جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
Est. 1978

Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss

AJSS

Leveraging Cybersecurity to the Safe Use of Artificial Intelligence in Education

توظيف الأمن السيبراني لاستثمار فرص الذكاء الاصطناعي والحد من تحدياته في مجال التعليم والتعلم

بدر عدنان الخبيزي
أكاديمية سعد العبد الله للعلوم الأمنية، الكويت

Badr Adnan Al-Khubaizi
Saad Al-Abdullah Academy for Security Sciences, Kuwait

Received on 22 May 2024, accepted on 01 Sep. 2024, available online on 24 Dec. 2024

المستخلص

تهدف الدراسة إلى توظيف الأمن السيبراني لاستثمار فرص الذكاء الاصطناعي، والحد من تحدياته في مجال التعليم والتعلم؛ ولتحقيق هذا الهدف استخدمت الدراسة المنهج الوصفي، وجاءت متضمنة إطارًا عامًا، شمل مقدمة الدراسة ومشكلتها وأسئلتها وأهدافها وأهميتها وحدودها، والتعقيب عليها، ثم خمسة محاور على النحو الآتي: عرض المحور الأول: الإطار المفاهيمي للأمن السيبراني من حيث مفهومه وأهدافه وأهميته وخصائصه وأبعاده، وتناول المحور الثاني: الإطار المفاهيمي للذكاء الاصطناعي من حيث مفهومه وأهدافه وخصائصه وأهم أنواعه؛ كما تناول المحور الثالث: أبرز التحديات المترتبة على الذكاء الاصطناعي؛ وتناول المحور الرابع: أبرز الفرص المرتبطة بالذكاء الاصطناعي، وكيفية الاستفادة منها في الواقع المعاصر؛ وعني المحور الخامس: بتناول كيفية توظيف الأمن السيبراني للحد من تحديات الذكاء الاصطناعي، واستثمار فرصه، ثم اشتملت الدراسة على خاتمة، بها أبرز النتائج والتوصيات والمقترحات.

الكلمات المفتاحية: الدراسات الأمنية، الأمن السيبراني، الذكاء الاصطناعي، التحديات، الفرص.

Abstract

The study aims to employ cybersecurity to exploit the opportunities of artificial intelligence and reduce its challenges. To achieve this goal, the study used the descriptive approach, and it included a general framework that included the introduction of the study, its problems, its questions, objectives, importance, limits, previous studies and commentary on them, and then five axes as follows: The first axis presented the framework. The conceptual framework of cybersecurity in terms of its concept, objectives, importance, characteristics and dimensions. The second axis dealt with the conceptual framework of artificial intelligence in terms of its concept, objectives, characteristics and most important types. The third axis presented the most prominent challenges resulting from artificial intelligence. The fourth topic dealt with the most prominent opportunities associated with artificial intelligence and how to benefit from them in contemporary reality. The fifth axis focused on addressing how to employ cybersecurity to reduce the challenges of artificial intelligence and exploit its opportunities. The study then included a conclusion with the most prominent results, recommendations and proposals.

Keywords: *security studies, cybersecurity, artificial intelligence, challenges, opportunities.*

Production and hosting by NAUSS

* Corresponding Author: *Badr Adnan Al-Khubaizi*
Email: bader.alkhubaizi@hotmail.com

doi: 10.26735/WZJM2885

1. المقدمة

تُعدُّ التكنولوجيا الرقمية والذكاء الاصطناعي أحد أهم الابتكارات الحديثة، التي غيرت مسار العديد من الصناعات والمجالات المختلفة، ومنها مجال التعليم والتعلم، فانتشار وسائل التقنية الحديثة من أجهزة ذكية وحواسيب، وظهور تقدم مذهل في البرمجيات والخوارزميات ساعد بدرجة كبيرة على ولوج هذه التطبيقات إلى الفصول الدراسية، وقد أسهم بقدر كبير في تحسين العملية التعليمية.

وفي ظل الثورة الصناعية الرابعة طور العقل العلمي والتكنولوجي مفهوم الذكاء الاصطناعي كأحد أهم الموضوعات الرئيسة الأكثر أثرًا وتأثيرًا في مجالات الحياة المعاصرة؛ الأمر الذي جعل البحث في الذكاء الاصطناعي وتطبيقاته المعاصرة والاطلاع عليها من الأشياء التي لا مناص منها لأبناء هذا الجيل وأجيال الحاضر والمستقبل (الكوار، 2023، 297).

ويواجه تطبيق الذكاء الاصطناعي في بعض الدول العربية العديد من المعوقات من أبرزها: ضعف البنية التحتية التي يحتاج إليها العالم الرقمي. (مثل: قلة توافر الشبكات والأجهزة المتطلبة - قلة توافر الخبراء والفنيين) وقد تكون المشكلة الكبرى نفسية، وهي إقناع المعلمين وأولياء الأمور بالتخلي عن الطرق التقليدية في التعليم والانخراط بحماسة في هذه الثورة الجديدة التي تحمل كثيرًا من المنافع للأجيال الجديدة، وبالتالي للمجتمع كاملًا (المكاوي، 2024).

ومع أهمية الذكاء الاصطناعي، فقد أشارتْ البُحوثُ الحديثةُ في علم اجتماعِ الجريمةِ إلى أن بعض تطبيقات الذكاء الاصطناعي تسببت في العديد من الآثار السلبية؛ حيث أسهمت في تكوينِ مفرداتِ الثَّقافاتِ الفرعيةِ المنحرفةِ والإجراميةِ، بغضِّ النَّظرِ عمَّا إذا كانت تَنْطَوي على جرائمَ، تَحدُثُ في بيئاتٍ حقيقيةٍ، أو افتراضيةٍ، وتُوفِّرُ وسائلُ التَّواصلِ الاجتماعيِّ، والمنصَّات الرَّقميةِ على شبكةِ الإنترنتِ منصةً مجهولةَ المصدرِ للأفرادِ؛ لتبادُلِ مصالِحِهم، ووِجْهاتِ نظرِهم، ومُعتقَداتِهِم المشترَكةِ حولَ الأنشطةِ، وقد تُشجِّعُ المُشارَكةُ في هذه المجتمعاتِ على تعزيزِ ثقافةٍ فرعيةٍ منحرفةٍ من خلالِ قَبُولِ مُبرِّرَاتٍ للأنشطةِ الإجراميةِ، وأساليب ارتكابِ الجرائمِ (Hamm, 2017).

لذلك، يُعتبر الأمن السيبراني من المجالات التي تحظى باهتمام عالمي واسع؛ لكونه من الأساسيات في العصر الرقمي الذي نعيشه اليوم. نسعى لمواكبة التطورات المستقبلية في هذا المجال؛ حيث يُعَد تعزيز الوعي بالأمن السيبراني ضرورة أساسية لجميع المجتمعات.

وانطلاقًا من ارتفاع معدلات استخدام الإنترنت، ونتيجة لما للفضاء السيبراني من أبعاد إيجابية هائلة، وانعكاسات سلبية ناتجة عن سوء الاستخدام؛ تُعدُّ توعية أفراد المجتمع بالأمن السيبراني ضرورة حتمية في هذا العصر الرقمي؛ حيث تزداد الحاجة إلى توعيتهم بإجراءات الأمن السيبراني نتيجة لما يمكن أن يواجهوا من مخاطر سيبرانية، أو يضعوا أنفسهم فيه من غير قصد نتيجة لعدم قدرتهم على تقييم هذه المخاطر، أو نقص وعيهم بإجراءات الأمن السيبراني التي تسهم في حماية الأجهزة والأنظمة الإلكترونية بشكل ملحوظ (quayyum, 2021؛ saravanakumar, & paavizhi, 2022؛ أبو زيد، 2019).

ويساعد الذكاء الاصطناعي وتطبيقاته المختلفة في مسايرة الاتجاهات الحديثة في التربية، وتوفير الجهد والوقت والتكلفة؛ إذ يمكِّن الباحثين من العثور على المعلومات بشكل أسرع، وتحرر الأساتذة والموظفين من الأعمال الروتينية، وإتاحة الفرصة للمتعلمين للتفاعل في المقرر التعليمي، والانغماس والإبحار داخله، وتلخيص النصوص الطويلة بدقة متناهية، وبطريقة سهلة للقراءة، وتحويل النصوص المكتوبة في المقرر الدراسي إلى ملفات صوتية مسموعة، وتحويل الصور المطبوعة أو النصوص المكتوبة بخط اليد إلى ملفات نصية يمكن تعديلها (الصبحي، 2020، 338).

وفى مجال التعليم بالذكاء الاصطناعي؛ فقد أحدث نقلة حقيقية وطفرة علمية، عندما قام بعمل جيد في تدابير الحد من انتشار وباء كورونا المستجِد؛ حيث اتُّخذت سياسات التعليم عن بعد للحد من حضور التلاميذ والطلاب، وتجنب الاختلاط في المدارس والجامعات، من خلال المنصات التعليمية (المهدي، 2021، والصياد والسالم، 2023).

وتوفر التقنيات القائمة على الذكاء الاصطناعي فرصًا لتعزيز تجربة تعلم الطلاب من خلال التدريس الذكي والتعلم الفردي، وتشير التقديرات إلى أن 47 ٪ من أدوات إدارة التعلم سيتم تدعيمها بقدرات الذكاء الاصطناعي، ويمكن أن تسهل هذه الفوائد على المعلمين مواجهة تحديات التدريس المختلفة عبر الإنترنت. كما تزود تقنيات الذكاء الاصطناعي الطلاب بفرص التعلم التي تسهل على المعلمين والطلاب الحصول على تعليقات تفاعلية وشخصية في الوقت المناسب. كما تساعد تقنيات الذكاء الاصطناعي في التعليم على تلبية احتياجات الطلاب المختلفة، ودعمهم للتغلب على صعوبات التعلم واستيعاب أساليب التعلم الخاصة بهم (Ouherrou et al., 2019).

