الاتحاد العربي للتنمية المستدامة والبيئة

المجلة الدولية للأبحاث العلمية والتنمية المستدامة

(IJSRSD)

تمكين الأمن السيبراني في ضوء مدخل الذكاء الإصطناعي بالجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان وإمكان الإفادة منها في مصر

إكرام عبد الستار محمد دياب

قسم العلوم التربوية والنفسية - كلية التربية النوعية – جامعة الزقازيق

معلومات البحث

الكلمات المفتاحية:
الأمن السيبراني ، الذكاء الاصطناعي ، الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان.

المؤلف:
إكرام عبد الستار محمد دياب

التسجيل: يونيو ٢٠٢٣

الموافقة: سبتمبر ٢٠٢٣

المستخلص

تهدف الدراسة إلى تقديم بعض الإجراءات المقترحة لتمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي وخبرة الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان لكون تمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي من أهم القضايا التي نادت بها نتائج الدراسات السابقة ، بل وأكدت علي ضرورة عمل بحوث ودراسات في هذا المجال ، لما لتلك المتغيرات من تأثير وبشكل كبير في تطوير جميع العمليات المتعلقة بالموارد البشرية وغير البشرية ؛ وذلك من خلال إجراء مقارنة لتمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي في ضوء خبرة الجامعة الوطنية بأستراليا وجامعة طوكيو باليابان، ولتحقيق ذلك استخدمت الدراسة المنهج المقارن ، وتعرض الدراسة إطارا نظريا لتمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي ، يلي ذلك مقارنة بين الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي، ثم التوصل لمجموعة من النتائج وتقديم بعض الإجراءات المقترحة التي تستهدف تمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي ، وفي ضوء خبرة الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان للسعي نحو تمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية ، وذلك بما يتناسب مع ظروف المجتمع المصري.

Enabling cyber security in light of the introduction of artificial intelligence at the National University of Australia and the University of Tokyo in Japan and the possibility of benefiting from it in Egypt

Ekram Abdelstar Mohamed Diab

Department of Educational and Psychological Sciences, Faculty of Specific Education, Zagazig University

ARTICLE INFO

Keywords:

Cyber Security, Artificial Intelligence, National University of Australia, and University of Tokyo, Japan

Corresponding author:

Ekram Abdelstar Mohamed Diab

Received Jun. 2023

Accepted Sept. 2023

ABSTRACT

The study aims to present some proposed measures to enable cyber-security in Egyptian universities in the light of the introduction of artificial intelligence and the experience of the National University in Australia and the University of Tokyo in Japan, because enabling cyber-security in universities in the light of the approach of artificial intelligence is one of the most important issues called for by the results of previous studies, and even stressed the need to work Research and studies in this field, because these variables have a great impact on the development of all processes related to human and non-human resources; This is done by conducting a comparison to enable cybersecurity in universities in the light of the introduction of artificial intelligence in the light of the experience of the National University in Australia and the University of Tokyo in Japan. The National University of Australia, and the University of Tokyo in Japan in the field of enabling cybersecurity in light of the introduction of artificial intelligence, and then reaching a set of results and presenting some proposed procedures aimed at enabling cybersecurity in Egyptian universities in light of the entrance of artificial intelligence, and in light of the experience of the National University of Australia and the University of Tokyo in Japan to strive Towards enabling cybersecurity in universities in light of the introduction of artificial intelligence in Egyptian universities, in proportion to the conditions of Egyptian society.

مقدمة:

قدمت الثورة العلمية والتكنولوجية المصاحبة للمجتمعات المعاصرة المزيد من تكنولوجيا المعلومات والاتصالات، مما فرض على الجامعات ضرورة مواكبة تلك التحولات المستمرة التي نشأ عنها أنماطا جديدة من مفاهيم التعلم في الجامعات قائمة على الذكاء الاصطناعي والتعلم الرقمي والتعلم الذكي والتعلم الافتراضي، الوضع الذي فرض على الجامعات ضرورة السعي نحو امتلاك بنية تحتية رقمية قادرة على المنافسة على مستوى العالم في الفضاء السيبراني المستحدث الذي يشتمل على أعداد من البيئات الافتراضية التي لا حصر لها.

ومع توجه الحكومات نحو تطبيق استراتيجيات الرقمنة لمختلف المؤسسات؛ وذلك لتحسين مستوى الأداء؛ تبنت الجامعات استراتيجيات تواكب الذكاء الاصطناعي وتطبيقاته المختلفة؛ وذلك لمواكبة التحديات والتغيرات السريعة التي تحيط بها. ولقد أصبحت المعلومات مادة سهلة لارتكاب الجرائم الإلكترونية أو ما يعرف بالجريمة السيبرانية، وخاصة مع تزايد اعتماد المجتمعات

على تطبيقات الذكاء الاصطناعي بالجامعات، والتطور المستمر في أعداد ووسائل المنصات الرقمية، وخاصة بعد توجه البعض إلى استغلال هذا التقدم في السطو على الآخرين (محمد علي العريان ، ٢٠١١م ، ص ٢٣)

وتجدر الإشارة إلى خطورة الأنشطة الإجرامية (الهاكرز)، والتي تدمر الممتلكات، وتعطل الخدمات؛ وذلك من خلال آليات إختراق متطورة ومتجددة باستمرار، وتتعدد هجمات الهاكرز وتتنوع حسب الجهات والأزمنة، والأماكن، ويتم ذلك من خلال العديد من الأساليب التي تستهدف إيذاء المستخدمين واختراق شبكات المعلومات والتلاعب به (Alkhatani,2020,p.5).

وتأسيسا على ما سبق أصبحنا نتعامل مع جرائم مكتملة الأركان تحدث بأشكال كثيرة ومتعددة، وتتم من خلال أجهزة الكمبيوتر وشبكات الإنترنت (المملكة العربية السعودية، الاستراتيجية الوطنية للأمن السيبراني ، ٢٠٢٠م ، ص١٣). ويقصد بالجرائم السيبرانية : أنها مجموعة من الأعمال والأنشطة غير النظامية، وغير المشروعة، وغير القانونية، والتي تحدث في مكون أو أكثر من مكونات الإنترنت مثل (البريد الالكتروني، أو غرف المحادثة، أو المواقع الإلكترونية)، والتي تعد من أخطر التحديات التي تواجه أمن المعلومات خاصة إذا تمكنت من فئات المجتمع ومؤسساته حيث تسبب خسائر وأضرار لاحصر لها وتعد الأنظمة الأمنية للذكاء الاصطناعي بالجامعات، والتي تتمثل أهمها في نظام الكشف التلقائي للاختراق (Intrusion Detection System IDS) ، نظام الجدار الناري المتقدم (Next Generation Fire Walls (NGFW، نظام الأمن السحابي Cloud (CS) Security، ونظام التعرف على السلوك غير العادي User and Entity Behavior Analytics(UEBA) ، ونظام الإدارة التلقائية للأمن Automated Security Management(ASM) ، ونظام الأمن الإداري المتقدم Advanced Administrative Security (AAS)، والتي تعد أهم أنظمة الذكاء الاصطناعي التي تساهم في إتاحة ودقة المعلومات وأيضا الحفاظ على سرية المعلومات بما يساهم في تمكين الأمن السيبراني (Yan, Z., Xue, Y., & Lou, Y., 2021,pp.1- 2).

وتجدر الإشارة إلى ارتفاع تكلفة مكافحة الجرائم السيبرانية، والتي تم تقديرها ب ٣ تريليون دولاراً عام ٢٠٢٠م ، وهذا يدل على تزايد عدد الجرائم إلى ٣٣% تزامنا مع انتشار جائحة (كوفيد ١٩) على مستوى العالم، كما وصل حجم الإنفاق على الأمن السيبراني إلى ١٨٠ دولاراً سنوياً؛ وذلك وفقا لتقرير إدارة تحالف القطاع الخاص العالمي التابعة للأمم المتحدة في ديسمبر ٢٠٢٠م ، كما تم تقدير الخسائر العالمية الناتجة عن الجرائم السيبرانية بنحو ٦ تريليون دولاراً مع حلول عام ٢٠٢١م ، ويمثل هذا ضعف المبلغ الذي تم رصده عام ٢٠١٥م (المركز المصري للدراسات الاقتصادية ، ٢٠١٩م ، ص٢).

وهذه التكاليف الباهظة جاءت نتيجة الخسائر الكبيرة التي نتجت عن الجرائم السيبرانية، والتي تمثل أهمها في سرقة الأموال، والتخريب، وسرقة البيانات، وتعطيل الإنتاجية وتشويه السمعة، واختراق الأنظمة (مركز المعلومات ودعم اتخاذ القرار ، ٢٠٢٠م ،ص ٥). هذا ومن المتوقع أن يصل الإنفاق العالمي على الأمن السيبراني إلى ١٣٣,٧ مليار دولار بنهاية عام ٢٠٢٢م (إيمان علاء الدين سليمان ، ٢٠٢١م ، ص ٦٢).

لذا اصبح من الضروري تطبيق مجموعة من الوسائل والإجراءات والاستراتيجيات اللازمة للحفاظ على دقة وسرية المعلومات الخاصة بالأفراد، والمؤسسات، و تحقيق الاستفادة من مميزات الأنظمة الأمنية للذكاء الاصطناعي (عبد الكريم سلمان اللصاصمه ، فايز عبد القادر مناور ، ٢٠٢٢م ، ص ٨٣)، وذلك لمنع الاستخدام غير المصرح به للمعلومات بالإضافة إلى منع الاختراقات عبر أجهزة الكمبيوتر؛ وذلك بتمكين الأمن السيبراني، والذي يعد بمثابة بعد جديد ضمن أبعاد الدراسات الأمنية، ونهجا استراتيجياً للتخطيط والتشغيل والتصميم حيث يعتمد على الإستفادة من التكنولوجيا الرقمية دون خوف، وزيادة فرص التطوير والابتكار بل أصبح بمثابة سلاحاً استراتيجياً فعالاً في أيادي الحكومات والمؤسسات، ويؤثر في جميع الجوانب الإنسانية، والاقتصادية، والاجتماعية، وله عظيم الأثر في الحفاظ على المعلومات لكل المؤسسات، والتي من أهمها الجامعات خاصة في عصر الذكاء الاصطناعي (أسماء أحمد أبو زيد علام ، ٢٠٢١م ،ص ٣).

وتجدر الإشارة إلى أن الجامعة تتميز بدورها الرائد في تطوير المجتمعات باعتبارها أحد أهم المؤسسات التربوية التي تقع في مقدمة الهرم التعليمي، ويقع على عاتقها العديد من المسؤوليات التي ترتبط بتلبية احتياجات المجتمع، وحل مشكلاته فضلا عن أنها

تعتبر حرما كبيراً لأعضاء هيئة التدريس، والفئات المتنوعة من حيث المستوى الاجتماعي، والاقتصادي، ومن حيث الفكر، ولها دور كبير في توعية أعضاء هيئة التدريس، والطلاب بمدى أهمية تمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي فتعد الجامعات الآن من أبرز المؤسسات التي تواجه المزيد من التحولات المستمرة المرتبطة بتدفق المعلومات اللانهائي الناتج عن الثورة التكنولوجية، والعلمية التي تزامن ظهورها مع المجتمعات المعاصرة (عبير أحمد علي كاعوه ، ٢٠٢٠م ، ص ١٣٧).

وتجد الإشارة إلى أن الذكاء الاصطناعي يساعد في القيام ببعض المهام مثل : الإجابة على استفسارات الطلاب، وينمي قدرات أعضاء هيئة التدريس والقيادات الجامعية على تغيير تركيزهم على الأمور البسيطة إلى حل المشكلات الأكثر تعقيداً، والتواصل مع جميع الطلاب على جميع المستويات (Klutka Justin,Ackerly Nathan,Magda Andrew,2018,p.4) .

ولكون الذكاء الاصطناعي من أبرز التطبيقات الحديثة لنظم المعلومات ومجالاً حديثاً للمعرفة التي تهتم بدراسة طبيعة الذكاء البشري وفهمه ومحاكاته؛ وذلك من خلال جيل جديد من أجهزة الحاسوب الذكية التي يمكن برمجتها للقيام بالمزيد من المهام المؤسسية التي تحتاج إلى قدرات فائقة على الإدراك والاستنتاج والاستدلال وهي الصفات التي يتمتع بها العاملون ومدرجة في قائمة سلوكيات ذكية (Aiyed Share Aldosari,2020,p.145) .

وتجدر الإشارة إلى أن الذكاء الاصطناعي يؤدي دوراً كبيراً في أبحاث علوم الإدارة، ويتم تناول الذكاء عموماً على أنه القدرة على جمع المعرفة لحل المشكلات المعقدة في المستقبل القريب للجامعات كما يقوم الذكاء الاصطناعي على دراسة الآلات، والبرمجيات الذكية التي يمكنها التعامل مع الأشياء وإدراكها والتفكير، وجمع المعرفة ، والتعلم ، والتواصل، ويختلف الذكاء الاصطناعي عن علوم الحاسوب في كونه يركز على العمل، والاستدلال، والادراك، ويجعل الآلات أكثر ذكاء وفائدة، وتطورت تقنيات الذكاء الاصطناعي إلى درجة كبيرة حيث استطاعت تحويل الجامعات من مجرد جامعات نظرية في العديد من المجالات إلى جامعات قادرة على تطبيق المعرفة من خلال الذكاء الاصطناعي (Mudit Verma ,2018,p.2) .

وتتميز الجامعة الوطنية باستراليا بقدرتها الفائقة في مجال الذكاء الاصطناعي وتمكين الأمن السيبراني، ومن خلال البرامج الأكاديمية التي تقدمها، ويظهر ذلك في مجال تمكين الأمن السيبراني في ضوء الأنظمة الأمنية للذكاء الاصطناعي، بل واستطاعت هذه الجامعة أن تحول رؤيتها إلى واقع ملموس، مما جعلها تشكل مركزًا بارزًا في مجال الذكاء الاصطناعي وتمكين الأمن السيبراني (National University of Australia." Retrieved from https://www.anu.edu.au)

كما تتميز جامعة طوكيو بأنها إحدى الجامعات الرائدة في مجال الذكاء الاصطناعي وتمكين الأمن السيبراني باليابان والعالم بأسره، حيث تستخدم الجامعة التكنولوجيا والبحث العلمي والتعليم لتعزيز الابتكارات والتقنيات المتطورة في هذين المجالين، والقيام باستخدام تطبيقات الذكاء الاصطناعي بشكل مكثف مما جعل الجامعه تكثف دراستها في مجال تمكين الأمن السيبراني فأصبحت بذلك أحد أهم وأبرز الجامعات في مجال تمكين الأمن السيبراني في ضوء الذكاء الاصطناعي (Academia.edu..pp.2٢٠٢١)

كما تواجه الجامعات تحديًا مستمرًا في مجال تمكين الأمن السيبراني ، وتعد الأنظمة الأمنية للذكاء الصناعي أحد أهم المداخل التي تساهم في تمكين الأمن السيبراني من خلال توفير التحليل الآلي للبيانات السيبرانية ، بالإضافة إلي مساعدة الجامعات في تحديد المخاطر الأمنية ووضع حلول لحماية النظام السيبراني من التهديدات الخارجية والداخلية. علاوة على ذلك، يمكن استخدام الأنظمة الأمنية للذكاء الصناعي لوقف التهديدات السيبرانية الجديدة (Li, X., Shen, J., & He, W. ,2020, p. 8)

وتجدر الإشارة إلي أن استخدام التكنولوجيا في تزايد مستمر في جميع أنحاء العالم بشكل متزايد، مما يؤدي إلى زيادة الخطر الذي يواجه الأفراد والمنظمات في عصرنا الحالي. وتعد من أبرز الجهود المصرية في مجال تمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي مشاركة وزير التعليم العالي والبحث العلمي المصري في فعاليات المؤتمر الدولي الذي نظمته وزارة التعليم بجمهورية الصين الشعبية بعنوان "الذكاء الاصطناعي والتعليم"، بالتعاون مع منظمة اليونسكو وحكومة بلدية بكين، وذلك في الفترة من ١٦-١٨ مايو (٢٠٢٠)، وقدّم الوزير الاستراتيجية الوطنية المصرية للذكاء الاصطناعي، وأكد على أن مصر

ستركز على ركنين أساسين في مجال الذكاء الاصطناعي، أولهما بناء القدرات من خلال رفع مهارات العاملين، وإعداد أجيال من الباحثين والخبراء المتخصصين في الذكاء الاصطناعي؛ لوضع مصر ضمن الدول الرائدة في تبني الذكاء الاصطناعي، وتزويد الأجيال القادمة بالمهارات والمعرفة اللازمة للمستقبل والتقنيات المتقدمة، والآخر يركز على التطبيقات مخالتي تتمثل في ريادة الأعمال، والقطاعات ذات الأولوية، ووضع إطار لتطوير التطبيقات (https://www.elwatannews.com, 2020). حيث يبدو الوضع في مصر في بداية طريق طويل نحو التوجه لرسم معالم استراتيجية.

الأمن السيبراني بكل جامعة مصرية، فمازالت جهود الجامعات قاصرة على تقديم القليل من البرامج التدريبية للمستفيدين ، وشراء بعض البرامج (antivirus) ضد بعض المهاجمين أو المخترقين لبرامج الجامعة، وهو ما يشير إلى ضرورة تمكين الأمن السيبراني بكل جامعة.

وفي ضوء ما سبق يعد الاهتمام بتمكين الأمن السيبراني باعتباره قضية أمن قومي وهدفاً ومقوماً أساسياً لحماية الأنظمة الإلكترونية ، والبيانات، والشبكات المتعددة من الاختراقات والهجمات أمراً في غاية الأهمية؛ وذلك للوصول إلى فضاء إلكتروني آمن كأحد مستحدثات التطورات التكنولوجية، والرقمية الحديثة التي نعيشها في عالمنا المعاصر مؤخراً مع ضرورة نشر الثقافة والوعي بمدى أهمية الأمن السيبراني، وماهيته التي أصبحت جزءًا أساسياً من تطور الذكاء الاصطناعي، وعليه تتضح ضرورة قيام الجامعات المصرية بتمكين الأمن السيبراني بها في ضوء مدخل الذكاء الاصطناعي وهذا ما تستهدفه الدراسة الحالية.

مشكلة الدراسة :

على الرغم من الجهود المصرية المبذولة في مجال تمكين الأمن السيبراني في ضوء الذكاء الاصطناعي بالجامعات المصرية إلا أنه وفي ظل زيادة التوجه العالمي من قبل الجامعات لمواكبة التطورات التقنية والمعلوماتية للذكاء الاصطناعي وتغلغله في سائر المعلومات والاتصالات وفي شتي نواحي الحياة المختلفة ، وأيضا في ظل ما شهدته الجامعات من تحول رقمي في أغلب عملياتها فقد زاد من حجم التوسع في تبادل البيانات والمعلومات الأمر الذي ساعد في انتشار حجم الاختراقات وظهور جرائم من نوع جديد تختلف بشكل كبير من حيث وسائلها ومرتكبيها عن مفهوم الجريمة التي اعتادت عليها المجتمعات، وهو ما اصطلح على تسميته بالجريمة الإلكترونية، والتي تزداد تبعاتها بانتشار عدد المستخدمين؛ وبذلك أصبح الفضاء السيبراني بيئة خصبة لتلك الجرائم والهجمات الإلكترونية التي تخطت خسائرها واحد تريليون دولار في عام ٢٠٢٠م، وزادت وانتشرت لتصل إلى ستة تريليون دولار في عام ٢٠٢١م ، ومن المتوقع أن يلحق بالعالم خسائر تقدر بحوالي ١٠,٥ تريليون دولار؛ وذلك بحلول عام ٢٠٢٥م من قبل المخترقين السيبرانيين سواء كانوا أفرادا أو مجموعات منظمة، بالإضافة إلى الأعمال الإرهابية التي يتم تمويلها من قبل بعض الدول؛ نتيجة للطبيعة المفتوحة لتلك البيئات الافتراضية والضعف في الرقابة القانونية الصارمة (تقرير مجلس الوزراء المصري ودعم اتخاذ القرار ، ٢٠٢٠م ، ص١٣) .

واتساقا مع ما سلف بيانه فقد أشارت المعلومات الصادرة عن الاستراتيجية الوطنية للأمن السيبراني أنها قامت بالتعامل مع العديد من التحديات والأخطار السيبرانية التي تمثلت في الحرب السيبرانية، وخطر الإرهاب، وخطر الاختراق والقرصنة، وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات، وخطر سرقة الهوية الرقمية، والبيانات الخاصة (الإستراتيجية الوطنية للأمن السيبراني ، ٢٠١٧-٢٠٢١م، ص٦).

وتعد تلك التحديات بمثابة دوافع أساسية لقيام مختلف مؤسسات التعليم خاصة الجامعي إلى وضع آليات لتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي وتأمين أنظمة البيانات والمعلومات واتساقا مع ما سلف بيانه جاءت العديد من توصيات الدراسات السابقة ، والتي من أهمها دراسة (عبير أحمد علي كاعوه ، ٢٠٢٠م) ، والتي أكدت على ضرورة تمكين سياسات الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي للجامعات مع الاهتمام بنشر الوعي والثقافة بمعايير أمن المعلومات بتلك الجامعات؛ وذلك لتدريب الجامعة على التعامل مع أي سطو أو اقتحام غير مصرح به مع أنظمة المعلومات أو مواجهة أي هجوم

محتمل خاصة بعد أن رصدت الدراسة أن هناك العديد من المخاطر السيبرانية المتعددة في ظل هلامية السياسات الخاصة ببرامج الحماية والأمن السيبراني وجاءت دراسة (رشا عبد القادر محمد الهندي ، ٢٠٢١م)، والتي تناولت دور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول، وتوصلت إلى العديد من النتائج ، والتي من أهمها تقديم تصور مقترح لدور جامعة القاهرة في توعيه طلاب الدراسات العليا بمدى أهمية الأمن السيبراني في ضوء خبرات بعض الدول كما توصلت للعديد من التوصيات، والتي من أهمها ضرورة نشر الوعي بمدى أهمية تمكين الأمن السيبراني، بالإضافة إلى توضيح مدي ضرورة إنشاء إدارة خاصة بالأمن السيبراني، وتشجيع البحوث العلمية التي تتناول مجال تمكين الأمن السيبراني وأكدت الدراسة على أن هناك ضعف معرفي واضح بجامعة القاهرة عن ماهية الذكاء الاصطناعي وسياساته، ومدى قدرته على المساهمة في حماية الأنظمة المعلوماتية بالإضافة إلى قلة الخبرة والوعي، والتدريب للفنيين والعاملين بنظم المعلومات مما أدى إلى حدوث تحديات كثيرة ذات علاقة بالاختراقات الأمنية ، والتهديدات المستمرة، والقرصنة لأنظمة الجامعة، وقد أدي إنتشار هذه الجرائم السيبرانية إلى الشعور بالقلق لدى العديد من الباحثين مما حدا بهم للتأكيد على أهمية تمكين الأمن السيبراني؛ وذلك للحفاظ على فعالية المؤسسات التعليمية، وكفاءه أمن المعلومات بالجامعات ، ولهذا تتضح أهمية الدراسة الحالية في كونها تسعى لتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية حتى يمكن المحافظة على معلوماتها الالكترونية، وتجنب أي قرصنة على المواقع الالكترونية الخاصة بالجامعات المصرية ، بالإضافة إلى الحفاظ على سريتها، وحمايتها من أي اختراق إلكتروني أو تخريب ، واتساقا مع ما سلف بيانه تأتي هذه الدراسة لتقديم مجموعة من الإجراءات المقترحة لتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية.

وعليه يمكن بلورة مشكلة الدراسة في السؤال الرئيسي التالي :

كيف يمكن تمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي في ضوء خبرة الجامعة الوطنية باستراليا وجامعة طوكيو باليابان؟

وفي سبيل ذلك ستعمد الدراسة الإجابة عن الأسئلة الآتية :

١. ما الإطار النظري لتمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي و الأدبيات المعاصرة ؟
٢. ما واقع تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا في ضوء العوامل البنيوية والقوى الثقافية المؤثرة فيه؟
٣. ما واقع تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بجامعة طوكيو باليابان في ضوء العوامل البنيوية والقوى الثقافية المؤثرة فيه؟
٤. ما أوجه التشابه والاختلاف بين الجامعة الوطنية باستراليا، وجامعة طوكيو باليابان في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي؟ وأسباب التشابه والاختلاف في ضوء بعض مفاهيم العلوم الاجتماعية ذات العلاقة؟
٥. ما أهم الجهود المصرية المبذولة في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية في ضوء العوامل البنيوية والقوى الثقافية المؤثرة فيه؟
٦. ما الإجراءات المقترحة لتمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي في ضوء خبرتي الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان؟ بما يساهم في تحقيق رؤية مصر ٢٠٣٠ م ، وبما يتناسب مع السياق الثقافي المصري؟

أهداف الدراسة :

يتمثل الهدف الرئيس للدراسة في تقديم إجراءات مقترحة لتمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي وفي ضوء خبرة الجامعة الوطنية باستراليا، وجامعة طوكيو باليابان، بالاستعانة بكل من الإطار النظري، وخبرات الدول محل الدراسة.

