية: عند بناء خدمة سحابية جديدة، ينشأ نوعان من المتطلبات: متطلبات العمل ومتطلبات الجودة. تحقق متطلبات العمل أتمتة العمليات، بينما تحقق متطلبات الجودة سمات مثل الأمان والتوفر وقابلية التوسع وقابلية الانكماش. الوضع المثالي في تطوير الخدمات السحابية هو أن هذين النوعين من المتطلبات يحتاجان إلى الموازنة لإنتاج منتج برمجي فعال، ولكن من الناحية العملية، ينصب التركيز عادة على تنفيذ متطلبات العمل في المراحل الأولى من التطوير قبل النظر في ميزات أخرى مثل الأمان. يزداد بمرور الوقت ومع إضافة المزيد من مستخدمي الخدمة. وتتجلى هذه الآلية في نضج الخدمات السحابية في معظم تطبيقات الهاتف المحمول، والتي يتم تحديثها بإصدارات متتالية مع مرور الوقت مع إضافة ميزات جديدة.

6- تناقل البيانات يتم تحديد متطلبات الأمان لكل نوع من البيانات حسب المسار الشبكي المتوقع لها، لذا فأن الخدمات السحابية التي تستخدم ضمن نطاق شبكي ضيق مثل تلك المستخدمة داخل حدود المؤسسة، تتطلب مستوى أمني اقل من الخدمات السحابية التي تنقل بها البيانات على مستوى جغرافي واسع مثل البيانات التي يتم نقلها بين دول مختلفة. ولابد من الإشارة لهذه النقطة في اتفاقية مستوى الخدمة (SLA) بين مقدم الخدمة والمشترك.

وبعد تحديد وتقييم كل عامل وتحديد المستوى الأمني المطلوب للخدمات السحابية، يسهل تحديد المتطلبات الأمنية لكل خدمة مستهدفة. ومن ثم عمليات تقييم الحلول الأمنية لتحقيق المتطلبات الأمنية. وغالبا ما تتاح طريقتان أمام المستفيد لتنفيذ الحلول الأمنية ١- التطوير الداخلي ٢- الاستفادة من الحلول الأمنية المجهزة على السحابة على شكل خدمات نموذج

البرمجيات كخدمة (SaaS). وتبعًا لتجدد والتطوير المستمر في مجال أمن المعلومات بشكل متسارع، وتجدد وتغير التهديدات الأمنية في مده زمنية قصيرة يصعب مجاراتها بتحديث ومتابعة الحلول الأمنية داخليًا؛ لذا ترجح أفضل الممارسات الاستفادة من الحلول الأمنية الجاهزة لتحقيق المتطلبات الأمنية.

3.15 المعايير العالمية لأمن الحوسبة السحابية:

الأمان السيبراني للحوسبة السحابية هو مجموعة من الإجراءات والمبادئ التي تهدف إلى حماية البيانات والمعلومات المخزنة والتي تعالج في بيئة الحوسبة السحابية. تُستخدم هذه المعايير ليتم التأكد من سلامة البيانات وخصوصيتها وتوفير الحماية والدفاع اللازم ضد التهديدات السيبرانية. وفيما يلي بعض المعايير الأمنية الشائعة للحوسبة السحابية:

- **ISO/IEC 27001:**

هو معيار دولي يقدم إطاراً شاملا لإنشاء و إدارة نظام أمن المعلومات، وتنفيذه وتحسينه وصيانته باستمرار داخل المؤسسات، بما في ذلك تلك المؤسسات التي تستخدم الحوسبة السحابية (ISO,2022).

- **ISO/IEC 27017:**

وهو معيار دولي يقدم قواعد وإرشادات ومتطلبات أمان السحابة، ويشمل توجيهات حول كيفية تنفيذ وإدارة الأمان في بيئة الحوسبة السحابية (ISO,2015).

- **ISO/IEC 27018:**

وهو معيار يتعلق بحماية البيانات الشخصية في بيئة الحوسبة السحابية. ويحدد المعيار المتطلبات الخاصة بخصوصية البيانات الشخصية المخزنة والحماية الأمنية اللازمة ومعالجتها في السحابة (ISO,2019).

- **CSA STAR:**

Cloud Security Alliance, Security, Trust, and Assurance Registry: وهي برنامج لضمان الأمن السحابي، يعمل على تعزيز الثقة والأمان وشفافية الحوسبة السحابية، لمساعدة المستخدم النهائي على تقييم واختيار مقدم الخدمة بناءً على مستوى الثقة والأمان والشفافية الذي يوفرها، للمساهمة في رفع أمان الحوسبة السحابية (CSA.2021).

- **NIST SP 800-144:**

وهي توجهات ومعايير تسهم في توفير الحماية الأمنية في بيئة الحوسبة السحابية مقدمة من المعهد الوطني للمعايير والتكنولوجيا (NIST) في الولايات المتحدة (NIST,2011).

- **COBIT:**

وهو نموذج المرجعي للأمن وإطار عالمي لإدارة وحوكمة تقنية المعلومات، لضمان عدم استغلال تقنية المعلومات بالشكل الخاطئ (ISACA, n.d).

- **CSA- CCM:**

وهي عبارة عن مصفوفة للتحكم في الأمن السيبراني للحوسبة السحابية (CSA,2021).

PCI DSS:

وهو معيار أمني لحماية معلومات البطاقات الائتمانية وضمان أمن المعاملات المالية (pci,2022).

- **Fips publication 200:**

هي وثيقة تحدد جزء من سلسلة المعايير الفيدرالية للمعلومات وأنظمة المعلومات. تحدد الأمان الأدنى للمعلومات وتنطبق على بيئة الحوسبة السحابية (NIST,2005).

- **CIS Benchmarks:**

وهي مجموعة من الممارسات والإرشادات الأمنية للحوسبة السحابية (CIS, n.d).

3.16 أبرز ضوابط الأمن السيبراني للحوسبة السحابية:

3.16.1 تنفيذ السياسات:

تعرف السياسات بأنها القواعد والأحكام التي يتم توظيفها لإدارة أمن الحوسبة السحابية. ولابد من تطبيق هذه السياسات في جميع الطبقات المكونة للحوسبة السحابية؛ كطبقة البنية التحتية، وطبقة الشبكة، وطبقة التطبيقات، وطبقة المستفيد، لذا نجد أن لدينا سياسات لأمن المعلومات، وسياسات للأمن المادي، وسياسات لاستمرارية الأعمال، وسياسات لأمن البنية التحتية، وسياسات لأمن التطبيقات. ولابد من فصل السياسات عند التطبيق والتنفيذ عن الخدمات السحابية التي تستخدمها لتأكد من الاستقلالية كل منهما ولتسهيل التحديثات

المستقبلية قد تطرأ، لذلك ينبغي ألا ترتبط إجراءات التغيير في السياسات بإجراءات مماثلة في التطبيقات، والعكس صحيح (آل حيان،2019).

3.16.2 التشفير:

هو القواعد التي تتضمن مبادئ ووسائل وأساليب تخزين ونقل البيانات أو المعلومات بأشكال محددة. وذلك لإخفاء محتواه الدلالي أو منع الاستخدام غير المصرح به أو منع التعديلات التي لم يتم اكتشافها، بحيث لا يتمكن سوى الموظفين المعنيين من قراءتها ومعالجتها. (NCA, 2020). وهو عملية تحويل البيانات من شكلها الأصلي (نص عادي). إلى نموذج غير قابل للقراءة (نموذج مشفر). بالنسبة لعملية فك التشفير، فهي عملية تحويل النص المشفر إلى نص عادي قابل للقراءة (الحيان، 2019).

3.16.3 إدارة المفاتيح:

الهدف الرئيسي من استخدام المفتاح هو حماية البيانات المشفرة من الوصول غير المصرح به عن طريق منع فك تشفيرها ما لم يتم استخدام المفتاح. تعد إدارة مفاتيح التشفير جزءًا مهمًا لتأكد من أمان البيانات المشفرة. تتكون دورة حياة إدارة المفاتيح من ثمانية مراحل:

- مرحلة التوليد: حيث يتم إنشاء المفتاح في بيئة آمنة، ويفضل أن يكون ذلك عن طريق تشفير المفتاح نفسه باستخدام ما يسمى بالمفتاح الرئيسي.