كما توفر تقنيات الذكاء الاصطناعي للمعلمين مزايا ووظائف جديدة لتسهيل تدريسهم. حيث يمكن للمعلمين القادرين على استخدام هذه التقنيات في التدريس تعزيز فاعليتهم، وتحفيز تعلم الطلاب، ورفع الكفاءة الذاتية لهم، وتعزيز تنظيمهم الذاتي، ومساعدة الطلاب على التفاعل مع الطلاب الآخرين. وفي سبيل ذلك يحتاج المعلمون إلى اغتنام الفرصة في الوقت المناسب لتطوير كفاءتهم الرقمية في الذكاء الاصطناعي؛ لإثراء الطلاب بتجارب تعلم أفضل (Ahmad et al., 2022).

ومن ثم أصبحت الاستفادة من الذكاء الاصطناعي رهانًا لتطوير النظم التعليمية؛ مما ينعكس على مناحي الحياة، وجعل التعلم متعة جميلة تغذي شعور المتعلم وتوفر المثير المكتوب والمسموع والمصور والمتحرك؛ مما يحقق تفاعل المتعلم مع التعليم والتعلم (السعودي، 2021).

ولذا أوصت بعض الدراسات السابقة بضرورة الاستفادة من تطبيقات الذكاء الاصطناعي مثل: دراستي (العياضي، 2022؛ محمود، 2020).

وعلى الرغم من المزايا والفوائد التي يوفرها الذكاء الاصطناعي وتطبيقاته في مجال البحث العلمي، فإن هناك العديد من المعوقات التي تقف دون الاستفادة بدرجة أكبر منه، والتي منها التكلفة العالية لبناء منظومات الذكاء الاصطناعي، وضعف الثقة في بعض تطبيقاته، وضعف توافر عنصر الأمان والسرية الخاص بمعلومات الأفراد، وندرة البيانات الخاصة بالذكاء الاصطناعي الخاصة بالبحث العلمي، واحتمالية خروجه عن أهدافه العلمية، كما تهدد تطبيقاته وظائف العنصر البشري (الصياد، والسالم، 2023، ص. 278).

ولذا أكدت نتائج دراسة فرج (2022) أهمية تثقيف الطلبة بالممارسات التي تحقق الوعي بسلبيات بعض تطبيقات الذكاء الاصطناعي، والعمل على تعزيز الأمن السيبراني لديهم؛ من خلال تضمينها في المقررات والمناهج الدراسية في كافة المراحل التعليمية.

مشكلة الدراسة

تتمثل مشكلة الدراسة في أن الذكاء الاصطناعي يترتب عليه العديد من الفرص والتحديات؛ ونظرًا لتزايد استخدامه في مختلف المجالات، فإن الحاجة تدعو لتوظيف الأمن السيبراني في استثمار فرص الذكاء الاصطناعي، والحد من تحدياته، وهذا ما تستهدفه الدراسة من خلال محاولتها الإجابة عن الأسئلة الآتية.

أسئلة الدراسة

سعت الدراسة للإجابة عن السؤال الرئيس التالي: كيف يمكن توظيف الأمن السيبراني في استثمار فرص الذكاء الاصطناعي والحد من تحدياته؟ وتفرعت عنه الأسئلة التالية:

1. ما الإطار المفاهيمي للأمن السيبراني، كما تعكسه الأدبيات التربوية والدراسات السابقة؟
2. ما الإطار المفاهيمي للذكاء الاصطناعي، كما تعكسه الأدبيات التربوية والدراسات السابقة؟
3. ما أبرز التحديات المترتبة على الذكاء الاصطناعي على المستويين الفردي والجماعي؟
4. ما أبرز الفرص المترتبة على الذكاء الاصطناعي على المستويين الفردي والجماعي؟
5. ما آليات توظيف الأمن السيبراني في استثمار فرص الذكاء الاصطناعي والحد من تحدياته؟

أهداف الدراسة

هدفت الدراسة بشكل رئيس إلى بيان كيفية توظيف الأمن السيبراني في استثمار فرص الذكاء الاصطناعي والحد من تحدياته؛ وذلك من خلال تحقيق الأهداف الفرعية التالية:

1. عرض الإطار المفاهيمي للأمن السيبراني، كما تعكسه الأدبيات التربوية والدراسات السابقة.
2. توضيح الإطار المفاهيمي للذكاء الاصطناعي، كما تعكسه الأدبيات التربوية والدراسات السابقة.
3. تحديد أبرز التحديات المترتبة على الذكاء الاصطناعي على المستويين الفردي والجماعي.
4. الكشف عن أبرز الفرص المترتبة على الذكاء الاصطناعي على المستويين الفردي والجماعي.
5. الوصول لآليات توظيف الأمن السيبراني في استثمار فرص الذكاء الاصطناعي والحد من تحدياته.

أهمية الدراسة

الأهمية النظرية:

1. إثراء الأدبيات التربوية حول موضوع الأمن السيبراني للذكاء الاصطناعي.
2. تزايد استخدامات وتطبيقات الذكاء الاصطناعي في مختلف المجالات الحياتية؛ مما يتطلب الكشف عن الفرص والتحديات المترتبة على ذلك، وبيان كيفية استثمارها، وآليات الحد منها.
3. تعد الدراسة استجابة لتوصية العديد من الدراسات والمؤتمرات التي أوصت بتعزيز مستوى الأمن السيبراني لدى مختلف الفئات العمرية.
4. أهمية موضوع الأمن السيبراني، وما يترتب على غيابه من مخاطر تؤثر سلبًا على المستويين الفردي والجماعي؛ مما يتطلب مزيدًا من الدراسات حول هذا الموضوع.

الأهمية التطبيقية:

1. يمكن للدراسة أن تفيد الأسرة بما تسفر عنه من نتائج، قد تعزز من دورها في تنمية مستوى الوعي بالأمن السيبراني لدى أبنائها.
2. يمكن للدراسة أن تفيد الجهات الأمنية في المجال التكنولوجي

بما تسفر عنه من نتائج للحد من تحديات الأمن الاصطناعي، وكذلك مخاطر غياب الأمن السيبراني؛ وذلك بتضمينها في برامج تأهيل وتدريب مسئولي الجهات الأمنية في المجال التكنولوجي.

3. يمكن للدراسة أن تفيد بما تسفر عنه من نتائج في نشر الوعي بالأمن السيبراني لدى المتعلمين بمختلف المراحل التعليمية؛ وذلك بتضمينها في بعض البرامج والمقررات الدراسية.
4. يمكن للدراسة أن تفيد الجهات المختصة بالإعداد والتأهيل التكنولوجي للأفراد بما تقدمه من نتائج يمكن الاستعانة بها في تدريب وتأهيل الأفراد لاستثمار فرص الذكاء الاصطناعي والحد من سلبياته.

حدود الدراسة

اقتصرت الدراسة على تناول تحديات الذكاء الاصطناعي والفرص المترتبة عليه، وكيفية توظيف الأمن السيبراني لاستثمار هذه الفرص والحد من تلك التحديات.

2. الإطار الفكري المفاهيمي للأمن السيبراني

2. 1 مفهوم الأمن السيبراني

عرفته (جبور، 2016، 5) بأنه النشاط الذي يؤمن حماية الموارد (البشرية والمالية) المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات التغلب على الخسائر والأضرار التي تؤدي في حال تحققها إلى مخاطر وتهديدات كثيرة، كما يتيح إعادة الوضع إلى ما كان عليه في أسرع وقت ممكن.

كما تعرفه السمحان (2020، 7) بأنه «جميع الإجراءات والتدابير والتقنيات والأدوات المستخدمة لحماية وسلامة الشبكات والبرامج والبيانات من الهجوم، أو التلف أو الوصول غير المصرح به ويشمل حماية الأجهزة والبيانات».

وترى الدراسة أن الأمن السيبراني يتمثل في حماية الشبكات ووسائل تكنولوجيا التعليم وتقنياته على المستويين الفردي والجماعي بكل ما تحتويه من مدخلات ومخرجات من أي هجمات فيروسية أو اختراق للخصوصية، أو الحصول على بيانات ومعلومات دون موافقة أو إذن مصدرها الرئيس.

2. 2 أهداف الأمن السيبراني

يذكر الصانع وآخرون (2020) أن للأمن السيبراني هدفين رئيسين، هما: حماية مختلف الأجهزة الإلكترونية من المخاطر المحتملة، مثل: الفيروسات والاختراقات الإلكترونية وغيرها، بالإضافة إلى تحقيق الاستخدام الآمن لمختلف الخدمات الإلكترونية؛ مما يتطلب لتحقيق هذه الأهداف نشر الوعي بالأمن السيبراني.

2. 3 أهمية الأمن السيبراني

أجمعت العديد من الدراسات (صائغ، 2018؛ المنتشري، 2020؛ السواط وآخرون 2020؛ قطب، 2021) على أن أهمية الأمن السيبراني تتمثل في:

- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف جميع الأجهزة الحكومية، ومؤسسات القطاعين الخاص والعام.
- توفير بيئة موثوقة وآمنة للتعاملات في مجتمع المعلومات.
- توافر المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.
- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات والمخاطر المختلفة.