ويتفرع من الهدف الرئيس مجموعة أهداف فرعية وهي كالتالي :

١. تقديم إطار نظري في مجال تمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي في ضوء الأدبيات المعاصرة .
٢. التعرف علي واقع تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا في ضوء العوامل البنيوية والقوى الثقافية المؤثرة فيه .
٣. التعرف علي واقع تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بجامعة طوكيو باليابان في ضوء العوامل البنيوية والقوى الثقافية المؤثرة فيه.
٤. الكشف عن أوجه التشابه والاختلاف بين تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بين الجامعة الوطنية باستراليا وجامعة طوكيو باليابان ، وتوضيح أهم أسباب تلك التشابهات والاختلافات في ضوء بعض مفاهيم العلوم الاجتماعية ذات العلاقة.
٥. الكشف عن أهم الجهود المصرية المبذولة في مجال تمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي ، و في ضوء العوامل البنيوية والقوى الثقافية المؤثرة فيه.
٦. التوصل إلي بعض الإجراءات المقترحة لتمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي ، وفي ضوء خبرة الجامعة الوطنية باستراليا وجامعة طوكيو باليابان، بما يساهم في تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية، وبما يتناسب مع السياق الثقافي المصري.

أهمية الدراسة:

١. أن مفهوم تمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي لم يلق الاهتمام الكافي من الدراسات السابقة على مستوى مؤسسات التعليم بشكل عام والتعليم الجامعي بشكل خاص على حد علم الباحث.
٢. أن هذه الدراسة تأتي تزامنا مع اهتمام الوزارة بالتعليم الجامعي- كما يتضح في خطتها الاستراتيجية .
٣. أن تمكين الأمن السيبراني بصفة عامة له أهميته وتأثيره الكبير في زيادة فعالية العملية التعليمية ، وفي الفعالية الجامعية بشكل خاص .
٤. قد تساعد متخذي القرار بمصر في الإطلاع على بعض الإجراءات المقترحة لتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية في ضوء خبرة الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان بما يساهم في تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية ، وبما يتناسب مع السياق الثقافي المصري.

مصطلحات الدراسة :

يعرض هذا الجزء المصطلحات الواردة في عنوان الدراسة ، ويأتي التحليل التفصيلي للمصطلحات بالإطار النظري للدراسة ، وذلك فيما يلي:

١-الأمن السيبراني:(Cyber Security) :

ويمكن تناوله علي النحو التالي :

أ- **الأمن:** هو مجموعة التدابير ، والإجراءات التي تساهم في تلبية الحاجات البشرية الأساسية ، والتي من أهمها تلبية حاجة البشر للحماية من الأخطار(Fouad Noran Shafik,2021,pp.33-34).

ب- **السيبراني:** لقد ظهر هذا المصطلح حديثا في قواميس اللغة الإنجليزية، وأصلها كلمة يونانية مأخوذة من كلمة cyber والمشتقة من cybernetics ، وتعني باللغة العربية (إلكتروني) وتشمل كل ما يتصل بأجهزة الكمبيوتر وتكنولوجيا المعلومات والواقع الافتراضي .وتعرف إجرائيا بأنها كل ما يرتبط بتقنية المعلومات والحاسب الآلي، ويقصد بها فضاء الإنترنت، أو العالم الافتراضي الذي يولج إليه عبر شبكات الإنترنت المترابطة والمفتوحة للجميع.

(Aljohni, Wejdan., Mohamed, Nazar Elfadil., Jarajreh, Mutsam and Gasmelsied, Mwahib ,2021,pp.22-23)

اتساقا مع ما سلف بيانه يمكن تعريف **الأمن السيبراني إجرائيا** : مجموعةالإجراءات التي ينبغي أن توفرها الجامعات المصرية، بهدف حماية المصادر المتنوعة والتي يتمثل أهمها في البيانات الرقمية الشخصية ، والبرمجيات والأجهزة المحمولة، من القرصنة ، والتدخلات غير المشروعة أو سوء الاستغلال، أو الحوادث غير المتوقعة، ومقاومة محاولات الاختراق وتعزيز خصوصيتها وتشفيرها، واتخاذ إجراءات لحماية الجامعات من مخاطر الفضاءالسيبراني.

٢-الذكاء الاصطناعي: Artificial intelligence: يعرف الذكاء - في اللغة – بأنه سرعة الفطنة، وذكى كرضى وسعى وكرم فهو ذكي (آبادي الفيروز، ٢٠٠٨م، ص٥٩٤). ويعرف الذكاء الاصطناعي بأنه دراسة كيفية جعل أجهزة الحاسب تقوم بأشياء يقوم بها الأشخاص في الوقت الحالي بشكل أفضل(Kriti , Brian , Anshuman, 2018, p.67)-.

ويعد الذكاء الاصطناعي (AI) أحد مجالات علوم الحاسب التي تركز على صناعة هذا النوع من الآلات الذكية التي تعمل وتقدم ردود فعل مشابهة للجنس البشري؛ ولذلك يمكن تعريفه بأنه: برمجة الآلات التي تستطيع أن تفكر وتتصرف بطريقة الجنس البشري نفسها، ويمكن تعريفه أيضًا بأنه: صناعة برامج الحاسبات لحل المشكلات المعقدة مشابها في ذلك للحلول البشرية التي يتم تقديمها لهذه المشكلات، ومن ثم فهو مقسم إلى جزأين أحدهما حل المشكلات المعقدة عن طريق الآلة، والآخر : تشابهه مع الجنس البشري (Verma, 2018,p.4).

ويعمل الذكاء الاصطناعي على تصميم أنظمة الكمبيوتر الذكية؛ أي الأنظمة التي تعرض الخصائص التي تربطها بالذكاء في السلوك البشري من حيث فهم اللغة والتعلم والاستدلال وحل المشكلات؛ أي استخدام الحاسب لتكرار أو استبدال الذكاء البشري لتوفير رؤى من خلال تطبيق العمليات التحليلية المختلفة التي تمكن الآلة من مجموعات البيانات الكبيرة , Kriti) (Anshuman, 2018,p. 68.

واتساقا مع ما سلف بيانه يمكن تعريف الذكاء الاصطناعي إجرائيا علي النحو التالي : توظيف الأنظمة الأمنية للذكاء الاصطناعي والتي من أهمها - نظام الكشف التلقائي للاختراق ، نظام الجدار الناري المتقدمة بالجامعات ، نظام الأمان السحابي ، نظام التعرف على ملامح السلوك غير العادي ، نظام الإدارة التلقائية للأمن ، نظام الأمن الإداري المتقدم ، وبرمجة الحواسيب الرقمية والآلات لمحاكاة مهام العنصر البشري في الجامعات من أجل أداء الأعمال بأعلى مستوى بالإضافة إلى حل المشكلات المعقدة.

حدود الدراسة:

تتناول الدراسة الحالية الحدود التالية :

١- **الحدود الموضوعية** ، وتشمل :

أ- **فيما يتعلق بدراسة أنظمة الذكاء الاصطناعي** ؛ فإن الدراسة قد اقتصرت علي :

١) نظام الكشف التلقائي للاختراق بالجامعات Intrusion Detection System (IDS)

٢) (٢) نظام الجدار الناري المتقدم بالجامعات (Next Generation Fire Walls (NGFW

٣) نظام الأمن السحابي بالجامعات. Cloud Security

٤) نظام التعرف على السلوك غير العادي بالجامعات.

٥) User and Entity Behavior Analytics(UEBA) :

٦) نظام الإدارة التلقائية للأمن بالجامعات(ASM)Automated Security Management .

٧) نظام الأمن الإداري المتقدم بالجامعات(AAS) Advanced Administrative Security

ب- أما بالنسبة للأمن السيبراني بالجامعات ، فإن الدراسة اقتصرت علي الأبعاد الرئيسية للأمن السيبراني بالجامعات والتي تتمثل فيما يلي :

١) السرية Confidentiality :حماية المعلومات من الاطلاع عليها من غير صلاحيات

٢) دقة المعلومات Integrity : ويقصد بها التأكد من أن المعلومة لم يتم تعديل أو إضافة أو حذف جزء منها دون تصريح.

٣) إتاحة المعلوماتAvailability : إتاحة الحصول على المعلومات لمن لديه الصلاحيات.

٤) يمكن تناول أهم مبررات اختيار الجامعة الوطنية بأستراليا وجامعة طوكيو باليابان كخبرتين رائدتين في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي وذلك علي النحو التالي:

ج- مبررات اختيار دول الخبرات :

يمكن تناول ذلك من خلال مايلي :

(١) الجامعة الوطنية بأستراليا:

هناك تشابه بين الجامعة الوطنية بأستراليا والجامعات المصرية في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي ، والتي تعكس التركيز العالمي المتزايد على هذه القضية ، والتي من أهمها على النحو التالي:

١. التركيز على تطوير برامج متخصصة في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي في كلا النظامين الجامعيين، الأسترالي والمصري.

٢. يسعيان جاهدين لتزويد الطلاب بالمعرفة والمهارات اللازمة لفهم ومكافحة التهديدات السيبرانية ولتطوير الأنظمة الأمنية للذكاء الاصطناعي. وتتضمن هذه البرامج دراسة التحليل السيبراني وأمن المعلومات وتقنيات التعلم العميق والشبكات العصبية الاصطناعية، إلخ (Cybersecurity Trends and Predictions , 2021,p.2) .

٣. برامج البحث تعد أيضاً أحد أهم أوجه التشابه بين الجامعة الوطنية باستراليا والجامعات المصرية ، حيث يعمل العديد من الباحثين على تطوير تقنيات وأدوات متطورة في مجالات تمكين الأمن السيبراني والذكاء الاصطناعي. وبالتعاون مع الشركات والجهات الحكومية، يسعى هؤلاء الباحثون لإيجاد حلول مبتكرة وفعالة لمجموعة متنوعة من التحديات.

٤. تشترك الجامعة الوطنية والجامعات المصرية في تنظيم ورش العمل والمؤتمرات والفعاليات المتعلقة بهذين المجالين. تُعقد هذه الفعاليات بهدف تبادل المعرفة والأفكار والابتكارات الجديدة في مجال الأمن السيبراني والذكاء الاصطناعي. وتعمل الجامعتان على تعزيز التعاون المشترك بين الباحثين والخبراء في هذه المجالات ، وذلك من خلال المشاريع المشتركة وتبادل الخبرات (Artificia Intelligence and Cyberecurity, 2022, pp 3-4) .

(٢) مبررات اختيار جامعة طوكيو باليابان:

هناك تشابه بين جامعة طوكيو باليابان والجامعات المصرية في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي، والتي من أهمها على النحو التالي:

١. تعتبر جامعة طوكيو باليابان من أبرز المؤسسات التعليمية التي تسعى لتطوير قدرات تمكين الأمن السيبراني والذكاء الاصطناعي، وتعزيز البحث العلمي والابتكار في هذا المجال، كما تتمتع جامعة طوكيو باليابان بسمعة عالمية ، وبتقدير

عالٍ في مجال الأمن السيبراني والذكاء الاصطناعي، حيث تُنشر العديد من الأبحاث العلمية والدراسات في هذا المجال من قبل جامعة طوكيو باليابان.

٢. توفر جامعة طوكيو والجامعات المصرية برامج ودورات متقدمة في مجال تمكين الأمن السيبراني والذكاء الاصطناعي ، حيث يتم تصميم هذه البرامج لتعليم الطلاب واكتساب المهارات اللازمة للعمل في هذه المجالات الحيوية . Tokyo (University Cybersecurity and Artificial Intelligence, 2022,pp.5-6)

٣. تقدم جامعة طوكيو باليابان والجامعات المصرية الفرصة للطلاب للتعاون مع الشركات والمؤسسات ذات الصلة، مما يتيح لهم التطبيق العملي للمعرفة التي اكتسبوها خلال فترة دراستهم .

٤. تتشابه جامعة طوكيو باليابان والجامعات المصرية في الهدف والتوجه العلمي في مجال الأمن السيبراني والذكاء الاصطناعي،كما تشترك جامعة طوكيو باليابان والجامعات المصرية في سعيهم الحثيث نحو تعزيز القدرات البشرية وحل المشكلات التي تواجه ، وتعزيز الشراكات والتعاون الدولي لتحقيق هذه الأهداف العلمية Egyptian) . Universities Cybersecurity and Artificial Intelligence Initiatives,2022,pp.9-10).

يتضح من مبررات اختيار تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان _مدى التشابه الكبير بينها وبين تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية ، والذي يمكن أن يساعد في تحقيق أفضل استفادة ممكنة منها في تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية .

الدراسات السابقة :

تم ترتيب الدراسات من الأقدم للأحدث ، بداية بالمحور الأول والذي يتناول الدراسات العربية ، ثم المحور الثاني والذي يتناول الدراسات الأجنبية ، ثم التعقيب علي الدراسات السابقة.

المحور الأول : الدراسات العربية:

تم ترتيب الدراسات العربية من الأقدم للأحدث وذلك علي النحو التالي :

١- الذكاء الاصطناعي: سياساته وبرامجه وتطبيقاته في التعليم العالي: منظور دولي ، ٢٠١٩م.

هدفت الدراسة إلي رصد سياسات وبرامج وتطبيقات الذكاء الاصطناعي في التعليم العالي من منظور دولي، واستخدمت الدراسة المنهج الوصفي ، وتوصلت الدراسة إلي العديد من النتائج والتي من أهمها، أن الذكاء الاصطناعي أصبح بتطبيقاته المستحدثة من أهم الآليات التي يجب أن يتم النظر إليها بعين الاعتبار وأن تقوم الجامعات باستحداث الذكاء الاصطناعي كآلية، وكبرنامج في حرمها .

٢- السيناريوهات المقترحة لدور الذكاء الاصطناعي في دعم المجالات البحثية والمعلوماتية بالجامعات المصرية ٢٠٢٠م .

هدفت الدراسة إلى التوصل إلى سيناريوهات مقترحة لدور الذكاء الاصطناعي في دعم المجالات البحثية والمعلوماتية بالجامعات المصرية ، واستخدمت الدراسة المنهج الوصفي ، وتوصلت الدراسة إلى العديد من النتائج والتي أهمها أن نظم الذكاء الاصطناعي يمكنها القيام بالمهام الإدارية مما يساهم في تخيف الأعباء الإدارية وتقديم خدمة أفضل وجودة عالية في العمل، وذلك من خلال تحويل نظام الإدارة لنظم إلكترونية تعتمد على الذكاء الاصطناعي، وبعد مناقشة حيثيات السيناريوهات المقترحة توصلت الدراسة إلى أن السيناريو الامتدادي يصعب تبنيه نظرًا لأنه لن يساهم في تطبيق الذكاء الاصطناعي على النحو المطلوب، أما السيناريو الاصطلاحي فهو يساهم في حدوث بعض الإصلاحات والتغيرات جزئيا بشكل تدريجي في الأوضاع الراهنة .

٣- تقنيات الذكاء الاصطناعي ودورها في التحول التنظيمي للجامعات المصرية: دراسة تطبيقية على جامعة كفر الشيخ ، سيناريوهات مقترحة ، ٢٠٢١م .

هدفت الدراسة إلى الوصول لسيناريوهات مقترحة للتحول التنظيمي بجامعة كفر الشيخ في ضوء تقنيات الذكاء الاصطناعي ، واستخدمت الدراسة المنهج الوصفي وأسلوب السيناريو من أجل الوصول إلى الأهداف التي تم تحديدها ، وتوصلت الدراسة إلى العديد من النتائج والتي أهمها : غياب التوجه الاستراتيجي لدى معظم الجامعات المصرية وسيادة الهياكل التنظيمية النمطية، وضعف نظام المعلومات والتكنولوجيا الحديثة في العمل الجامعي بالإضافة إلى قلة عدد الموارد البشرية المدربة على التكنولوجيا الذكية. كما أن الأنماط الثقافية السائدة في الجامعات المصرية تضعف من قدرتها وتطورها.

٤- دور تطبيقات الذكاء الاصطناعي في تعزيز الاستراتيجيات التعليمية في التعليم العالي: مراجعة الأدبيات ، ٢٠٢٣م

هدفت الدراسة إلى توضيح دور تطبيقات الذكاء الاصطناعي في تعزيز الاستراتيجيات التعليمية في التعليم العالي، واستخدمت الدراسة المنهج الوصفي التحليلي ، وذلك من خلال منهجية مراجعة الأدبيات السردية على عشرون دراسة ، وتوصلت الدراسة إلى العديد من النتائج والتي أهمها النتائج أن للذكاء الاصطناعي دور مهم في تعزيز دور المعلمين وتحسين أداء المتعلمين وجعل عملية التعلم أكثر كفاية، كما أكدت الدراسة على أهمية استخدام تطبيقات الذكاء الاصطناعي في استراتيجيات التعليم وعدم جعل التحديات عائقا في سبيل توظيفه .

٥- واقع استخدام طالبات كلية الدراسات العليا التربوية بجامعة الملك عبد العزيز لتطبيقات الذكاء الاصطناعي في ضوء بعض المتغيرات ، ٢٠٢٣م

هدفت الدراسة إلى إلقاء الضوء على واقع استخدام طالبات كلية الدراسات العليا التربوية بجامعة الملك عبد العزيز لتطبيقات الذكاء الاصطناعي في ضوء بعض المتغيرات ، واستخدمت الدراسة المنهج الوصفي التحليلي ، وتوصلت الدراسة إلى العديد من النتائج والتي من أهمها ضرورة عقد دورات تدريبية لتأهيل طالبات الدراسات العليا على استخدام تطبيقات الذكاء الاصطناعي في العملية التعليمية، وتوفير الميزانية الكافية والتجهيزات اللازمة لاقتناء واستخدام تطبيقات الذكاء الاصطناعي في الجامعة.

٦- متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس ، جامعة بنها أنموذجا ، ٢٠٢٣م .

هدفت الدراسة إلى التعرف على متطلبات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس ، واستخدمت الدراسة المنهج الوصفي ، وتوصلت الدراسة إلى العديد من النتائج أهمها أن هناك العديد من المتطلبات ، والتي تمثلت في مجموعة من المتطلبات التقنية والمادية والبشرية والمعرفية، بالإضافة إلى التوصل إلى معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها.

المحور الثاني : الدراسات الأجنبية :

تم ترتيب الدراسات الأجنبية من الأقدم للأحدث وذلك علي النحو التالي :

١-الذكاء الاصطناعي وعلاقته بالأمن السيبراني ، ٢٠٢٠م.

هدفت الدراسة إلى إلقاء الضوء علي أهمية الأمن السيبراني، وذلك لأن مجرمي الإنترنت يشكلون تهديدًا للجميع، وأشارت الدراسة إلي أن الذكاء الاصطناعي يعد حلاً رائعًا لهذا الأمر، واستخدمت الدراسة المنهج الوصفي التحليلي، وتوصلت الدراسة إلى العديد من النتائج أهمها أن الجمع بين قوة الذكاء الاصطناعي، والأمن السيبراني ، يجعل المؤسسات أكثر قدرة على الدفاع عن الشبكات والبيانات المعرضة للخطر من المهاجمين السيبرانيين.

٢-الذكاء الاصطناعي للأمن السيبراني ،، ٢٠٢١ م .

هدفت الدراسة إلى إلقاء الضوء على استخدام الذكاء الاصطناعي لمعالجة قضايا الأمن السيبراني، واستخدمت الدراسة المنهج الوصفي، وتوصلت الدراسة إلى العديد من النتائج أهمها الهدف الأساسي للأمن السيبراني هو الحفاظ علي دقة وسلامة ، وإتاحة البيانات ولن يتم ذلك إلا في ضوء أساليب الذكاء الاصطناعي.

٣-طبيعة العلاقة بين الذكاء الاصطناعي والأمن السيبراني بالمؤسسات ، ٢٠٢١م

هدفت الدراسة إلى إلقاء الضوء على طبيعة العلاقة بين الذكاء الاصطناعي والأمن السيبراني بالمؤسسات، استخدمت الدراسة المنهج الوصفي التحليلي، وتوصلت الدراسة إلى العديد من النتائج والتي أهمها أن هناك حاجة ماسة للتوسع في الدراسات التي تتناول طبيعة العلاقة بين الذكاء الاصطناعي والأمن السيبراني، وأهمية ذلك في جميع المؤسسات ، وخاصة مؤسسات التعليم العالي .

٤-الذكاء الاصطناعي وعلاقته بدقة وسرية المعلومات ٢٠٢١م.

هدفت الدراسة إلي إلقاء الضوء علي الذكاء الاصطناعي والأمن السيبراني، ومدي أهمية إدارة تعقيد العمليات وحجم المعلومات التي سيتم استخدامها لتأمين الفضاء الإلكتروني من أجل الحماية بنجاح من التهديدات الأمنية، واستخدمت الدراسة المنهج الوصفي ، وتوصلت الدراسة إلي العديد من النتائج والتي من أهمها أن الذكاء الاصطناعي يساعد في عملية صنع القرار الاستراتيجي، من خلال توفير وإتاحة المعلومات الشاملة المهمة لمتخذي القرار، والمساعدة المنطقية في اتخاذ القرار هي واحدة من أهم قضايا الأمن السيبراني

٥-تأثير الذكاء الاصطناعي على التعليم العالي والمؤسسات ، ٢٠٢٣م .

هدفت الدراسة إلى إجراء مراجعة شاملة لمدي تأثير الذكاء الاصطناعي علي الأمن السيبراني في التعليم العالي، واستخدمت الدراسة المنهج الوصفي التحليلي ، وتوصلت الدراسة إلى العديد من النتائج أهمها أن هناك حاجة إلى عمل المزيد من البحوث التي تهتم بإلقاء الضوء علي الفوائد الجوهرية لتطبيق الذكاء الاصطناعي كمدخل لتعزيز الأمن السيبراني بالجامعات .

التعليق علي الدراسات السابقة :

سيتم ذلك من خلال الجدول التالي :

الجدول رقم (١) التعقيب علي الدراسات السابقة

دراسة	الهدف	النتائج
استخدمت الدراسات السابقة التالية من (١-٥) المنهج الوصفي		
١-عبدالجواد السيد بكر : الذكاء الاصطناعي: سياساته وبرامجه وتطبيقاته في التعليم العالي: منظور دولي . ٢٠١٩م	هدفت الدراسة إلي إلقاء الضوء على التطبيقات التكنولوجية المتقدمة في العصر الثاني للآلة، أي تطبيق الذكاء الاصطناعي (artificial intelligence) في برامج داخل الجامعات ومراكز البحوث وفي التعليم العالي بصفة عامة	أن الذكاء الاصطناعي أصبح بتطبيقاته المستحدثه من أهم الآليات التي يجب أن يتم النظر إليها بعين الاعتبار وأن تقوم الجامعات باستحداث الذكاء الاصطناعي كآلية ، وكبرنامج في حرمها.
٢-أسماء أحمد خلف حسن :السيناريوهات المقترحة لدور الذكاء الاصطناعي في دعم	هدفت الدراسة إلى التوصل إلى السيناريوهات المقترحة لدور الذكاء الاصطناعي في دعم المجالات البحثية	أن نظم الذكاء الاصطناعي يمكنها أن تقوم بالإدارة بهدف تخيف الأعباء الإدارية وتقديم خدمة أفضل وجودة عالية في العمل، وذلك من

المجالات البحثية والمعلوماتية بالجامعات المصرية ٢٠٢٠م.	والمعلوماتية بالجامعات المصرية	خلال تحويل نظام الإدارة لنظم إلكترونية تعتمد على الذكاء الاصطناعي .
٣- رمضان محمد محمد السعودي : تقنيات الذكاء الاصطناعي ودورها في التحول التنظيمي للجامعات المصرية: دراسة تطبيقية على جامعة كفر الشيخ ، سيناريوهات مقترحة .٢٠٢١م.	هدفت الدراسة إلى الوصول لسيناريوهات المقترحة للتحول التنظيمي بجامعة كفر الشيخ في ضوء تقنيات الذكاء الاصطناعي	غياب التوجه الاستراتيجي لدى معظم الجامعات المصرية وسيادة الهياكل التنظيمية النمطية، وضعف نظام المعلومات والتكنولوجيا الحديثة في العمل الجامعي بالإضافة إلى قلة عدد الموارد البشرية المدربة على التكنولوجيا الذكية.
4-Raghav Sandhane: Artificial Intelligence in Cyber Security ٢٠٢١م	هدفت الدراسة إلي إلقاء الضوء علي الذكاء الاصطناعي والأمن السيبراني ، ومدي أهمية إدارة تعقيد العمليات وحجم المعلومات التي سيتم استخدامها لتأمين الفضاء الإلكتروني .	أن الذكاء الاصطناعي يساعد في عملية صنع القرار الاستراتيجي ، من خلال توفير وإتاحة المعلومات الشاملة المهمة لمتخذي القرار، والمساعدة المنطقية في اتخاذ القرار هي واحدة من أهم قضايا الأمن السيبراني
٥-صلاح الدين محمد توفيق ، شيرين عيد مرسي : متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمية من وجهة نظر أعضاء هيئة التدريس ، جامعة بنها أنموذجا .٢٠٢٣م	هدفت الدراسة إلى التعرف على متطلبات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس	أن هناك العديد من المتطلبات ، والتي تمثلت في مجموعة من المتطلبات التقنية والمادية والبشرية والمعرفية، بالإضافة إلى التوصل إلى معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها.
بينما استخدم الدراسات السابقة التالية (١-٦) المنهج الوصفي التحليلي		
1- Matthew N. ,Prairie View: Artificial Intelligence in Cyber Security.2020	هدفت الدراسة إلى إلقاء علي الأمن السيبراني لأن مجرمي الإنترنت يشكلون تهديدًا للجميع ، ويعد الذكاء الاصطناعي حلاً رائعًا لهذا الأمر	أن الجمع بين قوة الذكاء الاصطناعي ، والأمن السيبراني ، يجعل المؤسسات أكثر قدرة على الدفاع عن الشبكات والبيانات المعرضة للخطر من المهاجمين السيبرانيين.
2- Ishaq Azhar Mohammed:NOVATEUR PUBLICATIONS.2020	هدفت الدراسة إلى إلقاء الضوء على استخدام الذكاء الاصطناعي لمعالجة قضايا الأمن السيبراني	أنه يمكن معالجة بعض تحديات الأمن السيبراني من خلال استخدام أساليب الذكاء الاصطناعي.
3- Lakshit Malhotra, Bharat Bhushan :Artificial Intelligence	هدفت الدراسة إلى إلقاء الضوء على طبيعة العلاقة بين الذكاء الاصطناعي والأمن السيبراني بالمؤسسات	أن هناك حاجة ماسة للتوسع في الدراسات التي تتناول طبيعة العلاقة بين الذكاء الاصطناعي والأمن السيبراني ، وأهمية ذلك في جميع

and Deep Learning-based Solutions to Enhance Cyber Security.2021.		المؤسسات ، وخاصة مؤسسات التعليم العالي .
4- Bongs Lainjo ,Hanan Tmouche:The Impact of Artificial Intelligence On Higher Learning,2023.	هدفت الدراسة إلى إجراء مراجعة شاملة لتأثير الذكاء الاصطناعي على التعلم العالي .	أن هناك حاجة إلى عمل المزيد من البحوث التي تهتم بإلقاء الضوء علي الفوائد الجوهرية لتطبيق الذكاء الاصطناعي كمدخل لتعزيز الأمن السيبراني بالجامعات .
٥-حليمة حسن إبراهيم الفقيه ، لينا أحمد القرني : واقع استخدام طالبات كلية الدراسات العليا التربوية بجامعة الملك عبد العزيز لتطبيقات الذكاء الاصطناعي في ضوء بعض المتغيرات . ٢٠٢٣م	هدفت الدراسة إلى إلقاء الضوء على واقع استخدام طالبات كلية الدراسات العليا التربوية بجامعة الملك عبد العزيز لتطبيقات الذكاء الاصطناعي في ضوء بعض المتغيرات	ضرورة عقد دورات تدريبية لتأهيل طالبات الدراسات العليا على استخدام تطبيقات الذكاء الاصطناعي في العملية التعليمية، وتوفير الميزانية الكافية والتجهيزات اللازمة لاقتناء واستخدام تطبيقات الذكاء الاصطناعي في الجامعة.
٦- وفاء فواز المالكي : دور تطبيقات الذكاء الاصطناعي في تعزيز الاستراتيجيات التعليمية في التعليم العالي: مراجعة الأدبيات. ٢٠٢٣م.	هدفت الدراسة إلى توضيح دور تطبيقات الذكاء الاصطناعي في تعزيز الإستراتيجيات التعليمية في التعليم العالي	أن للذكاء الاصطناعي دور مهم في تعزيز دور المعلمين وتحسين أداء المتعلمين وجعل عملية التعلم أكثر كفاية.