- مرحلة النسخ الاحتياطي للمفتاح: حيث يتم العودة إليها في حال فقدت المفاتيح الأصلية.
- مرحلة الإطلاق: يتم بها البدء في استخدام المفاتيح الجديدة لتشفير البيانات.
- مرحلة المراقبة: يتم مراقبة بيئة التشفير وأدائها، بما في ذلك مفاتيح التشفير والبيانات المشفرة. لتأكد من اكتمال عملية إنشاء المفتاح والتشفير بشكل صحيح.
- -التدوير: إنشاء مفتاح جديد وإعادة تشفير جميع البيانات باستخدام المفتاح الجديد.
- -انتهاء صلاحية المفتاح: يبدأ بعد اكتمال مرحلة تدوير المفتاح لذلك يوصى ببدء مرحلة إعادة التدوير قبل انتهاء صلاحية المفتاح الحالي.
- مرحلة الأرشفة: أرشفة المفتاح القديم لفترة من الوقت، تحسبًا لوجود بيانات مشفرة بواسطة مفتاح قديم
- مرحلة التخلص من البيانات: يتم التخلص من مفاتيح منتهية صلاحيتها بعد التأكد من عدم وجود بيانات مشفرة تستخدم المفاتيح منتهية الصلاحية (آل حيان،2019)

3.16.4 تدوين السجلات:

هو عملية التسجيل والتوثيق الآلي لجميع الأحداث التي تجري داخل الخدمات السحابية أثناء تشغيلها، سوا كانت الأحداث مرتبطة بالبيانات، أو الشبكة، أو التجهيزات المادية، أو البرامج المشغلة للخدمات (آل حيان،2019).

3.16.5 المر اقبة:

الهدف من عملية المراقبة هو تتبع الأخطاء واكتشافها قبل وبعد حدوثها وتتبع نسبتها وكذلك مقدار وسلوك استخدام الموارد السحابية، من خلال مراقبة مؤشرات الأداء وتحديد الحالات الشاذة، من خلال مراجعة مؤشرات الأداء التي تركز بشكل خاص على هذا الجانب؛ مثل معدلات تشغيل المعالج، واستخدام وسائط التخزين، وحركة مرور الشبكة، وعدد مرات الوصول إلى موارد سحابية معينة (الحيان، 2019).

3.16.6 التدقيق:

التدقيق هو عملية مراجعة للعمليات والضوابط الأمنية للتأكد من أن الأنظمة والخدمات السحابية تلتزم باللوائح والضوابط والقواعد التنظيمية المطلوبة (آل حيان،2019).

3.16.7 إدارة واجهات التطبيقات البرمجية:

واجهة التطبيقات البرمجية (API) هي واجهة اتصالات وسيطة تسمح بالاتصال بين المستخدمين والتطبيقات، أو حتى بين تطبيقين مستقلين. تستخدم واجهات التطبيقات البرمجية مجموعة من البروتوكولات (مثل HTTP وHTTPS) ضمن تطبيقات الإنترنت للتواصل مع العالم خارج التطبيق. وبالنسبة لإدارة واجهة التطبيقات البرمجية، فهي عملية إنشاء ونشر وتسجيل ومراقبة أداء واجهات التطبيقات البرمجية والتأكد من أنها تعمل في بيئة آمنة ومرنة. (الحيان، 2019)

3.16.8 المصادقة:

هي عملية التحقق من هوية المستخدمين الذين يطلبون الوصول إلى الموارد السحابية المحمية مثل البيانات والتطبيقات. تحتاج عملية المصادقة إلى التأكد من استيفاء شرط واحد على الأقل لتحديد هوية المستخدم. يمكن أن يكون الشرط شيئًا يعرفه المستخدم فقط، مثل كلمة المرور، أو يمكن أن يكون شيئًا يمتلكه المستخدم، مثل البطاقة الذكية أو جهاز التحقق، أو شيئًا يحدد هوية المستخدم بشكل فريد، مثل بصمة الإصبع. عند تنشيط ما يسمى بالمصادقة متعددة العوامل، يتم استخدام عدة شروط لتأكد من هوية المستخدم (آل حيان،2019).

3.16.9 الصلاحية:

عملية إدارة الصلاحيات عالية الخطورة على الأنظمة والتي غالبًا ما تتطلب تعامل خاص لتقليل مخاطر التي قد تنشأ من سوء الاستخدام (NCA,2020).

3.16.10 التعافي من الكوارث:

الأنشطة والخطط والبرامج المصممة لاستعادة وظائف وخدمات الأعمال إلى حالة مقبولة بعد التعرض إلى الهجمات السيبرانية أو تعطل تلك الخدمات والوظائف (NCA,2020).

4. ضو ابط الامن السيبر اني للحوسبة السحابية في المملكة العربية السعودية:

4.1 نبذة:

تهتم المملكة العربية السعودية اهتماما كبيرًا في مجال الأمن السيبراني ونظرًا لأن موضوع الحوسبة السحابية يحظى بالمزيد من التداول على مستوى العالم ؛ فقد زاد التوجه له وتنفيذه داخل المملكة العربية السعودية بسرعة كبيرة، مما يكشف عن تحديات و تهديدات جديدة للأمن السيبراني للحوسبة السحابية، لذا مع تزايد هذه التهديدات والمخاطر المتعلقة بأمن الفضاء السيبراني قامت الهيئة الوطنية للأمن السيبراني بإصدار وثيقة تتعلق بضوابط الأمن السيبراني للحوسبة السحابية (CCC - 1 : 2020) وتأتي هذه الضوابط مكملة للضوابط الصادرة في وثيقة الضوابط الأساسية للأمن السيبراني.

4.2 الأهداف:

تهدف هذه الوثيقة إلى تحقيق الأهداف الوطنية للأمن السيبراني عن طريق التركيز على خدمات الحوسبة السحابية من منظور مقدمين الخدمات والمشتركين، وتحديد متطلبات أمان شبكة الحوسبة السحابية لهم، والعمل على تحقيقها وتلبية متطلبات الأمان وتحسين الاستعداد للمخاطر السيبرانية عبر جميع خدمات الحوسبة السحابية.

4.3 المبادئ الأساسية للأمن السيبر اني المتعلقة بالبيانات والمعلومات:

سرية المعلومات (Confidentiality)

سلامة المعلومات (Integrity)

توافر المعلومات (Availability)

4.4 المحاور الأساسية التي يرتكز عليها الأمن السيبراني:

الاستراتيجية (Strategy)

الأشخاص (People)

الإجراء (Procedure)

التقنية (Technology)

4.5 المعايير العالمية المتوائمة مع ضوابط الأمن السيبراني للحوسبة السحابية:

تم إصدار وثيقة ضوابط الأمن السيبراني للحوسبة السحابية بعد دراسة العديد من المعايير وأطر وضوابط وممارسات وتجارب دولية ومحلية في مجال الأمن السيبراني، وتتميز ضوابط الأمن السيبراني للحوسبة السحابية بكونها تتواءم مع معايير عالمية مثل: المعيار الأمريكي FedRAMP، ومعيار الأمن السحابي في سنغافورة (Multi-Tier Cloud Security Standard for Singapore (MTCS SS)، ومعيار Cloud Computing Compliance Control Catalogue (C5))، وضوابط Cloud Controls Matrix (CCM)، ومعيار ISO/IEC 27001. وتتألف ضوابط الامن السيبراني للحوسبة السحابية لمقدمي الخدمات والمشتركين من 4 مكونات أساسية و24 مكونا فرعيًا وتشتمل على 37 ضابطًا أساسيًا و96 ضابطًا فرعيًا لمقدمي الخدمات و18 ضابطًا أساسيًا و26 ضابطًا فرعيًا للمشتركين.

5. الإطار التطبيقي

5.1 تمهيد:

يتناول هذا الجزء التطبيقي من الدراسة في مقدمته نبذة عن جامعة طيبة وتأسيسها، يتم بعد ذلك استعراض نبذة عن قسم الأمن السيبراني لدى جامعة طيبة والغرض من إدارة الأمن السيبراني، ومن ثم يعرض بالتفصيل واقع الأمن السيبراني للحوسبة السحابية لدى الجامعة ويتكون من عدة محاور: أولاً الخدمات السحابية التابعة لجامعة طيبة، ثانيًا حوكمة الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة، ثالثًا تعزيز الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة، رابعًا صمود الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة.