2. 4 خصائص الأمن السيبراني

يتسم الأمن السيبراني بعدد من الخصائص التي يجب توافرها لضمان حماية المعلومات وهي كما ذكرها: (الصحفي وعسكول، 2019؛ المشاقبة والسرحان، 2020؛ Cains et al, 2021) على النحو التالي:

- **الاكتشاف والتتبع:** تعني القدرة على تتبع مسار نشاط أو حدث معين للوصول إلى منشئ النشاط، ويكون ذلك من خلال عدم الإنكار، وتشخيص الخطأ، واكتشاف وتتبع الجرائم الإلكترونية، ووضع إجراءات التغلب عليها.
- **السرعة:** يوفر الأمن السيبراني تقنيات حديثة قادرة على التغلب على الجرائم الإلكترونية بسرعة عالية.
- **السرية والأمان:** تتمثل في عدم إفشاء المعلومات أو عرضها لأشخاص غير مصرح لهم إلا في حال وجود تصريح لهم للوصول إليها؛ وذلك بوضع تدابير تحمي المعلومات وأنظمتها من خلال ضمان سريتها.
- **التحقق من الهوية:** أي التأكد من هوية المستخدم، أو الجهاز أو العملية لتبادل البيانات؛ إذ يجب على الطرفين التأكد من

هوية الآخر، وهناك بعض الإجراءات للتحقق من ذلك من خلال السماح بإعطاء التراخيص اللازمة؛ مثل: كلمات المرور والتوقيعات الرقمية للوصول إلى الموارد التقنية والأصول المعلوماتية.

- **سلامة المعلومات وتوافرها:** القدرة على حماية المعلومات من أي تعديل أو تخريب أو وصول غير مصرح به؛ وذلك لضمان الوصول للمعلومة الصحيحة والمحافظة على استمراريتها وتقديمها للمستخدمين.

2. 5 أبعاد الأمن السيبراني

للأمن السيبراني عدة أبعاد مختلفة؛ تشمل الجوانب السياسية، والاقتصادية، والاجتماعية، والإنسانية؛ وذلك لارتباطه بسلامة البيانات، وأمن المعلومات، التي تعتبر ثروة العصر، فهي منبع الإنتاج والإبداع والابتكار، وتمكن التواصل بين الأفراد في مختلف الدول (حمدان، 2021).

ويرتبط الأمن السيبراني بأبعاد مختلفة، تهدف إلى تحقيق منظومة أمن متكاملة تعمل على حماية الدولة وشعبها، وتتمثل تلك الأبعاد فيما أشار إليه (جبور، 2016؛ الجنفاوي، 2021؛ الشايع، 2019) على النحو التالي:

- **البعد التقني:** يتمثل في حماية البنى التحتية والاتصالات والمعلومات والتطبيقات والشبكات من أي عمليات غير مصرح بها.
- **البعد الأمني:** يقوم على حماية نظام الدولة العسكري والسياسي؛ حيث يمكن أن تستخدم التقنيات في بث معلومات قد يحدث من خلالها تهديدات تؤدي إلى زعزعة أمنها.
- **البعد الاقتصادي:** يتمثل في مجالين حماية اقتصاد الدولة المعرفي ومجال التجارة الإلكترونية من خلال فتح سوق حر على شبكات الإنترنت.
- **البعد القانوني:** يقوم على حماية مجتمع المعلومات من الهجمات التي تحدث داخل الفضاء السيبراني؛ وذلك من خلال تنفيذ القوانين والتشريعات.
- **البعد الاجتماعي:** يتمثل في حماية الهوية الثقافية للمجتمع، وتوفير سبل الراحة للمواطن في حياته اليومية وتطوير نشاطه في الفضاء السيبراني وذلك من خلال نشر ثقافة الأمن السيبراني.
- **البعدي الديني:** يتمثل في حماية القيم والمعتقدات الدينية للمجتمع.
- **البعد الفكري:** يتمثل في حماية الهوية الثقافية للمجتمع وتوفير سبل الراحة للمواطن في حياته اليومية، وتطوير نشاطه في الفضاء السيبراني؛ وذلك من خلال نشر ثقافة الأمن السيبراني.
- **البعد التوعوي:** يتمثل في التدريب الأمني لبناء مهارات الأمن السيبراني لدى الطلبة وتشجيعهم على الاستخدام الصحيح للإنترنت، ودفاعهم عن خصوصياتهم في الفضاء السيبراني.

3. الإطار المفاهيمي للذكاء الاصطناعي

3. 1 مفهوم الذكاء الاصطناعي

يعبر الذكاء الاصطناعي عن علم وتكنولوجيا تعتمد بصورة أساسية على عدة حقول علمية منها: علم الحاسوب، وعلم النفس، واللسانيات Linguistics، والرياضيات، والهندسة، فالذكاء الاصطناعي يمثل إنجاز العقل البشري على مر العصور السابقة (بوعوة، 2019).

ويعرف الذكاء الاصطناعي بأنه فرع من فروع علوم الحاسوب، وهو العلم الذي يتيح للآلات التفكير مثل: البشر، أي يمنح الحواسيب شكلًا من أشكال الذكاء. كما يتم تعريفه بأنه سلوكيات وخصائص معينة تتميز بها البرامج الحاسوبية، تجعلها، تحاكي القدرات الذهنية البشرية وأنماط تفكيرها. من أهم ميزات الذكاء الاصطناعي القدرة على التعلم، والاستنتاج، والتفاعل مع أوضاع لم تُبرمج عليها الآلة بشكل مسبق. فهو أنظمة أو أجهزة تحاكي الذكاء البشري لأداء المهام، وتتمكن من تحسين أدائها بناءً على البيانات التي تجمعها (رزق، 2021، 573).

وترى دراسة (لطفي، 2023، 33) أن الذكاء الاصطناعي محاكاة للذكاء البشري عن طريق برامج إلكترونية وتطبيقات رقمية، يمكن توظيفها بشكل يخدم كلًّا من أعضاء هيئة التدريس والطلاب على حد سواء، ويوفر الوقت والجهد، وييسر عملية متابعة الطلاب، عن بعد وتقييمهم، بالإضافة إلى تفعيل المشاركة النشطة للطلاب في سبيل تحقيق الأهداف التعليمية.

وبناءً على ما سبق ترى الدراسة أن الذكاء الاصطناعي هو الذكاء الذي تظهره الآلات والبرامج؛ بهدف محاكاة القدرات البشرية من حيث الحركة والقدرة على تحريك الأشياء والمهارات الذهنية للإنسان، التفكير السليم دون وجود برمجيات والقدرة على التصرف المناسب في الوقت المناسب. كل هذا من خصائص الإنسان التي يحاول الخبراء برمجتها في الآلات.

3. 2 أهداف الذكاء الاصطناعي

يهدف الذكاء الاصطناعي إلى تمكين الآلات التقنية من تقليد ومحاكاة عمليات الذكاء التي تجري في العقل البشري بحيث تصبح الآلة قادرة على حل المشكلات واتخاذ القرار حيالها بطريقة علمية ومنطقية ومشابهة لطريقة تفكير العقل البشري، وتمثيل البرامج المحاسبية لمجال من مجالات الحياة وتحسين العلاقة القائمة بين عناصره (جميل وعثمان،2012، ص. 240).

كما يهدف الذكاء الاصطناعي بجميع أنظمته وبرامجه إلى تقديم الدعم الإلكتروني للطلاب خلال عملية تعلمهم، ومساعدتهم على حل المشكلات التي تواجههم،والعمل على تكييف التعليم مع حاجات المتعلم، وأيضًا تقديم التغذية الراجعة لهم التي تساعدهم على تجويد تعلمهم، وتسهل عليهم عملية الاستنتاج والتنبؤ، وتستند إلى علم الخوارزميات الذي جعل من الذكاء الاصطناعي عنصرًا فاعلًا في مجال الجبر والهندسة والعلوم الأخرى، كما ساعد على تذليل بعض الصعوبات وتفسير بعض الظواهر، وجاءت برامجه كعوض عن هذه التحديات التي لا يحلها التعليم التقليدي (M. M. L. Cairns. 2017).

3. 3 خصائص الذكاء الاصطناعي

تتعدد خصائص الذكاء الاصطناعي، ويمكن عرض أبرزها على النحو الآتي:

- **التمثيل الرمزي:** وهو عن طريق استخدام الرموز في تمثيل المعلومات المختلفة.
- **استخدام الأسلوب التجريبي المتفائل:** من الصفات المهمة في مجال الذكاء الاصطناعي أن برامجه تقتحم المسائل التي ليس لها طريقة حل عامة معروفة، وهذا يعني أن البرامج لا تستخدم خطوات متسلسلة تؤدي إلى الحل الصحيح، ولكنها تختار طريقة معينة للحل تبدو جيدة مع الاحتفاظ باحتمالية تغيير الطريقة إذا اتضح أن الخيار الأول لا يؤدي إلى الحل سريعًا، أي التركيز على الحلول الوافية (مطاي، 2012).
- **البيانات غير المؤكدة أو غير الكاملة:** وذلك عن طريق إيجاد الحلول المناسبة في الوقت المناسب، وليس معنى ذلك أن نقوم بإعطاء حلول مهما كانت الحلول غير صحيحة أو صحيحة، وإنما يجب لكي تقوم بالأداء الجيد أن تكون قادرة على تقديم الحلول المقبولة، وإلا تصبح غير وافية.
- **القدرة على التعلم:** وهي قدرة مهمة، تهدف إلى إكساب الإنسان المزيد من المعلومات والمهارات الإضافية التي تساعده في تنمية قدراته.