تتفق الدراسة الحالية مع الدراسات السابقة في تناولها متغيرات الذكاء الاصطناعي ، والأمن السيبراني ، وقد استفادت الدراسة الحالية من تلك الدراسات في الاطلاع على الإطار النظري لتلك الدراسات ، وعلى طبيعة المناهج المستخدمه ، بينما تختلف الدراسة الحالية عن تلك الدراسات السابقة في استخدامها المنهج المقارن ، وأيضاً في استخدامها لمجموعة من الخبرات الرائدة في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي في ضوء خبرة الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان .

منهج وخطوات الدراسة:

تقتضى طبيعة الدراسة الحالية، وما تسعى إليه من أهداف استخدام المنهج المقارن، الذي لا يقتصر علي وصف الظواهر وإنما يقوم بتحليلها وتفسيرها في ظل ظروف مجتمعاتها والقوي الثقافية والمجتمعية السائدة فيها ويعطي بالإضافة إلي ذلك فرص الاستفادة منها بما يتفق وظروف المجتمع المصري (محمد سيف الدين فهمي ، ١٩٨٥م ، ص ص ٥٨٩- ٥٩٠) ، والذى يمكن ترجمته إجرائيا إلى الخطوات التالية:

الخطوة الأولى : تتضمن تحديد الإطار العام للدراسة، ويشمل المقدمة، المشكلة، الأهداف الحدود، الأهمية، منهج الدراسة ، وخطواته.

الخطوة الثانية : تمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي في العالم المعاصر: إطار نظري.

الخطوة الثالثة : تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا: دراسة وصفية تحليلية.

الخطوة الرابعة : تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بجامعة طوكيو باليابان : دراسة وصفية تحليلية.

الخطوة الخامسة : تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي في الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان : دراسة مقارنة تفسيرية.

الخطوة السادسة : تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية : دراسة وصفية تحليلية.

الخطوة السابعة : الإجراءات المقترحة لتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية ، وفيضوء خبرة الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان ، بما يساهم في تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية ، وبما يتناسب مع السياق الثقافي المصري

القسم الثاني للدراسة : تمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي في عالمنا المعاصر (إطار نظري) :

يعد التعليم الجامعي مادة ثرية جدا للبحث والدراسة في العديد من التخصصات ، في ظل ما يقوم به من وظائف وأدوار محورية في بناء استراتيجيات التنمية والابتكار الوطنية ، ويمكن تناول ذلك علي النحو التالي :

المحور الأول : تحليل المفاهيم الأساسية وتناول أبرز القضايا المتعلقة بتمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي.

سيتم تناوله علي النحو التالي :

أولا: السياق العالمي لتمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي:

ويمكن تناول ذلك على النحو التالي :

المحور الأول : الأسس النظرية لتمكين الأمن السيبراني بالجامعات :

يمكن تناوله على النحو التالي:

أولا - نشأة الأمن السيبراني بالجامعات :

ارتبطت نشأة الأمن السيبراني باعتماد الأفراد على الإنترنت في جميع أعمالهم من تنمية تجارتهم، وحساباتهم البنكية والتعليم، والتواصل الاجتماعي، وإنهاء إجراءاتهم الحكومية، بالإضافة إلى مهام عديدة ومختلفة، فالمعلومات التي يستخدمونها بالغة الحساسية ،والأهمية وأصبحت عرضة للخطر والاختراق والاستيلاء عليها، فنشأ مجال الأمن السيبراني لتأمين الأجهزة التقنية بجميع أشكالها وأنواعها بما تحتويه من أنظمة وبيانات ومعلومات يتم تداولها من خلال شبكة الإنترنت، وبات من أهم العلوم في عصر التكنولوجيا، والتي تستخدم للحفاظ على هذه الثروة المعلوماتية المهمة لكل من الجهات الحكومية والأهلية والأفراد في الفضاء السيبراني الذي يعد أعم وأشمل من شبكة الإنترنت؛ لارتباطه باستخدام العديد من الشبكات حول العالم، كشبكة الألياف البصرية والشبكات اللاسلكية .

كما ارتبط ظهور الأمن السيبراني بظهور الهجمات والقرصنة منذ منتصف الخمسينيات من القرن الماضي ، والتي زادت أهميتها مع ظهور وانتشار الإنترنت ، مما فتح الباب أمام مجالات جديدة يتم فيها تخزين المعلومات ونقلها إلكترونيا ، وهذا يرتبط بالتطور الموازي لمفهوم حماية المعلومات للابتعاد عن المادية ، كما يهدف الأمن السيبراني إلى تعزيز حماية سرية البيانات وخصوصيتها لجميع الأشخاص والمؤسسات العامة والخاصة ، وضمان توافر واستمرارية أنظمة المعلومات ، وضمان الحماية بمفاهيم جديدة

مثل جدران الحماية ، وأنظمة كشف التسلل ، وتطبيقات مكافحة الفيروسات ، وتكنولوجيا التشفير ، وإدارة المعلومات ، وغيرها ، والأمن الإلكتروني. من خلال مجموعة من الآليات التي تحد من المخاطر(وفاء حسن عبد الوهاب صائغ ، ٢٠١٨م،ص٣١).

مما سبق يتضح أن الأمن السيبراني يعد من أهم المراحل التي تهتم بتوفير الحماية والأمان للمعلومات والبيانات وتوفير السرية وتشفير المعلومات .

ثانيا - مفهوم الأمن السيبراني بالجامعات:

يُعد مفهوم الأمن السيبراني مفهوم حديث نسبيا ، وقد ظهر في إطار الثورات الرقمية والتكنولوجية الحديثة ،أدى ذلك إلى تدفق كبير وغير مسبوق للمعلومات بوسائل اتصال متعددة للمصادر من خلال أجهزة الكمبيوتر ، في هذا السياق ، ظهر مفهوم الأمن السيبراني لتمثيل جوانب الأمن المتعلقة بحماية تلك المعلومات، وكان هذا المفهوم موضع اهتمام العديد من الباحثين و المؤسسات. الأمن السيبراني هو مصطلح مشتق من اللاتينية (سايبر Cyber) ، بمعنى وهمي أو افتراضي ، والذي تم استخدامه لوصف مساحة تحتوي على شبكة كمبيوتر التي تعني (فضاء المعلومات)، ومعناها تخيلي أو افتراضي، ودرج استخدامها لوصف الفضاء الذي يضم الشبكات المحوسبة منير البعلبكي، ٢٠٠٤ م ، ص٢٤٣).

ومنها اشتقت صفة السيبراني والسيبرانية Cybernetic - وتعني : علم التحكم الآلي ، أو علم التحكم ، وبهذا الأمن السيبراني يعني أمن الفضاء المعلوماتي، ونتيجة لذلك ، فهو مهتم بالأمان المرتبط بشبكات الإنترنت وشبكات الاتصالات (خالد مخلف الحنفاوي ، ٢٠٢١م ، ص٨٥). يعتمد تعريف الفضاء السيبراني على طبيعة كل دولة ومؤسسة ، ورؤيتها واستراتيجيتها المختلفة عند التعامل مع مجال الفضاء السيبراني ، وعلى حسب الزاوية التي نظر إليه منها ، إلا أن جميع هذه التعاريف اشتركت في مضمون واحد متقارب في المعنى هو: استهداف المواقع بوسائل إلكترونية متعددة . لذلك ، يتم إلقاء الضوء على تعريف الأمن السيبراني علي النحو التالي : الأمن السيبراني وفقا لتعريف الاتحاد الدولي للاتصالات في تقريره حول اتجاهات الإصلاح في الاتصالات للعام ٢٠١٠م - ٢٠١١ م، هو: ويشمل أدوات الأمان والسياسات والإجراءات والمبادئ التوجيهية ونهج إدارة المخاطر والتدريب والممارسات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول الشركات والمستخدمين. (Hamadoun,،٢٠٠٨ ,p.٢)

وهو أيضا مفهوم يعبر عن مجموعة من الإجراءات والتدابير المتخذة و الآليات والوسائل لحماية أجهزة الكمبيوتر والشبكات من الوصول غير المصرح به ؛ يهدف إلى سلامة وأمن المعلومات المخزنة ويحمي البرامج وأجهزة الكمبيوتر من إساءة الاستخدام والهجوم والقرصنة والتهديدات للمعلومات الواردة فيها. (وليد عبدالرحيم جاب الله ، ٢٠٢١م ، ص٤٩)

كما يتم تعريفه أيضا على أنه : أمان الشبكات والأجهزة المتصلة بالإنترنت ، وأنظمة المعلومات والبيانات والمعلومات وبذلك يعد بمثابة المجال الذي يتعلق بالتدابير ومعايير الحماية التي يتعين اتخاذها ، أو الالتزام بها لمواجهة التهديدات ، ومنع الاختراقات ، وفي أسوأ الحالات ، التخفيف من تأثيرها (حنين جميل أبو حسين ٢٠٢١م، ص١٨)، كما يُعرف بأنه : عملية تضمن حماية الموارد البشرية والمالية المرتبطة بتكنولوجيا الاتصالات والمعلومات وإمكانية تقليل الأضرار والخسائر التي تترتب عند حدوث خطر أو تهديد ، ويمكنك إعادة الموقف إلى حالته الأصلية في أسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج ، ولا يصبح الضرر هدرا مستمرا (سعيد عبد اللطيف حسن، ٢٠١٧م ، ص ٢١) .

كما يتم تعريف الأمن السيبراني National Initiative for Cybersecurity Careers and Studies على أنه : الأنظمة والعمليات التكنولوجية الحديثة التي يتم فيها حماية المعلومات من التلف أو سوء الاستخدام المحتمل ، كما يوفر استعادة النظام والمعلومات في حالة وقوع هجوم إلكتروني.(NICCS, 2014,p.4)

كما تم تعريفه باعتباره : مجموعة من الممارسات التي تهدف إلى حماية الأنظمة والشبكات والبرامج من جميع أنواع الهجمات الرقمية ، تختلف هذه الممارسات بين التدابير الوقائية الاستباقية قبل حدوث الضرر والإجراءات التصحيحية بعد وقوعها(حسين بن سليمان بن راشد الطيار، ٢٠٢٠م، ص٢٦٤). كما تم تعريفه بأنه : مختلف الجهود والإجراءات التي اتخذتها الدول والمؤسسات

لتوفير بيئة آمنة من خلال الفضاء الإلكتروني،وما يتعلق بالمعلومات والتقنيات الرقمية، خاصة بطرق تقلل من المخاطر على المستخدمين ، خاصة لأفراد المجتمع بصفة عامة. (عهود أحمد الغامدي، ٢٠٢١م ، ص ١٤٨)

ويعرف كذلك بأنه : مجموعة من الممارسات التنظيمية والإجرائية والتقنية ، والأدوات التي تهدف إلى حماية أصول المعلومات مثل أجهزة الكمبيوتر والشبكات والبرامج والبيانات الداخلية من التهديدات والأضرار الداخلية والخارجية ، تغيير أو تعطيل الوصول إلى المعلومات أو الممارسات ، أو الأدوات ، أو التدابير ، من الضروري بناء وظائف أمنية عالية الجودة للبنية التحتية لأنظمة الاتصالات وتكنولوجيا المعلومات ، إنه أساس الفضاء السيبراني ، وجزء مهم من تدريب الطلاب والأفراد والمؤسسات على صد الهجمات والهجمات التي تستهدف الفضاء السيبراني .

مما سبق يتضح أنه على الرغم من الاختلافات في المفاهيم التي قدمها الباحثون ، فقد تبين أنها متسقة ومتكاملة في طبيعتها ، وتشير إلى أن الأمن السيبراني هو مجموعة من التقنيات والاستراتيجيات المرتبطة عادة بالعمليات الإلكترونية، كما أنه يمثل مفهوما أمنيا لحماية المعلومات وجميع العمليات والخدمات والأجهزة المرتبطة بها ، التكنولوجيا ضد الوصول غير المصرح به أو الاستخدام السلبي لتلك المعلومات أو الأساليب التي تشكل خطرا على الكيانات أو الأفراد المرتبطين بتلك المعلومات.

ثالثا: أهداف الأمن السيبراني بالجامعات :

على مدى السنوات القليلة الماضية ، كانت جميع الحكومات والمؤسسات مهتمة بتخطيط سياسات الأمن السيبراني ، ويرجع ذلك إلى العديد من الأهداف المهمة التي يحققها ويمكن تفسيرها على النحو التالي: (منى عبد الله السمحان ، ٢٠٢٠م، ص١).

إلى مجموعة متنوعة من أهداف الأمن السيبراني، تمثلت في:

١- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة تحدي اختراق الأجهزة التقنية بقصد إتلاف المعلومات الشخصية ، سواء عن طريق السرقة أو التلف.
٢- توفير بيئة آمنة وموثوقة للمعاملات في مجتمع المعلومات .
٣- مواجهة هجمات وحوادث أمن المعلومات التي تستهدف الجهات الحكومية والمؤسسات العامة والخاصة.
٤- يوفر المتطلبات اللازمة للحد من مخاطر استهداف المستخدمين والجرائم الإلكترونية.
٥- جسر الفجوة في أنظمة أمن المعلومات.
٦- مرونة البنية التحتية الحيوية للتصدي لهجمات السيبرانية.
٧- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر المحتملة في مختلف مجالات استخدام الإنترنت.
٨- مقاومة البرامج الضارة والأحداث المستهدفة ، والأضرار الجسيمة للمستخدمين وأنظمة المعلومات.
٩- الحد من التخريب والتجسس السيبراني على المستوى الفردي والحكومي.
١٠- جسر الثغرات الأمنية في أنواع مختلفة من الأجهزة المحمولة وأنظمة الكمبيوتر.

مما سبق يتضح أن من أهم أهداف الأمن السيبراني هو تعزيز التكنولوجيا التشغيلية على جميع المستويات ، وذلك لحماية النظام ومكوناته وأجهزته وبرامجه والخدمات التي يقدمونها والبيانات الواردة فيه.

رابعا : أنواع الأمن السيبراني بالجامعات:

في ضوء التعريفات المتنوعة للأمن السيبراني، يمكن تحديد أنواع مختلفة له، تتمثل في الآتي(triada network, 2019.p.2) :

١. أمن الشبكات (Network Security) يتم حماية الكمبيوتر من الهجمات التي يمكن أن تتعرض داخل وخارج الشبكة ،من أبرز التقنيات المستخدمة لتطبيق أمان الشبكة الحماية بين الأجهزة الشخصية والأجهزة الأخرى في الشبكة ، بالإضافة إلى أمن التطبيقات ، (Application Security)أمن البريد الإلكتروني، من بينها المعلومات المتعلقة بالتطبيق على الكمبيوتر، تعليمات إعداد كلمة المرور، المحمية، عمليات المصادقة، أسئلة الأمان التي تضمن هوية مستخدم التطبيق، إلخ.

٢. الأمن السحابي (Cloud Security) تعرف البرامج السحابية بأنّها برامج تخزين البيانات وتخزينها عبر الإنترنت ، وتعتمد العديد من المنتجعات على تخزين البيانات من خلال البرامج الإلكترونية بدلا من برامج التخزين المحلية ، يهتم البرنامج السحابي الذي جلب الحاجة إلى حماية بياناته بتوفير الحماية اللازمة لمستخدميه .

٣. الأمن التشغيلي (Operational Security) وهو في حالة وقوع هجوم إلكتروني على بيانات المستخدم ، ويتم توظيف خبراء إدارة المخاطر لإيجاد خطط بديلة لإدارة مخاطر عمليات الأمن السيبراني الداخلية ، ويشمل أيضا تثقيف وتدريب الموظفين على أفضل الممارسات لتجنب الأزمات.

خامسا : أبعاد الأمن السيبراني بالجامعات:

يمكن تناول ذلك علي النحو التالي:

١ -**السرية** : **Confidentiality** تعد سرية المعلومات أحد أهم أبعاد الأمن السيبراني التي تحظى بأهمية كبيرة حيث تعتبر سرية المعلومات جوهرية في حماية المعلومات الدقيقة.(Smith, J,2018,pp.7-8) والحفاظ على سلامة الأفراد والمؤسسات من الأضرار والتبعات الناجمة عن اختراقات سرية المعلومات ، والتأثيرات السلبية على الأفراد والمؤسسات والمجتمع بشكل عام ، والمجتمع الجامعي علي وجه التحديد. (Whitman, M. E., & Mattord, H. J. ,2019,pp.6-7)

٢ -دقة المعلومات : Integrity

تعد دقة المعلومات أحد أهم أبعاد الأمن السيبراني ، ويقصد بها ضمان صحة وموثوقية المعلومات المتداولة والمستخدمة في البيئة السيبرانية. يعد ضمان دقة المعلومات أمرًا بالغ الأهمية لما لها من تأثير على عمليات إتخاذ القرارات ، ويمكن تناول أهم العوامل الرئيسية لدقة المعلومات كما أشار .(Shabir, M, 2020,pp.111-113) علي النحو التالي:

أ- المصدر: يجب التأكد من مصداقية وموثوقية مصدر المعلومات المستخدمة في البيئة السيبرانية.

ب- التحقق والتحليل: يجب أن يتم التحقق من صحة المعلومات وموثوقيتها من خلال استخدام تقنيات التحليل والتقييم .

ت- التفاصيل والتحديث: يجب أن تقدم المعلومات المتاحة في البيئة السيبرانية تفاصيل دقيقة ومحدثة. يجب الاهتمام بتحديث المعلومات باستمرار لضمان دقتها وتطابقها مع الظروف والأحداث الحالية.

ث- توعية المستخدمين: يجب توعية المستخدمين بضرورة التحقق من المصادر وتحليل المعلومات قبل الاعتماد عليها أو تناقلها .

٣ -إتاحة المعلومات Availability : تعد إتاحة المعلومات أحد أهم أبعاد الأمن السيبراني، حيث تسعى المؤسسات والدول إلى إتاحة المعلومات بشكل آمن ومنهجي لتحقيق أهدافها ومصالحها دون التأثير السلبي على طبيعة الأمن السيبراني لديها ويتم ذلك من خلال العديد من الخطوات كما أشار (محمد عبدالله قاريزيكس، ٢٠٢٢م، ص ص ٢٢-٢٣).

أهمها على النحو التالي:

أ- تبني سياسات وإطار قانوني لضمان أمن المعلومات.

ب- استخدام التشفير والتوقيع الرقمي لحماية المعلومات المتاحة.

ت- تدريب وتوعية المستخدمين بأهمية الأمان السيبراني وممارساته الجيدة.

المحور الثاني : الأسس النظرية للذكاء الاصطناعي بالجامعات :

يمكن تناول الذكاء الاصطناعي بالجامعات من خلال ما يلي:

أولاً : ماهية الذكاء الاصطناعي:

منذ زمن بعيد دفع فضول الإنسان إلى البحث في كيفية عمل العقل البشري فعلى مدى العصور السابقة كان هناك العديد من المحاولات لفك رموز وشفرات عمل العقل البشري ، وكانت أبرز تلك الجهود في بداية القرن التاسع عشر حيث قام العالم الشاب

جورج بولي George Polley والمتخصص في علم الرياضيات بوضع الأسس النظرية لتلك الرموز ، وذلك لعرض عمليات ومنطق التفكير لدي العقل البشري.

وفي عام ١٩٣٤م قام العالم الشاب تشارلز باي بيج Charles Bay باختراع الحاسوب ،والذي كان بمثابة خطوة أولية نحو اختراع آلات لديها القدرة على محاكاة قدرات العقل البشري في الحساب والمنطق ، بل وقام بشرح وتوضيح مفهوم وآلية الذكاء ، وطرح فرضية أن التصرف الذكي جاء نتيجة مجموعة من العمليات والأنشطة القائمة على المعلومات ، وفيها يقوم الدماغ بجمع المعلومات ومعالجتها وتجهيزها ثم الرد عليها ، وكانت تلك الجهود بمثابة نتائج محفزة لقيام العديد من الباحثين بالمزيد من الدراسات في هذا المجال ، والذي يستهدف البحث عن آليات وطرق لمحاكاة طريقة إندماج الحاسب الآلي مع الفكر الانساني (منال البلقاسي ، ٢٠١٩م ، ص٥).

وفي مؤتمر معنون : ب " ميلاد الذكاء الاصطناعي " تم الإشارة إلى مسمى الذكاء الاصطناعي للمرة الأولى على يد العالم جون مكارثي John,McCarthy ، ومنذ منتصف الخمسينيات إلي منتصف سبعينيات القرن الماضي بدأت تطبيقات علمية جديدة تظهر للوجود قائمة على التناغم بين واقع الذكاء وتطبيقاته ، بل وتطور الذكاء الاصطناعي لدرجة أنه بدأ يتعامل مع العلوم شديدة الدقة ومتناهية الصغر Micro World ، والخوارزميات ، ولغة البرمجة ، والاهتمام بهندسة اللغة ، وبدأت الجهود الأولية المتفائلة التي تنادي بضرورة عمل إنسان آلي متكامل Robots (عبدالجواد السيد بكر ، ٢٠٢٠م ، ص ٥).

ومنذ ثمانينيات القرن الماضي أصبحت الشبكات العصبية الاصطناعية أكثر شيوعا وانتشرت في جميع المجالات بعد أن تطورت فكرتها وانتشرت في جميع الميادين البحثية وفرضت نفسها نتيجة لنجاحها في حل العديد من التحديات ، ولأول مرة دخلت الخوارزميات الوراثية مرحلة التطبيق وبالنسبة للنظم الخبيرة فقد كان لها نصيب كبير من النجاح خصوصاً في الولايات المتحدة الامريكية ، وكل هذا نتيجه للبحوث المتعددة في مجال تطوير الذكاء الاصطناعي (عادل عبد النور بن عبد النور ،٢٠٠٥م ، ص٢٦).

ويتكون الذكاء الاصطناعي (Artificial Intelligence) AI من كلمتين هما: الذكاء وكلمة الاصطناعي ولكل منهما معنى، فالذكاء حسب قاموس Webster هو القدرة على فهم الظروف أو الحالات الجديدة والمتغيرة أي هو القدرة على إدراك وفهم وتعلم الحالات أو الظروف الجديدة بمعنى آخر أن مفاتيح الذكاء هي الإدراك، الفهم، والتعلم. أما كلمة الصناعي أو الاصطناعي ترتبط بالفعل يصنع أو يصطنع، وبالتالي تطلق الكلمة على كل الأشياء التي تنشأ نتيجة النشاط أو الفعل الذي يتم من خلال اصطناع وتشكيل الأشياء تمييزا عن الأشياء الموجودة بالفعل والمولدة بصورة طبيعية من دون تدخل الإنسان، ومن ثم فالذكاء الاصطناعي هذا هو العلم والتكنولوجيا التي تهتم بدراسة تطوير وظائف الكمبيوتر بالتوازي مع الذكاء البشري ، بحيث يكون لدى أجهزة الكمبيوتر القدرة على إدراك التعلم ، وحل المشكلات ، واتخاذ القرارات بطريقة منطقية ، وتنفيذها بشكل يحاكي تفكير العقل البشري . (أمنية عثمانية ، ٢٠١٩م، ص١١)

كما أن الذكاء الاصطناعي (AI) :مجموعة من التقنيات الحسابية المستوحاة من الطريقة التي يستخدم بها الناس نظامهم العصبي وجسمهم للإحساس والتعلم والعقل واتخاذ الإجراءات ، لكنها عادة ما تكون مختلفة تماما، (Stone et.al, 2016,p.4)، ويعرف أيضا بأنه : نشاط متخصص في جعل الآلات ذكية ، ويسمح الذكاء للكيانات بالعمل بشكل صحيح(Nils,2010, P.6) .