5.2 نبذة عن جامعة طيبة:

تأسست جامعة طيبة عام 1424 هـ الموافق 2003 م. المدينة المنورة، المملكة العربية السعودية وهي جامعة سعودية شاملة ملتزمة بالتميز في نشر المعرفة وإنتاج المعرفة وتقديم خدمات للمجتمع وتتضمن رسالة جامعة طيبة المساهمة في بناء مجتمع يعزز التنمية المستدامة واقتصاد المعرفة من خلال التميز في التعليم والبحث النوعي والشراكات المجتمعية في بيئة تحفز التعلم والإبداع (جامعة طيبة، د.ت)

5.3 قسم الأمن السيبر اني لدى جامعة طيبة:

تم إنشاء قسم الأمن السيبراني بموجب المرسوم الملكي رقم 37140 بتاريخ 14 شعبان 1438 بشكل مستقل عن قسم تقنية المعلومات ويتبع من الناحية التنظيمية لرئيس الجامعة. خُصصت إدارة الأمن السيبراني لإدارة وحوكمة أمن المعلومات من خلال تطبيق الأطر والسياسات والإجراءات الأمنية اللازمة لضمان أمن أصول التقنية والمعلومات بجامعة طيبة. ولضمان إدارة جميع المخاطر والتهديدات المحتملة لأمن المعلومات بشكل فعال واعتماد الحلول التقنية الوقائية اللازمة، ومراقبة الأداء التشغيلي لتقنيات وأنظمة أمن المعلومات التي تستخدمها جامعة طيبة والتأكد من تحديثها وتطويرها باستمرار. لتتيح للجامعة إمكانية الوصول إلى الفضاء السيبراني الأمن والموثوق حيث يمكنها النمو والازدهار. والمساهمة في مسيرة المملكة للأمن السيبراني من خلال تحسين مستوى الأمن السيبراني بالجامعة، وحماية شبكاتها وأنظمتها والبيانات الإلكترونية، وزيادة الوعي بين منسوبي الجامعة حول الأمن السيبراني، وترسيخ مبادئ المسؤولية المشتركة لحماية الفضاء السيبراني للجامعة (جامعة طيبة، د.ت).

الغرض من إدارة الأمن السيبراني هو:

1- دعم استراتيجية عمل الجامعة
2- حماية أصول الجامعة المعلوماتية والتقنية
3- تعزيز أفضل الممارسات في مجال الأمن السيبراني

5.4 و اقع الأمن السيبر اني للحوسبة السحابية لدى جامعة طيبة:

تم الوصول الى البيانات بناءً على تحليل الملفات الموجودة في موقع إدارة الأمن السيبراني الخاصة بجامعة طيبه وعلى قائمة مراجعة تم إعدادها بناءً على ضوابط الأمن السيبراني للحوسبة

السحابية التابعة للهيئة الوطنية للأمن السيبراني، وعلى المقابلة التي قسمت على عدد من المحاور ويتضمن كل محور على مجموعة من الاسئلة ومن ثم تحليل إجابات المفحوص واستنتاج ما هو أتي:

5.4.1 الحوسبة السحابية لدى جامعة طيبة:

تعتمد جامعة طيبة نموذج السحابة الهجين هي عبارة عن مزيج من منصة الحوسبة السحابية العامة ومنصة الحوسبة السحابية الخاصة، تعتمد جامعة طيبة في خدماتها السحابية على Azure cloud وهو نظام سحابي أمن مقدم من Microsoft يضم 3500 وأكثر من خبراء الأمن الإلكتروني (Azure,n.d).

5.4.2 الخدمات السحابية لدى جامعة طيبة:

1. نظام التعلم الإلكتروني - Blackboard
2. منصة خدمة تك
3. الارشفة الإلكترونية للطلاب
4. المدن الصحية
5. تحديث بيانات الموظفين
6. الكراسي العلمية
7. أرشفة العهد
8. الشبكة الاجتماعية
9. البريد الالكتروني العام
10. البريد الالكتروني للطلاب

5.4.3 حوكمة الأمن السيبر اني للحوسبة السحابية لدى جامعة طيبة:

يركز هذا المحور على توضيح مدى التزام جامعة طيبة بتطبيق ضوابط حوكمة الأمن السيبراني للحوسبة السحابية التابعة للهيئة الوطنية للأمن السيبراني، ويوضح الجدول رقم (١) مجموعة من الضوابط التي ترتبط بحوكمة الأمن السيبراني

جدول رقم (١) *حوكمة الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة.*

حوكمة الأمن السيبر اني(Cybersecurity Governance)		
الضابط	نعم	لا
هل تم تحديد أدوار الأمن السيبراني، وتوزيع المسؤوليات (RACI) لكل أصحاب العلاقة في خدمات الحوسبة السحابية؟	✔	
هل تم تحديد ما المستوى المقبول للمخاطر فيما يخص خدمات الحوسبة السحابية؟	✔	
في منهجية إدارة مخاطر الأمن السيبراني هل تم الأخذ بالاعتبار تصنيف البيانات والمعلومات؟		✔
هل تم إنشاء سجل لجميع مخاطر الأمن السيبراني خاص بالعمليات وخدمات الحوسبة السحابية، والمتابعة دوريًا بما يتناسب مع طبيعة المخاطر؟		✔
هل تتم المراقبة المستمرة والدائمة لمدى التزام مايكروسوفت بالتشريعات، وبنود العقود التي تتعلق بالأمن السيبراني؟	✔	
هل يتم إجراء مسح أمني للعاملين الذين لهم حق الوصول إلى المهام الحساسة التابعة لخدمات الحوسبة السحابية، على سبيل المثال: إدارة المفاتيح، التحكم بالوصول، إدارة الخدمات؟	✔	

نستنتج من خلال الجدول رقم (١) ما يلي:

نسبة التزام جامعة طيبة في حوكمة الأمن السيبر اني:

تبلغ نسبة التزام جامعة طيبة في تطبيق ضوابط حوكمة الأمن السيبراني ٧٥٪، وذلك نتيجة لتطبيق 4 ضوابط من أصل 6 ضوابط، وتبلغ نسبة عدم التطبيق٢٥٪، وذلك نتيجة عدم تطبيق ضابط واحد فقط من أصل 6 ضوابط والتطبيق الجزئي لضابط واحد فقط.

- الأدواروالمسؤوليات الأمن السيبر اني:

تلتزم جامعة طيبة بتحديد مسؤوليات الأمن السيبراني للحوسبة السحابية داخل الجامعة لضمان تحديد المسؤوليات والمهام الواضحة لجميع الأطراف المشاركة في تطبيق الأمن السيبراني

في الجامعة. وتلتزم جامعة طيبة بالمراقبة الدائمة لمدى التزام مايكروسوفت بالتشريعات وبنود العقود الخاصة بالأمن السيبراني.

- معايير وتشريعات الأمن السيبراني:

تلتزم جامعة طيبة بمعايير وتشريعات الأمن السيبراني لضمان امتثال الأمن السيبراني في جامعة طيبة للمتطلبات التنظيمية والتشريعية ذات الصلة.

-إدارة مخاطر الأمن السيبراني:

تلتزم جامعة طيبة بتحديد المستوى المقبول للمخاطر المتعلقة بخدمات الحوسبة السحابية. ولكن لا توجد رؤية واضحة فيما يخص تصنيف البيانات والمعلومات في منهجية إدارة المخاطر الخاصة بالأمن السيبراني. وتعمل الجامعة بشكل جزئي على إنشاء سجلات لجميع مخاطر الأمن السيبراني خاص بالعمليات وخدمات الحوسبة السحابية، ومتابعتها دوريًا بما يتناسب مع طبيعة المخاطر.

-الأمن السيبراني الخاص بالموارد البشرية:

تلتزم جامعة طيبة بإجراء مسح أمني للموظفين الذين لديهم إمكانية الوصول إلى البيانات الحساسة التابعة لخدمات الحوسبة السحابية لتأكد من أن مخاطر ومتطلبات الأمن السيبراني المرتبطة بالموظفين والمتعاقدين في الجامعة تعالج بشكل فعال قبل وأثناء وفي نهاية عملهم وفقًا لإجراءات وسياسات الجامعة والتشريعات ذات الصلة، وتوفر الجامعة تدريب وتوعية للموظفين حول أمان الحوسبة السحابية بشكل مستمر بما يتوافق معهم.