لذلك يمكن القول بأن الذكاء الاصطناعي يتمتع بالعديد من الخصائص والمميزات نذكر منها (يوسف، 2021):

- استخدام الذكاء في حل المشكلات المعروضة مع غياب المعلومة الكافية عنها.
- القدرة على التفكير والإدراك.
- القدرة على التعامل مع الحالات الصعبة والمعقدة.

3. 4 أهم أنواع الذكاء الاصطناعي

هناك عدة أنواع من أنظمة الذكاء الاصطناعي أو الأنظمة القائمة على الذكاء الاصطناعي: الآلات التفاعلية، وآلات الذاكرة المحدودة، ونظرية العقل، والذكاء الاصطناعي المدرك للذات، ويمكن بيانها على النحو الآتي (يوسف، 2021):

- **الآلات التفاعلية:** هذه هي أقدم أشكال أنظمة الذكاء الاصطناعي ذات القدرات المحدودة للغاية، ولا يمكن استخدامها للاعتماد على الذاكرة لتحسين عملياتها على أساس نفس الشيء. مثال شائع لآلة الذكاء الاصطناعي التفاعلية هو Deep Blue من IBM، وهو آلة تغلبت على Grandmaster Garry Kasparov في لعبة الشطرنج في عام 1997.
- **ذاكرة محدودة:** آلات الذاكرة المحدودة هي آلات قادرة، بالإضافة إلى امتلاكها لقدرات الآلات التفاعلية البحتة، على التعلم من البيانات التاريخية لاتخاذ القرارات.
- **نظرية العقل:** في حين أن النوعين السابقين من الذكاء الاصطناعي تم العثور عليهما بكثرة، فإن النوعين التاليين موجودان، في الوقت الحالي، إما كمفهوم أو عمل قيد التقدم.
- **الوعي الذاتي:** وهذه هي المرحلة الأخيرة من تطوير الذكاء الاصطناعي والتي لا توجد حاليًّا إلا افتراضيًّا.
- **الذكاء الاصطناعي الضيق (ANI):** ويمثل هذا النوع من الذكاء الاصطناعي جميع أنظمة الذكاء الاصطناعي الموجودة، بما في ذلك أكثر الذكاء الاصطناعي تعقيدًا وقدرة على الإطلاق.
- **الذكاء الاصطناعي العام (AGI):** الذكاء الاصطناعي العام هو قدرة وكيل الذكاء الاصطناعي على التعلم والإدراك والفهم والعمل تمامًا مثل الإنسان.
- **الذكاء الاصطناعي الخارق (ASI):** سيؤدي تطوير AGI وASI إلى سيناريو يُشار إليه في الغالب باسم التفرد. وبينما تبدو إمكانية امتلاك مثل هذه الآلات القوية تحت تصرفنا جذابة،

فإن هذه الآلات قد تهدد أيضًا وجودنا أو على الأقل تهدد أسلوب حياتنا.

وعرض (المهدي، 2021، 109، 110) تصنيفًا آخر لأنواع الذكاء الاصطناعي طبقًا لمراحل تطوره كالتالي:

- **الذكاء الاصطناعي التفاعلي (Reactive AI)**: هو أبسط أنواع الذكاء الاصطناعي يميل إلى أن يكون ثابتًا إلى حد ما، وغير قادر على التعلم أو التكيف مع المواقف الجديدة مثل: أنظمة الذكاء الاصطناعي للعب الشطرنج، وهي أنظمة تفاعلية تعمل على تحسين أفضل إستراتيجية للفوز باللعبة، أيضًا نجد أجهزة Deep Blue التي تم تطويرها من شركة IBM ونظام Alpha Go التابع لشركة جوجل.
- **الذكاء الاصطناعي محدود الذاكرة (Limited-Memory AI)**: يمكن لهذا النوع التكيف مع التجربة السابقة، أو تحديث نفسه بناءً على الملاحظات أو البيانات الجديد، وغالبًا ما يكون مقدار التحديث محدودًا، وطول الذاكرة قصيرًا.
- **نظرية العقل (Theory of Mind)**: تتكيف بشكل كامل. ولديها قدرة واسعة على التعلم والاحتفاظ بتجارب الماضي، كما أن هذه الأنظمة يمكنها فهم المشاعر والتفاعل مع الأشخاص والتواصل معهم، ومن أمثلتها؛ روبوتات محادثة متقدمة يمكنها اجتياز اختبار تورينج، لتخدع أي شخص للاعتقاد بأن الذكاء الاصطناعي إنسان ومع ذلك، فإن هذا الذكاء الاصطناعي ليس واعيًا بذاته.
- **الذكاء الاصطناعي المدرك للذات (Self-aware AI)**: لا يزال هذا النوع في عالم الخيال العلمي، ويعتقد بعض الخبراء أن الذكاء الاصطناعي لن يصبح واعيًا أو "حيًا " أبدًا، بحيث يتكون لدى الآلات وعي ذاتي ومشاعر خاصة تجعلها أكثر ذكاء من الكائن البشري.

4. الذكاء الاصطناعي في التعليم

يشير الذكاء الاصطناعي في التعليم (AIED) إلى استخدام تقنيات وتطبيقات الذكاء الاصطناعي التي تعمل على صنع السياسات في البيئات التعليمية؛ لتسهيل التدريس والتعلم وصنع القرار، من خلال أدوات تحاكي الذكاء البشري «لاستنتاج الأحكام أو التنبؤات، حيث يمكن أن توفر أنظمة الحاسوب توجيهات أو دعمًا أو ملاحظات مخصصة للطلاب» (Hwang, Chen, 2020).

ويختلف مفهوم الكفايات الرقمية للذكاء الاصطناعي عن مفهوم الذكاء الاصطناعي في التعليم (AIED) من نواحٍ عدة كما بينها (Ng et al., 2023)؛ حيث أشار إلى أن الذكاء الاصطناعي في التعليم يعمل على استخدام تقنيات الذكاء الاصطناعي لتحسين التعليم والتعلم، بينما تركز الكفايات الرقمية للذكاء الاصطناعي على تمكين الأفراد من فهم وتطبيق تقنيات الذكاء الاصطناعي في حياتهم اليومية. كما تهدف الكفايات الرقمية للذكاء الاصطناعي إلى تحقيق الأهداف التالية: (فهم أساسيات الذكاء الاصطناعي، والتعرف على تطبيقات الذكاء الاصطناعي، وتقييم مخاطر وفوائد الذكاء الاصطناعي، واستخدام الذكاء الاصطناعي بشكل مسؤول).

واكتسبت تقنيات الذكاء الاصطناعي في التعليم (AIED) شعبيتها خلال الفترة الحالية؛ حيث بدأت الدراسات تناقش حول كيفية توظيف الذكاء الاصطناعي في التعليم لتقليل عبء عمل المعلمين، من خلال أتمتة بعض المهام غير المتعلقة بالتدريس، وتعزيز تحليل البيانات وتحسين التدريس عبر الإنترنت؛ إذ أصبحت التقنيات أكثر تركيزًا على المعلمين ومساعدتهم على تحديد أساليب التدريس الفعَّالة؛ بناءً على بيانات تعلم الطلاب، وأتمتة المهام التشغيلية، وإنشاء التقييمات، وأتمتة الدرجات والتعليقات؛ مما يوفر وقت المعلمين بشكل كبير، وتعزيز الكفاءات. كما أشارت الدراسات إلى أن تقنية الذكاء الاصطناعي يمكن أن تعزز بشكل فعَّال التعلم الشخصي للطلاب، وتعزز اكتسابهم للمعرفة، وتحفز تعلم الطلاب باستخدام وكلاء أذكياء (Hwang, Chen, 2020).

كما يمكن أن تسهل هذه الفوائد على المعلمين مواجهة تحديات التدريس المختلفة عبر الإنترنت (على سبيل المثال: تنوع التعلم، مشكلة التحفيز، التفاعل الاجتماعي). وتزود تقنيات الذكاء الاصطناعي الطلاب بفرص التعلم التي تسهل على المعلمين والطلاب الحصول على تعليقات تفاعلية وشخصية في الوقت المناسب. وأيضًا تساعد على تلبية احتياجات المتعلمين الفردية، وتدعم المتعلمين للتغلب على صعوبات التعلم، واستيعاب أساليب التعلم الخاصة بهم (Ouher-rou et al., 2019).