ويُشار إلى الذكاء الاصطناعي Artificial Intelligence إلى إنه : التدفق العلمي والتقني ، بما في ذلك الأساليب والنظريات والتقنيات التي تهدف إلى إنشاء آلة قادرة على محاكاة الذكاء البشري. (Li et ,al٢٠١٧ ،p.٨٦) ، ويعرف الذكاء الاصطناعي أيضا : بأنه تطوير أنظمة الكمبيوتر التي يمكنها أداء المهام التي تتطلب عادة ذكاء بشريا(٢٠٢٠p.١٢) Eriksson Djoeini

تعرف مجموعة خبراء الذكاء الاصطناعي التابعة لمنظمة التعاون الاقتصادي والتنمية "نظام الذكاء الاصطناعي" على النحو التالي:إنه نظام قائم على الآلة يمكنه تحقيق أهداف محددة يضعها البشر ، مثل التنبؤات والتوصيات والقرارات التي تؤثر على البيئات الحقيقية أو الافتراضية ، وأنظمة الذكاء الاصطناعي مصممة للعمل على مستوى من الاستقلالية. تتكون مراحل دورة حياة

نظام الذكاء الاصطناعي من (١) التخطيط والتصميم ، وجمع البيانات ومعالجتها ، وبناء النماذج وتفسيرها ، (٢) التحقق والاعتماد ، و (٣) النشر بطرق مختلفة ، (٤) التشغيل والمراقبة (OECD,٢٠٢٠ ، p.٧)

ويُعرف الذكاء الاصطناعي أيضاً على أنه : طرق وتقنيات وأدوات مختلفة لإنشاء النماذج وحل المشكلات من خلال محاكاة سلوك الأشخاص المدركين : .(Aldosari, 2020,p.46) ، و الذكاء الاصطناعي لديه قدرة ممتازة على تقليد قدرات الذكاء البشري ، والاستفادة منها من أبرز التطبيقات الحديثة لعلوم الكمبيوتر ، مما يسهل العمل في مختلف مجالات الحياة البشرية ، ويقصد به أيضا: العلم الذي يشارك في إنشاء آلات ذكية تعمل كما هو متوقع من البشر وتلمس الذكاء الاصطناعي.

ويتكون الذكاء الاصطناعي : من مفهومين يتم دمجهما ولكن يتم فصلهما نظريا ، علي النحو التالي :

أ- الذاكرة : يتم تمثيل ذلك عن طريق التخزين ، وهو شكل من أشكال الذكاء ، يسمى أيضا الذكاء السلبي.

ب- الاستدلال: إنها القدرة على تحليل وفهم العلاقة بين الأشياء والمفاهيم ، لفهم الحقائق ، باستخدام الذاكرة والمنطق والوسائل الأخرى المشتقة من العلوم الرياضية. (سهام العايب ، ٢٠١٩م، ص١٤٣)

وفي أواخر تسعينات القرن الماضي وحلول الألفية الثالثة شهد الذكاء الاصطناعي ازدهاراً ملحوظاً وتحديداً عام ١٩٩٧م حيث هزم بطل العالم في الشطرنج غاري كاسباروف أمام ديب بلو من آي بي أم وهو برنامج حاسوبي يلعب الشطرنج ولاقت المباراة دعماً كبيراً واهتماما إعلامياً غير عادي فلأول مرة يخسر فيها بطل العالم في لعبة الشطرنج أمام جهاز كمبيوتر (Rockwell Anyoha ,2017, pp.14-15)

وأصبح الذكاء الاصطناعي جزءًا لا يتجزأ من الحياة اليومية ، ومنتشرا وبشكل ملحوظ ، حيث ظهرت في العقود الأخيرة تطورات كبيرة ، والتي من أهمها تضاعف حجم البيانات الضخمة ، وأصبحت المعالجات ذات سرعات كبيرة وغير محدودة ، فضلاً عن التقدم الملحوظ في الأساليب الحسابية ، ومنذ عام ٢٠١٠م بدأ الذكاء الاصطناعي يتحرك أسرع خاصة في العقدين الماضيين ، وفي العديد من المجالات والتي من أهمها التشخيص الطبي ، وأيضاً في مجال الترجمة الآلية ، واستخراج البيانات ، ومحرك البحث جوجل ، علاوة على التعرف على الكلام(Emilia Bratu, 2018,p.14) .

إتساقا مع ما سلف بيانه يعد ذكاء الاصطناعي أحد أهم التحولات التي نتج عنها أتمتة العمليات الإنتاجية والرقمنة، والشبكات العالمية للاتصال والإنتاج، وقد تم تسميته بثورة الخوارزميات، ومجتمع المعلومات، واقتصاد المعرفة، ولقد تم استخدام جميع الأساليب الحديثة نسبياً للذكاء الاصطناعي مثل : التعلم المعزز، وغير الخاضع للإشراف ، وتحت الإشراف، والشبكات العصبية، بما في ذلك التعلم العميق، والخوارزميات التطويرية في مجموعة متنوعة من التطبيقات حيث أن تطبيق واحد للذكاء الاصطناعي قد يعتمد على العديد من تقنيات الذكاء الاصطناعي المختلفة؛ وذلك أحد الأسباب التي تجعل العديد من الأفراد المشاركين في الذكاء الاصطناعي حاصلين علي درجات علمية متقدمة في الفيزياء والرياضيات (Ilkka Tuomi. 2018,pp.32-33)

ثانيا : أهداف الذكاء الاصطناعي بالجامعات :

تتعدد أهداف الذكاء الاصطناعي بالجامعات والتي أهمها على النحو التالي:

١- إتاحة فرص الوصول العادل ، والشامل في التعليم لهؤلاء الذين يعيشون في مجتمعات معزولة ، وتوفير فرص الوصول المناسب للتعليم ، والتدريب وأيضا الاهتمام بالاشخاص ذوي الاعاقات واللاجئين ومن هم خارج الجامعات.

٢- المعالجة المتوازية Paralle Processing ويقصد بها تمكين الآلات من تجهيز ومعالجة المعلومات بشكل أقرب إلى طريقة الإنسان في حل المسائل ، حيث يتم تنفيذ عدة أوامر في الوقت نفسه ، وتلك الطريقة هي أقرب طريقة للإنسان في حل المسائل.

٣- فك أغوار الدماغ حتى تتمكن الآلات من محاكاة الدماغ البشري ؛وذلك من خلال محاولات فهم أفضل لماهية الذكاء البشري وتجدر الإشارة إلى أن الجهاز العصبي والدماغ البشري أكثر الأعضاء تعقيداً ، وهما يعملان بشكل دائم ، ومترابط في التعرف على طبيعة الأشياء.

(the Division for Policies and Lifelong Learning Systems in UNESCO's Education (et.als),2019,p.12)

كما يهدف الذكاء الاصطناعي أيضاً إلى قيام الكمبيوتر بمحاكاة عمليات الذكاء التي تتم داخل الدماغ البشري بحيث يكون الحاسب لديه القدرة على إتخاذ القرارات ، وحل المشكلات باسلوب منطقي ، وبنفس طريقة تفكير العقل البشري ، ويمكن توضيح بعض أهداف الذكاء الاصطناعي بالجامعات على النحو التالي:

١- تصحيح الاختبارات : حيث قامت بعض الشركات بتوفير مجموعة من التطبيقات ، والبرامج التي تستطيع إجراء الاختبارات والتدريبات ، ويعد تحديد الدرجات من أهم المهام في عمليتي التدريس والتدريب ، كما أن هذه العملية تأخذ وقتاً كبيراً من الممكن توفيره للمدربين مثل تطوير المهارات أو تخطيط البرامج

٢- المساهمة في قياس وتحديد أساليب وطرق تعلم الأفراد ؛ وذلك من خلال بناء برامج ومواقع تدريب ذكية يمكن من خلالها تقديم تدريبات مخصصة تتناسب مع ما حصل عليه كل فرد بالإضافة إلى تقييم المعرفة لدى الأفراد.

٣- مساعدة الأفراد على تطوير مستواهم ، وذلك من خلال تقييم مهاراتهم المعرفية بشكل فوري و فردي.

٤- توفير الاتصال على جميع المستويات التي من أهمها : الحاسوبي الحاسوبي ، والإنساني الحاسوبي ، والإنساني الإنساني.

٥- توفير رؤية عامة عن حالة العاملين بالجامعات ، وذلك من خلال توفير البيانات الضخمة للقيادات الجامعية عن المرؤوسين.

٦- يساعد في تحليل البيانات ، ودعم اتخاذ القرار ، بالإضافة إلى تعزيز القدرات ، والمساهمات البشرية على أعلى مستوى.

٧- يستطيع الذكاء الاصطناعي تحديد الفجوات في مستوى البرامج ، وذلك استناداً إلى أداء العاملين في الإختبارات ، والتدريبات مما يحقق ضمان جودة البرامج التدريبية (Elana Zeide, 2019, p 34).

ثالثا : أهمية الذكاء الاصطناعي بالجامعات :

يعمل الذكاء الاصطناعي بالجامعات على تقليل الحاجة إلى المهارات الشخصية والمعرفية، والخبرة، والتأكيد على أهمية المرجعية السلوكية نتيجة لذلك لا يحتاج البشر بالضرورة إلى تعلم المعرفة الخاصة بالمجال التي كانت مطلوبة سابقاً بشكل ضروري لتحقيق الأداء المتميز، كما يمكن الذكاء الاصطناعي من إنشاء قدرات معرفية لن تكون ممكنة بدون التكنولوجيا فقد مكنت الماكينة أو العمل البشري من تحقيق أشياء كانت مستحيلة بدونها، وبالمثل الميكنة من العمل المعرفي الذي يجعل الأنشطة الجديدة التي لم تكن ممكنة من قبل أصبحت الآن أكثر إمكانا، بالإضافة إلى تسريع التطور المعرفي (Tuomi Ilkka ,2018,pp.30-31) . كما يتميز الذكاء الاصطناعي بثباته النسبي حيث لا يتعرض لما يتعرض له البشر من عوامل بشرية كالنسيان ، بالإضافة إلى أنه يهتم بالتقنيات والأساليب ، والمفاهيم المرتبطة بهذا المجال ، وكيفية استخدامها لتطوير وظائف الحاسب الآلي بحيث تتمكن من محاكاة القدرات البشرية. (رياض زروقي، ، أميرة فالتة ، ٢٠٢٠م ، ص٦)

رابعا : خصائص الذكاء الاصطناعي بالجامعات:

تتعدد خصائص الذكاء الاصطناعي بالجامعات والتي أهمها إجراء معظم عمليات إتخاذ القرار دون الحاجة إلى التدخلات البشرية ، والمشاركة في تفاعلات البشر أو الآلات الأخرى ، اتخاذ الإجراءات المناسبة لتحقيق الأهداف المطلوبة للاستجابة السريعة ، استيعاب المعلومات الجديدة ، بالإضافة إلى تفسير المعلومات المقدمة ، علاوة على طرح حلول وآليات جديدة لمواجهة التحديات التي قد تعاني منها الجامعات (لووران بروبست وآخرون ، ٢٠١٨م ،ص٩).

كما يتميز الذكاء الاصطناعي بالعديد من الخصائص الأخرى ، والتي أهمها:

١- **البيانات والبرامج مفتوحة المصدر** : حيث تساعد البيانات ، والبرامج مفتوحة المصدر في سرعة أداء الذكاء الاصطناعي له على أنها تسمح بقضاء وقت أقل في البرمجة الروتينية .

٢- **البيانات الضخمة :** ويقصد بها توفير كميات أكبر للمصادر والبيانات المنظمة ، وغير المنظمة ؛ وذلك يسمح بزيارة قدرات الذكاء الاصطناعي لم تكن ممكنة قبل ذلك والتي أهمها الحجم المحدود للعينات ، ونقص البيانات.

٣- **منصات ووسائل التواصل الاجتماعي:** حيث يساعد وجود مصادر مفتوحة في تطور أدوات وتطبيقات الذكاء الاصطناعي وفي تسريع تقدم العديد من جوانب الذكاء الاصطناعي : مثل التعلم العميق والتعزيز.

٤- **الحوسبة السحابية :** حيث أدت الاختراقات في تكنولوجيا الحوسبة السحابية إلى تقليل التكلفة وسرعة التعامل مع كميات ضخمة من البيانات عبر أنظمة معززة بالذكاء الاصطناعي من خلال المعالجة المتوازنة.

وتعد القفزات المتتالية في مجال الذكاء الاصطناعي من أهم ما يميزه حيث عقب ذلك تطور في مجال التعلم الآلي ، والذي فتح أمام الجامعات مسارات جديدة مكنتها من التغلب على التحديات بصورة مستمرة كما أن التطور الملحوظ في الذكاء الاصطناعي قد انعكس على تطور قدرة الجامعات على إعادة هيكلة الخدمات الإدارية بها خاصة التي تتعلق بالمهام التي تم ميكنتها وأتمتتها (Popenici Stefn A. D. & Kerr Sharon, 2017, pp 2-3).

خامسا : مميزات الذكاء الاصطناعي بالجامعات:

يتمتع الذكاء الاصطناعي بالجامعات بالعديد من المزايا والتي من أهمها على النحو التالي:

١- تسريع القرارات حيث يتمتع الذكاء الاصطناعي بالقدرة على تطوير عملية صناعة ، واتخاذ القرار ، وتوجد العديد من تقنيات الذكاء الاصطناعي التي يتم استخدامها في الأنظمة التعليمية ، وخاصة عند اقتراح تقنيات شجرة القرار لتكون فعالة في ضمان المتطلبات الفردية ، وفي تحسين كفاءة التعلم وخاصة في سياق التعلم من خلال الذكاء الاصطناعي.

٢- فعالية الإدارة حيث يمكن الذكاء الاصطناعي العاملين من التعامل مع الرسائل الاخبارية بكل سهولة ، ويسر مثل غياب العاملين والطلاب.

٣- يعد من أهم الأدوات التي تساعد عضو هيئة التدريس حيث تؤدي الروبوتات دوراً كبيراً في قاعات المحاضرات ، والتدريبات من خلال تيسير أداء المهام المعقدة ، والتي تستغرق المزيد من الوقت.

٤- يستطيع ذكاء الاصطناعي تتبع مسارات التعلم بشكل فوري وقياس مدى اكتساب العاملين والطلاب للمهارات وذلك من خلال إجراء التقييم المستمر لهم.

٥- تحسين عمليات البحث بالجامعات على مستوى العالم ، وذلك من خلال التطور المستمر لمحركات البحث على الإنترنت ، والمميزات المستحدثة باستمرار ، وتطبيقاتها على الهواتف الذكية.

٦- تقديم المساعدة للطلاب والعاملين في أداء اعمالهم المنزلية ، كما يمكنهم من القيام بالعمل المنزلي بما يتناسب مع مهاراتهم ، والتحديات الأكاديمية.

٧- توفير قدر كبير من الوقت الذي يمكن قضاءه بشكل معتاد في المهام الروتينية ؛ وذلك من خلال تحقيق المهام الآلية.

٨- توفير الكفاءة حيث يقوم الذكاء الاصطناعي على اكتساب أفراد المجتمع الكفاءات اللازمة لتحقيق النجاح في مجتمع جامعي قائم على الذكاء الاصطناعي.

٩- توفير منصات التدريب الذكية للتعلم من بعد ؛ وذلك بالإضافة إلى التوسع السريع في تكنولوجيا الهاتف المحمول حيث أنه يفتح فرصاً متعددة للعاملين على حد سواء من طلاب ، وأعضاء هيئة التدريس.

١٠- تحسين الإنتاجية حيث تعد تقنية الذكاء الاصطناعي تقنية إستراتيجية حتمية تعمل على الحصول على تعزيز ولاء المستفيدين ، وتحقيق أكبر كفاءة كما أنها تتحول لميزة تنافسية لدي العديد من الجامعات فمع الذكاء الاصطناعي يتم توفير المزيد من المهام في وقت أقل ، والتنبؤ بنتائج الأعمال ، وذلك لزيادة الربحية ، مما يمكن الجامعات من التطور المستدام Thierry) . Karsenti,2019,pp108-110)

سادسا : آليات تمكين الأمن السيبراني في ضوء أنظمة الذكاء الاصطناعي بالجامعات :

هناك العديد من أنظمة الحماية الخاصة بالذكاء الاصطناعي ، والتي تستهدف تمكين الأمن السيبراني ، وذلك من خلال حماية الأنظمة والشبكات من هجمات الاختراق السيبرانية بالجامعات ، ومن بين أنظمة الحماية الأكثر شيوعاً:

١) نظام الكشف التلقائي للاختراق بالجامعات (IDS) Intrusion Detection System:

٢) نظام الجدار الناري المتقدمة بالجامعات(NGFW) Next Generation Fire Walls :

٣) نظام الأمن السحابي بالجامعات: **(CS) Cloud Security:** .

٤) نظام التعرف على ملامح السلوك غير العادي بالجامعات. **(UEBA)**

User and Entity Behavior Analytics:

١. نظام الإدارة التلقائية للأمن بالجامعات . (ASM)

٢. نظام الأمن الإداري المتقدم بالجامعات. :Advanced Administrative Security: (AAS)

ويمكن تناول تلك الأنظمة علي النحو التالي:

١- نظام الكشف التلقائي للاختراق بالجامعات : (IDS) Intrusion Detection System:

يعتبر نظام الكشف التلقائي للاختراق أحد أهم أنظمة الذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعات حيث يساهم هذا النظام في مراقبة حركات الشبكات وتنبيه الجهاز الإداري عن أي تغييرات غير متوقعة في النظام ، ويتميز هذا النظام بقدرته على استخلاص البيانات التي تشير إلى أي نشاط غير مشروع دون الحاجة إلى تدخل بشري ، مما يجعل هذا النظام أكثر فعالية في الوقاية من الاختراقات وحماية البيانات الدقيقة ، حيث تتعرض العديد من المشاريع والأنظمة الحاسوبية لمخاطر الاختراق السيبراني من قبل القراصنة والمتسللين، وتتعرض المؤسسات والحكومات بوجه عام والجامعات على وجه الخصوص لخسائر مالية وفقدان البيانات الدقيقة وبصفة عامة يهدف نظام كشف الاختراق التلقائي علي عبر شبكاته تحديد أي نشاط غير متوقع، وبالتالي تنبيه المسؤولين عن النظام لاتخاذ التدابير اللازمة بالجامعات ، هناك عدة أنواع من أنظمة كشف الاختراق التلقائي، وكل نوع منها يحتوي على أساليب وتقنيات مختلفة للكشف عن الاختراقات، ومن بين تلك الأنظمة هي نظام الكشف التلقائي بالتعلم الآلى، ويستخدم تقنيات الذكاء الاصطناعي لتحليل البيانات والحد من الاختراقات، وتهدف إلى تحسين كفاءة الأنظمة الحاسوبية في الكشف عن الاختراقات والتعامل معها بفعالية. ويمكن أن تعتمد هذه الأنظمة على أساليب مختلفة، مثل استخدام الشبكات العصبية والتعلم الآلي لتحليل سلوك المستخدمين والتحقق من صحته ، ومن ثم يعد نظام كشف الاختراق التلقائي أحد أهم أنظمة الزكاة الاصطناعي التي تساهم في تمكين الأمن السيبراني بالجامعات.(Cai, Y. and Wang, T., 2020,p.8)

كما تعتمد أنظمة الذكاء الاصطناعي التي تستهدف الكشف التلقائي للاختراق من أجل تمكين الأمن السيبراني على العديد من التقنيات والمفاهيم الرئيسية للذكاء الاصطناعي، مثل التعلم الآلي وتحليل البيانات وتقنيات المنطق الرمزي، وتتميز هذه الأنظمة بقدرتها على استخلاص البيانات التي تشير إلى أي نشاط غير مشروع دون الحاجة إلى تدخل بشري، وتحديد أي نشاط غير متوقع أو غير مطابق للسلوك الطبيعي. ويستخدم هذا النظام بشكل خاص في الكشف عن الاختراقات التي تستهدف التطبيقات والمعلومات الدقيقة .

كما يتميز نظام الكشف التلقائي للاختراق بكشف الاختراقات وبقدرته على تحديد أي محاولة لإيقاف النظام ، كما يستخدم نظام الكشف التلقائي للاختراق تقنية التعلم العميق لتحسين الكفاءة والكشف عن الاختراقات وتحليل البيانات باستمرار Zhang, W., Wu, J., Jia, F. and Lv, Y., 2021,p. 9

كما تجدر الإشارة إلي أن الجامعات والمؤسسات التعليمية تتعرض لخطر الاختراق السيبراني من قبل المتسللين والقراصنة، مما يؤدي إلي التسبب في تعطيل النظام وسرقة البيانات الدقيقة. ولحماية هذه المؤسسات، يتم استخدام أنظمة كشف الاختراق التلقائي التي تعتمد على أحد أهم أنظمة الذكاء الاصطناعي

وأهم ما يميز نظام الكشف التلقائي أنه يستهدف المعلومات المالية والبيانات الحساسة الأخرى. وتساعد هذه الأنظمة الجامعات على الوقاية من الاختراقات وحماية البيانات الدقيقة، وتحسين كفاءة الأنظمة الحاسوبية في التعامل مع تهديدات الاختراقات السيبرانية ، ومن ثم تمكين الأمن السيبراني ، وتجدر الإشارة إلي أنه لا يوجد نظام حماية يمكنه ضمان الحماية المطلقة، ولذلك يجب استخدام عدة أنظمة مختلفة للذكاء الاصطناعي ، وذلك لتوفير حماية بشكل متزامن لزيادة فعالية تمكين الأمن السيبراني بالجامعات. (Wang, Z., Wang, G., Wang, T. and Song, W., 2021,p.9)

١- نظام الجدار الناري المتقدم Next Generation Fire Walls (NGFW) :

يعتبر نظام الجدار الناري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعات ، ففي ظل تزايد التهديدات السيبرانية والاختراقات الإلكترونية المتعددة، أصبحت الجامعات تواجه تحديات عديدة فيما يتعلق بحماية أنظمتها وبياناتها الحساسة. لذلك، أصبح البحث عن آليات وأساليب فعالة لتطبيق الأمن السيبراني ضرورة ملحة في تلك المؤسسات الأكاديمية. ويعد الجدار الناري المتقدم بمثابة حجر الأساس لأي استراتيجية أمنية ناجحة في الجامعات. يتم استخدامه لرصد ومراقبة حركة المرور عبر الشبكة، والتحقق من صحة البيانات ، ومنع التهديدات الخبيثة من الوصول إلى الأنظمة الحاسوبية والبيانات الحيوية. يتميز النظام بقدرته على رصد التهديدات المحتملة والاستجابة السريعة لمواجهتها بواسطة تحليل السلوك الشبكي والتحقق من البيانات(Stark, J. 2020,pp.6-7). .

ومع تقدم التكنولوجيا، تم استحداث التطبيقات المتقدمة للذكاء الاصطناعي في تعزيز الأمان السيبراني بالجامعات. فعلى سبيل المثال، يمكن للذكاء الاصطناعي أن يعين في تشخيص التهديدات والاختراقات وفحص الشبكات للتعرف على نقاط الضعف والتحذير من الهجمات المحتملة. يمكن أيضًا استخدام الذكاء الاصطناعي في تطوير نماذج التعلم الآلي للتنبؤ بالتهديدات المستقبلية وتحسين استجابة أنظمة الأمان في الوقت الفعلي. بالإضافة إلى ذلك، تعتبر إجراءات الأمن السيبراني في الجامعات مرتبطة أيضًا بالتوعية والتدريب العام لأفراد المؤسسة. يجب أن يكون هناك وعي وقدرة على التعرف على الهجمات الاحتيالية والبرمجيات الخبيثة والبريد الإلكتروني المشبوه. علاوة على ذلك، يتعين على الجامعات اعتماد سياسات أمنية صارمة وتحديثها بشكل منتظم لمواجهة التهديدات المستمرة وتعزيز الاستعداد لأي حالات طوارئ.

نجد أنه لضمان أمن البيانات والأنظمة الحاسوبية في الجامعات، يجب توفير منظومة شاملة ترتكز على نظام الجدار الناري المتقدم واستخدام التكنولوجيا المتقدمة للذكاء الاصطناعي. كما يجب أخذ احتياطات الأمان اللازمة وتنفيذ سياسات الأمن القوية والتوعية المستمرة للعاملين والطلاب في الجامعة(White, A. ,2021,pp.5-6) .

٤-نظام الأمن السحابي Cloud Security (CS):

يعتبر نظام الأمن السحابي أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعات، حيث تطورت التكنولوجيا بشكل كبير في العقد الماضي، وتحولت الحوسبة إلى خدمة سحابيةCloud Computing ، (الهيئة الوطنية للأمن الإلكتروني ، " الإصدار الأول ، ٢٠١٩ م ، ص٣). حيث يتم تخزين البيانات وتشغيل البرامج على الأجهزة البعيدة التي تقع في مراكز البيانات المنتشرة في أنحاء العالم بدلاً من تخزينها وتشغيلها على الأجهزة المحلية، وذلك لتوفير المرونة، والكفاءة، والتوفير في التكاليف. وقد أدى هذا التطور إلى زيادة حجم البيانات التي يتعامل معها الأفراد والشركات والحكومات بشكل يومي، مما يتطلب حماية وتأمين هذه البيانات الحيوية. (المنظمة الدولية للمعايير، ٢٠١٨ ، ص١٢.