5.4.4 تعزيز الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة:

يركز هذا المحور على توضيح مدى التزام جامعة طيبة بتطبيق ضوابط تعزيز الأمن السيبراني للحوسبة السحابية التابعة للهيئة الوطنية للأمن السيبراني، ويوضح الجدول رقم (٢) مجموعة من الضوابط التي ترتبط بتعزيز الأمن السيبراني.

جدول رقم (٢) *تعزيز الأمن السيبراني للحوسبة السحابية.*

تعزيز الأمن السيبر اني(Cybersecurity Defense)		
الضابط	نعم	لا
هل يتم حصر كافة الخدمات السحابية والأصول المعلوماتية والتقنية المتعلقة بها؟	✔	
هل تتم إدارة هويات الدخول والصلاحيات لكافة الحسابات، التي تملك صلاحية الوصول إلى الخدمات السحابية، خلال دورة حياتها؟	✔	
هل تم التأكد من سرية هوية المستخدم والصلاحيات والحسابات، ويشمل ذلك الطلب من المستخدمين حفظ خصوصيتها (للمستخدمين من جهة الجامعة والعاملين، وأيضًا الأطراف الخارجية)؟	✔	
هل هناك إدارة الآمنة للجلسات وتشمل موثوقية الجلسات، وإقفالها، وإنهاء مهلتها؟	✔	
هل يتم التحقق من الهوية متعدد العناصر لجميع الحسابات السحابية للمستخدمين ذوي الصلاحيات الحساسة والهامة؟	✔	
هل هناك إجراءات لكشف محاولات الوصول غير المصرح به ومنعها مثل: (الحد الأقصى من محاولات عمليات الدخول غير الناجحة)؟	✔	
هل تم التحقق من قيام مايكروسوفت بعزل الحوسبة السحابية عن أي حوسبة سحابية أخرى مقدمة للجهات خارج نطاق العمل؟		✔
هل تتم حماية القناة المستخدمة للاتصال الشبكي مع مايكروسوفت؟	✔	
هل يتم التأكد من عدم احتواء الأجهزة المحمولة قبل إعادة استخدامها أو التخلص منها على أي بيانات أو معلومات باستخدام وسائل آمنة؟		✔
هل تقدم مايكروسوفت ضمانات للقدرة على حذف البيانات بطرق آمنة عند الانتهاء من العلاقة؟		✔
هل يتم استخدام طرق وسائل آمنة لتصدير ونقل البيانات؟	✔	

تعزيز الأمن السيبراني (Cybersecurity Defense)		
الضابط	نعم	لا
هل تلتزم الجامعة باستخدام طرق وخوارزميات وأجهزة ومفاتيح تشفير محدثة وآمنة، وفقاً للمستوى المتقدم ضمن المعايير الوطنية للتشفير؟	✔	
هل يتم تشفير البيانات والمعلومات المنقولة إلى ومن الخدمات السحابية، بحسب المتطلبات التشريعية والتنظيمية ذات العلاقة؟	✔	
هل يتم تقييم ومعالجة الثغرات الخاصة بالخدمات السحابية كل ثلاثة أشهر على الأقل؟	✔	
عندما يتم إشعار الجامعة من قبل مايكروسوفت بوجود ثغرات هل تتم إدارة الثغرات ومعالجتها؟	✔	
هل تم تفعيل وجمع جميع سجلات الأحداث الخاصة بعمليات الدخول، وسجلات الأحداث الخاصة بالأمن السيبراني على الأصول المتعلقة بالخدمات السحابية؟	✔	
هل تشمل عمليات المراقبة جميع أحداث الأمن السيبراني التي تم تفعيلها على الخدمات السحابية الخاصة بالمشترك؟	✔	
هل تم تحديد وتوثيق وتطبيق متطلبات الأمن السيبراني التابع لإدارة المفاتيح؟	✔	
هل تم تحديد ملاك لمفاتيح التشفير (Key Owner) ؟	✔	
هل توجد آليات آمنة لاسترجاع مفاتيح التشفير في حال تم فقدانها على سبيل المثال: وجود نسخ احتياطيه وتخزينها خارج الأنظمة السحابية بطرق آمنة؟	✔	

نستنتج من خلال الجدول رقم (٢) ما يلي:

- نسبة التزام جامعة طيبة في تعزيز الأمن السيبراني:

تبلغ نسبة التزام جامعة طيبة في تطبيق ضوابط تعزيز الأمن السيبراني 85٪، وذلك نتيجة لتطبيق 17 ضابط من أصل 20 ضابط، وتبلغ نسبة عدم التطبيق 15%، وذلك نتيجة عدم تطبيق 3 ضوابط من أصل 20 ضابط

-إدارة الأصول:

تلتزم جامعة طيبة بحصر كافة الخدمات السحابية والأصول المعلوماتية والتقنية الخاصة بها.

إدارة هويات الدخول والصلاحيات:

تلتزم جامعة طيبة بإدارة هويات الدخول والصلاحيات لجميع الحسابات التي لديها صلاحية الوصول إلى الخدمات السحابية لضمان حماية الأمن السيبراني للوصول المنطقي Access Logical إلى الأصول المعلوماتية والتقنية من أجل منع الوصول غير المصرح به، وتقوم الجامعة بتقيد الوصول إلى ما هو مطلوب لتمكين إنجاز الأعمال الخاصة بالجامعة. والتأكد من سرية هوية المستخدم والصلاحيات والحسابات.

وتشمل سياسة إدارة هويات الدخول والصلاحيات:

أولًا: إدارة الصلاحيات

تتكون إدارة الصلاحيات من العديد من السياسات على سبيل المثال: توثيق واعتماد إجراءات إدارة الوصول، وتوضيح آلية منح وتعديل وإلغاء الوصول إلى أصول المعلومات والأصول التقنية بجامعة طيبة، ومراقبة هذه الآلية والتأكد من تنفيذها، إنشاء هويات المستخدمين بما يتوافق مع المتطلبات التنظيمية و التشريعية لجامعة طيبة، التحقق من هوية المستخدمين والتحقق من صحتهم قبل منحهم حق الوصول إلى أصول المعلومات والأصول التقنية، اعتماد و توثيق مصفوفة (Matrix) لإدارة التصاريح والصلاحيات الخاصة بالمستخدمين وفق مبادئ التحكم في الوصول والصلاحيات التالية:

- مبدأ الحاجة إلى المعرفة والحاجة إلى الاستخدام.
- مبدأ الفصل بين المهام.
- مبدأ الصلاحيات والامتياز الأقل

ثانيًا: منح حق الدخول

وعلى سبيل المثال فيما يتعلق بمتطلبات الدخول لحساب المستخدم: منح حق الدخول استنادًا على طلب المستخدم نفسه من خلال تقديم نموذج أو من خلال النظام المعتمد من مديره مباشرةً ومالك النظام يُحدد فيه اسم النظام ونوع طلب المستخدم وصلاحيته والمدة الزمنية في حال كانت صلاحيته مؤقتة وغيرها من المتطلبات. وفيما يتعلق متطلبات حق الوصول للحسابات الحساسة والهامة على سبيل المثال: يتم التحقق من الهوية متعدد العناصر.

تلتزم جامعة طيبة بالتحقق من الهوية متعدد العناصر لجميع حسابات المستخدمين السحابية ذات الأذونات المهمة والحساسة من خلال آلية التحقق من الهوية متعدد العناصر (MFA) باستخدام طريقتين على الأقل مما هو أتي:

1- المعرفة: شيء يعرفه المستخدم مثل كلمة المرور.

2- الحيازة: شيء مملوك للمستخدم فقط، مثل جهاز أو برنامج يقوم بإنشاء أرقام عشوائية أو تسجيلات دخول مؤقتة عبر الرسائل النصية القصيرة، تسمى كلمات المرور لمرة واحدة (One-Time-Password).

3- الملازمة: خصائص أو سمات حيوية ترتبط فقط بالمستخدم نفسه مثل بصمة الأصابع. إن الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة ومراقبة الأنظمة الحساسة يجب أن يتطلب استخدام MFA لجميع المستخدمين.

وعلى سبيل المثال فيما يتعلق بالدخول عن بعد: تمنح صلاحيات الدخول عن بعد للأصول المعلوماتية والأصول التقنية عند الحصول على إذن من قبل إدارة الأمن السيبراني، وتقيد دخول المستخدم باستخدام MFA.