4. التحديات والمخاطر المترتبة على بعض تطبيقات الذكاء الاصطناعي وغياب الأمن السيبراني

باستقراء الأدبيات (القحطاني، 2015، الموسى، 2016، العضياني، 2021) لتحديد تحديات ومخاطر بعض تطبيقات الذكاء الاصطناعي، وغياب الأمن السيبراني تبين أن هناك أنواعًا متعددة من هجمات التطبيقات والشبكات، كل نوع من الهجمات له طريقته الخاصة وأساليبه المتنوعة في الوصول إلى المعلومات، وإذا وصل الهجوم إلى المعلومات، فإنها تقوم على نسخها أو تعديلها أو حذفها أو إساءة استخدامها، ومن هذه الهجمات: هجمات الأكواد أو البرامج

الخبيثة Melicious Code attacks، وهجمات الأبواب الخلفية Back Door attacks، وتفجير البريد الإلكتروني Mail Bomb-ing، وكسر كلمات المرور Password Crack، والهجوم الأعمى (الاستقصائي) Brute Force attacks، وهجمات المعجم Dic-tionary attacks، وهجمات الرجل في الوسط Man-in-the-middle attacks، وهجوم تعطيل الخدمة Denial of service (dos) attacks وهجمات الخداع spoofing attacks، والرسائل غير المرغوب فيها أو المزعجة Spam، وهجمات التشمم أو الالتقاط Sniffer attacks، وهجمات الهندسة الاجتماعية Social Engi-neering attacks، وهجمات تصفح الكتف Shoulder Surfing attacks، وهجمات المعلومات الجانبية Side Channel attacks، كما أن للجرائم الإلكترونية أنواعًا منها: القرصنة، والبرامج الخبيثة، والسرقة، والمطاردة السيبرانية، وناشرو الفيروسات، ولمواجهة ذلك يجب الالتزام بالمبادئ الأخلاقية عند التعامل مع المصنفات الرقمية، والتحقق وتوفير عناصر أمن المعلومات وهي: التحقق من الهوية، والتحكم بالوصول، والسرية، وسلامة المعلومة وتكاملها، وعدم الإنكار، وتوافر المعلومة، والمتابعة أو التدقيق، كما أن التشفير قد يؤدي دورًا مهمًّا؛ حيث ينقل المعلومات بواسطة برامج تترجمها إلى رموز تكون غير ممكنة القراءة إلا للأفراد المالكين لمفتاح فك التشفير للحفاظ على سرية المعلومات.

ويضيف كل من (الصياد والسالم، 2023، 278) بعض التحديات التي تواجه الذكاء الاصطناعي، ومنها ضعف توافر عنصر الأمان والسرية الخاص بمعلومات الأفراد، وندرة البيانات الخاصة بالذكاء الاصطناعي، واحتمالية خروج الذكاء الاصطناعي عن أهدافه العلمية، وضعف الثقة في بعض تطبيقاته، وتهديد تطبيقاته لوظائف العنصر البشري.

5. أبرز الفرص المترتبة على الذكاء الاصطناعي

يترتب على الذكاء الاصطناعي العديد من الفرص التي يمكن استثمارها في مختلف المجالات الحياتية عامة، وفي المجال التعليمي خاصة، حيث أشارت العديد من الدراسات والبحوث السابقة إلى أهمية استخدام تطبيقات الذكاء الاصطناعي في التعليم؛ وذلك مثل: دراسة كل من (عباس، 2020؛ السعودي، 2021؛ القحطاني، والدايل، 2023)، حيث تكمن أهمية استخدام تطبيقات الذكاء الاصطناعي في تحقيق ما يلي:

- إتاحة فرصة التفاعل مع المتعلمين، والرد على استفساراتهم، وتقديم إجابات أكثر كفاءة.
- جعل تعلم التجربة والخطأ أقل خطورة وترهيبًا.
- تقديم أنماط من التعليم والتعلم التكيفي الذي يتناسب مع طبيعة وقدرات كل متعلم.
- توفير إمكانات تعلم اللغات الأجنبية، باستخدام تقنيات التعرف التلقائي على الكلام (ASR) ومعالجة اللغات الطبيعية NEP واكتشاف أخطاء اللغة، ومساعدة المستخدمين على تصحيحها.
- التوصل لحل المسائل حتى مع عدم اكتمال البيانات، والتعامل مع البيانات المتناقضة والمتضادة أحيانًا.
- إكساب المتعلمين عنصر التشويق، والتحدي والخيال، والمنافسة في العملية التعليمية.
- تحليل أداء المتعلمين، وإبراز نقاط القوة والضعف لديهم، وتقديم الدعم اللازم لهم في الوقت المناسب.
- تطوير أداء المتعلمين ذوي الخبرة البسيطة، وتقديم الحلول المناسبة للمشكلات التعليمية.
- الإسهام في إدارة بيانات المؤسسات التعليمية، وحفظها على شكل قواعد بيانات ضخمة تستطيع التنبؤ بالضعف على المستوى الفردي للمتعلم، والنقص في الموارد المادية والبشرية على مستوى المدارس والجامعات قبل حدوثه.

يمكن تحسين التعليم من خلال تطبيقات الذكاء الاصطناعي عبر استخدام الروبوتات التعليمية في الفصول الدراسية، كما هو الحال في الدول المتقدمة، لتعليم الطلاب المفاهيم الأساسية وتقييم أدائهم وتوجيههم نحو مسارات تعليمية تتناسب مع قدراتهم وإمكاناتهم. كما تُستخدم تطبيقات الذكاء الاصطناعي لتحليل البيانات التعليمية الكبيرة وتقديم توصيات ونتائج تعليمية تستند إلى أدلة علمية موثوقة. إضافةً إلى ذلك، يمكن لهذه التطبيقات اكتشاف الطلاب الموهوبين وذوي صعوبات التعلم، وتوفير برامج تعليمية وتدريبية مخصصة لهم. كما تسهم في تعزيز التواصل المستمر بين المدرسة وأولياء الأمور (الغامدي والعباسي، 2023).

كما يشير محمود (2020) إلى إمكانية استخدام الذكاء الاصطناعي في التعليم من خلال: إنشاء المحتوى الذكي (Smart Control)، ونشر هذه المحتويات باستخدام تطبيقات الذكاء الاصطناعي، بالإضافة إلى إمكانية إنشاء منصات تعلم ذكية متكاملة مع دمج المحتوى بتمارين ووسائط متعددة وتقييم ذاتي، كذلك استخدام تطبيقات الواقع الافتراضي (VR) والواقع المعزز (AR).

ومن التقنيات الجديدة التي أتاحها ظهور الذكاء الاصطناعي، وأدت بدورها إلى تسهيل العمل البشري تقنية محول الدردشة المدرب

سلفًا (Generative Pre-trained Transformer, ChatGPT)، حيث تم تطويره بواسطة OpenAI في نوفمبر 2022؛ لإنشاء نصوص مشابهة للكتابة البشرية. وقد أظهر ChatGPT نتائج واعدة في مختلف المجالات، ففي مجال الرعاية الصحية، ساعد في عملية اكتشاف الأدوية وتطويرها، وفي عمليات تشخيص الأمراض، والعلاج، وتقديم المشورة، والمساعدة في العمليات الجراحية، والصيدلة (Patel et al., 2023). وكذلك في المجال الإداري، وفر (شات جي بي تي) ChatGPT الوقت للإداريين للتركيز على أتمتة المهام المتكررة مثل: الجدولة، وإدارة البيانات. وهذا يمكن أن يعزز الإنتاج والكفاءة، أما في مجال علم النفس فقد استطاعت هذه التقنية محاكاة المحادثات العلاجية للمستخدمين، وتقديم رؤى حول اضطرابات الصحة العقلية، وتوفير معلومات حول الأساليب والتقنيات العلاجية (Aithal & Aithal, 2023).

وتعد (شات جي بي تي) ChatGPT أداة تعليمية أتاحت العديد من الفرص والممارسات في التعليم العالي (Schönberger, 2023). وتتمثل هذه الممارسات في تحليل النصوص، وأتمتة مهام الكتابة، وإمكانية الوصول السريع، وإجراء الدروس الخصوصية، ومصدر للتعلم التكاملي، وتعزيز الفهم، وتعلم اللغة، وتعلم مهارات الاتصال، ودعم المعلمين، وتجربة تعليمية مبتكرة، تساعد في البحث والتحليل (Michel-Villarrea at al., 2023; Schönberger, 2023).

كما أنه يمكن دمج ممارسات (شات جي بي تي) ChatGPT في التعليم، لأنها تساعد المحاضرين في تحسين عملية التدريس، والطلاب على ممارسة عملية التعلم، وتحقق التعلم التعاوني، وأن ذلك لا يتعارض مع مهام المؤسسة التعليمية. كما أنها تعزز التفاعل بين المستخدم والحاسوب، وتحسن الخدمات المقدمة للطلاب، وتدعم البحث العلمي، وتساعد الباحثين (Dempere et al., 2023)، بالإضافة لذلك فإنها تسهم في تطوير التعلم الشخصي، والتواصل غير المتزامن، وتقديم التغذية الراجعة (Memarin & Doleck, 2023).

6. كيفية توظيف الأمن السيبراني للحد من تحديات الذكاء الاصطناعي واستثمار فرصه

يعد تطوير الأمن السيبراني مطلبًا عالميًّا يتطلب تحقيقه العديد من الإجراءات؛ حيث يذكر العضياني (2021) عددًا من التطبيقات اللازمة لتطويره على مستوى الدول، ومن أبرز هذه التطبيقات التوعية الاجتماعية؛ وذلك من خلال وضع الخطط وتنظيم الحملات للتوعية بأهمية الأمن السيبراني ودوره في حماية الخصوصية لدى جميع أفراد المجتمع من المخاطر السيبرانية التي تزداد حدتها في الآونة الأخيرة، وذلك يعود إلى كون العامل البشري يشكل السبب الرئيس وراء نجاح العديد من الجرائم الإلكترونية؛ حيث يُعدُّ المستخدم النهائي للأنظمة الإلكترونية الذي لا يمتلك الوعي بالأمن السيبراني الحلقة الأضعف التي يستهدفها القائمون على هذه الجرائم (Richardson et al., 2020).

