Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Journal of University Studies for Inclusive Research
Vol.3, Issue 33 (2024), 14738- 14754
USRIJ Pvt. Ltd

تحليل مفاهيم الأمان السيبراني في بيئات الحوسبة السحابية في القطاع التعليمي

الملخص:

جاءت هذه الدراسة لتحليل مفاهيم الأمان السيبراني في بيئات الحوسبة السحابية بالقطاع التعليمي، بهدف تعزيز الوعي بين الإداريين والمعلمين والطلاب حول الجرائم السيبرانية التي قد تؤثر على القيم الأساسية والنظام التعليمي. إذ تهدف الدراسة إلى فهم الواقع الحالي للأمن السيبراني، والتعرف على التحديات التي تواجه تفعيله، واستكشاف الآليات المقترحة لتحسينه. اعتمدت الدراسة على المنهج الوصفي وجمعت بياناتها من الدراسات السابقة والملاحظات المباشرة. أسفرت النتائج عن اقتراح آليات لزيادة فعالية الأمان السيبراني، مثل نشر الوعي لدى القيادات والمعلمين، وتعزيز وعي الطلاب بمخاطر الروابط الضارة. تكمن أهمية الدراسة في كونها تسهم في تحسين جودة واستمرارية العملية التعليمية من خلال تطوير استراتيجيات شاملة لحماية الأنظمة التعليمية من المخاطر السيبرانية.

الكلمات المفتاحية: *السيبراني، الأمان السيبراني، الحوسبة السحابية، القطاع التعليمي*

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Abstract:

This study analyzes cybersecurity concepts in cloud computing environments within the educational sector, aiming to enhance awareness among administrators, teachers, and students about cybercrimes that may impact core values and the educational system. The study seeks to understand the current state of cybersecurity, identify challenges in its implementation, and explore proposed mechanisms for its improvement. Utilizing a descriptive methodology, the study collected data from previous research and direct observations. The findings propose mechanisms to boost cybersecurity effectiveness, such as increasing awareness among leaders and teachers and enhancing student awareness of harmful links. The study is significant as it contributes to improving the quality and continuity of the educational process by developing comprehensive strategies to protect educational systems from cybersecurity threats.

Key words: *Cyber, Cyber security, Cloud Computing, Education Sector*

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

١. المقدمة:

يعيش العالم اليوم تحولات هائلة في المجالات التكنولوجية، مما يؤثر بشكل كبير على العملية التعليمية. تتسارع التغيرات التكنولوجية والابتكارات الرقمية، مما يتيح للأدوات الرقمية فرصة لتعزيز فعالية التعليم التقليدي. يتجلى تأثير هذه التحولات في قدرة الأدوات التكنولوجية على دعم وتحسين تجربة التعلم عن بعد، مما يجعلها أداة قوية في تعزيز وتسهيل التعليم . ساهمت الحوسبة السحابية بشكل كبير في تجاوز التحديات التي أفرزتها جائحة فيروس كورونا على العملية التعليمية. عندما تم إغلاق المدارس والجامعات في العديد من البلدان، كان التحول إلى التعلم عن بُعد ضرورة ملحة، حيث وفرت الحوسبة السحابية الحلول المناسبة لهذا التحدي. من خلال هذه التقنية، تمكن الطلاب من متابعة دراستهم والوصول إلى المحتوى التعليمي والأدوات اللازمة عبر الإنترنت. وفي الوقت نفسه، استطاع أعضاء هيئة التدريس إدارة الموارد التعليمية، وتوزيع الواجبات والاختبارات، ومراقبة تقدم الطلاب عن بُعد بكل سهولة (القاضي و سلطان، ٢٠٢٤).

مع تزايد الاعتماد على التكنولوجيا والحوسبة السحابية في التعليم، يصبح تأمين الأنظمة التعليمية أمرًا بالغ الأهمية. تتطلب الحماية من المخاطر السيبرانية إجراءات وقائية قوية لضمان سلامة المعلومات وحمايتها من الهجمات. من الضروري تبني استراتيجيات أمان متعددة الطبقات تشمل تدابير قوية لمراقبة وحماية البيانات . لذا، فإن من الأهمية بمكان تطوير بنية تحتية تعليمية آمنة وموثوقة، مع التركيز على تعزيز الإجراءات الأمنية للحفاظ على سلامة المعلومات وضمان استمرارية العملية التعليمية بشكل فعّال. ونظرًا لما قد تسببه المخاطر من خسائر مادية واقتصادية واجتماعية، اتجهت العديد من الدول المتقدمة إلى تبني مبادرات تهدف إلى تعزيز الأمن السيبراني لجميع مستخدمي الإنترنت، وخصوصًا الطلاب في المدارس (المنتشري ، ٢٠٢٠). لتحقيق أقصى استفادة من المنصات التعليمية في التعليم العام وتقليل الهدر الناتج عن الاستخدام غير الآمن لها، أصبح الأمن السيبراني جزءًا أساسيًا من أي سياسات أمنية أو اقتصادية أو سياسية على مستوى العالم. إذ بدأ صناع القرار في مختلف الدول بإعطاء الأولوية للأمن السيبراني في استراتيجياتهم (الصحفي و مصباح، ٢٠١٩). لذا تأتي هذه الدراسة لتحليل مفاهيم الأمان السيبراني في بيئات الحوسبة السحابية في القطاع التعليمي.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

١,١ مشكلة الدراسة:

في عصر العولمة والانفتاح الإلكتروني، الذي يعتمد بشكل رئيسي على المعرفة المتاحة عبر شبكة الإنترنت، أصبحت المجتمعات والمؤسسات التربوية تعتمد بشكل متزايد على الأنظمة المعلوماتية. يتجلى هذا الاعتماد في الاستخدام المكثف للأجهزة المتصلة بالشبكة مثل الهواتف الذكية، وأجهزة الكمبيوتر الشخصية، والأجهزة اللوحية، والتي تسهم في زيادة عدد المتصلين بالفضاء السيبراني (الخضرى، سلامي، و كليب، ٢٠٢٠).