الإدارة الآمنة للجلسات:

تلتزم جامعة طيبة بإدارة أمن الجلسات، وضبط إعدادات النظام ليتم إغلاقه تلقائيا بعد وقت محدد (Session Timeout) لذا يوصى بأن لا يزيد الوقت عن 15 دقيقة، وتم ضبط إعدادات كافة نظم إدارة الهوية والوصول لإرسال سجلاتها إلى أنظمة التسجيل والمراقبة المركزية وذلك وفقًا لسياسة إدارة سجلات الأحداث والمراقبة للأمن السيبراني.

كشف محاولات الوصول غير المصرح بها:

تلتزم جامعة طيبة بتطبيق الإجراءات لاكتشاف ومنع محاولات الوصول غير المصرح بها، يتضمن عدد المحاولات 5 محاولات فاشلة لكل حساب مستخدم يتمتع بأذونات مهمة وحساسة ولجميع المستخدمين بشكل عام. ولا توجد أي محاولة لحسابات الخدمات، وتبلغ مدة إغلاق الحساب 30 دقيقة، أو حتى يقوم النظام بإلغاء قفل الحساب، حيث يقوم المدير بفك إغلاق الحساب المغلق يدويًا. يقوم قسم الأمن السيبراني لدى جامعة طيبة بإرسال رسائل منتظمة للمستخدمين يطلب منهم تغيير كلمات المرور الخاصة بهم، حيث إن الحد الأقصى لعمر كلمة المرور هو 45 يومًا. وتتم مراقبة جميع الأحداث النشطة على الخدمات السحابية. وتفعيل وجمع

سجلات أحداث عمليات تسجيل الدخول وسجلات أحداث الأمن السيبراني على الأصول الخاصة بخدمات الحوسبة السحابية.

-الحماية للأنظمة وأجهزة معالجة المعلومات:

وفقًا لإجابة المفحوص لا تقدم مايكروسوفت عزل للحوسبة السحابية عن أي حوسبة سحابية أخرى.

-إدارة أمن الشبكة:

تحرص جامعة طيبة على حماية القناة المستخدمة للاتصال الشبكي مع مايكروسوفت.

- أمن الأجهزة المحمولة:

لا يتم بشكل دائم التحقق من عدم احتواء الأجهزة المحمولة على أي بيانات أو معلومات قبل إعادة استخدامها أو التخلص منها بطرق آمنة.

-حماية البيانات والمعلومات:

وفقًا لسياسات مايكروسوفت يتم حذف البيانات بطرق أمنة خلال مدة محدد حسب تصنيف البيانات، ولكن لا توجد ضمانات مقدمة للجامعة للقدرة على حذف البيانات بطرق آمنة عند الانتهاء من العلاقة، وتلتزم جامعة طيبة باستخدام وسائل وطرق آمنة لتصدير ونقل البيانات.

- التشفير:

تلتزم جامعة طيبة باستخدام أحدث الطرق والخوارزميات وأجهزة التشفير والمفاتيح الآمنة لضمان الاستخدام الصحيح والفعال للتشفير، لحماية أصول المعلومات الإلكترونية للجامعة، وفقًا للإجراءات والسياسات التنظيمية للجامعة والمتطلبات التنظيمية والتشريعية ذات الصلة. وتلتزم الجامعة بوجود آلية آمنة لاستعادة مفاتيح التشفير في حالة فقدانها، مثل النسخ الاحتياطي وتخزينها خارج الأنظمة السحابية بطريقة آمنة.

- إدارة الثغرات:

ووفقًا لإجابة المفحوص تتم معالجة الثغرات الأمنية في الحوسبة السحابية ومراقبتها بشكل منتظم، حيث تكون المراقبة على مدار 24 ساعة يوميًا، 7 أيام في الأسبوع، لضمان اكتشاف الثغرات التقنية في الوقت المناسب وحلها بشكل فعال. لمنع استغلال الثغرات الأمنية وتقليل المخاطر السيبرانية وتأثيرها على أعمال الجامعة. ويتم تحديث البرامج والتطبيقات الموجودة على السحابة بانتظام لمنع الثغرات الأمنية وتقليل المخاطر السيبرانية وحمايتها من التهديدات

الداخلية والخارجية. والتركيز على أهداف الحماية الأساسية وهي: سرية المعلومات، سلامة المعلومات، توافر المعلومات. وتلتزم جامعة طيبة باستخدام برامج مكافحة الفيروسات وحماية الجدران النارية لحماية الأجهزة والأنظمة من الهجمات السيبرانية. تُستخدم الحوسبة السحابية لدى جامعة طيبة لإجراء عمليات النسخ الاحتياطي واستعادة البيانات، وأيضا يتم التأكد من توافر أدوات النسخ الاحتياطي واستعادة البيانات في حالة حدوث خلل في الحوسبة السحابية خارج الأنظمة السحابية. ويتم العمل على صيانة الأجهزة والبرامج وتحديثها بشكل دوري. وتعمل الجامعة على تحليل البيانات المخزنة في الحوسبة السحابية للحصول على إحصائيات وتحليلات تسهم في رفع أمان الحوسبة السحابية وحماية المعلومات.

اختبار الاختراق:

يتم إجراء اختبارات الاختراق على الحوسبة السحابية المستخدمة في جامعة طيبة لتقييم فعالية قدرات تعزيز الأمن السيبراني واختباره في الجامعة، وذلك من خلال محاكاة التقنيات التي تستخدم في الهجمات السيبرانية الفعلية وأساليبها، لاكتشاف الثغرات الأمنية غير المعروفة، والتي من الممكن أن تؤدي إلى الاختراقات السيبرانية، وفقاً للمتطلبات التنظيمية والتشريعية ذات الصلة.

- إدارة سجلات الأحداث:

تلتزم جامعة طيبة بتفعيل وجمع جميع سجلات الأحداث الخاصة بعمليات الدخول، وسجلات الأحداث الخاصة بالأمن السيبراني على الأصول المتعلقة بالخدمات السحابية، وتشمل المراقبة جميع العمليات الخاصة بالحوسبة السحابية بشكل مستمر للكشف عن أي تهديدات أمنية.

-إدارة المفاتيح:

تلتزم جامعة طيبة بتحديد وتوثيق وتطبيق متطلبات الأمن السيبراني التابعة لإدارة المفاتيح، وتحديد الملاك لمفاتيح التشفير، والحرص على وجود آليات آمنة لاسترجاع مفاتيح التشفير عند فقدانها على سبيل المثال: وجود نسخ احتياطيه مخزنة خارج الأنظمة السحابية بطرق آمنة.

5.4.5 صمود الأمن السيبر اني للحوسبة السحابية لدى جامعة طيبة:

يركز هذا المحور على توضيح مدى التزام جامعة طيبة بتطبيق ضوابط صمود الأمن السيبراني للحوسبة السحابية التابعة للهيئة الوطنية للأمن السيبراني، ويوضح الجدول رقم (٣) مجموعة من الضوابط التي ترتبط بصمود الأمن السيبراني.

جدول رقم (٣) *صمود الأمن السيبراني للحوسبة السحابية.*

صمود الأمن السيبر اني(Cybersecurity Resilience)		
الضابط	نعم	لا
هل تم تنفيذ الإجراءات اللازمة لتعافي من الكوارث وتطويرها واستمرارية الأعمال بطرق آمنة؟		✔

نستنتج من خلال الجدول رقم (٣) ما يلي:

-نسبة التزام جامعة طيبة في صمود الأمن السيبر اني:

تبلغ نسبة التزام جامعة طيبة في تطبيق ضوابط صمود الأمن السيبراني 30 % تقريبًا، وذلك نتيجة التطبيق الجزئي لضابط صمود الأمن السيبراني، وتبلغ نسبة عدم التطبيق% 70، وذلك نتيجة عدم استكمال تطبيق ضابط صمود الأمن السيبراني بشكلٍ كلي.

- التعافي من للكوارث:

تم تحديد البُنى الأساسية لتطبيق الضابط التابع لتنفيذ وتطوير إجراءات التعافي من الكوارث والتأكد من استمرارية الأعمال الخاصة بالحوسبة السحابية بطرق آمنة، ولكن ما زالت مرحلة أولية ولم يتم التطبيق بشكلٍ كلي لإكتشاف وتحديد حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعال، وللتعامل بشكل استباقي مع تهديدات الأمن السيبراني.