ومع تقدم التقنية والظهور الفعال للذكاء الاصطناعي Artificial Intelligence تم تحويل هذه التقنيات على نطاق الأمن والحماية ليصبح نظام الأمن السحابيCloud Security ، والذي يعد أحد أهم أنظمة الذكاء الاصطناعي الحل المثالي لحماية هذه البيانات والحفاظ عليها. (محمد محمود، ٢٠١٩، ص ٢٢) ، ويقصد بنظام الأمن السحابي : هو آلية قائمة على تخزين ومعالجة البيانات من خلال الإنترنت بدلا من الحواسيب ، ويعد هذا النظام تقنية حديثة تستخدم بشكل واسع في العديد من الميادين والمجالات المهنية كالتجارة الإلكترونية وتوفير الخدمات السحابية.

وتتعدد مهام الأمن السحابي حيث يحتاج العديد من الطلاب والموظفين في الجامعات إلى الوصول إلى المعلومات المختلفة المتعلقة بالجامعة عبر تنزيل المستندات الإلكترونية وملفات البيانات ، ومع زيادة الطلب على البيانات الإلكترونية، يزداد أيضًا خطر التعرض للاختراق الإلكتروني. وهنا يدخل نظام الأمن السحابي لحماية هذه البيانات المهمة ، ومن ثم المساهمة في تمكين الأمن السيبراني. ويتيح نظام الأمن السحابي للجامعة إمكانية التمتع بالمرونة والتحكم في الأمن والوصول إلى كافة البيانات الرقمية. كما يُعد هذا النظام الوسيلة الأفضل والأسهل لتحويل البيانات المهمة إلى شكل مشفّر ومن ثم حمايتها ضد التهديدات الإلكترونية ، ومن الجدير بالذكر أنه باستخدام نظام الأمن السحابي بالجامعة، يمكن للطلاب والموظفين الوصول إلى البيانات عن بُعد ومُشاركتها بتناغمٍ مع زملائهم في العمل أو الدراسة. وبفضل هذه الخدمة، يستطيع الطلاب والموظفين في الجامعات زيادة إنتاجيتهم وتسريع عملياتهم التعليمية والإدارية. ويعد تحسين السرعة والكفاءة والأمن في الوصول إلى البيانات محفزًا لاستخدام نظام الأمن السحابي بالجامعات.

٤- نظام التعرف على ملامح السلوك غير العادي : (UEBA)

:User and Entity Behavior Analytics

يعد نظام التعرف على ملامح السلوك غير العادي أحد أهم الأنظمة الأمنية الذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني ، حيث يتمتع السلوك الإنساني بمجموعة من الصفات الفريدة، التي تجعله يتفاوت كثيرًا عن بعضه البعض. ومن هذه الصفات، السلوك غير العادي الذي يمكن أن يكون مؤشرًا على حدوث مشاكل أمنية في المؤسسات الكبيرة مثل الجامعات ، وتجدر الإشارة إلي أن التعرف على ملامح السلوك غير العادي (UEBA) في الجامعات تقوم بتحليل البيانات والتفاصيل المتعلقة بسلوك زوار الجامعة أو موظفيها، ويتم ذلك من خلال تحليل العناصر التي يقوم بها الأفراد داخل الشبكة الإلكترونية، وكذلك عن طريق مراقبة الأفراد عبر مراقبة الكاميرات(User and Entity Behavior Analytics, 2019,p.6) .

ويحتاج نظام التعرف على ملامح السلوك غير العادي بالجامعات مهارات خاصة للقيام بالتحليل الكبير لسجلات البيانات ، والحفاظ على سرية هذه البيانات.

ويحتاج نظام التعرف على الملامح السلوك غير العادي إلى دعم تقني قوي، لضمان التشخيص السريع والدقيق للسلوك الغير عادي، ويتم ذلك من خلال فحص النوعية والكمية من البيانات المتاحة، وتطبيق نظم التعلم الآلي والذكاء الاصطناعي ، ومن خلال نظام التعرف علي ملامح السلوك غير العادي يتم الكشف عن السلوك غير العادي الذي يحدث في الكثير من الحالات.

(Using User and Entity Behavior Analytics, 2019,p.9). تم تصميم نظام التعرف على الملامح السلوك غير العادي لمساعدة الجامعات في اكتشاف الانفعالات النفسية والتعبيرات الجسدية التي من الممكن ان تكون مؤشرًا على مشاكل أمنية محتملة داخل الجامعات. ويستطيع هذا البرنامج كذلك كشف التغييرات المفاجئة والمثيرة للاهتمام في الأنشطة، مما يمنح الجامعات الأمان الكافي خلال تنفيذها لأنشطتها اليومية.

(How UEBA Tools Help Protect Against Insider Threats, 2019,p.4)

وعلى الرغم من أن نظام التعرف على ملامح السلوك غير العادي قد صممت خصيصًا للجامعات، فإنها يمكن استخدامها بسهولة في العديد من المجالات الأخرى. ومن بين الأمثلة المستخدمة لهذا النظام والقائمة على نفس المبدأ، هي مراقبة الشبكات الاجتماعية، والحجز، والتعرف البيومتري. وتحتاج كافة هذه المجالات إلى مجموعة متكاملة من الخوارزميات الإحصائية ونظم التعلم الآلي لسرعة الكشف عن المشاكل التي تتطلب اتخاذ إجراءات فورية.

(Reaping Benefits of UEBA Tech for Security Operations, 2019,pp.4-5)

إن الاستخدامات المختلفة لنظام التعرف على الملامح السلوك غير العادي في تزايد مستمر بالجامعات في المستقبل، وذلك في ظل التعاظم المستمر لاستخدام التكنولوجيا في كل المجالات. والشيء الجيد هو أن هذه البرامج توفر حلاً فعالًا وتقنيًا للعديد من المشاكل التي يعاني منها العالم، من خلال تحليل سلوكيات الأفراد والمؤسسات من خلال البيانات، الذي يوفّر وقتًا ومالًا، ويضمن الأمن

الكافي للمؤسسة ، لذا يعد نظام التعرف على الملامح السلوك غير العادي يعد أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعات .

٥- نظام الإدارة التلقائية للأمن Automated Security Management(ASM) :

يعد نظام الإدارة التلقائية للأمن أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعات ، خاصة في ظل الظروف الأمنية العالمية الراهنة، وازدياد الاعتداءات الإرهابية، يعتبر الأمن والسلامة أمرًا حيويًا وضروريًا في المجتمع الحديث. ولعلّ الجامعات من بين أهم الأماكن التي تتعرض للعديد من المخاطر، مثل الاعتداءات، والسرقات، والحرائق، وغيرها من المخاطر. ومن هنا وجب على الجامعات اعتماد نظام الإدارة التلقائية للأمن (ASDM Automated Security Management)، الذي يساعد على تحسين مستوى الأمان والحد من المخاطر المحتملة، وبالتالي تحقيق بيئة دراسية آمنة ومحفوفة بالحماية.

وتجدر الإشارة إلي أن الأمن والسلامة هما عنصران أساسيان لأيّ مؤسسة تعليمية، ولا سيما الجامعات. تعرض للكثير من المخاطر، التي تهدد حياتهم وممتلكاتهم، في إطار ظروف الأمن العالمية الصعبة، الأمر الذي يجعل الجامعات تستهدف اعتماد أنظمة حديثة تمكنهم من إدارة وتحسين مستوى الأمن بطريقة فعّالة وموثّقة، ويشار للإدارة التلقائية للأمن بأنها نظام حاسوبي يتحكم في الأنظمة الأمنية والمراقبة المتعلقة بالجامعات، والذي يعتمد على تقنية الذكاء الاصطناعي. ويوفر هذا النظام العديد من الخدمات المتعلقة بالأمن والسلامة، مثل إدارة الوصول والمراقبة، والكشف المبكر عن أي تهديدات ومخاطر قد تواجه الجامعة، وكذلك عمليات تنظيم الطوارئ.

ويتكون نظام الإدارة التلقائية للأمن بالجامعات من العديد من المكونات، والتي من أهمها علي النحو التالي :

أ- نظام قفل الأبواب الذكي: وهو نظام يعمل بالكهرباء ويستخدم لتأمين الأبواب وغيرها من أنظمة الدخول.

ب- نظام كاميرات المراقبة: وهو نظام يستخدم كاميرات للمراقبة المستمرة لجميع أنحاء الجامعة.

ج- نظام التحذير المبكر: وهو نظام يحذر من أي خطر ويتيح لإدارة الجامعة فرصة الرد والتعامل مع المخاطر.

د- نظام التتبع بالجي بي أس: وهو نظام يتيح تتبع موقع الأشخاص المفقودين والمختطفين.

ه- نظام إدارة المخاطر: وهو نظام يستخدم للتعرف على المخاطر وتقييمها، وتحديد الحلول المناسبة لإدارتها.

يوفر نظام الإدارة التلقائية للأمن بالجامعات العديد من الفوائد والتحسينات أهمها علي النحو التالي :

- توفير الوقت والمجهود في التحقق من هوية الأشخاص والوصول إلى الأماكن.
- تحسين مستوى الأمن والحماية لأنظمة الجامعة، وبالتالي توفير بيئة دراسية آمنة للطلاب والهيئة التدريسية.
- تقليل مخاطر السرقة والاعتداءات والحرائق.
- تحسين عمليات التحقق بالحضور والانصراف من الجامعة.
- إيجاد حلول سريعة وفعالة للطوارئ والمخاطر التي يمكن أن تحدث في الجامعة.

٦- الأمن الإداري المتقدمAdvanced Administrative Security(AAS):

يعتبر نظام الأمن الإداري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي والتي تستهدف تمكين الأمن السيبراني ، والتي تحظى باهتمام الجامعات حاليًا، حيث يساعد على تحسين أمن الجامعات ورفع كفاءة العمليات الإدارية. ، كما أنه يساهم في تحسين كفاءة العمليات الإدارية ويحمي الطلاب والعاملين بالجامعات من القرصنة والهجمات السيبرانية ، مما يساهم في تلبية احتياجات الجامعات وتحسين نظام الأمن الإداري .

(Cheng-Jian Lin, Shih-Jen Huang, 2021,p.22)

نظرا لمدي أهمية الحفاظ على سرية المعلومات في جامعاتنا، وبما أن العمليات الإدارية في الجامعات تتعدد، وتكثر أنواع المعلومات المحفوظة بها، لذلك تزداد أيضًا حاجة الجامعات لنظام الأمن الإداري المتقدم بهدف تمكين الأمن السيبراني. (محمد

رفيق عمر، ٢٠٢١م، ص٢٢). وتجدر الإشارة إلى أن مراكز البيانات في الجامعات تقوم بتخزين ومعالجة كميات كبيرة من البيانات والمعلومات المتعلقة بالطلاب والموظفين والمصادر التعليمية والأبحاث العلمية وغيرها. ولتأمين هذه البيانات، يعتمد النظام الإداري المتقدم على التشفير، والوسائل التكنولوجية العالية الكفاءة. (سلمان العتيبي، ٢٠٢٢م ، ص ٤). ونظراً لكون الأمن السيبراني يؤدي دورًا حيويًا في حماية الجامعات من الهجمات الإلكترونية، والتي يتم تنفيذها بشكل يومي، ويمكن أن تسبب تأثيرًا سلبيًا على الجامعات وطلابها وموظفيها. (ياسر العمري، وياسين الشريف، ٢٠٢٣م، ص٢٢). لذلك يعتمد تمكين الأمن السيبراني في الجامعات على استخدام مجموعة متنوعة من الأنظمة الأمنية المتطورة، بما في ذلك الحماية من الفيروسات، والقرصنة، والنسخ الاحتيالية، والتطفل، وغيرها من الاختراقات الإلكترونية.(ياسمين الكريم، ٢٠٢٤م ، ص١٤)

المحور الثالث : طبيعة العلاقة بين الذكاء الاصطناعي والأمن السيبراني بالجامعات :

تتمتع أنظمة الذكاء الاصطناعي بقدره فائقة على تلبية متطلبات تكنولوجيا المعلومات ، والتي من أهمها الأمن السيبراني حيث يمتلك الذكاء الاصطناعي القدرة على مراقبة الشبكات ٣٦٥ يوماً في السنة ، ويمكن لأنظمة الذكاء الاصطناعي الإستجابة لأي خطر أمني تشعر به في غمضة عين ، وتجدر الإشارة إلى أن أنظمة الذكاء الاصطناعي تساعد الجامعات في الإلتزام بتطبيق أفضل الممارسات الأمنية ، وذلك من خلال التعرف على أنماط البيانات ، ويمكن توضيح طبيعة العلاقة بين الذكاء الاصطناعي وتمكين الأمن السيبراني بالجامعات كما أشار (Choo, K-K. R, 2023,pp. 48-49)

على النحو التالي :

١-التحقق من هوية المستخدم :

يعتبر التحقق من هوية المستخدم من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات ؛ وذلك من خلال تحديد هوية الشخص والتحقق اذا ما كانت هي الهوية الأصلية للمالك أم لا، كي لتسمح له بالدخول للبيانات، كل ذلك يتم من خلال تقنية الذكاء الاصطناعي، التي ترفع من مستوى الأمان وتنفيذ المهام بجودة عالية، لذا يعتبر التحقق من هوية المستخدم من أهم آليات أنظمة الذكاء الاصطناعي والتي تساعد في تمكين الأمن السيبراني بالجامعات.

٢- زيادة أمن الشبكات :

تعتبر زيادة أمن الشبكات من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات؛ حيث تقوم أنظمة الذكاء الاصطناعي بدور كبير ومهم فيما يخص زيادة أمن الشبكات، التي قد لا يستطيع الانسان دائما أن يصل بها للمستوي المطلوب من الأمن. لذا يعتبر زيادة أمن الشبكات من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات .

٣-تحليل سلوك المستخدمين :

يعتبر تحليل سلوك المستخدمين من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات ، فأنظمة الذكاء الاصطناعي تستطيع أن تحفظ تكرار الأنماط وبالتالي يرفع ذلك من قدرتها على حفظ السلوك البشري، ومن ثم تحليله بشكل دقيق، الأمر الذي يجعل إمكانية التنبؤ بوجود أخطاء أو أي سلوك غير طبيعي لدى المستخدم أم سهل بالنسبة لها، لذا يعتبر تحليل سلوك المستخدمين من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات .

(Smith, J., & Johnson, R, 2023,pp. 290-291)

٤-التقليل من الهجمات السيبرانية :

يعتبر التقليل من الهجمات السيبرانية من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات ؛ على الرغم من أن وظيفة الأمن السيبراني الأساسية هي تحقيق الأمن المعلوماتي والتقليل من الهجمات السيبرانية واكتشافها، إلا أنه في ظل التطور الكبير للتكنولوجيا والانترنت على حدٍ سواء، فقد قلل ذلك من فرص الامن السيبراني منفرداً في اكتشاف الهجمات السيبرانية بشكل سريع، ولكن في ظل وجود الذكاء الاصطناعي يساعد ذلك على تقليل من هذه الهجمات وإعادة التوازن

للأمن السيبراني؛ لذا يعتبر التقليل من الهجمات السيبرانية من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات .

٥-التعامل مع الثغرات بفعالية :

يعتبر التعامل مع الثغرات بفعالية من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات ، ويعد توظيف أنظمة الذكاء الاصطناعي في مجال إدارة الثغرات والتعامل معها بفاعلية كان له دور كبير خاصة في ظل صعوبة التعامل معه من قبل فرق الأمن السيبراني دون التدخل التقني، لذا يعتبر التعامل مع الثغرات بفعالية من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات . (Ahmed, S., & Lee, D., ,2023,pp. 130-131)

٦-مشكلة إمكانية الخطأ البشري:

يعتبر التغلب علي مشكلة إمكانية الخطأ البشري من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات ، حيث تعتبر مشكلة الخطأ البشري أمر لا يمكن تفاديه أو السيطرة عليه في كثير من حالات الأمن السيبراني؛ فنجد ان أي نظام يمكن انشائه وبنائه على الانترنت لابد من اكتشاف أخطاء لاحقة فيه، تتطلب وجود فريق من الخبراء والتقنيين من أجل تحديثها وإجراء التعديلات المناسبة عليها، وباستخدام أنظمة الذكاء الاصطناعي يمكننا تفادي هذه المشكلات، أو على الأقل إعطاء الحلول المناسبة للفرق والخبراء عند الحاجة وتقليل الوقت والجهد ، لذا يعتبر التغلب علي مشكلة إمكانية الخطأ البشري من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات .

٧- ضعف الأداء البشري وكفاءته :

يعتبر الاعتراف بضعف الأداء البشري وكفاءته من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات .ففي حال تكرار الأنشطة وأداء المهام المختلفة، نتيجة لاستخدام العقل البشري الذي يتوقع منه الخطأ، حتى في حال تكرار المهمة اكثر من مرة، الامر الذي يضطر التقنيين لإعادة ضبط الأجهزة لاكتشاف الأخطاء وتصحيحها، ومن هنا فإن وجود نظام يقوم على أساس الذكاء الاصطناعي الامر الذي يقلل من إمكانية تكرار الأخطاء البشرية في الأنشطة المختلفة ، لذا يعتبر الاعتراف بضعف الأداء البشري وكفاءته من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات .

٨- التهديدات المستمرة التي تسبب الانهاك لفريق الأمن السيبراني :

يعتبر التعامل مع التهديدات المستمرة التي تسبب الانهاك لفريق الأمن السيبراني من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات ؛ ويحدث ذلك نتيجة لتكرار التهديدات والتنبيهات الصادرة عنها، حيث يسبب في إنهاك وإضعاف فريق الأمن السيبراني، الأمر الذي يشكل عامل تهديد بحد ذاته، لذا فإن وجود تكنولوجيا وأنظمة تعتمد عليها فرق الأمن السيبراني يعد أمر مهم وضروري ويساهم في التقليل من التهديدات والتعامل معها بطريقة سريعة ودون تعرض الفرق للإنهاك من خلال تقنيات التعلم الآلي لحل المشكلات ومعالجتها؛ لذا يعتبر التعامل مع التهديدات المستمرة التي تسبب الانهاك لفريق الأمن السيبراني من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات.

(Kim, Y., & Park, S, 2023,pp. 75-76)

٩- سرعة الاستجابة للأخطار والتهديدات

تعتبر سرعة الاستجابة للأخطار والتهديدات من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات، حيث يعتبر الوقت من اكثر الأمور أهمية في الاستجابة لتهديدات الحماية السيبرانية، لذا لابد من وجود فريق امن سيبراني متيقظ على دار الساعة، الامر الذي قد يكون شبه مستحيل خاصة في ظل التطور الهائل لهذه الاخطار التي تهدد الامن السيبراني، حيث يقوم المهاجمين بشن هجمات بسرعات كبير وقد يغفل الامن السيبراني عنها في بعض الأحيان، ولكن في حال وجود أنظمة للذكاء الاصطناعي التي تتعامل مع الأمن السيبراني، لذا قد يصبح أسهل وأسرع في الاستجابة لهذه التهديدات ومنعها،

من خلال إرسال تقرير فوري بوجود تهديد للفريق فيتوجه لحل هذه المشكلة ومواجهة التهديد؛ لذا تعتبر سرعة الاستجابة للأخطار والتهديدات من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات .

١٠- التقليل من الأيدي العاملة :

يعتبر التقليل من الأيدي العاملة من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات ، حيث يعتبر استخدام أنظمة الذكاء الاصطناعي من أهم الأمور التي تساعد في تقليل الأيدي العاملة، وزيادة جودة العمل، فهو يقلل من الميزانية التي من الممكن دفعها لأعداد أكبر من الموظفين، وبذلك فإن استخدام الذكاء الاصطناعي يقلل من الميزانية ولكن يفرض على من يتعاملون معه التعرف أكثر على آليات العمل ؛ وذلك لمواكبة التطور المستمر في هذا المجال ؛ لذا يعتبر التقليل من الأيدي العاملة من أهم آليات أنظمة الذكاء الاصطناعي ، والتي تساعد في تمكين الأمن السيبراني بالجامعات (Gupta, A., & Singh, P.., 2023, pp. 89-90).

مما سبق يتضح أن هناك علاقة وطيدة بين أنظمة الذكاء الاصطناعي وتمكين الأمن السيبراني بالجامعات .

القسم الثالث للدراسة : تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي في الجامعة الوطنية بأستراليا : دراسة وصفية تحليلية.

يعد تمكين الأمن السيبراني من أهم القضايا الأساسية بالجامعات في أستراليا، وذلك لأن مجتمع الجامعة يمثل مجتمعا كبيراً من الطلاب والباحثين في هذه المؤسسات. ولمواجهة التهديدات السيبرانية، تبذل الجامعات جهوداً كبيرة، من بينها استخدام أنظمة الذكاء الاصطناعي لتمكين الأمن السيبراني. ويعتمد نظام تمكين الأمن السيبراني بالجامعة الوطنية باستراليا على استخدام الأنظمة الأمنية للذكاء الاصطناعي ، وذلك من خلال التعرف على الأنماط: يمكن للذكاء الاصطناعي مساعدة الجامعات في تحديد الأنماط الغير مألوفة التي يمكن أن تكون مؤشراً على اختراق سيبراني.

بالإضافة إلي التعرف على الأخطار: يمكن أن يساعد الذكاء الاصطناعي على تحليل السجلات والأدلة التي تشير إلى الاختراق السيبراني وتحديد نقاط الضعف في نظام أمن الجامعة. علاوة علي الكشف عن الهجمات: يساعد الذكاء الاصطناعي في كشف الهجمات السيبرانية قبل حدوثها، حيث يستطيع تحليل البيانات الضخمة والتعرف على الاتجاهات الشائعة للهجمات وإجراء التحليل الكمي للسيطرة عليها (Australian Government Department of Education and Training,2018,p.6)

أيضا من خلال التحكم في الوصول: يُتيح الذكاء الاصطناعي القدرة على السماح بالوصول للمستخدمين المشروعين فقط، وذلك بتحديد المستخدمين والأدوات الموثوق بها. بالإضافة إلي التعرف على الهوية: يساعد الذكاء الاصطناعي في التعرف على الهوية المشروعية للمستخدمين والمركبات والأدوات وتحديد ما إذا كانوا مؤهلين للوصول إلى البيانات المحمية أم لا. (Akbar, M., & Gao, J. ,2019,p.2)

أيضا من خلال تحليل البيانات: يستخدم الذكاء الاصطناعي بشكل واسع في تحليل البيانات السيبرانية لتحديد نقاط الضعف واكتشاف الأنماط الغير مألوفة وكشف الهجمات قبل حدوثها(Chowdhury, N., & Abawajy, J. H. ,2018,p.27) . أيضا من خلال المراقبة والتشخيص: تعتمد الجامعات على التقنيات الذكية للمراقبة والتشخيص الذاتي لمعالجة التهديدات السيبرانية (The University of Melbourne ,2019, pp.4-5). بالإضافة إلي تحديد سلوك الهجوم: يستخدم الذكاء الاصطناعي في تحليل سلوك الهجمة وتحديد كيفية الاستجابة المثلى لها.(Kourdi, M., & Alsaidan, S. ,2020,p.11). علاوة علي تقييم مستوى الخطر: يستخدم الذكاء الاصطناعي في تقدير مستوى الخطر السيبراني وتحديد الإجراءات الأمنية اللازمة للتغلب عليه(Black, J. ,2018, pp.10-11). بالإضافة إلي تشفير البيانات: تستخدم الجامعات أيضًا تقنيات تشفير البيانات المستخدمة في الاتصالات السيبرانية والتي تستخدم الذكاء الاصطناعي لتمكين الأمن السيبراني(Deakin University,2021,pp.2-3) .

لقد استطاعت الجامعة الوطنية باستراليا أن تصبح ذات خبرة واسعة في مجال تمكين الأمن السيبراني في ضوء الذكاء الاصطناعي وهذا ما سيتم تناوله على النحو التالي :

أولا : مدخل تاريخي عن الجامعة الوطنية باستراليا:

تأسست الجامعة الوطنية الاسترالية (the Australian National University (ANUعام ١٩٤٦م ، وهي الجامعة الأولى التي قامت الحكومة الفيدرالية بتأسيسها في أستراليا ، وتعتبر الآن واحدة من أرقى الجامعات في العالم، وتتميز بتقديم البحث والتعليم العالي على أعلى مستوى، تتمتع الجامعة الوطنية ANU بتاريخ طويل وحافل بالإنجازات العلمية، وهي تشهد على إرث استثنائي من الشخصيات الجيدة والطلاب الموهوبين.

تقع الجامعة الوطنية ANU في قلب العاصمة الأسترالية كانبيرا، وتتألف من ست كليات. يوجد القسم الرئيسي للجامعة في منطقة أكتون الساحرة التي تطل على بحيرة بورتير في جنوب المدينة، وهي بالقرب من حدائق العاصمة ومكتبة البرلمان الوطني ، كما تتابع الجامعة الوطنية ANU اهتماماتها العالمية وتتبنى العالمية في تحديد نطاق دراستها وخدماتها. حققت ANU مكانتها كواحدة من أفضل الجامعات في العالم، مع تقديم برامج الدراسات العليا والبحث الذي يتمتع بالتعرف على العالم في القرن الحادي والعشرين((National University of Australia,2023,pp.1-2.