ومع هذا الارتفاع في الاتصال، تزداد أيضًا المخاطر المرتبطة بالاعتداءات المعلوماتية واختراقات الأمن الرقمي. وقد أشار الأصفر(٢٠١١) في دراسته إلى أن هذه الظاهرة تبرز بوضوح في ظل تطور وسائل الاتصال والاعتماد المتزايد على التقنية، مما يتطلب تعزيز التدابير الأمنية لحماية المعلومات والأصول الرقمية. إذ تشير الدراسات إلى أن الاستخدام المتزايد للإنترنت وتطبيقاته المتنوعة يتطلب تعزيز الأمان السيبراني كحل رئيسي للحد من المخاطر المرتبطة بالإساءة. تتضمن هذه المخاطر المحتويات غير المشروعة التي تؤثر سلباً على القيم والأخلاقيات الاجتماعية، مما قد يؤدي إلى تغييرات في سلوك الأفراد، وزيادة في الجرائم عبر التقليد أو ممارسة ألعاب تحفز على سلوكيات منحرفة. وبالتالي، يصبح من الضروري بناء مجتمع واعٍ قادر على التعامل مع هذه المخاطر بوعي قانوني وأخلاقي (الصانع، السواط، و أبوعيشة، ٢٠٢٠). ورغم الجهود الكبيرة التي تبذلها الدول في تعزيز الأمن السيبراني، والتي لا تزال مستمرة، إلا أن هذا المجال يظل من الموضوعات البحثية الحديثة التي لم تلقَ الاهتمام الكافي في الأبحاث العلمية داخل المؤسسات التعليمية (الظويفري، ٢٠٢١). وفي ظل ضعف الوعي بمفاهيم الأمان السيبراني بين الطلاب، وعدم إدراكهم للمخاطر المحتملة عبر الإنترنت، تبرز الحاجة إلى توعية شاملة تشمل الإداريين والمعلمين والطلاب في كافة المراحل التعليمية. يجب تحذيرهم من الجرائم السيبرانية التي قد تستهدف بنية الوطن وقيمه الأساسية، وذلك بهدف تحسين الاستفادة من المنصات التعليمية وتقليل الهدر التعليمي. وفي ضوء ما سبق تمثلت مشكلة الدراسة في العمل على **تحليل مفاهيم الأمان السيبراني في بيئات الحوسبة السحابية في القطاع التعليمي.**

١,٢ أسئلة الدراسة:

تمثلت أسئلة الدراسة فيما يلي:

١. ما واقع الأمن السيبراني للحوسبة السحابية في القطاع التعليمي؟

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

٢. ما التحديات التي تواجه تفعيل الأمن السيبراني في القطاع التعليمي؟

٣. ما الآليات المقترحة لزيادة فعالية الأمن السيبراني في القطاع التعليمي؟

١,٣ أهداف الدراسة:

تسعى الدراسة لتحقيق الأهداف التالية:

١. التعرف على واقع الأمن السيبراني للحوسبة السحابية في القطاع التعليمي.

٢. الكشف عن التحديات التي تواجه تفعيل الأمن السيبراني في القطاع التعليمي.

٣. التعرف على الآليات المقترحة لزيادة فعالية الأمن السيبراني في القطاع التعليمي.

١,٤ أهمية الدراسة:

تأتي أهمية الدراسة من أهمية الموضوع المتناول حيث يعتبر الأمن السيبراني موضوعًا حيويًا وذا أهمية بالغة، كما أنه من العوامل الأساسية التي تؤثر بشكل كبير على جودة العملية التعليمية واستمراريتها. حيث يتطلب الحفاظ على سلامة المعلومات وإدارة الأنظمة التعليمية اتخاذ تدابير أمنية دقيقة وفعالة. لذلك، فإن البحث في أهمية الأمان السيبراني وتطوير استراتيجيات شاملة لحماية البيانات أصبح ضرورة ملحة لضمان استقرار البيئة التعليمية . كما أَصبح من الضروري أن يكون هناك اهتمام خاص بالبحث وتطوير استراتيجيات فعّالة لحماية الأنظمة التعليمية من المخاطر السيبرانية، حيث تسهم هذه الدراسات في تعزيز الفهم والتعامل مع التهديدات الأمنية في بيئات الحوسبة التعليمية بالإضافة إلى ذلك، قد تساعد هذه الدراسة في توجيه أنظار الباحثين والقائمين على إدارة ورعاية القطاعات التعليمية نحو تعزيز الوعي بمفاهيم الأمن السيبراني وكيفية التصدي لها.

١,٥ مصطلحات الدراسة:

الأمن السيبراني: هو مجال متخصص يركز على حماية المعلومات وكل ما يتعلق بها من عمليات وخدمات وأجهزة وتقنيات. يهدف إلى تأمين هذه المعلومات من الوصول غير المصرح به، وكذلك من الاستخدام الضار الذي قد يهدد الأفراد أو الجهات المعنية. يشمل الأمن السيبراني حماية الشبكات والبرمجيات والبيانات من الهجمات والتلف، بالإضافة إلى تأمين الأجهزة والبيانات ضد أي تهديدات قد تؤدي إلى تجاوز الأذونات المصرح بها (المنتشري ، ٢٠٢٠).