ويتطلب توظيف الأمن السيبران في الحد من تحديات الذكاء الاصطناعي واستثمار فرصه ما يلي:

- الوعي بالمخاطر السيبرانية

لا يمكن للأفراد منع الانتهاكات الأمنية، وتحقيق الأمن السيبراني في الفضاء السيبراني، إلا إذا كان لديهم علم بالمخاطر السيبرانية المحتملة وتأثيرها عليهم (Richardson et al., 2020). ويذكر أبو حجاب (2022) وأبو زيد (2021) وعبد العزيز (2020) عددًا من المخاطر السيبرانية التي يمكن أن يتعرض لها الأطفال، ومنها: العنف الإلكتروني، والتنمر الإلكتروني، والوصول إلى المحتوى الحساس، والتشوه المعرفي، وتزييف الوعي؛ وذلك من خلال التعرض للمعلومات المغلوطة، كما يتعرض بعض الأفراد للتحرش الإلكتروني والابتزاز، بالإضافة إلى استدراجهم للقيام بأفعال غير مشروعة، وكذلك الحث على العنصرية، فضلًا عن الاستغلال المادي من خلال سهولة شراء البضائع المغشوشة، أو الوصول إلى البيانات المالية الخاصة بأفراد الأسرة.

- الدعم الاجتماعي

إن الأفراد في ظل الانفتاح الرقمي بحاجة إلى الدعم من كافة مؤسسات المجتمع؛ وذلك للاستفادة من إيجابيات الفضاء السيبراني وتجنب مخاطره؛ حيث إن مسؤولية حمايتهم في الفضاء السيبراني يشترك فيها كل من المجتمع الدولي، وصناع السياسات والأخصائيون النفسيون والمعلمون والآباء ومقدمو الرعاية الاجتماعية، وهذا يؤكد أهمية التعاون بين الجهات الأمنية والتربوية والاجتماعية لنشر الوعي بالأمن السيبراني من خلال إعداد البرامج التوعوية، وتمكين أفراد المجتمع من تحصين أنفسهم من مختلف الهجمات السيبرانية (حمادي، 2017).

وفي هذا السياق يشير معتوق ومهاوات (2020) إلى فاعلية دور المؤسسات الرسمية وغير الرسمية في دعم الوعي بالأمن السيبراني من خلال تضمين موضوعاته في المناهج الدراسية، بالإضافة إلى تفعيل دور المساجد ودور التحفيظ، وإنشاء جمعيات متخصصة وغير ربحية للتوعية بالاستخدام الأمثل للفضاء السيبراني. كما يؤكد أهمية دعم الدول المتقدمة في هذا المجال للدول النامية، وإجراء ورش عمل دولية لتبادل المعرفة في مجال التوعية بالأمن السيبراني. ويذكر فوزي (2019) أن معظم الحكومات تؤمن بأن أقوى أساليب الحماية

والدفاع السيبراني تتمثل في نشر الوعي والمعرفة بالأمن السيبراني لدى المستخدمين النهائيين.

- المهارات الشخصية

حتى يكون الأفراد قادرين على اكتساب مفاهيم الأمن السيبراني، والعمل بها لا بد لهم من تعلّم عدد من المهارات التي تعدُّ مزيجًا من المعارف والخبرات والقدرات، وتشكل المهارات الشخصية الخطوة الأولى لتحقيق الأمن السيبراني، وتتمثل في عدد من المهارات العامة الضرورية لجميع المستخدمين للفضاء السيبراني؛ وذلك لتحقيق الاستخدام الآمن، فمن الواجب أن يتحمل الأفراد مسؤولية حمايتهم الشخصية في الفضاء السيبراني (العلوان، 2021؛ هاشم، 2020).

ومن خلال مراجعة الأدب البحثي تم التوصل إلى عددٍ من هذه المهارات التي يجب أن يكتسبها الأفراد كحاجة ملحة في ضوء ما نعيشه من تطور تقني، فقد أشارت دراسة النجراني وكريم (2022) إلى أهمية تنمية الذكاء الرقمي لدى الأفراد؛ لكونه يتضمن عددًا من المهارات، هي: إدارة وقت الشاشة، وإدارة البصمة الرقمية، وإدارة الخصوصية، وإدارة التنمر الإلكتروني، والتعاطف الرقمي، والهوية الرقمية. حيث أكدت دراسة الدهشان (2019) أن امتلاك مهارات الذكاء الرقمي يمكن أن يحمي من كافة المخاطر التي يمكن التعرض لها في الفضاء السيبراني.

كما يوجه بارك (Park, 2016) إلى بضرورة إكساب الأفراد للمواطنة الرقمية في سنّ مبكرة؛ حتى يتمكنوا من تحقيق الاستخدام الآمن للفضاء السيبراني. ويعرف كفافي (2016) المواطنة الرقمية بأنها: الانتماء إلى مجتمع افتراضي والمشاركة الفعَّالة فيه مع مراعاة القواعد الأخلاقية واحترام حقوق الأفراد الرقمية. وتضيف دراسة الدمرداش (2022) عددًا من المهارات الشخصية اللازم توافرها لدى المستخدمين النهائيين للفضاء السيبراني، منها: مهارة حل المشكلات، ومهارة التفكير الناقد. ويؤكد الدهشان (2015) أن تنمية التفكير الناقد الرقمي لدى الفرد ضرورة لإكسابه القدرة على الانتقاء والانتفاع من تلك التقنيات المتوافرة؛ وذلك من خلال أساليب التساؤل والاستقصاء.

ولتنمية مستوى الأمن السيبراني وتوظيفه في الحد من تحديات الذكاء الاصطناعي واستثمار فرصه، فإنه توجد العديد من الإجراءات التي تتخذها العديد من مؤسسات المجتمع، ولكن هنا سنسلط الضوء على الإجراءات التي تقدم من قبل الإدارات التعليمية بمستوياتها المختلفة كما أوضحتها المنتشري (2020) ومنها ما يلي:

- وضع خطط للتوعية بالأمن السيبراني على مستوى المؤسسات التعليمية بشكل عام، وتقوم بالتحذير من المخاطر السيبرانية، وتشمل جميع المعلمين والطلبة.
- تعميم سياسات واضحة للتعامل مع التكنولوجيا، وتشمل الأمن السيبراني، والتأكد من تطبيقها في جميع المؤسسات التعليمية، والإشراف على ذلك من قبل الجهات المختصة كوزارة التعليم.
- وجود خطة عمل محددة وواضحة لدى المؤسسات التعليمية للتعامل مع الأخطار والانتهاكات السيبرانية.
- عقد دورات تدريبية للمعلمين لتوعيتهم بالإجراءات التي تمكن الطلاب من اتباعها عند تعرضهم ووقوعهم كضحايا للمخاطر السيبرانية.
- اعتبار الوعي بالأمن السيبراني من المهارات اللازمة في الحياة، وإتاحته في القضايا المثارة أثناء التدريس، وكذلك في الأنشطة المدرسية.
- إدراج موضوع الأمن السيبراني ضمن أدلة المعلمين.

7. النتائج والتوصيات

أبرز نتائج الدراسة:

- يتمثل الذكاء الاصطناعي في حماية الشبكات ووسائل تكنولوجيا التعليم وتقنياته على المستويين الفردي والجماعي بكل ما تحتويه من مدخلات ومخرجات من أي هجمات فيروسية أو اختراق للخصوصية، أو الحصول على بيانات ومعلومات دون موافقة أو إذن مصدرها الرئيس.
- يعبر الذكاء الاصطناعي عن مجموعة البرامج والتطبيقات، التي تمكن الأجهزة الحاسوبية من محاكاة بعض الاستجابات البشرية، والقيام بعمليات منطقية، وممارسة بعض المهام البشرية بشكل أسرع ودقة أعلى.
- يهدف الذكاء الاصطناعي إلى حماية مختلف الأجهزة الإلكترونية من المخاطر المحتملة، بالإضافة إلى تحقيق الاستخدام الآمن لمختلف الخدمات الإلكترونية.
- يتسم الأمن السيبراني بعدد من الخصائص التي يجب توافرها لضمان حماية المعلومات وهي: الاكتشاف والتتبع والسرعة والسرية والأمان والتحقق من الهوية وسلامة المعلومات وتوافرها.
- تتمثل أبرز أبعاد الأمن السيبراني فيما يلي: البعد التقني، البعد الاقتصادي، البعد الأمني، البعد القانوني، البعد الاجتماعي، البعد الديني، البعد الفكري، البعد التوعوي.
- يتسم الذكاء الاصطناعي بالسمات الآتية: التمثيل الرمزي، استخدام الأسلوب التجريبي المتفائل، البيانات غير المؤكدة أو غير الكاملة، القدرة على التعلم.