تتمتع الجامعة الوطنية باستراليا ANU بشبكة واسعة من التحالفات والشراكات الدولية. يتم استقطاب الطلاب من مختلف أنحاء العالم، ويأتون إلى الجامعة للدراسة والبحث ولتوسيع اتصالاتهم الثقافية. ترعى الجامعة أيضاً برامج التبادل الأكاديمي والثقافي مع جامعات أخرى في جميع أنحاء العالم ، بالاضافه إلى أنها تتمتع بالريادة في البحث العلمي ، حيث بالإضافة إلى التعليم يعتبر البحث متطلبًا ضرورياً لسير الجامعة الوطنية الاسترالية. تكرس ANU الكثير من الجهود والمال في تمويل البحث، والذي يمتد إلى مختلف المجالات مثل العلوم الإنسانية والاجتماعية والعلوم والتقنية ، هذا وتجدر الاشاره الى ان الجمع الوطنيه باستراليا ANUتستقطب باحثين موهوبين من جميع أنحاء العالم، وتقدم لهم وسائل دعم فعالة للتميز البحثي. تدعم الجامعة الأبحاث والرسائل العلمية في مختلف المجالات، وتخرج أبحاث موثقة في أهم المجلات العلمية في جميع أنحاء العالم rankings university) . subject rankings,2021,pp.99-100)

علاوة على أن الجامعة الوطنية باستراليا تتمتع بمناخ ثقافي متميز وجذاب ، حيث تحتضن الجامعة الوطنيةANU طلابًا من جميع أنحاء العالم، مما يخلق جوًا ديناميكيًا وانعتاقاً وثقافيًا في الحرم الجامعي. كما أن هناك العديد من النوادي والمنظمات الطلابية والتي يمكن للطلاب الانضمام إليها لتوسيع معارفهم والاستفادة من تجارب الطلاب في أماكن أخرى ، بالإضافة إلى ذلكيلتقي الطلاب في أعمال المسرح والموسيقى والرياضة والتمثيل والقوافل الرياضية وغيرها ، وتتوفر في الجامعة الوطنية ANU وحدات إسكان متخصصة ومرافق رياضية عالية الجودة.

ومن أبرز ما يميز الجامعة الوطنية باستراليا أنها تتواجد في قلب المجتمع المدني والحكومي حيث تقع في المحيط السياسي والحكومي المتعدد الثقافات والنشط، في العاصمة الأسترالية كانبيرا. تحافظ الجامعة على وجود حيوي وفعال في النقاشات العامة والمسائل السياسية، ومع تقديم الخبرة التي يضيفها طلاب الجامعة إلى الحياة المدنية والديمقراطية في أستراليا وخارجها.

يأتي الأمر بسهولة بفضل موقع إقامة الجامعة في قلب العاصمة، والتي تفعل الكثير من الفعاليات والأنشطة المتنوعة التي يجتمع بها الناس المحليون والزوار. كما أن الاتصال الثمين بالمجتمع الأكاديمي والمشاريع البحثية المحلية يهدف إلى دعم حل وتحليل القضايا التي تواجه المجتمعات المحلية والوطنية

وتجدر الإشارة إلى أن الجامعة الوطنية بأستراليا تضم ٧ كليات، وتوفر أكثر من ٢٥٠ برنامجاً دراسياً، وتستقطب الطلاب من جميع أنحاء العالم. وقد حصلت الجامعة على العديد من الجوائز المرموقة، كالرتبة الأولى في أستراليا والثامنة في العالم كأفضل جامعة عام ٢٠٢١م ، بحسب مؤشر .QS للجامعات وهو تصنيف ثانوي لافضل ٨٠٠ جامعه في العالم تنشره شركة كوا كولا ريلي سيمون سي متخصصة في التعليم(QS World University Rankings by Subject, 2021,pp.27-28)

تتميز الجامعة الوطنية الاسترالية بتقديم برامج دراسية متعددة في العلوم الزراعية والطبيعية والعلوم الإنسانية والتكنولوجيا والاقتصاد والقانون والطب وغيرها، مما يجعلها تلبي احتياجات الطلاب من مختلف الأصول والثقافات والتخصصات، كما تقدم الجامعة الوطنية الاسترالية بيئة تعليمية رائعة تجمع بين الدراسة النظرية والتطبيق العملي، وتولي اهتماماً كبيراً بالأبحاث العلمية والتطوير التكنولوجي، وتتوفر فيها فرص العمل والتدريب الداخلي والخارجي للاستفادة من الخبرات والمعارف العلمية العالية.

يوجد في الجامعة العديد من المراكز البحثية المتخصصة في مجالات مختلفة، مثل مركز الدراسات الآسيوية والمحيط الهادئ ومركز البيئة والتغيرات المناخية، ويعمل بها باحثون وأساتذة ذوو خبرات ومهارات عالية في مجالات تخصصاتهم.

تركز الجامعة الوطنية الاسترالية على الابتكار وتمكين الطلاب وإعدادهم للعمل في مجالات العمل حول العالم، وتعمل على تشجيع الابتكار والإبداع وتنمية مهارات القيادة والتفاعل الاجتماعي. وتقدم الجامعة الوطنية الاسترالية برامج ودورات تدريبية مكثفة لتعزيز مهارات الطلاب ومساعدتهم على تحقيق أهدافهم الأكاديمية والمهنية (Research institutes and centres,2022,pp.8-9) .

وتتعدد مجالات تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا حيث يشهد استخدام الذكاء الاصطناعي في مجال تمكين الأمن السيبراني تطورات إضافية، حيث تقوم الجامعة الوطنية باستراليا بذلك من خلال العديد من المجالات والتي من أهمها :

١- **الكشف عن المزيد من الهجمات السيبرانية:** حيث يمكن تحسين قدرات الذكاء الاصطناعي بالتعلم العميق من خلال تحليل كميات كبيرة من البيانات، والتي يمكن أن تساعد على اكتشاف هجمات سيبرانية جديدة.(Kshetri, N. ,2019,pp.27-28)

٢- **توفير أفضل حماية وقت الاستجابة:** حيث يمكن للذكاء الاصطناعي أن يتعلم من الأخطاء السابقة ويتحسن المرة القادمة. ولذلك، يمكن توفير أفضل حماية وضمان الوقت الفعال للرد على الهجمات السيبرانية.

٣- **تطوير الخوارزميات الذكية: حيث يمكن تحديث الخوارزميات بعد تحليل البيانات الحية. وهكذا، يمكن للذكاء الاصطناعي تحسين الأمن السيبراني والتعلم من الأخطاء السابقة لمواصلة العملية التعليمية .**(Samaniego, J. A., & Alfaro, E ,2019,pp.6-7)

ثانيا : آليات تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا :

وتتعدد آليات تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية بأستراليا والتي أهمها على النحو التالي:

استخدام خوارزميات التعلم الآلي:يمكن استخدام خوارزميات التعلم الآلي لتحليل سجلات البيانات الخاصة بالشبكة الإلكترونية في الجامعة وتحديد أي نشاط غير مشروع يحدث، حيث يتم تطوير نماذج الذكاء الاصطناعي بناءً على سجلات البيانات التاريخية المتعلقة بالهجمات الإلكترونية، وذلك لتحديد أي نشاط غير مشروع في الوقت الحقيقي. (Saeed, N., Naeem, M., & Riaz, Z. ,2018,pp.30-31)

١- **تطوير تطبيقات الذكاء الاصطناعي:**يمكن استخدام التطبيقات الخاصة بالذكاء الاصطناعي لتحليل سلوك المستخدمين وتحديد أي نشاط غير مشروع يحدث على الشبكة الإلكترونية في الجامعة، وذلك لضمان سلامة البيانات وأنظمة الحاسوب.

(Sahlin, R. K.,2018,pp.18-19).

٣- استخدام الروبوتات الذكية: يمكن استخدام الروبوتات الذكية لمتابعة النشاط على الشبكة الإلكترونية في الجامعة، وتحليل السجلات الخاصة بالنشاط وتحديد أي نشاط غير مشروع يحدث، وذلك لحماية نظام الحاسوب والشبكة الإلكترونية من الهجمات الإلكترونية. (Yaqoob, I., Ahmed, E., Imran, M., & Al-Qurishi, M. ,2019,pp.6-9)

وتجدر الإشارة إلى أن الجامعة الوطنية الأسترالية تعد من أهم الجامعات العالمية التي تستخدم أحدث التقنيات في مجال الحماية الإلكترونية، حيث تعمل بإستخدام أحدث الأساليب والتقنيات في مجال الذكاء الاصطناعي وتطوير برمجيات الحماية الخاصة بها، ولذلك تعتبر الجامعة الوطنية باستراليا من الجامعات الرائدة في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي،

حيث تعتمد على أحدث التقنيات في هذا المجال، وذلك لضمان سلامة بيانات الطلاب والموظفين في الجامعة والذي يعد أحد أهم الأهداف الرئيسية لمؤسسات التعليم ؛ وذلك لحماية نظامها الإلكتروني والحفاظ على سرية بياناتها، وتعتبر جامعة الوطنية الأسترالية أحد أفضل الأمثلة على ذلك.

يعتبر الذكاء الاصطناعي وحماية الأمن السيبراني من أهم مجالات الحوسبة الحدي، والتي تعد أكثر النواحي التي يتم فحصها وتحسينها بشكل مستمر. وقد استطاعت جامعة الوطنية الاسترالية، التي تقع في العاصمة كانبرا، أن تصبح مركزًا مشهورًا للأبحاث في هذا المجال، فتتنافس مع رواد العالم في الحصول على نتائج استثنائية في تقديم الحلول المبتكرة للتحديات الحديثة.

تقوم جامعة الوطنية الاسترالية بعمل جاد وحثيث على تحقيق رؤيتها، التي تهدف إلى دعم صناعة الذكاء الاصطناعي والأمن السيبراني، وذلك من خلال توفير البحوث المرموقة والمناسبة بالإضافة إلى البرامج الأساسية لتجميع خبرات مهنية تحتل المركز الريادي في هذا الميدان، بحيث يتم تعزيز التنمية الثقافية في العالم على المدى القصير والطويل.(https://www.anu.edu.au,2023,pp.1-2)

تخصص جامعة الوطنية الاسترالية في تزويد طلابها بعلوم الحوسبة والبرمجة، والذكاء الاصطناعي والتعلم الآلي، وأساليب البحوث والتحليل، وحماية الأمن السيبراني، إلى جانب إمكانية الحصول على شهادات متخصصة في هذا المجال. ومن خلال برامجها الأكاديمية، تسعى الجامعة إلى تدريب الطلاب على استخدام التقنيات الحديثة، وكيفية التعامل مع التحديات المختلفة التي يواجهونها في هذا المجال.

تعمل الجامعة على إشراك الطلاب في برامج تدريبية، وفرص التطوير المهني، إلى جانب الحصول على فرص العمل على مشاريع حقيقية، حيث يتم تقديم محفزات كي يحصل الطالب على فرص العمل في هذا المجال. وتتميز جامعة الوطنية الاسترالية بأنها توفر برامجها الأكاديمية بأسعار معقولة، مما يتيح فرصًا أكبر للطلاب للوصول إلى مصادر التعليمية المتاحة في هذا المجال.(https://www.anu.edu.au,2023,pp.3-4). تشجع الجامعة الأبحاث العلمية والتفرد في المشاركة في إيجاد حلول ملموسة لتحديات المستقبل، حيث تقوم بدعم العالم الأكاديمي والصناعي على حد سواء، وذلك من خلال بناء شراكات مع القطاع الصناعي لتحقيق أهداف مشتركة.(https://www.cio.com.au,2023,pp.6-7)

وبالإضافة إلى الجهود التي تبذلها الجامعة في مجال البحث والتعليم في التكنولوجيا، تقدم الجامعة مجموعة من الخدمات لدعم الأمن السيبراني للمؤسسات الأخرى والمجتمع الأسترالي. ومن هذه الخدمات مراجعة الأمن السيبراني، والتي توفرها الجامعة للعديد من المؤسسات الحكومية والشركات الخاصة، وتعتمد فيها على فرقها المتخصصة في مجال الأمن السيبراني. وتوفر الجامعة أيضاً خدماتها في مجال عمليات التدريب والتعليم، خاصة للمنظمات ذات الصلة بالمجتمع الأسترالي.

مما سبق يتضح أن جامعة الوطنية الاسترالية قد حققت الاستقرار على الساحة العالمية والتزمت بمهمتها في توفير التعليم والبحث والخدمات في مجال الذكاء الاصطناعي وتعزيز الأمن السيبراني، وتمكنت الجامعة من أن توفر البرامج التعليمية المناسبة، التي تعزز المهارات المطلوبة لتحقيق النجاح في هذا المجال الحيوي. وبفضل الجهود المبذولة، تولي جامعة الوطنية الاسترالية دورًا بارزًا في بناء الأساس اللازم لصناعة الذكاء الاصطناعي والأمن السيبراني في المجتمع العالمي.

ثالثا: أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعة الوطنية باستراليا :

ويمكن تناول ذلك من خلال ما يلي :

١- نظام الكشف التلقائي للاختراق Intrusion Detection System (IDS):

يعد نظام الكشف التلقائي للاختراق أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني ، وتعد الجامعة الوطنية باستراليا واحدة من أفضل الجامعات علي مستوي العالم في توظيف نظام الكشف التلقائي للاختراق (Takeuchi, Y., Shibuya, M., & Fujisaki, Y.,2017,p.2). ولقد استطاعت الجامعة الوطنية باستراليا الحفاظ على سرية المعلومات وتشفيرها واكتشاف الهجمات السيبرانية أول بأول من خلال نظام الحماية الأمنية والذي يتمثل في نظام الكشف التلقائي للاختراق

. (Varshney, S., & Sharma, 2018, p.433)، ويساهم هذا النظام في تحويل الجامعة الوطنية باستراليا من مجرد جامعة عادية تقليدية إلى جامعة متمكنة في مجال تمكين الأمن السيبراني (Rastogi, M., & Mishra, P, 2016,p.90)

والحفاظ على سرية المعلومات من أي هجمات وفي ظل كل ذلك أيضا إتاحة المعلومات ليصبح نظام الكشف التلقائي للاختراق أحد أهم الأنظمة الأمنية للذكاء الاصطناعي والتي تستهدف الحفاظ على سرية المعلومات ودقتها وإتاحة المعلومات تحت إشراف الجامعة وبذلك نجحت الجامعة الوطنية في تمكين الأمن السيبراني بها (Seraj, A., et al.. , 2018,p.80) . ويشار إلي نظام الكشف التلقائي للاختراق بأنه عبارة عن : عملية تقوم علي فحص نظام المعلومات ، وكشف أي هجمات قبل حدوثها مما يساهم في الحفاظ على سرية المعلومات ودقتها ، ويتم ذلك بطريقة إلكترونية ذاتية التشغيل والتي تهدف إلى البحث عن الثغرات الأمنية وتقديم توصيات لتعزيز الأمن والحماية ، ومن ثم تمكين الأمن السيبراني .

(Almorsy, Mohamed, Sitalakshmi Venkatraman, and Salmin Sultana. 2018,p.44)

وتتم هذه العملية من قِبل فريق من المتخصصين في الأمن السيبراني، والذين يقومون بتحليل النتائج وتقديم التوصيات، ويساعد نظام الكشف التلقائي للاختراق على تمكين الأمن السيبراني في الجامعات ، ومنع الهجمات المعتادة.

(Automated Penetration Testing- HackSeal. 2021,p.6)

وقد قام فريق من الباحثين بجامعة وطنية في استراليا بتنفيذ هذا النوع من الكشف الآلي في بيئة باستخدام جهاز البرمجة القابل للبرمجة(FPGAs) ، وذلك باستخدام طريقة التحليل الموحدة لبرمجيات الحماية المتقدمة (Unified Analysis Method for Advanced Security Softwares)وبتكنولوجيا جديدة تسمى بـ ."Test-Based Analysis"

ويعتبر نظام الكشف التلقائي للاختراق من أفضل الطرائق الأساسية في اكتشاف الثغرات الأمنية بالجامعة ، لأنه يمكن الجامعة من الكشف المبكر عن الثغرات الموجودة في بيئة النظام ، وتم إثبات فعاليته في تقييم الحماية السيبرانية بالجامعة ، مما يساعد على تعزيز الأمان السيبراني وتجنب الهجمات والاختراقات. (Unified Testing Methodology for Security Vulnerability Analysis, 2019, p.7)

كما يقصد بنظام الكشف التلقائي للاختراق بأنه : عملية فحص أمنية تستخدم لتحديد ثغرات الأمان الموجودة في نظام معين، ويتم استخدام هذه الأساليب بشكل واسع في مجال الأمن السيبراني، وهي تهدف إلى تحديد وإغلاق الثغرات التي يمكن استغلالها من قبل مهاجمين محتملين. وتعد الجامعة الوطنية باستراليا من الجامعات الرائدة في مجال توظيف الأنظمة الأمنية للذكاء الاصطناعي في تمكين الأمن السيبراني، والتي من أهمها نظام الكشف التلقائي للاختراق

وتقوم الجامعة الوطنية باستراليا بتوظيف نظام الكشف التلقائي للاختراق من خلال ثلاث خطوات على النحو التالي :

أ- **شبكات الاختراق الوهمية : "Honeypots"** وهي شبكات وهمية تم إنشاءها لجذب المهاجمين. تقوم الجامعة باستخدام هذه الشبكات لجمع معلومات حول الهجمات المحتملة والضارة، وتحديد نقاط الضعف والثغرات الموجودة في نظام الأمان(Hu, W. and Tan, C.C. ,2015..,p.8)

ب- **الاختبار التلقائي للاختراق** : "Automated Penetration Testing" وهي عملية فحص تستخدم أدوات وبرامج متخصصة للكشف عن ثغرات الأمان. يتم استخدام هذه الأدوات لتحديد الثغرات الموجودة في النظام وتصحيحها وإغلاقها.

التعرف على الهجمات : "Intrusion Detection" وهي عملية مراقبة المناطق الحساسة في النظام للكشف عن أي هجوم محتمل. يتم استخدام أنظمة متخصصة وبرامج للتعرف على الهجمات والتحذير منها ، وتقوم الجامعة الوطنية باستراليا من خلال هذه الخطوات بتصحيح الثغرات في نظام الأمان ومنع هجمات القراصنة. ويمكن تطوير هذه الأساليب باستمرار لجعل النظام أكثر أماناً وسلاسة،ومن ثم يتم استخدام نظام الكشف التلقائي للاختراق كأحد أهم الأنظمة الأمنية للذكاء الاصطناعي في تمكين الأمن السيبراني بالجامعة . (Feng, Y., Shi, Q. and Zhang, Y., 2020,pp.5-6).

٢- نظام الجدار الناري المتقدم بالجامعات (Next Generation Fire Walls (NGFW:

يعد نظام الجدار الناري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي والتي تساهم في تمكين الأمن السيبراني بالجامعة، وذلك من خلال استخدامه لحماية الشبكات من الهجمات الخارجية والداخلية، ويتم ذلك عن طريق حجز كافة المعلومات الخارجية التي تستخدم لغرض الحصول على معلومات الشبكات ، ويتم تغيير تطبيقات حجب الاتصالات والبرمجيات الحماية ، مما يجعلها أكثر قابلية للتطبيق على مستوى المؤسسة الواسعة ويحمي موارد الشبكة، من الإتاحة غير المقننة .

ويشار لنظام الجدار الناري المتقدم علي أنه : عملية أمنية خاصة بالإنترنت ، ويتم استخدامه لحماية الشبكات المحلية والسيرفيرات من الهجمات الخبيثة ، وتجدر الإشارة إلى أن الجامعة الوطنية باستراليا تحتوي على قسم للأمن السيبراني ، ومن أهم مهام هذا القسم هو تدريب الموظفين والطلاب حول آليات الأمن السيبراني ، ونظام الجدار الناري المتقدم للشبكات، وكل ذلك بهدف تمكين الأمن السيبراني والحفاظ على سرية المعلومات.

(Australian Computer Emergency Response Team, 2021,pp.99-100)

ويعد نظام الجدار الناري المتقدم من أفضل الأنظمة الأمنية للذكاء الاصطناعي المستخدمة لحماية الجامعة الوطنية باستراليا من الهجمات السيبرانية والحفاظ على أمانها ، وتعد الجامعة الوطنية باستراليا واحدة من الجامعات الرائدة في مجال تمكين الأمن السيبراني، حيث تكرس الجامعة جهودها لتطوير أساليب عمل نظام الجدار الناري المتقدم والأمن السيبراني(Al- . Mayadhmi, M. S., & Al-Qudsi, H. A, 2021,pp.60-61)

وتجدر الإشارة إلي أن تطوير أساليب عمل نظام الجدار الناري المتقدم ذات الكفاءة العالية ، من خلال تحسين التقنيات المستخدمة وتطوير نظم معقدة للكشف عن الهجمات السيبرانية والحافظ على سلامة البيانات ، كما تهدف الجامعة إلى توفير حلول الأمن السيبراني الشاملة والتي يمكن أن توفر حماية كاملة للشبكات ضد أنواع مختلفة من الهجمات الإلكترونية، بدءًا من الهجمات الموجهة بالبريد الإلكتروني والهجمات السيبرانية المتقدمة المستهدفة للأجهزة والشبكات وحتى الهجمات السيبرانية الجماعية ، لذلك يعد نظام الجدار الناري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني .(pp.7-8, . (National University of Australia,2022

وتقوم الجامعة الوطنية باستراليا باستخدام نظام الجدار الناري المتقدم من خلال العديد من الخطوات والتي من أهمها على النحو التالي :

أ- الفلترة

ب- تصفية النطاقات

ج- حجب المواقع الخطرة

د- أساليب الكشف عن الاختراق

هـ - حجب البريد الإلكتروني غير المرغوب فيه

مما سبق يتضح أن نظام الجدار الناري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعة الوطنية بأستراليا .

٣- الأمن السحابي Cloud Security:

يعد الأمن السحابي أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني ، حيث يمكن الأمن السحابي الجامعات من الاستفادة من المصادر الرقمية والبيانات الحساسة بطريقة آمنة ومحمية.

(N. Alshammari, M. Kim, M. A. Al-Khasawneh and A. Al-Faries, 2018, pp.50-51)

ويشار لمفهوم الأمن السحابي علي أنه : عملية تستهدف تخزين والوصول إلى البيانات عن طريق الإنترنت في مختلف الأماكن في العالم ، ويعتمد النظام على مشاركة الموارد والبنية التحتية للحوسبة بشكل مشترك في بيئة مشاركة ومرنة مع شركة خارجية تقوم

بإدارة البنية التحتية وحماية البيانات. وتقوم الجامعة الوطنية باستراليا باستخدام نظام الأمن السحابي لحماية المعلومات المهمة والبيانات الدقيقة ، وتقوم الجامعة بتنفيذ سياسات وإجراءات الأمان للحفاظ على سلامة البيانات والمعلومات حتى في حالات الكوارث(X. Chen and B. Mao, 2014, pp. 364-365)

تتضمن الأدوات الأساسية التي تستخدمها الجامعة الوطنية الأمن السحابي عددًا من التقنيات والمنهجيات العلمية لتوفير الحماية والأمان في البيئات السحابية، وتقوم الجامعة الوطنية باستراليا باستخدام الأمن السحابي من خلال العديد من الخطوات والتي من أهمها على النحو التالي :

أ- **أمان محرك البحث :** يتم استخدام التشفير الموحد لحماية الاتصالات والبيانات المتاحة عبر شبكة الإنترنت.

ب- **إدارة الهوية:** يتم استخدام التحقق من الهوية في الوصول إلى النظام السحابي باستخدام المصادقة الثنائية.

ج- **الحماية من البرمجيات الخبيثة:** يتم استخدام برامج مضادات الفيروسات لحماية النظام السحابي.

د- **المراقبة والتحليل:** يتم استخدام نظام المراقبة للكشف عن أي نشاط غير مشروع.

كما يساهم نظام الأمن السحابي في الجامعة الوطنية باستراليا بإتاحة مستوى جيد من الحماية في الوصول إلى البيانات وفعالية أعلى للأنظمة الرقمية المتعلقة بالجامعة ويتيح ذلك تحقيق الكفاءة في العمل وسرعة البيانات والمعلومات.

وتجدر الإشارة إلي أن نظام الأمن السحابي يساهم في عملية التحول بالجامعة الوطنية باستراليا نحو الأمام في تكنولوجيا المعلومات والتوجه نحو المعلوماتية والحماية السحابية. ويشكل هذا النظام خطوة مهمة لتمكين الأمن السيبراني ، والحماية من جرائم القرصنة الإلكترونية وسرقة البيانات. (A. Ghorbani, M. A. Alazab, R. Acarman and M. Hayes, 2019, pp. 3-4)

وتجدر الإشارة إلي مميزات الأمن السحابي المتعددة ، والتي من أهمها توفير سعة تخزين كبيرة والتي يمكن للمستخدمين استخدامها لحفظ الملفات الخاصة بهم، كما يمكن للجهات المختصة في الشركات والجامعات استخدام الحوسبة السحابية لتوزيع الخدمات بشكل أكثر كفاءة وأماناً ، وتعد الجامعة الوطنية بأستراليا أحد أهم الجامعات التي تقوم بتنفيذ ذلك (Mirza, A. M., & Abbas, H. 2021, pp. 70-71). وتقوم الجامعة الوطنية بأستراليا بتوفير خدمات الحوسبة السحابية للطلاب وأعضاء الهيئة التدريسية والإدارية، وتنتقل كافة سياسات إدارة تلك الخدمات إلى موقع المستخدم بشكل آمن للغاية. وتتضمن هذه الخدمات جميع النصائح والتوجيهات التي تمكن المستخدم من تحسين الأمن السحابي للمعلومات الخاصة به، وكذلك الحصول على التحديثات المستمرة للنظام(Alfandi, O. O., & Alhaboby, Z. I. ,2019, p. 30) .