ويعرف الأمن السيبراني إجرائياً :بأنه مجموعة الإجراءات التي يتخذها القادة والمعلمون والمديرون لحماية شبكات المعلومات من جميع الأنشطة والممارسات التي تهدف إلى التلاعب بالبيانات. يتضمن ذلك حماية

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

المعلومات من الاختراقات والبرمجيات الخبيثة والفيروسات، بالإضافة إلى التصدي للتنمر الإلكتروني، وإدارة الوصول غير المصرح به، والتعامل مع كافة الممارسات الإلكترونية الضارة الأخرى.

الحوسبة السحابية: هي تقنية تقدم خدمات حوسبة عبر الإنترنت، مما يتيح للمستخدمين الوصول إلى الموارد الحاسوبية مثل الخوادم والتخزين وقواعد البيانات والتطبيقات عبر الشبكة. حيث تتيح هذه التقنية التوسع السلس في الموارد وتوفير الوصول إليها عن بُعد، دون الحاجة إلى امتلاك أو إدارة الأجهزة المادية (القاضي و سلطان، ٢٠٢٤).

تُعرَّف الحوسبة السحابية إجرائياً: بأنها مجموعة من الخدمات التقنية التي تُقدّم للمستخدمين عبر الإنترنت، وتشتمل على مجموعة متنوعة من الموارد مثل الخوادم وقواعد البيانات والتطبيقات. تتميز هذه الخدمات بتكلفة أقل مقارنةً بالخدمات التقنية التقليدية.

١,٦ منهجية الدراسة:

لتحقيق أهداف البحث والتمكن من الإجابة على أسئلته سيعتمد الباحث على المنهج الوصفي، الذي يعتمد على وصف وتحليل الظواهر كما هي دون التلاعب بالمتغيرات. حيث يعتمد هذا المنهج على جمع البيانات من خلال الدراسات السابقة والملاحظات المباشرة لتقديم صورة واضحة وشاملة عن موضوع الدارسة.

١,٧ الدراسات السابقة:

في هذا الجزء، سنلقي نظرة موجزة على مجموعة من الدراسات السابقة ذات الصلة التي تمثل الإطار الفكري للبحث الحالي. تم استعراض عدد من المصادر والمراجع العلمية التي تناولت المتغيرات ذات الصلة بالدراسة الحالية.

ركزت دراسة **(القاضي و سلطان، ٢٠٢٤)** على تحليل أبرز جوانب الأمان السيبراني في الحوسبة السحابية وتوضيح المعايير الأمنية المتعلقة بها في المملكة العربية السعودية. كما شملت الدراسة تقييم الوضع الفعلي للأمان السيبراني في الحوسبة السحابية بجامعة طيبة. استخدمت الدراسة المنهج الوصفي من خلال التحليل ودراسة الحالة، واعتمدت على قائمة مراجعة معدة وفقًا لضوابط الأمان السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني كأداة لجمع البيانات. تم جمع المعلومات من خلال تحليل محتوى المصادر الأولية من موقع جامعة طيبة وإجراء مقابلات مفتوحة مع مهندسي الأمان السيبراني وتقنية المعلومات في الجامعة. وجدت الدراسة ضرورة تطبيق الضوابط الأمنية لحماية البيانات والمحتوى المخزن في السحابة، وأوصت

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

بإنشاء دليل إرشادي من الهيئة الوطنية للأمن السيبراني يتضمن التدابير والممارسات الأمنية اللازمة لحماية الأنظمة والشبكات السيبرانية.

سعت دراسة **(الكردي، ٢٠٢١)** إلى استكشاف واقع الأمن السيبراني والتعلم الإلكتروني في جامعات فلسطين من منظور أعضاء هيئة التدريس، باستخدام جامعة النجاح الوطنية كمثال. اعتمد الباحث على المنهج الوصفي نظراً لملاءمته لأهداف الدراسة. شملت عينة الدراسة ٥٠ عضو هيئة تدريس من أصل المجتمع الكلي في الجامعة. أظهرت نتائج الدراسة وجود فروق ذات دلالة إحصائية في واقع التعليم الإلكتروني بين كليات التربية الرياضية، حيث أظهرت الفروق تبايناً في معوقات استخدام التعليم الإلكتروني بين المحاضرين بناءً على سنوات الخبرة، حيث كانت الفروقات لصالح المحاضرين ذوي الخبرة التي تتجاوز ١٠ سنوات مقارنة بالذين تقل خبرتهم عن ٥ سنوات. في حين لم تكن هناك فروق دالة إحصائياً في المجالات الأخرى المتعلقة بثقافة الطلاب ومتغيراتهم.

جاءت دراسة **(المنتشري ، ٢٠٢٠)** لتقييم دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من منظور المعلمات. استخدمت الدراسة المنهج الوصفي التحليلي، حيث تم إعداد استبانة وتطبيقها على عينة مكونة من ٤٢٠ معلمة في عدة مدارس حكومية. أظهرت نتائج الدراسة أن الدور الذي تلعبه القيادة المدرسية في تعزيز الأمن السيبراني، سواء بالنسبة للمعلمات أو الطالبات، يتسم بفعالية محدودة، خصوصاً في الجوانب التوعوية مثل تنظيم أيام مفتوحة أو ندوات أو دورات تدريبية للتعريف بالأمن السيبراني، بالإضافة إلى نشرات توعوية بشأن أخلاقيات الأمن السيبراني. بناءً على هذه النتائج، اقترحت الدراسة تصوراً لتطوير دور القيادة المدرسية في تعزيز الأمن السيبراني، والذي يتضمن تنسيقًا مع الجهات المختصة بالأمن السيبراني في المملكة العربية السعودية، فضلاً عن اتخاذ إجراءات لحماية البيئة المادية لشبكة الإنترنت. وشمل التصور آليات محددة تتعلق بالمعلمات والطالبات على حد سواء، وأخرى تتعلق بتكامل الجهود بينهما.