6. الخاتمة:

يعد الالتزام بضوابط الامن السيبراني للحوسبة السحابية في جامعة طيبة أمرًا بالغ الأهمية لتعزيز الحماية والحفاظ على سلامة المعلومات الرقمية ونظام المعلومات الجامعي. يساعد الالتزام في تنفيذ ضوابط الامن السيبراني للحوسبة السحابية في تأكيد قيمة المعلومات المخزنة والمعالجة داخل الجامعة، ويحميها من التهديدات السيبرانية والاختراقات. وفي ظل التوسع الرقمي واعتماد التكنولوجيا في إدارة الجامعة، يصبح تطبيق هذه الضوابط ضرورة حتمية. وتعمل جامعة طيبة حاليًا على وضع خارطة طريق شاملة لتطبيق ضوابط الأمن السيبراني للحوسبة السحابية. يتم أيضًا التركيز على تعزيز الوعي الأمني بين أعضاء هيئة التدريس والطلاب والموظفين من خلال برامج تدريبية وتوعوية للحفاظ على بيئة تعليمية رقمية آمنة وموثوقة لأعضاء الجامعة والطلاب.

7. النتائج والتوصيات

يستعرض هذا الجزء نتائج الدراسة التي تم التوصل إليها وربطها مع تساؤلات الدراسة ومن ثم عرض توصيات الدراسة العامة والخاصة.

7.1 ملخص نتائج الدراسة:

ركزت الدراسة على الإجابة عن التساؤلات التالية:

1- ما الحوسبة السحابية وما استخداماتها في التعليم؟
2- ما هي أبرز مواضيع الأمن السيبراني في الحوسبة السحابية؟
3- ما هي ضوابط الأمن السيبراني للحوسبة السحابية في المملكة العربية السعودية؟
4- ما واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة؟

وفيما يلي عرض لملخص نتائج الدراسة التي تجيب عن كل تساؤل من هذه التساؤلات:

أولا فيما يتعلق بالحوسبة السحابية واستخداماتها في التعليم تعد الحوسبة السحابية نموذج يقدم خدمات رقمية عبر الشبكة ويتيح للشركات والأفراد الوصول الشبكي للموارد الحاسوبية القابلة للتوسع، مثل الشبكات والتخزين والتطبيقات واستخدامها عن بعد دون الحاجة لامتلاك الأجهزة المشغلة، وقدمت الحوسبة السحابية ميزة مهمة في المجال التعليمي حيث اتاحت التعليم عن بعد، وأصبح من الممكن للطلاب وأعضاء هيئة التدريس الوصول إلى المصادر والموارد التعليمية في أي وقت ومن أي مكان.

ثانيًا فيما يتعلق بأبرزمواضيع الأمن السيبر اني في الحوسبة السحابية يشير الأمن السحابي إلى مزيج من التقنيات والسياسات والممارسات لتأمين وحماية النظام السحابي والحفاظ على سلامة البيانات والمعلومات التي تم تخزينها أو معالجتها أو نقلها عبر السحابة من أي استخدام غير قانوني أو التهديدات أو الهجمات السيبرانية لضمان استمرارية الاعمال. ويعد تطبيق ضوابط ومعايير الأمن السيبراني للحوسبة السحابية من أبرز مواضيع الأمن السيبراني للحفاظ على أمن البيانات والمحتوى المخزن في السحابة، ويشمل ذلك اتخاذ إجراءات آمنة مثل استخدام تقنيات قوية لتشفير البيانات، وتنفيذ سياسات الوصول والصلاحيات، وتفعيل آليات المصادقة متعددة العوامل، لتعزيز أمان الحسابات ومنع الوصول غير المصرح به وغيرها من الإجراءات.

ثالثًا فيما يتعلق بضوابط الأمن السيبراني للحوسبة السحابية في المملكة العربية السعودية هي وثيقة تهدف إلى تحقيق الأهداف الوطنية للأمن السيبراني عن طريق التركيز على خدمات الحوسبة السحابية من منظور مقدمي الخدمات والمشتركين، وتحديد متطلبات أمان شبكة الحوسبة السحابية لهم، والعمل على تحقيقها وتلبية متطلبات الأمان وتحسين الاستعداد للمخاطر السيبرانية عبر جميع خدمات الحوسبة السحابية. وتأتي هذه الضوابط مكملة للضوابط الصادرة في وثيقة الضوابط الأساسية للأمن السيبراني. تم إصدارها بعد دراسة العديد من المعايير وأطر وضوابط وممارسات وتجارب دولية ومحلية في مجال الأمن السيبراني، وتتميز ضوابط الأمن السيبراني للحوسبة السحابية في المملكة العربية السعودية بكونها تتواءم مع معايير عالمية مثل: المعيار الأمريكي FedRAMP، ومعيار الأمن السحابي في سنغافورة (Multi-Tier Cloud Security Standard for Singapore (MTCS SS)، ومعيار Cloud Computing Compliance Control Catalogue (C5)، وضوابط Cloud Controls Matrix (CCM)، ومعيار ISO/IEC 27001. وتتألف ضوابط الامن السيبراني للحوسبة السحابية لمقدمي الخدمات والمشتركين من 4 مكونات أساسية و24 مكونا فرعيًا وتشتمل على 37 ظابطًا أساسيًا و96 ضابطًا فرعيًا لمقدمي الخدمات و18 ضابطًا أساسيًا و26 ضابطًا فرعيًا للمشتركين.

رابعًا فيما يتعلق بو اقع الأمن السيبر اني للحوسبة السحابية لدى جامعة طيبة

1- بلغت نسبة التزام جامعة طيبة في تطبيق ضوابط حوكمة الأمن السيبراني للحوسبة السحابية 75٪، وذلك نتيجة لتطبيق 4 ضوابط من أصل 6 ضوابط، وتبلغ نسبة عدم التطبيق 25٪، وذلك نتيجة عدم تطبيق الضابط المتعلق بأخذ تصنيف البيانات والمعلومات بالاعتبار في منهجية إدارة مخاطر الأمن السيبراني، والتطبيق الجزئي لضابط إنشاء سجل لجميع مخاطر الأمن السيبراني خاص بالعمليات وخدمات الحوسبة السحابية، والمتابعة دوريًا بما يتناسب مع طبيعة المخاطر.

2- بلغت نسبة التزام جامعة طيبة في تطبيق ضوابط تعزيز الأمن السيبراني للحوسبة السحابية 85٪ ، وذلك نتيجة لتطبيق 17 ضابط من أصل 20 ضابط، وتبلغ نسبة عدم التطبيق 15%، وذلك نتيجة عدم تطبيق 3 ضوابط من أصل 20 ضابط وتشمل عدم التحقق من قيام مايكروسوفت بعزل الحوسبة السحابية عن أي حوسبة سحابية أخرى مقدمة للجهات خارج نطاق العمل، وعدم التأكد من عدم احتواء

الأجهزة المحمولة قبل إعادة استخدامها أو التخلص منها على أية بيانات أو معلومات باستخدام وسائل آمنة، و عدم وجود ضمانات مقدمة من مايكروسوفت فيما يتعلق بالقدرة على حذف البيانات بطرق آمنة عند الانتهاء من العلاقة.

3- بلغت نسبة التزام جامعة طيبة في تطبيق ضوابط صمود الأمن السيبراني للحوسبة السحابية 30 % تقريبًا، وذلك نتيجة التطبيق الجزئي لضابط صمود الأمن السيبراني، وتبلغ نسبة عدم التطبيق 70٪، وذلك نتيجة عدم استكمال تطبيق ضابط صمود الأمن السيبراني بشكلٍ كلي.

4- لذلك نستنتج أن نسبة التزام جامعة طيبة بتطبيق ضوابط الأمن السيبراني للحوسبة السحابية هي 81.48٪ وذلك نتيجة تطبيق21 ضابط بشكل كلي وتطبيق ضابطان بشكل جزئي، وبلغت نسبة عدم التطبيق لضوابط الأمن السيبراني للحوسبة السحابية 18.52٪ وذلك نتيجة عدم تطبيق ٤ضوابط وعدم استكمال تطبيق ضابطان.