- يضمن الذكاء الاصطناعي الأنواع الآتية: الآلات التفاعلية، الذاكرة المحدودة، نظرية العقل، الوعي الذاتي، الذكاء الاصطناعي العام، الذكاء الاصطناعي الضيق، الذكاء الاصطناعي الخارق.
- هناك العديد من المعوقات التي تقف دون الاستفادة بدرجة أكبر منه، والتي منها التكلفة العالية لبناء منظومات الذكاء الاصطناعي، وضعف الثقة في بعض تطبيقاته، وضعف توافر عنصر الأمان والسرية الخاص بمعلومات الأفراد، وندرة البيانات الخاصة بالذكاء الاصطناعي الخاصة بالبحث العلمي، واحتمالية خروجه عن أهدافه العلمية، كما تهدد تطبيقاته وظائف العنصر البشري
- أسهمت بعض تطبيقات الذكاء الاصطناعي في العديد من الآثار السلبية؛ حيث أسهمت في تكوينِ مفرداتِ الثَّقافاتِ الفرعيةِ المنحرفةِ والإجراميةِ.
- تتمثل أبرز التحديات والمخاطر المترتبة على الذكاء الاصطناعي فيما يلي: هجمات الأكواد أو البرامج الخبيثة، هجمات الأبواب الخلفية، تفجير البريد الإلكتروني، كسر كلمات المرور، الهجوم الأعمى (الاستقصائي)، هجمات المعجم، هجمات الرجل في الوسط، هجوم تعطيل الخدمة، هجمات الخداع، الرسائل غير المرغوب فيها أو المزعجة، هجمات التشمم أو الالتقاط، هجمات الهندسة الاجتماعية، هجمات تصفح الكتف، هجمات المعلومات الجانبية.
- تشمل المخاطر والسلبيات المترتبة على بعض تطبيقات الذكاء الاصطناعي جميع المستخدمين حول العالم أفرادًا ومؤسسات ووزارات.
- يترتب على الذكاء الاصطناعي العديد من الفرص التي يمكن استثمارها في مختلف المجالات الحياتية عامة، وفي المجال التعليمي خاصة، ومنها ما يلي: إتاحة فرصة التفاعل مع المتعلمين، والرد على استفساراتهم، وتقديم إجابات أكثر كفاءة، وجعل تعلم التجربة والخطأ أقل خطورة وترهيبًا، وتقديم أنماط من التعليم والتعلم التكيفي الذي يتناسب مع طبيعة وقدرات كل متعلم، وتوفير إمكانات تعلم اللغات الأجنبية، والتوصل لحل المسائل حتى مع عدم اكتمال البيانات، والتعامل مع البيانات المتناقضة والمتضادة أحيانًا، وإكساب المتعلمين عنصر التشويق، والتحدي والخيال، والمنافسة في العملية التعليمية، وتحليل أداء المتعلمين، وإبراز نقاط القوة والضعف لديهم، وتقديم الدعم اللازم لهم في الوقت المناسب، وتطوير أداء المتعلمين ذوي الخبرة البسيطة، وتقديم الحلول المناسبة للمشكلات التعليمية، والإسهام في إدارة بيانات المؤسسات التعليمية، وحفظها على شكل قواعد بيانات ضخمة تستطيع التنبؤ بالضعف على المستوى الفردي للمتعلم، والنقص في الموارد المادية والبشرية على مستوى المدارس والجامعات قبل حدوثه.
- يتطلب توظيف الأمن السيبراني في الحد من تحديات الذكاء الاصطناعي واستثمار فرصه ما يلي: الوعي بالمخاطر السيبرانية، والدعم الاجتماعي، والمهارات الشخصية.

التوصيات:

1. عقد برامج لتوعية جميع أفراد المجتمع بالمخاطر السيبرانية وآليات التعامل الإيجابي معها وقائيًّا وعلاجيًّا.
2. تدريب المعلمين بالمرحلة التعليمية المختلفة على امتلاك المهارات التي تعزز من دورهم في توعية طلابهم بالأمن السيبراني وآليات تحققه.
3. تدريب المتعلمين على كيفية توظيف الذكاء الاصطناعي في العملية التعليمية.
4. الانفتاح على تجارب بعض الدول المتقدمة في مجال توظيف الذكاء الاصطناعي في التعليم ومحاولة الاستفادة من خبراتها.
5. تضمين المناهج الدراسية بالمراحل التعليمية المختلفة موضوعات عن الذكاء الاصطناعي من حيث إيجابياته وسلبياته وآليات تعزيز الإيجابيات، والحد من السلبيات.
6. تنظيم أنشطة طلابية عملية للطلاب في مراحل التعليم المختلفة، تتضمن نماذج من المخاطر السيبرانية وسلبيات الذكاء الاصطناعي، وكيفية التعامل معها إجرائيًّا.
7. تقديم برامج إعلامية متخصصة لرفع مستوى الوعي المجتمعي بالمخاطر السيبرانية، وتحديات الذكاء الاصطناعي وفرصه، وكيفية الحد من السلبيات واستثمار الفرص.

المقترحات

يمكن إجراء دراسات حول:

1. مستوى الوعي بالمخاطر السيبرانية لدى طلاب المرحلة المتوسطة وسبل تعميقه من وجهة نظرهم في ضوء بعض المتغيرات.
2. تصور مقترح لتوظيف الذكاء الاصطناعي في العملية التعليمية بالمرحلة المتوسطة في ضوء خبرات بعض الدول.

3. تصور مقترح لدو المدرسة الثانوية في التوعية بالتعامل الوقائي والعلاجي مع الجرائم الإلكترونية.
4. مستوى التمكين الرقمي لدى أعضاء هيئة التدريس وعلاقته بتعزيز مستوى الوعي بالأمن السيبراني لدى طلابهم.
5. السلبيات المترتبة على توظيف الذكاء الاصطناعي في المجال التعليمي وآليات الحد منها من وجهة نظر الخبراء.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس له أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن المؤلف بأن البحث المنشور لم يتلقَ أي منحة ماليَّة، من أي جهة تمويل في القطاعات الحكوميَّة، أو التجاريَّة، أو المؤسسات غير الربحية.

المراجع

أولًا: المراجع العربية

أبو حجاب، سارة، (2022). إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء بعض الممارسات الدولية. مجلة الإدارة التربوية، (34)، 333 - 526.

أبو زيد، أسماء، (2021). الفضاء السيبراني واقع يقدم الفرص والتحديات: الرقمنة: أبعادها وتأثيرها على الأطفال. مجلة خطوة، (43)،37-39.

أبو زيد، عبد الرحمن، (2019). الأمن السيبراني في الوطن العربي: دراسة حالة المملكة الغربية السعودية. آفاق سياسية، (48)، 61- 55.

بوعوة، هاجر، (2019). تطبيقات الذكاء الاصطناعي الداعمة للقرارات الإدارية في منظمات العمل، كتاب الذكاء الاصطناعي كتوجه حديث، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، ألمانيا.

جبور، منى، (2016). السيبرانية: هاجس العصر. مجلة المكتبات والمعلومات والتوثيق في العالم العربي، (5). 262-263.

جميل، أحمد عادل؛ وعثمان حسين عثمان، (2012). إمكانية استخدام تقنيات الذكاء الصناعي في ضبط جودة التدقيق الداخلي: دراسة ميدانية في الشركات المساهمة العامة الأردنية. المؤتمر العلمي السنوي الحادي عشر: ذكاء الأعمال واقتصاد المعرفة 26-23 نيسان (إبريل (2012) عمان الأردن ع (1).

الجنفاوي، خالد، (2021). التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت. المجلة العربية للآداب والدراسات الإنسانية، (19). 75 - 123.

حمدان، سماح، (2021). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته بالإجراءات الاحترازية للحماية من الهجمات الإلكترونية في ظل جائحة كورونا. المجلة العربية للعلوم الاجتماعية، 1 (19)، 69-18.

خلف، صلاح ساهي خلف، (2023). دور تطبيقات الذكاء الاصطناعي في تطوير المهارات التربوية والتعليمية في الوطن العربي وانعكاساتها على نظم التعليم التقليدية- دراسة ميدانية. مجلة آداب الفراهيدي، 15(52)، 327-351.

الدمرداش، نانسي، (2022). أثر تفاعل العناصر الافتراضية المدعومة بالذكاء الاصطناعي وأدوات إدارة المعرفة في تنمية مهارات الأمن السيبراني وحل المشكلات لدى طلاب الحاسبات والذكاء الاصطناعي. مجلة البحوث في مجالات التربية النوعية، (41)،1331-1427.

الدهشان، جمال، (2015). المواطنة الرقمية مدخلًا لمساعدة أبنائنا على الحياة في العصر الرقمي. مجلة كلية التربية، 30 (4)،1042.

الدهشان، جمال، (2019). تنمية الذكاء الرقمي لدى أطفالنا أحد متطلبات الحياة في العصر الرقمي. المجلة الدولية للبحوث في العلوم التربوية،2 (4)،51-88.

رزق، هناء رزق محمد، (2021). أنظمة الذكاء الاصطناعي ومستقبل التعليم، مجلة دراسات في التعليم الجامعي، جامعة عين شمس - كلية التربية - مركز تطوير التعليم الجامعي، ع52.

السعودي، رمضان، (2021). تقنيات الذكاء الاصطناعي ودورها في التحول التنظيمي للجامعات المصرية: دراسة تطبيقية على جامعة كفر الشيخ: سيناريوهات مقترحة، مجلة الإدارة التربوية، (32)، 223 - 279.

السمحان، منى، (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية بالمنصورة، 111 (1)، 2-29.

الشايع، خالد، (2019). الأمن السيبراني: مفهومه وخصائصه وسياساته، الدار العالمية.

صائغ، وفاء، (2018). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية. المجلة العربية للعلوم الاجتماعية، 3(14)،18-70.

الصانع، نورة؛ عسران، عواطف؛ السواط، حمد؛ منصور، إيناس؛ وأبو عيشة، زاهدة، (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية، 36 (6)، 41-90.

الصبحي، صباح عيد رجاء، (2020). واقع استخدام أعضاء هيئة التدريس بجامعة نجران لتطبيقات الذكاء الاصطناعي في التعليم، مجلة كلية التربية في العلوم التربوية، كلية التربية، جامعة عين شمس، 44 (4)، 319 - 368.

الصحفي، مصباح وعسكول، سناء، (2019). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمي في التربية، 20 (10)، 493-534.

الصياد، مي محمد يحيى؛ والسالم، وفاء عبد الله، (2023). دور الذكاء الاصطناعي في تطوير مهارات البحث العلمي لدى طالبات كلية التربية بجامعة الملك سعود، مجلة البحوث التربوية والنوعية، (19)، 247 - 288.