تناولت دراسة **(Liando, Kapahang, & Batmetan, 2022)** مسألة أمان المعلومات في المؤسسات التعليمية، مع التركيز على العوامل التي تؤثر في تبني إجراءات الأمان في هذا السياق. تمثل الهدف الرئيسي للدراسة في استكشاف أهمية الحفاظ على أمان المعلومات وتقييم التحديات التي تواجه المؤسسات التعليمية عند تطبيق استراتيجيات الأمان الخاصة بالبيانات. اعتمدت الدراسة على تحليل شامل للأدوات والممارسات الحالية في مجال حماية المعلومات، بما في ذلك استراتيجيات الإدارة والتقنيات المعتمدة. أظهرت النتائج

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

ضرورة توفير حماية قوية للبيانات والتعامل مع التهديدات التي تواجه المؤسسات التعليمية بشكل فعال. كما أبرزت الدراسة أهمية التوعية والتدريب للموظفين حول أمان المعلومات والقدرة على تحديد وتفادي المخاطر المحتملة. أوصت الدراسة بضرورة أن تعتمد المؤسسات التعليمية على معايير مثل ISO 27001 أو COBIT لتحسين مستوى الأمان وحماية البيانات بشكل موثوق.

قدمت دراسة **(Wendy & Gunawan, 2019)** تقييم لفعالية أمان المعلومات والأمن السيبراني في نظم المعلومات الإدارية الخاصة بالمؤسسات التعليمية، جامعة XYZ أنموذجاً. استخدمت الدراسة منهجيات كمية ونوعية لجمع وتحليل البيانات، حيث تم توزيع استبيان على قسم تكنولوجيا المعلومات في جامعةXYZ ، وتم الحصول على ردود من ١١ مشاركًا. تم تحليل البيانات باستخدام برنامج.Excel أظهرت نتائج الدراسة أهمية تعزيز أمان المعلومات والأمن السيبراني في نظم المعلومات الإدارية الخاصة بجامعة XYZ، وركزت على تحسين سياسات الأمان وإجراءات الحماية. كشفت الدراسة عن التحديات المرتبطة بالأمن السيبراني وأمان المعلومات في الجامعة، وأوصت بضرورة تنفيذ سياسات شفافة وتحديث الإجراءات الأمنية بشكل دوري. كما اقترحت الدراسة تبني معايير مثل ISO 27001:2013 وCOBIT لتعزيز أمان المعلومات وتحسين الأداء الأمني في المؤسسات التعليمية.

أجرى **كوريجان وروبرتسون (Corrigan & Robertson, 2015)** دراسة تستهدف استكشاف دور قادة المدارس في التصدي للجرائم السيبرانية في كندا. شملت الدراسة مقابلات مع تسعة من مديري مدارس كندية، وكشفت النتائج أن هؤلاء القادة يلعبون أدواراً محورية في التصدي للجرائم السيبرانية، حيث يقومون بتحركات سريعة عند حدوث مثل هذه الجرائم ويتعاونون مع أولياء الأمور لمتابعتها. بالإضافة إلى ذلك، أظهرت الدراسة أهمية دور قادة المدارس في وضع سياسات تدعم الاستخدام الآمن للإنترنت والاستجابة للأحداث السيبرانية التي قد تحدث خارج نطاق المدرسة.

٢. الإطار النظري:

٢,١ الحوسبة السحابية:

٢,١,١ مفهوم الحوسبة السحابية:

قدمت هيئة الاتصالات والفضاء والتقنية تعريفاً للحوسبة السحابية باعتبارها نموذجاً يتيح الوصول الشبكي السريع والمرن إلى مجموعة من الموارد الحاسوبية القابلة للتخصيص، مثل الخوادم والشبكات والتخزين والخدمات البرمجية والتطبيقات. يتم توفير هذه الموارد وإتاحتها بسرعة مع أقل

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

قدر من الجهد الإداري أو الحاجة للتفاعل المباشر مع مزودي الخدمة (هيئة الاتصالات والفضاء والتقنية، ٢٠٢٢). من جهة أخرى، يعرف تحالف أمن الحوسبة السحابية الحوسبة السحابية كنموذج تشغيلي حديث يتضمن مجموعة من التقنيات لإدارة تجمعات مشتركة من موارد الحوسبة. تتميز هذه التقنية بقدرتها على تعزيز التعاون، والمرونة، والتوسع، والتوافر، مما يوفر فرصاً لتقليل التكاليف وزيادة فعالية الأداء. يصف نموذج السحابة عالماً يمكن فيه تنظيم وتوفير وتنفيذ وإيقاف تشغيل المكونات بسرعة، مع إمكانية توسيع أو تقليص نطاقها حسب الحاجة، مما يوفر نموذجاً شبيهاً بالمرافق عند الطلب للتخصيص والاستهلاك (Mogull, et al., 2021). كما يُنظر إلى الحوسبة السحابية كنموذج يتيح الوصول الشبكي في كل مكان وبشكل ملائم وعند الطلب إلى مجموعة مشتركة من الموارد الحاسوبية القابلة للتخصيص، مع القدرة على توفيرها وإصدارها بسرعة وبأقل جهد إداري أو تفاعل مع مزود الخدمة (NIST, 2011).