7.2 توصيات الدراسة:

وبناءً على نتائج الدراسة وما توصلت إلية الباحثة، نوصي بإتباع التوصيات التالية:

1. نظرًا لأن مجال الأمن السيبراني مجالاً جديدًا وسريع التطور، أصبح من الضرورة للهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية تقديم خارطة استرشادية وتوجيهية بشأن التدابير والممارسات الأمنية المطلوبة لحماية الأنظمة والشبكات السيبرانية، وتهدف إلى التطبيق الفعال لكافة الضوابط ذات الصلة.
2. تعاون جامعة طيبة مع مقدِم خدمات سحابية داخل المملكة العربية السعودية للتأكد من الاستجابة السريعة والامتثال للتشريعات والقوانين الخاصة بالدولة ودعم اقتصادها المحلي
3. استكمال المجال البحثي في مجال الأمن السيبراني للحوسبة السحابية من خلال إعداد دراسات لقياس مستوى تنفيذ ضوابط ومعايير الأمن السيبراني للحوسبة السحابية في مؤسسات التعليم العالي.

الملاحق

الملحق رقم (1) يعرض قائمة المراجعة (أداة الدراسة)

حوكمة الأمن السيبر اني(Cybersecurity Governance)		
الضابط	نعم	لا
هل تم تحديد أدوار الأمن السيبراني، وتوزيع المسؤوليات (RACI)لكل أصحاب العلاقة في خدمات الحوسبة السحابية؟		
هل تم تحديد ما المستوى المقبول للمخاطر فيما يخص خدمات الحوسبة السحابية؟		
في منهجية إدارة مخاطر الأمن السيبراني هل تم الأخذ بالاعتبار تصنيف البيانات والمعلومات؟		
هل تم إنشاء سجل لجميع مخاطر الأمن السيبراني خاص بالعمليات وخدمات الحوسبة السحابية، والمتابعة دوريا بما يتناسب مع طبيعة المخاطر؟		
هل تتم المراقبة المستمرة والدائمة لمدى التزام مايكروسوفت بالتشريعات، وبنود العقود التي تتعلق بالأمن السيبراني؟		
هل يتم إجراء مسح أمني للعاملين الذين لهم حق الوصول إلى المهام الحساسة التابعة لخدمات الحوسبة السحابية، على سبيل المثال :إدارة المفاتيح، التحكم بالوصول، إدارة الخدمات؟		

تعزيز الأمن السيبر اني (Cybersecurity Defense)		
الضابط	نعم	لا
هل يتم حصر كافة الخدمات السحابية والأصول المعلوماتية والتقنية المتعلقة بها؟		
هل تتم إدارة هويات الدخول والصلاحيات لكافة الحسابات، التي تملك صلاحية الوصول إلى الخدمات السحابية، خلال دورة حياتها؟		
هل تم التأكد من سرية هوية المستخدم والصلاحيات والحسابات، ويشمل ذلك الطلب من المستخدمين حفظ خصوصيتها (للمستخدمين من جهة الجامعة والعاملين، وأيضًا الأطراف الخارجية)؟		

تعزيز الأمن السيبراني (Cybersecurity Defense)		
الضابط	نعم	لا
هل هناك إدارة الآمنة للجلسات وتشمل موثوقية الجلسات، وإقفالها، وإنهاء مهلتها؟		
هل يتم التحقق من الهوية متعدد العناصر لجميع الحسابات السحابية للمستخدمين ذوي الصلاحيات الحساسة والهامة؟		
هل هناك إجراءات لكشف محاولات الوصول غير المصرح به ومنعها مثل) :الحد الأقصى من محاولات عمليات الدخول غير الناجحة؟		
هل تم التحقق من قيام مايكروسوفت بعزل الحوسبة السحابية عن أي حوسبة سحابية أخرى مقدمة للجهات خارج نطاق العمل؟		
هل تتم حماية القناة المستخدمة للاتصال الشبكي مع مايكروسوفت؟		
هل يتم التأكد من عدم احتواء الأجهزة المحمولة قبل إعادة إستخدامها أو التخلص منها على أي بيانات أو معلومات باستخدام وسائل آمنة؟		
هل تقدم مايكروسوفت ضمانات للقدرة على حذف البيانات بطرق آمنة عند الانتهاء من العلاقة؟		
هل يتم استخدام طرق وسائل آمنة لتصدير ونقل البيانات؟		
هل تلتزم الجامعة باستخدام طرق وخوارزميات وأجهزة ومفاتيح تشفير محدثة وآمنة، وفقاً للمستوى المتقدم ضمن المعايير الوطنية للتشفير؟		
هل يتم تشفير البيانات والمعلومات المنقولة إلى ومن الخدمات السحابية، بحسب المتطلبات التشريعية والتنظيمية ذات العلاقة؟		
هل يتم تقييم ومعالجة الثغرات الخاصة بالخدمات السحابية كل ثلاثة أشهر على الأقل؟		
عندما يتم إشعار الجامعة من قبل مايكروسوفت بوجود ثغرات هل تتم إدارة الثغرات ومعالجتها؟		
هل تم تفعيل وجمع جميع سجلات الأحداث الخاصة بعمليات الدخول، وسجلات الأحداث الخاصة بالأمن السيبراني على الأصول المتعلقة بالخدمات السحابية؟		

تعزيز الأمن السيبر اني (Cybersecurity Defense)		
الضابط	نعم	لا
هل تشمل عمليات المراقبة جميع أحداث الأمن السيبراني التي تم تفعيلها على الخدمات السحابية الخاصة بالمشترك؟		
هل تم تحديد ملاك لمفاتيح التشفير (Key Owner)؟		
هل توجد آليات آمنة لاسترجاع مفاتيح التشفير في حال تم فقدانها على سبيل المثال: وجود نسخ احتياطيه وتخزينها خارج الأنظمة السحابية بطرق آمنة		

صمود الأمن السيبر اني (Cybersecurity Resilience)		
الضابط	نعم	لا
هل تم تنفيذ الإجراءات اللازمة لتعافي من الكوارث وتطويرها واستمرارية الأعمال بصورة آمنة؟		

المراجع

أحمد، فايزة دسوقي .(2018) .*أسياسات أمن المعلومات*. مكتبة الملك فهد الوطنية.

إدارة الأمن السيبراني. (2020). *سياسات الأمن السيبراني*. تم الاسترجاع من خلال https://www.taibahu.edu.sa/Pages/AR/Sector/SectorPage.aspx?ID=155&PageId=19

آل حيان، خالد بن ناصر. (2019). *الحوسبة السحابية أساسيات ومبادئ وتطبيقات*. مركز البحوث والدراسات. تم الاسترجاع من خلال https://archive.org/details/20211018_20211018_0859/page/n11/mode/2up

بخات، سهاس، و بروك، مايكل جون سي، والياهو، تل، و جيتزين، أليكس، وهارجريف، فيك، وأوسيم، إيبودو، وروزا، مايكل، ويوه، جون، ويوسف، نبيل. (2022). أبرز تهديدات الحوسبة السحابية بحث متعمق لإحدا عشر تهديد *Egregious Eleven Deep Dive*. (إبراهيم العساكر، مترجم). تحالف أمن الحوسبة السحابية. (2020). تم الاسترجاع من خلال https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven-deep-dive-arabic-translation/

جامعة طيبة. (د.ت). عن الجامعة. تم الاسترجاع من خلال https://www.taibahu.edu.sa/Pages/AR//:https/www.taibahu.edu.sa/Pages/AR/CustomPage.aspx?ID=41

جامعة طيبة. (د.ت). *عن الإدارة*. تم الاسترجاع من خلال https://www.taibahu.edu.sa/Pa//:https/ges/AR/Sector/SectorPage.aspx?ID=155&PageId=4

الجنفاوي، خالد مخلف. (2021). التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت. المجلة العربية للآداب والدراسات الإنسانية، 5(19)، 75-123. تم الاسترجاع من خلال https://ajahs.journals.ekb.eg/article_182274_5c34dd367d05bf98e1b4eb4baa5bba0e.pdf

علي، فتح الرحمن عوض العليم شـــمس الدين. (2020). تأمين وترقيع ثغرات تطبيقات خدمة الحوسبة السحابية بالتطبيق على ثغرتي(xss& SQL Injection). جامعة النيلين.