ويعد نظام الأمن السحابي في الجامعة الوطنية بأستراليا من الأنظمة الأكثر فعالية بفضل تقديم هذه الخدمات، والتي تعتمد بشكل كبير على تقنيات التشفير بالإضافة إلى حماية البرامج ضد الهجمات الإلكترونية. وهذا يسمح للمستخدمين بالاستفادة من الخدمات السحابية مع الحفاظ على البيانات آمنة مما يساهم في تمكين الأمن السيبراني بالجامعة . (Mohanty, S., & Chaki, R. 2018, p. 53)

٤- نظام التعرف علي السلوك غير العاديUser and Entity Behavior Analytics (UEBA):

يعد نظام التعرف علي السلوك غير العادي أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعة الوطنية باستراليا، وخاصة بعد تزايد حوادث الاختراق السيبرانية بشكل متزايد في الأونة الأخيرة، ولا سيما في المؤسسات الأكاديمية ، وكجزء من استراتيجية الأمن السيبراني، تقوم الجامعات بتحديد سلوكيات الطلاب والعاملين في الجامعة لتحليل المخاطر المتعلقة بالأمن السيبراني وتمكين الأمن السيبراني على نحو أكثر كفاءة وفعالية. (D. Whitty and P. O'Shea, 2018,p.1199). من خلال التعلم الآلي لتحليل تجميعات بيانات المستخدمين في النظام، من خلال تحديد نماذج السلوك العادية وغير العادية.(A. Saxena, S. Raj and N. Agrawal,2016,p50)

ويعتمد هذا النظام على تقنيات تحليل البيانات والتعلم الآلي، لتحليل المؤشرات السلوكية غير العادية والمتعلقة بالمستخدمين المشتبه فيهم وتقييم مخاطرهم السلوكية. وتعتمد طريقة تعريف ملامح السلوك على تحليل السجلات الموجودة في قواعد البيانات الموجودة في النظام، واستخدام تقنيات تحليل البيانات لتحليل النماذج المتعلقة بالسلوك غير العادي(A. Alattas, 2018,p.166)..

وتقوم الجامعة الوطنية باستراليا باستخدام نظام التعرف علي السلوك غير العادي من خلال العديد من الخطوات والتي من أهمها علي النحو التالي :

أ- **تأثير التقنيات المتقدمة:** يمكن استخدام نظم التحليل المتقدمة للتعرف على أي تحركات غير طبيعية داخل الشبكات والأنظمة الحيوية للجامعة.

ب- **تشكيل فرق الأمن:** يجب تعيين فرق أمنية متخصصة يتابعون عن كثب كل الأنشطة التي تحدث داخل الجامعة والتي يمكن أن تشكل خطورة على سلامة المعلومات الحساسة.

ج- **المراقبة الدورية:** يجب على الجامعة المراقبة الدورية لجميع أنظمة الحاسوب والشبكات والتأكد من سلامتها وعدم تعرضها لأي هجمات سيبرانية(Dumitru, G. C., Ghiba, R. C., & Blaj, M. A. ,2017p.525) .

د- **تحديث برامج الحماية:** تقوم الجامعة بتحديث نظام الحماية باستمرار لتوفير حماية أمنية مستمرة من الهجمات السيبرانية. (Hashim, H., Kasim, N. F. M., Ibrahim, R., & Rahman, S. A. ,2020, P. 1529)

ه- **التدريب والتوعية:** تقوم الجامعة بتوعية الطلاب والموظفين حول أهمية الأمن السيبراني وكيفية **تفادي الخروقات الأمنية.**

و- **التزام الجامعة بالتشريعات الأمنية:** تلتزم الجامعة بالتشريعات الأمنية والتي تسهم في تحسين السلامة الإلكترونية للجامعة.(Watts, T., & Hare, R. (2019,p.10) .

٥- نظام الإدارة التلقائية للأمن : Automated Security Management(ASM)

يعد نظام الإدارة التلقائية للأمن أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني، حيث تركز الجامعة الوطنية باستراليا على ثلاثة مفاهيم أساسية لتمكين الأمن السيبراني: الوعي الأمني للأفراد، وفهم الأسس المتعلقة بالموثوقية وحدود الحماية، والابتكار في مناهج التدريب ومراقبة تلك المناهج، خاصة بعد تزايد عدد الهجمات السيبرانية على المؤسسات والمنظمات الحكومية والشركات الخاصة. (Kankanamge, T. W., & Warren, M. ,2018,p. 740) وبالتالي فإن الجامعة الوطنية باستراليا تأخذ عدة إجراءات لتمكين الأمن السيبراني وضمان سلامة البيانات والمعلومات بها ويعد تطبيق نظام الإدارة التلقائية للأمن من أهم النظم الفعالة التي تستخدم حالياً لتحقيق أعلى مستوى من الأمن السيبراني.

وتقوم الجامعة الوطنية باستراليا باستخدام نظام الإدارة التلقائية للأمن من خلال العديد من الخطوات والتي من أهمها على النحو التالي :

تقييم المخاطر: حيث يقوم فريق الأمن بتحديد الأوجه الضعيفة في النظام وتحديد مدى التأثير الذي يمكن أن يحدث.(Hu, Q., Dinev, T., Hart, P., & Cooke, D.,2012,650**).**

الحماية: تشمل هذه المرحلة توفير الأدوات اللازمة للأمان السيبراني، مثل حماية البيانات والإصدارات الخاصة بالبرمجيات.

الكشف: يشمل هذا الجانب عملية المراقبة المستمرة لتحديد وكشف العمليات غير المرغوبة في النظام .(Wang, X., Tsai, S. B., & Lee, C.,2016,30).

التعرف على المخاطر :يتطلب إدارة الأمن التلقائي التحقق من النظم باستمرار، والتحقق من وجود أي ثغرات في الأمن. ويعتمد ذلك على تحديد المخاطر، وتخطيط الاستجابة السريعة على الفور إذا تم الكشف عن أي اختراق محتمل.(Australian Cyber Security Centre ,2018,pp.34-35)

التعلم الآلي:تستخدم الجامعة تقنيات التعلم الآلي لتحليل البيانات وتحديد الشكل الأمثل لعملية الأمن السيبراني. ويتفق الخبراء على أن استخدام التعلم الآلي مع تقنيات الذكاء الاصطناعي يمكن أن يوفر الكثير من الوقت والجهد.

التحكم السريع :تعمل أنظمة الأمن التلقائية على العمل على إجراء تحليل البيانات المتعلقة بنشاط الشبكة، ومع ملاحظة أي اختلالات، يمكن للنظام التفاعل بسرعة وإطلاق إجراءات الحماية المناسبة للتعامل مع الاختراق.

إنشاء ثقافة الأمن السيبراني :تهدف الجامعة إلى توفير برامج وتدريبات في مجال الأمن السيبراني والتوعية بها، حتى يتمكن المستخدمون في الجامعة من التعرف على المخاطر السيبرانية والمشاكل المتعلقة بالأمان.

الرصد والتحليل :يتم تفحص الشبكات باستمرار ودقة لإجراء التحليل والكشف المبكر عن أي تهديد أمني.

إجراءات الحماية الوقائية:تضم هذه الإجراءات تشغيل نظم الإنذار المبكر في حالة الهجوم السيبراني، وفي بعض الاختراقات يتم اتخاذ الإجراءات اللازمة بسرعة لإيقاف الهجوم.

التشفير : يتم تشفير المعلومات الحساسة والبيانات لجعلها غير قابلة للوصول لمن تخترق الأمن.(Australian Cyber Security Centre ,2021,pp.22-23) ، وتجدر الإشارة إلي أن الإدارة التلقائية للأمن تساهم في توفير بيئة آمنة للأنظمة الإلكترونية، ورصد المشكلات والتحديات المختلفة التي تواجهها الجامعة في هذا المجال. وقد تمتلك الجامعة قاعدة بيانات متقدمة وموثوقة تساعد في إدارة الأمن السيبراني في الجامعة، وتتخذ الجامعة إجراءات حماية خاصة لتمكين الأمن السيبراني بها .

مما سبق يتضح أن نظام الإدارة التلقائية للأمن يعد أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعة الوطنية باستراليا .

٦- نظام الأمن الأداري المتقدم (AAS) :Advanced Administrative Security:

يعد نظام الأمن الأداري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني حيث يعتبر الأمن السيبراني من القضايا المهمة في عصرنا الحالي، حيث تزداد الهجمات الإلكترونية والاختراقات المختلفة على الجامعات (Cybersecurity at Universities, 2020,pp.22-23)

لذا تقوم الجامعة الوطنية باستراليا بتطبيق نظام الأمن الإداري المتقدم وتمكين الأمن السيبراني للحد من هذه الهجمات والحفاظ على سلامة بيانات الطلاب بالجامعة الوطنية باستراليا. تبين أن الجامعة الوطنية في أستراليا اتخذت العديد من الإجراءات والسياسات لتطبيق أساليب الأمن الإداري المتقدم وتمكين الأمن السيبراني. فقد تم تجهيز الشبكة الداخلية والخارجية للجامعة بأحدث التقنيات الأمنية، وتم تدريب الموظفين والطلاب على كيفية التعامل مع الهجمات الإلكترونية والوقاية منها. كما تم إنشاء فريق الأمن السيبراني في الجامعة للتعامل مع الهجمات الإلكترونية والتحقق من سلامة بيانات الطلاب والموظفين، بالإضافة إلى توفير برامج الحماية من الفيروسات والبرامج الخبيثة للكمبيوترات(Cybersecurity in Australian Universities,2018,pp.33-34) .

وتقوم الجامعة الوطنية باستراليا باستخدام نظام الأمن الأداري المتقدم من خلال العديد من الخطوات والتي من أهمها على النحو التالي :

أ- إنشاء فرق خاصة بالأمن السيبراني والتي تساهم في رصد التهديدات الأمنية والتصدي لها. (الجامعة الوطنية أستراليا: تقرير الأمن السيبراني،٢٠٢١م، ص ص ٢٢-٢٣)

ب- تزويد أعضاء الجامعة بأحدث تقنيات الحماية السيبرانية والتي تشمل الحماية من الفيروسات والبرامج الخبيثة والاختراقات الإلكترونية.

ج- عقد العديد من الورشات التدريبية والدورات المتخصصة في مجال الأمن السيبراني والذي يهدف إلى تحسين القدرات والمهارات للأفراد المسؤولين عن الأمن السيبراني في الجامعة.(اللجنة الأمنية للجامعة الوطنية أستراليا ، ٢٠٢٠م ، ص ص ١٢-١٣)

د- اعتماد أحدث الأدوات الإلكترونية المتطورة التي تساعد على تحليل البيانات ورصد النشاطات الغير المشروعة في الشبكات. (مورجان، ب ،٢٠٢١م ، ص ص ٦-٧)

خامسا : أهم القوي والعوامل الثقافية المؤثرة علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا :

هنالك العديد من القوي والعوامل الثقافية المؤثرة علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا ، والتي من أهمها علي النحو التالي :

أولا : العوامل الجغرافية:

تعد العوامل الجغرافية أحد أهم العوامل التي لها أثر أكبر علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا ، حيث تعد أستراليا دولة اتحادية فدرالية يرأسها ملك المملكة المتحدة عاصمتها كانبرة ، وتقع بين خطي العرض ١٠ درجات و٤٠ درجة جنوب خط الاستواء، وبين خطي الطول ١١٣ درجة و١٥٣ درجة شرق غرينتش. وقد اشتق اسمها من كلمة «أوستراليس Australis «اللاتينية أي الجنوب. وتضم جغرافية أستراليا تنوعاً واسعاً من مناطق الجغرافيا الحيوية بالرغم من كونها أصغر قارة في العالم، ولكنها سادس أكبر بلد في العالم. سكان أستراليا يتركزون على طول السواحل الشرقية والجنوبية الشرقية. وتتباين جغرافيا البلد بشدة، إذ تتراوح من الجبال المكللة بالثلوج في الألب الأسترالية وتزمانيا إلى صحاري شاسعة، وغابات مدارية وباردة(Map of Australia ,2023,pp.1-3) . وتتميز استراليا بإمتلاكها ثروة من المعارف الفنية والعلمية في مجال الذكاء الاصطناعي. ومع ذلك، فإن التأثير الجغرافي لأستراليا والتي إنعكست علي إتاحة العناصر الأساسية التي تدعم الذكاء الاصطناعي، بما في ذلك البيانات والكفاءات الفنية، ويرجع هذا إلي تأثير العوامل الجغرافية (Australian Computer Society,2018,pp.2-3)

وقد إنعكس أثر العوامل الجغرافية علي تمكين الأمن السيبراني في ضوء الذكاء الاصطناعي من خلال توسيع المعرفة سعي استراليا الدائم نحو التطور التكنولوجي والتقني خاصة في مجال الذكاء الاصطناعي على المستوى الأكاديمي في الجامعات الأسترالية. (عبد الله الخالدي، ونورة العضيبي ، ٢٠١٨م ، ص ٥٣٣). حيث ساعدت مساحة استراليا في تطوير تكنولوجيا الذكاء الاصطناعي، ونمو المعارف والتقنيات في هذا المجال. وتضم مراكز البحث والتطوير أكاديميين وخبراء في الذكاء الاصطناعي الذين يسعون إلى تطوير هذه التكنولوجيا بما يلبي الحاجات المحلية والدولية. وعلاوة على ذلك، يتم توظيف الأنظمة الأمنية للذكاء الاصطناعي في تمكين الأمن السيبراني باستراليا (Commonwealth of Australia,2019,p.9) .

ثانيا : العوامل الاقتصادية :

تعد العوامل الاقتصادية أحد أهم العوامل التي لها أثر أكبر علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا ، حيث تعتبر التكنولوجيا والذكاء الاصطناعي من أهم القطاعات التي تمثل الركيزة الأساسية للاقتصاد العالمي. وقد أدى التزايد المستمر في استخدام التكنولوجيا والتطور السريع الذي حدث في الذكاء الاصطناعي إلى ظهور جديدة لتمكين الأمن السيبراني ، وفي سبيل مواكبة هذا التطور، قامت العديد من الجامعات حول العالم بإطلاق أنظمة أمنية جديدة للذكاء الاصطناعي والتي تساهم في تمكين الأمن السيبراني(Lo, K., Chandra, A. and Harris, S., 2021, pp.3-4) . حيث يعد استخدام التكنولوجيا الحديثة وخاصة الأنظمة الأمنية للذكاء الاصطناعي أحد الاتجاهات الرئيسية في مجال التعليم والبحث العلمي ، وتعتبر الجامعة الوطنية بأستراليا من أبرز الجامعات التي تتبنى الأنظمة الأمنية للذكاء الاصطناعي وتوظفه بهدف تمكين الأمن السيبراني . وتجدر الإشارة إلي أن العوامل الاقتصادية تؤثر على استخدام التكنولوجيا والذكاء الاصطناعي في الجامعة الوطنية باستراليا ، ويؤثر تمكين الأمن السيبراني علي الاقتصاد والأمن الوطني والدولي ، ولاسيما في ظل التهديدات الإلكترونية المتزايدة

في العالم ، مما دفع استراليا إلي زيادة الاستثمارات في الذكاء الاصطناعي بهدف تمكين الأمن السيبراني بالجامعات الأسترالية) National Cyber Security Adviser.,2020,pp.4-5)

القسم الرابع للدراسة : تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي في جامعة طوكيو باليابان : دراسة وصفية تحليلية.

يتزايد اعتمادنا على التكنولوجيا والإنترنت في حياتنا اليومية، لهذا يُعتبر الأمن السيبراني أمرًا هامًا ولابد من الحرص الشديد على تأمينه، إذ أن التهديدات السيبرانية تزداد يومًا بعد يوم. وبهدف تعزيز الأمن السيبراني في جامعة طوكيو باليابان، تم تبني تقنيات الذكاء الاصطناعي التي تساعد على حماية بيانات المؤسسة، وتحديد الهجمات السيبرانية ومنعها Asghar, S. H., & Rehman, (H. U.,2019, 39-40)

ويُعد الذكاء الاصطناعي من أهم التقنيات المتاحة اليوم ويمكن استخدامه في العديد من المجالات، ومن بين تلك المجالات مجال الأمن السيبراني. فالذكاء الاصطناعي يستطيع تحديد السلوكيات الغريبة والمشكوك فيها التي تتم في الشبكات والحاسوبات، ويساعد على الكشف عن الهجمات السيبرانية ومنعها قبل حصولها في جامعة طوكيو، تم تحقيق ذلك بالتعاون بين الباحثين والخبراء في مجالات الأمن السيبراني والذكاء الاصطناعي. وتم تعيين خبراء متخصصين في هذا المجال للعمل على إنشاء نظام الحماية السيبرانية الذي يعتمد على تقنيات الذكاء الاصطناعي.

(Liu, J., Shu, T., Yang, W., & Ding, Y. ,2018,pp.89-90)

ويعتمد نظام الحماية السيبرانية في جامعة طوكيو على استخدام تقنيات الذكاء الاصطناعي مثل الشبكات العصبونية الاصطناعية والتعلم الآلي وتقنيات التصنيف والرصد. ويتيح نظام الحماية السيبرانية الذي يعتمد على التقنيات الذكية، الكشف عن الهجمات السيبرانية ومنعها دون إبطاء أداء النظام. ولتحقيق هذا الهدف، تم اختيار البنية التحتية للحصول على البيانات المطلوبة لتدريب النظام، وتم جمع البيانات اللازمة لتدريب الشبكات العصبونية الاصطناعية الموجودة في نظام الحماية السيبرانية

ويمكن القول بأنه تم بناء نظام الحماية السيبرانية بجامعة طوكيو بنجاح، وعززت التقنيات الذكية المستخدمة فيه الأمن المعلوماتي على المستوى الحكومي. فقد حصد نظام الحماية السيبرانية الذي يعتمد على التقنيات الذكية جائزة الأمن المعلوماتي اليابانية في عام ٢٠٢٠، ويُعتبر ذلك إنجازًا كبيرًا لجامعة طوكيو(Tshilenge, D. M., Abbas, H., Hu, J., & Hao, Q., 2020,pp.8-9)

ولقد استطاعت جامعة طوكيو باليابان أن تصبح ذات خبرة واسعة في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي ، وهذا ما سيتم تناوله على النحو التالي :

أولاً: مدخل تاريخي عن جامعة طوكيو باليابان :

تأسست جامعة طوكيو عام ١٨٧٧م ، وتعتبر جامعة طوكيو واحدة من أبرز الجامعات على مستوى العالم، وتعد الجامعة رائدة في العديد من المجالات الأكاديمية مثل العلوم والهندسة والطب والاقتصاد والقانون والعلوم الاجتماعية والإنسانية. About the (University of Tokyo,2023,pp.3-4)

تتمتع جامعة طوكيو بسمعة عالمية، حيث أنها تحتل مركز القيادة في اليابان وفي العالم أيضًا، وتعتبر من أفضل الجامعات في العالم كما ترتبط بتاريخ وثقافة اليابان. تضم الجامعة ١٠ كليات رئيسية تشمل على ٣٠ قسمًا، وتوفر حوالي ٢٧,٠٠٠ فرصة دراسية لشتى أنحاء العالم مع أفضل المرافق الدراسية، والمختبرات، والمنشآت الرياضية

(University of Tokyo rankings, QS Top Universities,2023,pp.6-7)

تُعد جامعة طوكيو مركزًا للأبحاث العلمية الرائدة في اليابان، حيث إنها مرتبطة بالعديد من المشاريع الوطنية والمعاهد البحثية، كما أنها الجامعة الرائدة عالميًا في مجال الصحة والتكنولوجيا، إضافة إلى اهتمامها بمواكبة التطورات الحديثة والتقنيات الحديثة.

وتفتخر جامعة طوكيو بخريجيها الذين يتمتعون بمهارات ومعرفة عميقة في مختلف المجالات، ولهذا السبب فإن حملة الدراسة في جامعة طوكيو تعتبر خطوة هامة في بناء مستقبل مهني ناجح.

(The University of Tokyo, Times Higher Education,2023,pp.3-4). كما تعد جامعة طوكيو رائدة في التعليم العالي والبحث العلمي. وتؤدي دورا حيويا في تطوير الذكاء الاصطناعي من خلال العلوم الحاسوبية والرياضيات والاحصاء وقد وضعت الجامعة نصب عينيها توظيف طاقات الذكاء الاصطناعي. (Academia.edu., 2021,pp.8-9)

تعد جامعة طوكيو قائدة في تطوير الذكاء الاصطناعي وتعزيز الأمن السيبراني في اليابان والعالم بأسره. وقدمت الجامعة اليابانية مؤخرا خطة جديدة تهدف إلى تسريع تحقيق التقدم في تقنيات الذكاء الاصطناعي وتخفيض التسريبات الإلكترونية. وتقوم الجامعة أيضا بتحديث مسارها التعليمي والبحثي لمواكبة التغيرات المتسارعة في العالم الحالي. وتوفر الجامعة للطلاب والأساتذة مرافق وادي من الابتكار والتفوق الابداعي والتنافس الصناعي، مما يعزز التعاون بين الجامعة والشركات المحلية والدولية .AI news) (89-2021,pp.88, تهدف جامعة طوكيو إلى تطوير التقنيات وانتقالها من نموذج البحوث والمعاملة الصغيرة إلى مجال الصناعة والخدمات والبيئة الاقتصادية..(Cybersecurity Ventures,2021,pp.5-6). وبالتعاون مع الصناعة اليابانية والعالمية، يعمل فريق البحث في جامعة طوكيو على تطوير تقنيات الذكاء الاصطناعي والأمن السيبراني لتلبية احتياجات المجتمعات بشكل فعال. (Hindawi. ,2021,pp.4-5). وهذا يساعد على زيادة الابتكار وخلق فرص عمل جديدة، وتنمية اقتصادية وتطور المجتمع (Collective innovation. ,2021,pp.3-4).

وتتعدد مجالات تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بجامعة طوكيو، حيث يعد الأمن السيبراني اليوم أحد أهم القضايا العالمية ويشكل تهديدا خطيرا للشركات والحكومات والأفراد على حد سواء. ويقوم فريق أبحاث الأمن السيبراني في جامعة طوكيو بدراسة التهديدات الإلكترونية وتوفير الحلول المتقدمة والرؤى التنبؤية للأمن السيبراني. وتركز جامعة طوكيو على الأمن السيبراني في مجالات عديدة، منها تحسين دعم الأمن في المنتجات الإلكترونية الذكية: يشدد فريق الأبحاث في جامعة طوكيو على أهمية تطوير التقنيات الجديدة التي يمكنها توفير درجات أكبر من الأمان والحماية في المنتجات الإلكترونية الذكية، بالإضافة إلي حماية النظم الحسابية الصحية: تعد النظم الحسابية الصحية هدفا للكثير من هجمات القراصنة عبر الإنترنت، وتعد جامعة طوكيو من المؤسسات الرائدة في العالم في حماية هذه النظم وحماية سرية المعلومات الطبية، علاوة علي تعزيز الأمن في أثناء العمليات الآلية: حيث تعمل جامعة طوكيو على تعزيز الأمن في المجال الصناعي والمفتوح وتعزيز تقنيات الأمان والوثوقية في العمليات الآلية، علاوة علي تطوير تقنيات البيانات الحكومية: حيث يوجد اليوم زيادة تشغيل أنظمة الحواسيب الكمية لتحل المشاكل المعقدة، وبالتالي تطوير تقنيات الأمن المتقدمة لظاهرة "التنصت" على المعلومات الحيوية الخاصة بهذه الأنظمة وحماية الخصوصية في المستقبل.

ثانياً: آليات تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بجامعة طوكيو باليابان

تتعدد آليات تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بجامعة طوكيو باليابان أهمها علي النحو التالي :

١- **تحليل البيانات:** تتيح التقنيات المتقدمة المتاحة في الذكاء الاصطناعي تحليل كميات كبيرة من البيانات بكفاءة ودقة عالية. وتستخدم جامعة طوكيو تقنيات الذكاء الاصطناعي في التحليل الكمي للبيانات الكبيرة في المجالات المختلفة مثل الطب وعلوم الحاسوب .

٢- **-تطوير البرمجيات:** يستخدم الذكاء الاصطناعي في صناعة البرمجيات من أجل تحسين تصميم البرمجيات وبنائها بشكل أفضل وأسرع. وتنظر جامعة طوكيو إلى إمكانية تطوير برامج الذكاء الاصطناعي للتفاعل مع حواسيب الخوادم والهواتف الذكية.

٣- **تطوير الذكاء الاصطناعي القوي:** يشير الذكاء الاصطناعي القوي إلى تقنيات تستطيع حل المشاكل التي تحتاج إلى تفكير بشري. ويشارك فريق بي دبليو أي ويب زيرو قسم الذكاء الاصطناعي في جامعة طوكيو بنشر ابتكارات الذكاء الاصطناعي القوي بشكل واسع كتصميم الذكاء الاصطناعي بأداء عالي والتصنيف منه إلى بعض التدريس.

٤- **التعلم الآلي:** تستخدم تقنيات الذكاء الاصطناعي المرتبطة بالتعلم الآلي في نطاقات مختلفة، منها الصناعية والطبية والخدمات وسواها. وتنظر جامعة طوكيو إلى إمكانية استخدام التعلم الآلي لتحسين وتبسيط عمليات الإنتاج الصناعي والخدمات المقدمة إن الفريق الذي يترأسه البروفيسور كازويوكي تشيبا، مدير بي دبليو أ يفخر فريق الذكاء الاصطناعي بالعمل الذي يقوم به في تطوير التقنيات الحديثة للذكاء الاصطناعي.

ثالثا: أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بجامعة طوكيو باليابان :

ويمكن تناول ذلك من خلال ما يلي :

١- نظام الكشف التلقائي للاختراق (Intrusion Detection System (IDS:

يعد نظام الكشف التلقائي للاختراق أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني ، وتعد جامعة طوكيو باليابان واحدة من أفضل الجامعات علي مستوي العالم في توظيف نظام الكشف التلقائي للاختراق.