من خلال ما سبق، يمكن تعريف الحوسبة السحابية على أنها مجموعة من الخدمات التقنية التي يتم تقديمها للمستخدمين عبر الإنترنت. تشمل هذه الخدمات موارد مثل الخوادم وقواعد البيانات والشبكات والبرمجيات. تتميز الحوسبة السحابية بتقديمها تكلفة أقل ، مما يجعلها خياراً اقتصادياً أكثر فاعلية.

٢,١,٢ خصائص الحوسبة السحابية:

تتمتع الحوسبة السحابية بعدد من الخصائص المميزة، والتي تشمل:

١. الخدمة الذاتية عند الطلب: يتيح النظام للمستخدمين الحصول على خدمات الحوسبة تلقائيًا من جانبهم دون الحاجة إلى تدخل بشري مباشر مع مزودي الخدمة، مما يوفر مرونة عالية في إدارة المتطلبات حسب الحاجة (Mogull, et al., 2021).
٢. الوصول الشبكي الواسع: يتم توفير الخدمات عبر الشبكة بحيث يمكن الوصول إليها من خلال أدوات وطرق قياسية مثل أجهزة الكمبيوتر المحمولة والهواتف الذكية، مما يتيح للمستخدمين التفاعل مع الخدمات عبر منصات متنوعة (هيئة الاتصالات والفضاء والتقنية، ٢٠٢٢).
٣. تجميع الموارد: يتم تجميع الموارد الحاسوبية لتلبية احتياجات العديد من المستخدمين عبر نموذج متعدد المستأجرين، حيث يتم تخصيص وإعادة تخصيص الموارد المالية والافتراضية بشكل

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

ديناميكي وفقًا لاحتياجات العملاء. عادةً ما يكون لدى المستخدمين مستوى محدود من التحكم أو المعرفة بموقع الموارد، لكن يمكنهم تحديد الموقع على مستوى أعلى(NIST, 2011) .

٤. المرونة والسرعة: توفر الحوسبة السحابية إمكانية توسيع أو تقليص نطاق الموارد بسرعة وكفاءة، مع إمكانية التعديل التلقائي في بعض الحالات. يمكن للمستخدمين الحصول على الخدمات غير المحدودة في أي وقت وبكميات كبيرة (هيئة الاتصالات والفضاء والتقنية، ٢٠٢٢).

٥. قياس الخدمة: تتيح الحوسبة السحابية قياس استخدام الموارد بدقة وفقًا لمستوى معين من التجريد، بما يتناسب مع نوع الخدمة مثل التخزين، وسعة النطاق، والمعالجة، وحسابات المستخدمين النشطة. هذا يسمح بحساب وتقييم استخدام الموارد وتوفير الشفافية لكل من مزود الخدمة والمستخدم (هيئة الاتصالات والفضاء والتقنية، ٢٠٢٢).

٢,١,٣ فوائد الحوسبة السحابية:

تتمتع الحوسبة السحابية بعدد من الفوائد الرئيسية، أبرزها (الهيئة السعودية للبيانات والذكاء الاصطناعي، ٢٠٢٣):

- تقليل التكاليف: تقلل الحوسبة السحابية من النفقات المرتبطة بشراء وإعداد وتشغيل وصيانة الخدمات التقنية، مما يسرع من عملية التحول الرقمي.
- مرونة الخدمات: توفر القدرة على تلبية الطلب المتزايد على الخدمات الإلكترونية خلال أوقات الذروة دون التأثير على استمرارية الخدمة.
- استمرارية الأعمال: تعزز الحوسبة السحابية الاستعداد للتعامل مع الانقطاعات المحتملة التي قد تنتج عن الكوارث الطبيعية أو الهجمات السيبرانية أو غيرها من الأسباب.
- تشغيل التقنيات المتقدمة: تدعم تشغيل التقنيات الحديثة مثل الذكاء الاصطناعي وتعلم الآلة، التي تتطلب موارد حوسبة قوية ومساحات تخزين واسعة.
- مواكبة التطورات: تسهم في تحديث البنية التحتية والتخزين والمعالجة بشكل مستمر لمواكبة أحدث التطورات التقنية حسب الحاجة.
- الموثوقية والأمان: تضمن الحوسبة السحابية استخدام أحدث الأساليب والتقنيات لحماية البيانات والأنظمة، بالإضافة إلى إجراء تحديثات دورية لمواجهة أي تهديدات أمنية.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

٢,٢ الأمن السيبراني:

٢,٢,١ مفهوم الأمن السيبراني:

شهدت تكنولوجيا المعلومات تطوراً هائلاً خلال العقدين الماضيين، مما أدى إلى ظهور ما يُعرف بالفضاء السيبراني، وهو مفهوم أوسع يتيح للناس الوصول إلى المعلومات في جميع المجالات ومن أي مكان حول العالم. مع ذلك، أدت هذه الفرص إلى ظهور مشاكل في الفضاء السيبراني، حيث زادت الجرائم السيبرانية بشكل مستمر وأصبح من الصعب ملاحقة الجناة (حيمد، ٢٠١٩).

ومع تطور تكنولوجيا المعلومات في مجال الشبكات العالمية مثل الإنترنت، أصبحت المنظمات تعتمد بشكل متزايد على حماية أمن شبكات الكمبيوتر وأجهزة الحوسبة الخاصة بها. ومع ذلك، فإن الأجهزة التنظيمية مثل أجهزة الكمبيوتر المكتبية والمحمولة والهواتف الذكية أصبحت أهدافاً متزايدة للهجمات الإلكترونية (Alexander, 2017).