منشآت. (د.ت). الحوسبة السحابية ومستقبلها في المملكة العربية السعودية. تم الاسترجاع من https://fikra.sa/system/files/inline-files/تقرير%20فرص%20المنشآت%20الابتكارية%20السعودية%20في%20سوق%20تقنية%20الحوسبة%20السحابية.pdf

الهيئة الوطنية للأمن السيبراني. (2020). *ضوابط الأمن السيبراني للحوسبة السحابية*. تم الاسترجاع من خلال https://nca.gov.sa/ccc-ar.pdf

الهيئة الوطنية للأمن السيبراني. (2020). *ضوابط الأمن السيبراني للحوسبة السحابية*. تم الاسترجاع من خلال https://nca.gov.sa/legislation?slug=controls-&item=179 list

هيئة الإتصالات والفضاء والتقنية. (2022). *ماهي الحوسبة السحابية*. تم الاسترجاع من خلال: https://www.cst.gov.sa/ar/Digitalknowledge/Pages/cloudcomputing.aspx

Al-Shqeerat, k., Al-Shrouf, F., Hassan, M.,& Fajraoui, H. (2017). Cloud Computing Security Challenges in Higher Educational Institutions - A Survey. International Journal of Computer Applications, 161(6), 22-29. Retrieved from https://www.researchgate.net/profile/Khalil-Al-Shqeerat/publication/315111319_Cloud_Computing_Security_Challenges_in_Higher_Educational_Institutions_-A_Survey/links/58ca98e2aca272a5508ab1bc/Cloud-Computing-Security-Challenges-in-Higher-Educational-Institutions-A-Survey.pdf?origin=publication_detail

Liando, O. E. S., Kapahang, M. R., & Batmetan, J. R. (2022). Cloud Security Adoption Factors in Educational Institutions. International Journal of Information

Technology and Education (IJITE), 1(3), 117-126. Retrieved from https://www.ijite.jredu.id/index.php/ijite/article/view/67

Mary, A. C., & Rose, A. L. (2019). Implications, Risks and Challenges of Cloud Computing In Academic Field – A State-Of-Art. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 8(12), 3268-3278. Retrieved from Implications, Risks And Challenges Of Cloud Computing In ...International Journal of Scientific & Technology Researchhttp://www.ijstr.org › final-print › dec2019 › I...

Tout, S., Sverdlik, W., &Lawver, G. (2009). Cloud Computing and its Security in Higher Education. Retrieved from https://www.researchgate.net/profile/Samir-Tout/publication/255618308_Cloud_Computing_and_its_Security_in_Higher_Education/links/553841300cf226723ab62be6/Cloud-Computing-and-its-Security-in-Higher-Education.pdf?origin=publication_detail

Al-Shqeerat, k., Al-Shrouf, F., Hassan, M., &Fajraoui, H. (2017). Cloud Computing Security Challenges in Higher Educational Institutions - A Survey. International Journal of Computer Applications,161 (6), 22-29. Retrieved from https://www.researchgate.net/profile/Khalil-Al-Shqeerat/publication/315111319_Cloud_Computing_Security_Challenges_in_Higher_Educational_Institutions_-A_Survey/links/58ca98e2aca272a5508ab1bc/Cloud-Computing-Security-Challenges-in-Higher-Educational-Institutions-A-Survey.pdf?origin=publication_detail

Azure. (n.d). *What is a public cloud*?. Retrieved from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-public-cloud/

Azure. (2021). *Strengthen your security posture with Azure*. Retrieved fromhttps://azure.microsoft.com/en-us/explore/security/

Chaudhary, A. (2023). *Cloud Security Threats to Watch Out for in 2023: Predictions and Mitigation Strategies.* CSA. Retrieved by https://cloudsecurityalliance.org/blog/2023/06/29/cloud-security-threats-to-watch-out-for-in-2023-predictions-and-mitigation-strategies/

CIS. (n.d). *CIS Benchmarks*. Retrieved by https://www.cisecurity.org/cis-benchmarks-overview

CSA. (2021). Cloud Controls Matrix (CCM). Retrieved by https://cloudsecurityalliance.org/research/cloud-controls-matrix/

CSA. (2021). *Security, Trust, Assurance and Risk (STAR).* Retrieved by https://cloudsecurityalliance.org/star/

IBM. (n.d). *What is cloud security*?. Retrieved by https://www.ibm.com/topics/cloud-security#How+should+you+approach+cloud+security%3F%09%09%09%09%09%09%09

ISACA. (n.d). *Why COBIT*. Retrieved by https://www.isaca.org/resources/cobit

Iso. (2015). *ISO/IEC 27017:2015.* Retrieved by https://www.iso.org/standard/43757.html

Iso. (2019). *ISO/IEC 27018:2019*. Retrievedby https://www.iso.org/standard/76559.html

Iso. (2022). *ISO/IEC 27001:2022.* Retrieved by https://www.iso.org/standard/27001

Liando, O. E. S., Kapahang, M. R., & Batmetan, J. R. (2022). Cloud Security Adoption Factors in Educational Institutions. International Journal of Information Technology and Education (IJITE), 1(3), 117-126. Retrieved from https://www.ijite.jredu.id/index.php/ijite/article/view/67

Mary, A. C., &Rose, A. L. (2019). Implications, Risks And Challenges Of Cloud Computing In Academic Field – A State-Of-Art. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 8(12), 3268-3278. Retrieved from Implications, Risks And Challenges Of Cloud Computing In ...International Journal of Scientific & Technology Researchhttp://www.ijstr.org › final-print › dec2019 › I...

Mogull, R., Arlen, J., Gilbert, F., Lane, A., Mortman, D., Peterson, G., &Rothman, M. (2021). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. CSA. Retrieved by https://cloudsecurityalliance.org/artifacts/security-guidance-v4/#related_resources

NIST. (2005). Announcing Draft Federal Information Processing Standard (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems. Retrieved by https://csrc.nist.gov/News/2005/Announcing-Draft-FIPS-Publication-200

NIST. (2011). *NIST SP 800-144 Guidelines on security and privacy in public cloud computing*. Retrieved by https://csrc.nist.gov/pubs/sp/800/144/final

NIST. (2011). The NIST Definition of Cloud Computing. Retrieved byhttps://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Pci. (2022). *Document library*. Retrieved by https://www.pcisecuritystandards.org/document_library/?document=pci_dss

Wendy., &Gunawan, W. (2019). MEASURING INFORMATION SECURITY AND CYBERSECURITY ON PRIVATE CLOUD COMPUTING. Journal of Theoretical and Applied Information Technology, 97(1), 156-168. Retrieved from http://www.jatit.org/volumes/Vol97No1/14Vol97No1.pdf

Arab International Journal of Information Technology & Data
Vol. 4, No. 2 April - June 2024

The Reality of Cloud Cybersecurity in Taibah University: a case study

By

Marwah raja alkadi

Faculty of Arts and Humanities
King Abdulaziz University
Jeddah-Saudi Arabia
marwa.alkadi12@gmail.com

Supervisor by

Dr. Suzan Ahmad Sultan

Faculty of Arts and Humanities
King Abdulaziz University
Jeddah-Saudi Arabia
suzanlegend@gmail.com

Abstract:

From an operational, administrative and scientific perspective, cyber security is one of the most important factors affecting the quality of the educational process and the continuity of operations in universities. Therefore, it is crucial to take the necessary security measures to ensure the security of cloud computing. The aim of this study was to identify the key cybersecurity issues in cloud computing and clarify the cybersecurity regulations for cloud computing in the Kingdom of Saudi Arabia. In addition, the study comprehensively examined the current state of cybersecurity for cloud computing at Taibah University. The study used a descriptive methodology that included analytical aspects and a case study, and used a checklist based on cybersecurity controls for cloud computing issued by the National Cybersecurity Authority as a data collection tool. The data were supplemented by content analysis of primary sources from the cybersecurity department of the Taibah University website and open-ended interviews with a sample of participants consisting of cybersecurity engineers and IT engineers from Taibah University. The study found several findings, including the need to implement security controls and standards to ensure the security of data and content stored in the cloud. It

was also highlighted that the cybersecurity controls for cloud computing aim to achieve national cybersecurity objectives by focusing on cloud computing services from the perspective of service providers and subscribers and improving cyber risk preparedness across all cloud computing services. Additionally, the study found that cybersecurity regulations for cloud computing are highly implemented at Taibah University. The study also recommended that the National Cybersecurity Authority provide guidelines on the necessary security measures and practices to protect cyber systems and networks. The aim is to ensure the effective implementation of all relevant controls. In addition, the study proposed collaboration between Taibah University and cloud service providers in the Kingdom of Saudi Arabia to ensure rapid response and compliance with government regulations and laws and to support the local economy. The study encourages further research in the area of cybersecurity for cloud computing by conducting studies to measure the level of implementation of cybersecurity regulations and standards for cloud computing in higher education institutions.

Keywords: Cyber security; Cloud Computing; Cloud security