عباس، رياض عزيز، (2020). الاتجاه نحو الذكاء الاصطناعي وعلاقته بالتوجه نحو المستقبل لدى طلبة الجامعة، مجلة الآداب، جامعة بغداد، (135)، 367 - 406.

عبد العزيز، إبراهيم، (2020). التنشئة الأسرية وحماية الطفولة من مخاطر التقنية الحديثة: دراسة ميدانية. حوليات آداب عين شمس، 22، 48 - 52.

العضياني، فهد بن مزيد، (2021). الأمن السيبراني وتحديات الذكاء الاصطناعي، الرياض، شركة تكوين العالمية للنشر والتوزيع.

العلوان، جعفر، (2021). الألعاب الرقمية الجادة وتنمية مهارات الأمن السيبراني: دراسة استكشافية. مجلة المثقال للعلوم الاقتصادية والإدارية، 7 (3)، 83-114.

العياضي، خليوي سامر خليوي، (2022). توظيف خوارزميات الذكاء الاصطناعي في معالجة أبواب الصرف السماعية. حولية كلية اللغة العربية بنين بجرجا جامعة الأزهر، 4 (26)، 3502-3530.

الغامدي، حنان محمد؛ العباسي، دلال عمر، (2023). واقع تفعيل تطبيقات الذكاء الاصطناعي في البرامج الإثرائية للطلبة الموهوبين في مدارس ينبع وجدة من وجهة نظر الطلبة ومنفذي البرامج الإثرائية، المجلة الدولية لنشر البحوث والدراسات، 3 (28)، 633- 591.

فرج، علياء عمر، (2022). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي-جامعة الأمير سطام بن عبد العزيز نموذجًا. المجلة التربوية لكلية التربية بسوهاج، (94)، 509-537.

فوزي، إسلام، (2019). الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجي. المجلة الاجتماعية القومية، 56 (2)، 99-139.

القحطاني، أمل بنت سفر، والدايل، صفية بنت صالح، (2023). واقع توظيف تقنيات الذكاء الاصطناعي في جامعة الأميرة نورة بنت عبد الرحمن من وجهة نظر أعضاء هيئة التدريس وتوجههم نحوه، مجلة الشمال للعلوم الإنسانية، جامعة الحدود الشمالية- مركز النشر العلمي والتأليف والترجمة، 8 (1)، 509- 548.

القحطاني، ذيب، (2015). أمن المعلومات، الرياض، مدينة الملك عبدالعزيز للعلوم والتقنية.

كفافي، حنان. (2016). تصور مقترح لتنمية وعي تلاميذ مرحلة التعليم الأساسي بثقافة المواطنة الرقمية. دراسات عربية في التربية وعلم النفس، 345-378.

الكوار، محمد محمود. (2023). الذكاء الاصطناعي وتطبيقاته المعاصرة، المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات، مصر المجلد الثالث- العدد الثاني، أبريل - يونيو. الشريدة. نادية عبد الجبار محمد والسامرائي عمار عصام عبد الرحمن (2021) الذكاء الاصطناعي في التعليم المحاسبي ودوره في تحقيق أهداف التنمية المستدامة في مملكة البحرين / جامعة العلوم التطبيقية نموذجًا مجلة دراسات محاسبية ومالية 16 (خاص).

لطفي، أسماء محمد السيد، (2023). الاتجاه نحو استخدام تطبيقات الذكاء الاصطناعي وعلاقته بالهوية المهنية والاندماج الوظيفي لدى أعضاء هيئة التدريس في ضوء بعض المتغيرات الديموجرافية، مجلة كلية التربية، كلية التربية، جامعة عين شمس، 3 (47)، 15 - 134.

محمود، عبد الرازق مختار، (2020). تطبيقات الذكاء الاصطناعي: مدخل لتطوير التعليم في ظل تحديات جائحة فيروس كورونا (covid-19)، المجلة الدولية للبحوث في العلوم التربوية، 3 (4)، 171-224.

المشاقبة، محمد. السرحان، حنين، (2020). أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية، مجلة المفرق. 1-99.

مطاي، عبد القادر، (2012). «تحديات ومتطلبات استخدام الذكاء الاصطناعي في التطبيقات الحديثة لعملية إدارة المعرفة»، الملتقى الوطني العاشر حول أنظمة المعلومات المعتمدة على الذكاء الاصطناعي. جامعة سكيكدة، الجزائر.

معتوق، الزبير؛ مهاوات، عبدالقادر، (2020). مخاطر الجريمة المعلوماتية على الأطفال وسبل حمايتهم: دولة الجزائر أنموذجًا. مجلة آداب النيلين،5(1)، 32-58.

المكاوي، مرام عبد الرحمن، (2018). الذكاء الاصطناعي على أبواب التعليم، مجلة القافلة، شبكة الإنترنت، مسترجع بتاريخ 2024/3/16م.

المنتشري، فاطمة يوسف، (2020). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للعلوم التربوية والنفسية، 4(17)، 457-484.

المهدي، صلاح طه، (2021). التعليم وتحديات المستقبل في ضوء فلسفة الذكاء الاصطناعي، مجلة تكنولوجيا التعليم والتعلم الرقمي، مج2 (5).

الموسى، عبد الله، (2016). مقدمة في الحاسب والإنترنت ويندوز. 10 الطبعة السابعة، مؤسسة شبكة البيانات، الرياض.

النجراني، خديجة؛ كريم، منى، (2022). مستوى وعي المعلمات والطالبات بمهارات الذكاء الرقمي من وجهة نظر معلماتهن في مرحلتين المتوسطة والثانوية بمدينة جدة. المجلة العربية للتربية النوعية،6 (12)، 139-184.

هاشم، هبة، (2020). برنامج مقترح قائم على جغرافية الحروب السيبرانية لتنمية الوعي بمخاطرها وتعزيز قيم المواطنة الرقمية للطلاب المعلمين بكلية التربية. مجلة كلية التربية في العلوم التربوية،44 (3)،81-150.

يوسف، حمزة أيوب، (2021). التحول في مجال الذكاء الاصطناعي من الماضي إلى المستقبل، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 38، يوليو.

ثانيًا: المراجع الأجنبية

Ahmad, S. F, Alam, M. M., Rahmat, M. K., Mubarik, M. S., & Hyder, S. I. (2022). Academic and administrative role of artificial intelligence in education. Sustainability, 14(3), 1101.

Aithal, P. S., & Aithal, S. (2023). Application of ChatGPT in higher education and research - a futuristic analysis. International Journal of Applied Engineering and Management Letters (IJAEML), 7(3), 168-194. https://doi.org/10.5281/zenodo.8386867

Alharbi, Talal. Tassaddiq, Asifa. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data Cogn. Comput, 5 (23). 2-15.

Cains, Mariana. Flora, Liberty. Taber, Danica. Henshel, Diane. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation.

Chen, X., Xie, H., Zou, D., & Hwang, G. J. (2020). Application and theory gaps during the rise of artificial intelligence in education. Computers and Education: Artificial Intelligence, 1, 100002.

Dempere, J., Modugu, K., Hesham, A., & Ramasamy, L. K. (2023, September). The impact of ChatGPT on higher education. In Frontiers in Education (Vol. 8, p. 1206936). Frontiers Media SA. http://dx.doi.org/10.3389/feduc.2023.1206936

Hamm, M. S., & Spaaij, R. (2017). The age of lone wolf terrorism. New York: Columbia University Press.

M. M. L. Cairns "Computers in education.(2017). The impact on schools and class rooms," in Life Schools Classrooms. Singapore: Springer, 2017,pp. 603-617.

Memarian, B., & Doleck, T. (2023). ChatGPT in education: Methods, potentials and limitations. Computers in Human Behavior: Artificial Humans, 1(2), 100022. https://doi.org/10.1016/j.chbah.2023.100022

Michel-Villarreal, R., Vilalta-Perdomo, E., Salinas-Navarro, D. E., Thierry-Aguilera, R., & Gerardou, F S. (2023). Challenges and opportunities of generative AI for higher education as explained by ChatGPT. Education Sciences, 13(9), 856. https://doi.org/10.3390/educsci13090856

Ng, D. T. K., Leung, J. K. L., Su, J., Ng, R. C. W., & Chu, S. K. W. (2023). Teachers' AI digital competencies and twenty-first century skills in the post-pandemic world. Educational technology research and development, 71(1), 137-161.

Ouherrou, N., Elhammoumi, O., Benmarrakchi, F, & El Kafi, J. (2019). Comparative study on emotions analysis from facial expressions in children with and without learning disabilities in virtual learn-

WALLER, R. (2020). PLANNING FOR CYBER SECURITY IN SCHOOLS: THE HUMAN FACTOR. Educational Planning, 27(2),23-39.

Saravanakumar, A., & paavizhi, K. (2022). Digital Innovation on Cyber Security-An Overview. Alagappa University.

Schönberger, M. (2023). ChatGPT in higher education: the good, the bad, and the university. In 9th International Conference on Higher Education Advances (HEAd'23) (pp.9-22). Universitat Politecnica. http://dx.doi.org/10.4995/HEAd23.2023.16174.

ing environment. Education and Information Technologies, 24(2), 1777–1792.

Park, Y. (2016). 8digital life skills all children need and a plan for teaching them. World Economic Forum. Retrieved from.

Quayyum, F (2021). Cyber Security Education for Children Through Gamification: Challenges and Research Perspectives. Norwegian University of Science and Technology.

RICHARDSON, M., LEMOINE, P., STEPHENS, W., &