يشير الأمن السيبراني إلى استخدام تقنيات الحوسبة لحماية المعدات والمعلومات والخدمات من الوصول غير المصرح به أو غير القانوني (مانيطة، ٢٠١٧). تُرتكب الجرائم السيبرانية عبر استخدام الحاسوب والإنترنت، وليس هناك فئة محددة من الناس مسؤولة عن هذه الجرائم؛ فقد يكون الجناة من مختلف الطبقات الاجتماعية، بما في ذلك الفقراء والأغنياء، والبالغين والأحداث، والرجال والنساء على حد سواء (الردفاني، ٢٠١٤). كما يمكن تعريف الأمن السيبراني بأنه "الجهود المبذولة لضمان حماية الموارد البشرية والممتلكات المرتبطة بتقنيات المعلومات والاتصالات، والحد من الأضرار والخسائر التي قد تنجم عن المخاطر والتهديدات. كما يهدف إلى استعادة الوضع إلى طبيعته بأسرع وقت ممكن لتجنب توقف الإنتاج وتحويل الأضرار إلى خسائر دائمة (الظويفري، ٢٠٢١).

ويُعرف الأمن السيبراني أيضاً بأنه الحماية التي تُبذل في البيئة الرقمية الافتراضية، حيث يمثل سيادة الدولة وحقها في حماية فضائها السيبراني المرتبط بالأمن القومي والمصالح والأهداف الحيوية (الجمل ، ٢٠٢٠). ومن ثم، يشمل الأمن السيبراني اتخاذ تدابير لحماية أجهزة الكمبيوتر والشبكات من الوصول غير المصرح به، وذلك لضمان سلامة وأمن المعلومات المخزنة على هذه الأنظمة. يمكن أن تشمل التدخلات الفنية التي تهدف إلى حماية البيانات والمعلومات الشخصية والأجهزة من التهديدات غير المصرح بها أو الأضرار، مع التركيز على تأمين الأصول الرقمية. يُعتبر الأمن السيبراني عملية متكاملة تتطلب تنسيق الموارد والعمليات والهياكل لحماية الأصول في الفضاء الإلكتروني والأنظمة التي تدعمه، من الأحداث التي قد تتعارض مع

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

الحقوق القانونية للممتلكات الفعلية . إذ تتوزع مسؤولية الأمن السيبراني بين جميع الأفراد، حيث يجب على كل مستخدم اتخاذ قرارات مدروسة بشأن كيفية الوصول إلى بياناتهم الشخصية وتخزينها، وكذلك التوجيه حول كيفية التفاعل مع أنظمة وشبكات الكمبيوتر. يمكن تحقيق أقصى فعالية من خلال تعزيز ثقافة عمل تدعم الأمن السيبراني داخل المؤسسة. ويعني ذلك أن الهيئة الحاكمة والتنفيذية للمؤسسة يجب أن توفر القيادة اللازمة لضمان حماية الموظفين والطلاب والباحثين، بالإضافة إلى حماية المؤسسة وأصحاب المصلحة من آثار انتهاكات أمن المعلومات العرضية والهجمات السيبرانية الضارة (Chapman, 2019).

في ضوء ما سبق، يمكن تعريف الأمن السيبراني في مجال التعليم على أنه حماية المعلومات والبيانات الرقمية في المؤسسات التعليمية، كالمدارس والجامعات، من الهجمات الإلكترونية، بالإضافة إلى تأمين الشبكات التعليمية لضمان سلامة الطلاب وأعضاء الهيئة التعليمية.

٢,٢,٢ التحديات والتهديدات التي تواجه الأمن السيبراني:

تزايدت الجرائم المرتكبة باستخدام تقنيات المعلومات والاتصالات، وخصوصاً عبر الإنترنت، مما أدى إلى تفاقم الخسائر المالية والبشرية، فضلاً عن التأثير على استقرار الدول وأمن الشعوب. هذا التزايد في الجرائم السيبرانية يأتي في ظل زيادة استخدام هذه التقنيات (الراظمي، ٢٠١٩).

أظهرت دراسة حديثة في مجال تكنولوجيا المعلومات أن تكاليف الجرائم السيبرانية قد تصل إلى حوالي ٦ تريليونات دولار سنوياً بحلول عام ٢٠٢١، وهو ضعف المبلغ المسجل في عام ٢٠١٥. تشمل هذه التكاليف الأضرار الناتجة عن سرقة البيانات، وتخريبها، وسرقة الأموال، وفقدان الإنتاجية، وسرقة الملكية الفكرية، والاختلاسات، والاحتيال، والتلاعب التجاري، واختراق الأنظمة، والأضرار التي تلحق بالسمعة (فوزي ، ٢٠١٩).

تشمل التهديدات الأمنية في هذا السياق الهجمات السيبرانية التي تستغل نقاط الضعف في الشبكات المعلوماتية، مما يسمح للمهاجمين بالتحكم في الأنظمة. تتمثل هذه التهديدات في الاستغلال المتعمد لأجهزة الكمبيوتر والشبكات عبر البرمجيات الضارة، ويمكن تصنيف أبرز هذه التهديدات على النحو التالي:

- الأنشطة غير المصرح بها: تتضمن مسح أو تعديل أو تعطيل أنظمة التشغيل، بما في ذلك الدخول غير المصرح به إلى نظم المعلومات والإضرار بالبيانات وتعطيل عملها، ومعالجة البيانات الشخصية دون تصريح أو ترخيص مسبق، وإنشاء معلومات شخصية لأشخاص غير مخولين بالاطلاع عليها (قارة، ٢٠١٦؛ الردفاني، ٢٠١٤).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

- البرمجيات الخبيثة: تشمل استخدام تقنيات التخمين والخداع، بالإضافة إلى البرمجيات الضارة التي تتيح الوصول إلى كلمات المرور والتحكم في الأجهزة (بونيف، ٢٠١٩).
- محاولات الاختراق: تستهدف بنية النظام التحتية مثل شبكات الاتصال، ومحطات الطاقة، وأنظمة الصرافة. تزداد تأثيرات هذه الهجمات بشكل كبير كلما كانت البنية التحتية متصلة بشبكة الإنترنت، مما يتطلب تعزيز الرقابة ووضع خطط حماية مناسبة (السرحان و المشاقبة، ٢٠٢٠).
- الاحتيال الإلكتروني: يتخذ أشكالاً متعددة، مثل الإيهام بوجود مشاريع كاذبة أو استخدام أسماء وصفات زائفة لسرقة بيانات الضحية، من خلال التلاعب عبر الشبكة أو التعامل المباشر مع بيانات الحاسب (المنتشري ، ٢٠٢٠).
- انتحال اسم المجال: يستغل نقاط الضعف في بروتوكولات الاستقبال والإرسال لمحاولة التسلل إلى النظام، بما في ذلك إعادة توجيه الرسائل أو منع إرسالها إلى أطراف معينة، نظراً لأن معظم البروتوكولات تعتمد على معلومات عامة يسهل معرفتها (السرحان و المشاقبة، ٢٠٢٠).
- الدخول والتعديل: تشمل الأفعال المتعلقة بالتحكم غير المشروع في الأجهزة أو الكلمات السرية أو الأكواد بغرض ارتكاب الجرائم السيبرانية (الردفاني، ٢٠١٤).
- الهجمات المستهدفة: تستهدف شبكة أو جهازاً معيناً بهدف سرقة معلومات هامة مثل البيانات العسكرية، الاقتصادية، الصناعية، أو التجارية، مما يترتب عليه آثار استراتيجية كبيرة على الطرف المستهدف (العيسى، ٢٠١٩).
- تسريب البيانات: من أبرز الجرائم، وتشمل الدخول غير المشروع إلى البريد الإلكتروني للآخرين وإنشاء مواقع للتشهير (فوزي ، ٢٠١٩).
- الهندسة الاجتماعية: تشير إلى خداع الأشخاص للحصول على بيانات أو معلومات خاصة كانت ستظل محمية وآمنة، بهدف اختراق النظام (الصحفي و عسكول، ٢٠١٩).
- التنمر الإلكتروني: يشير إلى استخدام تكنولوجيا الاتصالات للتحرش والإزعاج والتهديد والابتزاز، وقد تزايدت هذه الظاهرة مع انتشار الأجهزة اللوحية والهواتف الذكية (المنتشري ، ٢٠٢٠).

٢,٢,٣ آليات زيادة فعالية الأمن السيبراني:

لضمان حماية البيانات والمعلومات، يجب التركيز على مجموعة من العناصر الأساسية التالية كما يلي: (الصانع، السواط، و أبوعيشة، ٢٠٢٠):

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

- السرية والأمان: ضمان عدم تعرض المعلومات للكشف أو الوصول من قبل أشخاص غير مصرح لهم.
- تكاملية وسلامة المحتوى: التأكد من أن المحتوى يظل صحيحاً ولم يتم تعديله أو تدميره أو تغييره بشكل غير مصرح به أثناء معالجته أو تبادله، سواء داخلياً أو عبر تدخل غير مشروع.
- استمرارية توفر المعلومات أو الخدمة: ضمان استمرار عمل النظام المعلوماتي وتوفير القدرة على الوصول إلى المعلومات دون انقطاع، وعدم منع المستخدمين من الدخول إلى النظام.

وفي هذا الإطار، قدمت الهيئة الوطنية للأمن السيبراني عدداً من التوصيات لتعزيز مستوى الأمن السيبراني، كما ورد في تقرير الهيئة (٢٠٢١). تشمل هذه التوصيات تعزيز القدرة على العمل عن بُعد، مما يتيح للموظفين أداء مهامهم دون الحاجة للتواجد في مقر العمل. كما شملت التوصيات إرشادات للأمن السيبراني عن بُعد، مثل: تعزيز الوعي بأهمية الأمن السيبراني، تنظيم إدارة هويات الدخول والصلاحيات، تأمين الأنظمة وأجهزة معالجة البيانات، إدارة أمن الشبكات بفعالية، تطبيق التشفير لحماية المعلومات، مراقبة النشاطات السيبرانية بشكل مستمر، وإدارة الحوادث بشكل متقن. بالإضافة إلى ذلك، قدمت الهيئة مجموعة من المبادرات والبرامج الوطنية التي تسعى إلى تحسين فعالية الأمن السيبراني على مستوى واسع (الهيئة الوطنية للأمن السيبراني ، ٢٠٢٠).

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

قائمة المراجع:

الصحفي، حمد حامد و مصباح، صالح (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. *مجلة البحث العلمى فى التربية*، ٢٠(الجزء العاشر), ٤٩٣-٥٣٤.

الأصفر، أحمد (٢٠١١). *عوامل ارتفاع معدلات الجريمةالمستحدثة وسبل مواجهتها* . الرياض: جامعة نايف العربية للعلوم الأمنية.

فوزي، إسلام (٢٠١٩). الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجي . *المجلة الاجتماعية القومية: المركز القومي للبحوث الاجتماعية والجنائية*، ٥٦(٢): ٩٩-١٣٣.

الهيئة السعودية للبيانات والذكاء الاصطناعي (٢٠٢٣). *الحوسبة السحابية: تجارب عالمية* . المملكة العربية السعودية: SDAIA.

الهيئة الوطنية للأمن السيبراني (٢٠٢٠). *االستراتيجية الوطنية لألمن السيبراني*. المملكة العربيةالسعودية: الهيئة الوطنية للأمن السيبراني.

الخضرى، جيهان؛ و سلامي، هدى؛ وكليب، و نعمة (٢٠٢٠). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية. *مجلة تطوير الأداء الجامعى*، ١٢(١), ٢١٧-٢٣٣.

الجمل، حازم (٢٠٢٠). الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠. *مجلة البحوث الأمنية: كلية الملك فهد الأمنية - مركز الدراسات*، مج٣٠, ع٧٧، ٢٤٣-٣٢٨.

السرحان، حنان ، و المشاقبة، محمد (٢٠٢٠). *أثر تطبيق سياسة الأمن السيبراني على جودة املعلومات املحاسبية في البنوك التجارية ألردنية*. المفرق: جامعةآل البيت.

بونيف، سامي (٢٠١٩). دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني أنموذجا. المجلة الجزائرية للحقوق والعلوم السياسية: المركز الجامعي أحمد بن يحي الونشريسي تيسمسيلت. *معهد العلوم القانونية والإدارية*، ٤ (٧) ١٢١-١٣٥.

الراظمي، سيدي (٢٠١٩). الجريمة السيبرانية وتكاملية النص الوطني، الإقليمي والدولي. . *مجلة القانون والأعمال: جامعة الحسن الأول*، ٤٧ (٢٤-٣٤).

العيسى، طلال (٢٠١٩). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر. *مجلة الزرقاء للبحوث والدراسات الإنسانية-جامعة الزرقاء*، ٨١-٩٥.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

الصانع عمر؛ والسواط، حمود؛ وأبوعيشة، حمد جميل (٢٠٢٠). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. *مجلة كلية التربية جامعة أسيوط*، ٣٦ (٦) ٤١-٩٠.

المنتشري، فاطمة يوسف (٢٠٢٠). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للعلوم التربوية والنفسية*، ٤(١٧), ٤٥٧-٤٨٤.

الكردي، مجدي كاظم (٢٠٢١). الأمن السيبراني والتعليم الإلكتروني في جامعات فلسطين من وجهة نظر أعضاء الهيئات التدريسية-جامعة النجاح الوطنية انموذجاً. *المجلة العربية للمعلوماتية وأمن المعلومات*، ٢(٥), ١٠٣-١٢٤.

الردفاني، محمد (٢٠١٤). تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية. *المجلة العربية للدراسات الأمنية: جامعة نايف العربية للعلوم الأمنية*، مج ٣٠ عدد ٦١ (١٥٧-١٩٢).

حيمد، محمد (٢٠١٩). رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة. *المجلة العربية الدولية للمعلوماتية: اتحاد الجامعات العربية*، ٧ (١٢) ٨٣-١٠٠.

القاضي، مروه وسلطان، سوزان أحمد (٢٠٢٤). واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة: دراسة حالة. *المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات*، ٤(٢), ١٥-٧٤.

الظويفري، مشاعل (٢٠٢١). و اقع الأمن السيبراني وزيادة فاعليته في مدارس التعليم العام بمنطقة المدينة المنورة من وجهة نظر القيادة المدرسية. *International Journal of Educational Psychological Studies (EPS)*، ١٠(٣).

الصحفي، مصباح أحمد وعسكول، سناء (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. *مجلة البحث العلمي في التربية-جامعة عين شمس*، ٢٠ (١٠) ٤٩٣-٥٣٤.

قارة، ملاك (٢٠١٦). الجريمة املعلوماتية في القطاع البنكي وأساليب مكافحتها: إشارة لحالة الجزائر. *مجلة جامعة الأمير عبد القادر للعلوم الإسلامية*، ٣٩ (١١٤-٤٣٠).

هيئة الاتصالات والفضاء والتقنية (٢٠٢٢). *ما هي الحوسبة الحسابية*.

مانيطة، يوسف (٢٠١٧). نظرة عامة عن الجريمة اإللكترونية في الفضاء السيبراني. *المجلة الليبية العالمية: جامعة بنغازي-كلية التربية بالمرج*، (٣٢) ١-١٠.

Alexander, R. (2017). *Can the analytical hierarchy process model be effectively applied in the prioritization of information assurance defense in-depth measures? - a quantitative study* . Capella University.

Chapman, J. (2019). *How Safe is Your Data?: Cyber-security in Higher Education.* . Higher Education Policy Institute.

Corrigan, L., & Robertson, L. (2015). *Inside the Digital Wild West: How School Leaders Both Access and Avoid social media.* International Association for Development of the Information Society.

Liando, O., Kapahang, M., & Batmetan, J. (2022). Cloud Security Adoption Factors in Educational Institutions. *International Journal of Information Technology and Education (IJITE)*, 1(3), 117-126.

Mogull, R., Arlen, J., Gilbert, F., Lane, A., Mortman, D., Peterson, G., et al. (2021). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. CSA. 0.*

NIST. (2011). *NIST SP 800-144 Guidelines on security and privacy in public cloud computing.* NIST.

Wendy, & Gunawan, W. (2019). MEASURING INFORMATION SECURITY AND CYBERSECURITY ON PRIVATE CLOUD COMPUTING. *Journal of Theoretical and Applied Information Technology*, 97(1), 156-168.