(H. Takeuchi, M. Ohki, Y. Oda, and Y. Watanabe. ,2018,pp.1-2).

ويشار لمفهوم نظام الكشف التلقائي للاختراق علي أنه استخدام تقنيات البرمجة والحوسبة لتحليل الأنظمة وتحديد الثغرات الأمنية التي يمكن استغلالها لاختراق هذه الأنظمة. وفي السنوات الأخيرة، تشهد تلك التقنيات تطورات ملحوظة وتحديثات مستمرة في مختلف أنحاء العالم (M. Okada and T. Miyajima. ,2019,pp.5-6) . واحدة من تلك الأماكن هي جامعة طوكيو في اليابان، والتي تستخدم الأنظمة الأمنية للذكاء الاصطناعي ، وذلك بهدف تمكين الأمن السيبراني (K. Hasegawa, S. Nakayama, and K. Sakurai. ,2019,pp.7-8) .

وتجدر الإشارة إلي أن تطوير "نظام الكشف التلقائي للاختراق" في جامعة طوكيو كان بهدف التغلب على مشكلة الاختراقات الإلكترونية في المؤسسات. بدلاً من الاعتماد على استخدام المراقبين البشريين لتحليل نمط الشبكة والبحث عن علامات تشير إلى وجود هجمات، يستخدم النظام التلقائي تقنية الذكاء الاصطناعي والتعلم الآلي لتحليل بيانات الشبكة والكشف عن أي نمط غير طبيعي. (Y. Matsuda, S. Goto, A. Kakei and H. Sato. ,2019,pp. 907-908)

وتقوم جامعة طوكيو باليابان باستخدام الكشف التلقائي للاختراق من خلال العديد من الخطوات والتي من أهمها على النحو التالي :

أ- جمع بيانات النظام في الوقت الحقيقي كمعلومات الاختراق السابقة ونمط استخدام الشبكة.

ب- تحليل بيانات النظام باستخدام تقنيات التعلم الآلي لتحديد الأنماط غير العادية والتي من المرجح أنها تشير إلى اختراق.

ج- إصدار تقرير يحتوي على تفاصيل الاختراق والرد الذي تم اتخاذه لديمومة النظام.

(Yusuke Saito, 2020,pp.65-66)

وتجدر الإشارة إلي أن نظام الكشف التلقائي للاختراق قد أثبت فعالية كبيرة في جامعة طوكيو ، حيث يمكنه اكتشاف الاختراقات في وقت قصير وبشكل دقيق، ويعمل بشكل تلقائي دون الحاجة لتدخل بشري. يعمل أيضًا كأداة مساعدة لفرق الأمن لتحديد مصادر الاختراقات ومكافحتها(A. Mohamad et al. ,2019, pp. 10555-10556 .)

بالإضافة إلي أن نظام الكشف التلقائي للاختراق بجامعة طوكيو باليابان قد أصبح إضافة قوية للجهود المبذولة لمكافحة الاختراقات الإلكترونية. بالاعتماد على تحليل بيانات الشبكة باستخدام التعلم الألي، يمكن للنظام تحديد الأنماط غير العادية والتي من المرجح أنها تشير إلى وجود هجوم ضار. وبما أن النظام يعمل بشكل تلقائي دون الحاجة لتدخل بشري يزيد من كفاءته. يمكن اعتبار هذا النظام رائدًا في مجال الكشف التلقائي عن الاختراقات الإلكترونية.

(H. Abeer, F. Zohair, and S. Hussam 2020, pp. 93121-93122).

٢- نظام الجدار الناري المتقدم بالجامعات Next Generation Fire Walls (NGFW):

يعد نظام الجدار الناري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي والتي تساهم في تمكين الأمن السيبراني ، وتجدر الإشارة إلي أن جامعة طوكيو اليابانية متخصصة في المجالات التكنولوجية المتقدمة، وتعمل جامعة طوكيو على تطوير نظام الجدار الناري المتقدم وذلك من خلال التعرف الآلي Automatic Recognition على البيانات وفرز البيانات التي تم اكتشافها، وذلك بفضل الخوارزميات الحديثة المستخدمة في هذا النظام(Tokyo University. ,2021,pp.4-5) .

وتعمل جامعة طوكيو على تحليل النماذج الكبيرة لتحديد تصنيفات مختلفة للبيانات، ويتم تحليل البيانات وفرزها بما يتوافق مع تصنيفاتها، وهناك العديد من التفاصيل التي تتميز بسرية تقنية عالية ، تدعم طرق حماية الأمن السيبراني، مثل فيروسات الحماية وحماية البرامج الضارة Malware protection وتنبيهات الأمان، بجانب استخدام خوارزميات التعريف الآلي Automatic Identification algorithmsالمتنوعة، مما يؤمن إضافة أمان على النظام.

(Firewall Security for an enterprise network, 2020,pp.5-7).

وتجدر الإشارة إلى أن جامعة طوكيو باليابان تعد من أهم الجامعات الرائدة في هذا المجال ، حيث تتبع سياسة قوية في استخدام الأنظمة الأمنية للذكاء الاصطناعي والتي تستهدف تمكين الأمن السيبراني بالجامعة ، فضلا عن دور الجامعة في توفير الأدوات اللازمة لدراسة المنشآت السيبرانية، كما تهدف إلى توفير الحلول الفعالة لمواجهة التهديدات المختلفة.

٣- الأمن السحابي Cloud Security:

يعد الأمن السحابي أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني، حيث يتضمن نظام الأمن السحابي جميع الإجراءات والإمكانيات التي تشمل حماية البيانات، والاستجابة للمخاطر والهجمات، وبناء نظام متكامل لحماية الأصول والموارد الرقمية. ومن أجل ضمان أمان وسلامة البيانات الموجودة في السحابة، تعتمد الشركات والمؤسسات في جميع أنحاء العالم على تبني نظام الأمن السحابي.(Murakami, T., & Suga, Y. ,2017,pp. 1428-1429) . ومن بين الجامعات العالمية التي تتميز بنظام أمن سحابي متقدم هي جامعة طوكيو في اليابان. تعد جامعة طوكيو واحدة من أفضل الجامعات في العالم بحسب تصنيفQS ، وهي مشهورة بأبحاثها المتقدمة في مجال الحوسبة وتقنية المعلومات بما في ذلك الأمن السحابي.

وخلال هذا البحث، سنلقي نظرة على أساليب نظام الأمن السحابي بجامعة طوكيو باليابان. بدأت الجامعة في تبني تقنيات الأمان السحابية في وقت مبكر، وقامت بتشكيل فرق خاصة لمتابعة وتحديد الأمن السحابي بجميع أنشطتها. وتشمل استراتيجياتها الأساسية تحديد المخاطر والتهديدات والاستجابة للهجمات بسرعة وفعالية، واستخدام تقنيات متقدمة مثل تقنية الإيقاف المؤقت ومتابعة الوصول لضمان سلامة المعلومات.(Fujiwara, H., & Nakayama, H. ,2016,pp. 41-42) . أيضًا، يتم تشكيل بنية تحتية قوية تتضمن أمن الاتصالات والشبكات والخوادم والأنظمة وقواعد البيانات، بالإضافة إلى استخدام تقنيات متقدمة لتشفير البيانات وتحديد الوصول. ويتم تدريب الموظفين والطلاب بشكل دوري على تحديثات الأمن وتقنيات الحماية (Sato, N., & Seki, H.,2014,pp. 265-274) .

وتجدر الإشارة إلي أن نظام الأمن السحابي بجامعة طوكيو يستند إلى تقنيات وأساليب متقدمة وفرق مختصة وبنية تحتية قوية وتدريب دوري للموظفين والطلاب. وقد أثبتت جامعة طوكيو نجاح نظامها الأمني السحابي من خلال توفير بيئة آمنة لتخزين ومشاركة المعلومات والبيانات. ، وقد ساهم كل هذا في تمكين الأمن السيبراني بها .خاصة مع الانتشار الواسع للتخزين السحابي وتطبيقات الويب، ويعد نظام الأمن السحابي واحد من النظم الرئيسية لإدارات تكنولوجيا المعلومات في العالم. ويُعد تمكين الأمن السيبراني في الجامعات، عامةً، وجامعة طوكيو تحديدًا، هو التحدي الذي تواجهه الجامعات لحماية البيانات الدقيقة والملفات المهمة، ويُعتبر جزءًا أساسيًا من المعيار الدولي للأمن السيبراني. وعندما يتعلق الأمر بالحفاظ على سلامة البيانات وتحقيق الأمن، فإن استخدام نظام الأمن السحابي يُعد حلًا جيدًا، كما أنه يوفر مزيدًا من الأمان للمستخدمين ويقلل من المخاطر الإضافية. وتعتبر

جامعة طوكيو، ذات الشهرة العالمية، من بين الجامعات التي تتبنى هذا النظام وتحرص على تمكين الأمن السيبراني في ضوء الأنظمة الأمنية للذكاء الاصطناعي

ويتم تطبيق نظام الأمن السحابي في جامعة طوكيو بعناية، وذلك لتوفير الحماية من الهجمات المختلفة والنوافذ الزمنية للإصلاحات والتحديثات ومستويات الدخول والاستخدام، وحماية البيانات الدقيقة والتشفير والعمليات الداخلية للأمن، والأمان على الإنترنت.

وتقوم جامعة طوكيو باليابان بتطبيق نظام الأمن السحابي كأحد الأنظمة الأمنية للذكاء الاصطناعي والتي تستهدف تمكين الأمن السيبراني بالجامعة من خلال العديد من الخطوات والتي من أهمها على النحو التالي :

أ- استخدام تقنيات البرمجة العالية والتعلم الآلي لتحليل وتقييم المخاطر السيبرانية.

ب- تطوير نظام تحليل السلوك من خلال المستخدمين وتحديد الخلل المحتمل والتهديدات المرتقبة.

ج- استخدام تقنيات التشفير القوية والحماية الأمنية المتعلقة بالشبكات محركات البحث.

د- تدريب موظفي قسم الأمن السيبراني وتزويدهم بالمهارات والخبرات اللازمة لمكافحة التهديدات المختلفة.

٤- نظام التعرف علي السلوك غير العاديUser and Entity Behavior Analytics (UEBA):

يعد نظام التعرف علي السلوك غير العادي أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بجامعة طوكيو باليابان، ويُعد السلوك غير العادي أحد التهديدات الأمنية المتزايدة على شبكة الإنترنت، حيث يقوم المهاجمون بتنفيذ أنشطتهم الخبيثة من خلال استغلال هذا السلوك وتجنب الكشف عن هويتهم. ولمكافحة هذه التهديدات، تعمل العديد من الجامعات ومؤسسات البحث على تطوير أدوات وتقنيات للكشف عن هذا السلوك وتحليله. وتشتهر جامعة طوكيو في اليابان بأنها تعمل جاهدةً على تطوير طرق للكشف عن السلوك غير العادي وتمكين الأمن السيبراني. وتجدر الإشارة إلي أن جامعة طوكيو قد قامت بتطوير طريقة فعالة للكشف عن السلوك غير العادي وتمكين الأمن السيبراني، وذلك من خلال تحليل السلوك المتعلق بتصفح الإنترنت واستخدام البريد الإلكتروني والشبكات الإجتماعية وغيرها، والتي تسمح بتحديد الأنشطة الخبيثة والتعرف على الجهات العاملة وراء هذه الأنشطة.

واتساقا مع ما سلف بيانه تعمل جامعة طوكيو على استخدام التقنيات الحديثة في مجال التعرف على ملامح السلوك غير العادي لتمكين الأمن السيبراني، حيث تعتمد في ذلك على استخدام الذكاء الاصطناعي والتحليل الإحصائي واستخدام تقنيات تحليل البيانات. وتستخدم الجامعة أيضًا تقنيات التعلم الآلي والشبكات العصبية لتطوير نماذج التنبؤ بالتهديدات السيبرانية.

(D. Christopoulos, I. Tsalamanis, D. Kounelis, N. V. Karadimas and S. A. Karkanis, 2017,pp.22789-22790).

تعمل جامعة طوكيو على تطوير أنظمة مراقبة الشبكات والخوادم، والتي تتيح للمستخدمين تعقب الأنشطة غير المسموح بها والتي يمكن أن تشكل تهديدًا للأمن السيبراني. وتعتمد لجامعة طوكيو على تحليل البيانات وتتبع مجموعة متنوعة من المعلومات الرقمية لتحديد السلوك غير العادي والمتطرف. على سبيل المثال، تستخدم جامعة طوكيو الذكاء الاصطناعي في مجال اكتشاف الاختراقات، يعتمد هذا النظام على تحليل النمط السلوكي للمستخدمين لتحديد اذا كان المستخدم يحاول الوصول إلى مواقع ليست له الصلاحية في الوصول لها. كما يعتمد نظام الذكاء الاصطناعي على تحليل البيانات في الوقت الحقيقي لتحديد الحركات الغير عادية لتصفية الأنشطة المشبوهة.(S. Zhang, X. Zhang, Y. Yang and Y. Liu, 2020, pp. 105-106) .

ويعد نظام التعرف على ملامح السلوك غير العادي يعد من أهم الأنظمة المستخدمة في الوقت الحالي.

٥- نظام الإدارة التلقائية للأمن : Automated Security Management(ASM)

يعد نظام الإدارة التلقائية للأمن أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني ، حيث تولي جامعة طوكيو باليابان اهتمامًا خاصًا بتكنولوجيا الأمن السيبراني وتطويرها، حيث استحدثت العديد من الإجراءات والخطط لتعزيز مستوى الأمان والحماية للبيانات والمعلومات الدقيقة. ومن أبرز ما تم تطبيقه في جامعة طوكيو هو نظام الإدارة التلقائية للأمن وهو

أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني ، والذي يتم إدارته بواسطة فريق متخصص من الخبراء والمتخصصين في مجال الأمن السيبراني. وتتميز هذه المنصة بأنها توفر نظامًا متكاملًا للحماية السيبرانية لجميع الأجهزة والبيانات التي تتعامل معها الجامعة، ما يعزز من مستوى الأمان ويحميها من الجرائم السيبرانية المختلفة. (Izumida, T., & Tokuda, H. 2018,pp. 586-596).

ويؤكد الخبراء المتخصصون في الأمن السيبراني بأن نظام الإدارة التلقائية هذا يعتبر من الحلول الرائدة في مجال الأمان والحماية السيبرانية، ومن ثم تمكين الأمن السيبراني. بالإضافة إلى ذلك، تعتبر جامعة طوكيو باليابان من الجامعات الرائدة في مجال البحث والتطوير في مجال الأمن السيبراني، حيث توفر الجامعة برامج متخصصة في هذا المجال، إلى جانب العديد من الدورات التدريبية وورش العمل والندوات التي تستضيفها الجامعة لتعزيز وتحفيز التطوير في مجال الأمن السيبراني بهدف تمكين الأمن السيبراني . (Onuma, Y., & Akiyama, H. 2019,p.811). وتجدر الإشارة إلي أن جامعة طوكيو باليابان تعد من الجامعات الرائدة في مجال الأمن السيبراني، حيث توفر نظامًا متكاملاً للحماية السيبرانية لجميع الأجهزة والبيانات التي تتعامل معها الجامعة. ومن مميزات هذا النظام هو إدارته التلقائية بواسطة فريق متخصص من الخبراء في مجال الأمن السيبراني، مما يوفر أعلى مستوى من الأمان والحماية، إلى جانب العديد من برامج التعليم والتدريبات التي توفرها الجامعة لتحفيز التطوير في مجال الأمن السيبراني.

(Taniguchi, M., Inoshita, Y., Eguchi, H., & Yamadai, M.,2017,pp. 503-504)..

في ظل الاتجاه العالمي المتزايد نحو التحول الرقمي والاعتماد على التكنولوجيا، أصبح تمكين الأمن السيبراني قضية من أهم القضايا التي تواجه العالم بأسره. وتعتبر جامعة طوكيو باليابان من الجامعات الرائدة في العالم في مجال الرقمنة والتحول الرقمي، ولذلك فإن الأمان والحماية السيبرانية هما أمور بالغة الأهمية للجامعة.

(Managing Cybersecurity Risks, 2021, pp.33-34)

وقد استطاعت جامعة طوكيو باليابان تمكين الأمن السيبراني في ضوء نظام الإدارة التلقائية للأمن ، والذي يعد أحد أهم الأنظمة الأمنية للذكاء الاصطناعي ، والتي تساهم في تمكين الأمن السيبراني بالجامعة لذا قامت جامعة طوكيو بالعديد من الخطوات أهمها على النحو التالي :

أ- تم إنشاء منظومة متكاملة للأمن السيبراني تشمل مراقبة الشبكات وتحليل البيانات وتطبيق قرارات الأمن المتقدمة. وعلاوة على ذلك.

ب- تم إنشاء قواعد بيانات محدثة بشكل دوري للحفاظ على مستوى عالٍ من الحماية والأمان.

ج- استخدام التكنولوجيا والذكاء الاصطناعي لتحليل البيانات وتطبيق القرارات الأمنية المناسبة، مما يساعد على الحفاظ على مستوى عالٍ من الأمن السيبراني.

د- تحسين مستوى حمايتها الإلكترونية، وتعززت قدرتها على التعامل مع الهجمات السيبرانية والتحكم في المخاطر الرقمية.

ه- الكشف الآلي عن المخاطر، وتحليل تدفقات البيانات الجارية، وتحليل سجلات الأنشطة على المنصات الرقمية.

(Cybersecurity Best Practices for Universities,2021,pp.44-45)

لذلك يعد نظام الإدارة التلقائية للأمن أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بجامعة طوكيو .

٦- نظام الأمن الأداري المتقدم (AAS) :Advanced Administrative Security :

يعد نظام الأمن الأداري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني ، وتجدر الإشارة إلي أن جامعة طوكيو تتميز بأحدث التقنيات الأمنية، وتحظى بخبرات متنوعة لمكافحة التهديدات السيبرانية، وبوجودها على الساحة العالمية، تمكنت الجامعة من تطبيق أساليب الأمن الإداري المتقدمة وتمكين الأمن السيبراني بكفاءة عالية.

(Narumiya, M., Ishibashi, Y., & Tanabe, Y. :2020, pp.146-154).

وتجدر الإشارة إلى أنه تم تطوير هذا النظام في جامعة طوكيو باليابان، وهو يعتبر منصة بحثية توفر حلولا متقدمة لمتطلبات الأمن السيبراني في العصر الرقمي احديث ، كما يستهدف هذا النظام تزويد المستخدمين بإجابات دقيقة وشاملة عن استفساراتهم في مختلف المجالات .ويتم تحسينه باستمرار لتوفير أفضل تجربة ممكنة للمستخدمين .تتجاوز فوائد نظام الأمن الإداري المتقدم استخدامه كمحرك بحث متقدم. فبفضل تكامله مع تقنيات الذكاء الاصطناعي، يمكن للنظام تحليل وفهم البيانات الكبيرة المتدفقة من مصادر متعددة بشكل فعال وموثوق. تستخدم الذكاء الاصطناعي في التحليل المتقدم للبيانات لتحديد السلوكيات التي قد تشير إلى تهديدات سيبرانية والتصدي لها قبل حدوث أي تأثير كبير .

تعتبر جامعة طوكيو من الجامعات الرائدة في مجال البحث العلمي والتكنولوجيا، بل وتعتبر مركزًا لتطوير نظام الأمن الإداري المتقدم الذي يعتمد على الذكاء الاصطناعي. وتعمل جامعة طوكيو على توظيف الباحثين والعلماء المتميزين في هذا المجال، وتكرس جهودها لتعزيز المعرفة وتطبيق التقنيات الحديثة في مجال الأمن السيبراني ، وذلم لرفع مستوى الأمان وحماية المعلومات الدقيقة في البيئة الرقمية المتغيرة. يمكن أن يكون للنظام تأثير إيجابي على مجالات متعددة، بما في ذلك الشركات والمؤسسات الحكومية والتعليمية .(Tokyo University Official ,2022,pp.66-67). لذلك يعد نظام الأمن الأداري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بجامعة طوكيو .

خامسا : أهم القوي والعوامل الثقافية المؤثرة علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بجامعة طوكيو باليابان :

هنالك العديد من القوي والعوامل الثقافية المؤثرة علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بجامعة طوكيو باليابان ، والتي من أهمها علي النحو التالي :

أولا : العوامل الجغرافية :

تعد العوامل الجغرافية أحد أهم العوامل التي لها أثر أكبر علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي علي جامعة طوكيو باليابان.حيث تعتبر الطبيعة الجغرافية واحدة من العوامل المؤثرة بشكل كبير على تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي ، حيث تتمتع اليابان بموقع استراتيجي في شرق آسيا، مما يعزز دورها كواحدة من القوى العالمية الرائدة في مجال التكنولوجيا والإبتكار. بالإضافة إلى أن اليابان تمتلك بنية تحتية متقدمة ، وتمتاز بموقعها الزلزالي المعقد والمتغير وجغرافيتها الفريدة، بالإضافة إلى أنها واحدة من البلدان الأكثر كثافة سكانية في العالم.

وتجدر الإشارة إلى أن جامعة طوكيو تتمتع بسمعة قوية في مجال البحث والتطوير في مجال السيبرانية والذكاء الاصطناعي.، وهذا يساعد في تعزيز التعاون الوثيق مع القطاع الصناعي والحكومة، مما يسهم في تنمية حلول مبتكرة وذكاء اصطناعي متقدمة لحماية المجتمع وضمان أمان النظم الحيوية والآلية.(Tan, L. P. ,2019, p.55). وتعكس الطبيعة الجغرافية المعقدة لليابان تحديات فريدة تؤثر على الأمن السيبراني وتكنولوجيا الذكاء الاصطناعي في الجامعة. فعلى سبيل المثال، تعتبر الكوارث الطبيعية مثل الزلازل والتسونامي تحديات كبيرة تعيق استقرار الشبكات التكنولوجية وتهدد الأمن السيبراني. ولذلك، تعمل جامعة طوكيو على تطوير تقنيات الحماية المتقدمة وتقييم استعداد الشبكات للكوارث الطبيعية وتقديم حلول فعالة لمواجهتها.

بالإضافة إلى ذلك، توفر الجامعة فرصًا كبيرة للطلاب والباحثين للعمل على مشاريع مبتكرة في مجالات السيبرانية والذكاء الاصطناعي ، كمايتم تشجيع الابتكار والاكتشاف في هذه الجامعة من خلال دعم مبادرات البحث والتطوير، وتوفير الامكانيات والموارد لتعزيز القدرات الفكرية والتكنولوجية.

بشكل عام، فإن الطبيعة الجغرافية لليابان وتأثيرها على تمكين الأمن السيبراني وتطوير الذكاء الاصطناعي في جامعة طوكيو تعكس التزام اليابان الراسخ بالابتكار والتكنولوجيا المتقدمة. مما تؤدي جامعة طوكيو باليابان دورًا حاسمًا في ريادة التقنية وتطبيقات الذكاء الاصطناعي، بالإضافة إلى تعزيز الأمن السيبراني على المستوى الوطني والعالمي (Chen, H., Ishigaki, K., Fang, F. C., & Otsuka, A. ,2017,p. 776) .

ثانيا العوامل الاقتصادية :

تعد العوامل الاقتصادية أحد أهم العوامل التي لها أثر أكبر علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي علي جامعة طوكيو باليابان، حيث تعتبر العوامل الاقتصادية للدول والمنظمات عاملاً حاسماً في تطوير الأمن السيبراني واستخدام التكنولوجيا الذكية مثل الذكاء الاصطناعي. وتعد جامعة طوكيو في اليابان من الجامعات العالمية الرائدة في هذا المجال، إذ تعمل على تعزيز دور الابتكار والأبحاث العلمية في تطوير الأمن السيبراني واستخدام التكنولوجيا الحديثة لتعزيزه (Yamada, T. et al, 2023, pp. 50-51).

كما يعد الأمن السيبراني من أهم التحديات التي تواجهها الدول والمنظمات في العصر الحديث، حيث تزداد التهديدات الإلكترونية والهجمات السيبرانية التي تستهدف الحكومات والشركات والمؤسسات الكبرى. وتشكل هذه التهديدات خطراً على الأمن القومي والاقتصادي للدول، وتتطلب استراتيجيات وأدوات فعالة لمكافحتها(Sato, K., 2022, pp. 123-124) . تتعاون جامعة طوكيو مع القطاع الاقتصادي والحكومي لتعزيز الأمن السيبراني، وتطوير الحلول التكنولوجية المبتكرة والاستراتيجيات الفعالة لحماية البيانات والمعلومات الحيوية للدولة والمنظمات الكبرى. وتهدف الجامعة إلى تشجيع التعاون وتبادل المعرفة بين الأكاديميين والممارسين في هذا المجال لبناء بنية تحتية قوية ومستدامة للأمن السيبراني.

وتتبنى الجامعة استراتيجية شاملة تعتمد على التعاون الداخلي والخارجي، وتعزيز التواصل وتبادل المعرفة بين الباحثين والمتخصصين والممارسين في المجال الأمني والتقني ، وذلك لتعزيز الأمن القومي والاقتصادي لليابان وتحقيق التنمية المستدامة. كما تعتبر هذه الجهود نموذجًا يحتذى به لتعزيز الأمن السيبراني واستخدام التكنولوجيا الذكية في تمكين المجتمعات وحمايتها من الهجمات السيبرانية. (Takahashi, M., 2021, pp. 89-90)

القسم الخامس للدراسة : تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا وجامعة طوكيو باليابان : دراسة مقارنة تفسيرية.

في ضوء ما تم عرضه في أقسام الدراسة السابقة حول تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية بأستراليا وجامعة طوكيو باليابان والعوامل البنيوية الثقافية المؤثرة فيها ، يتطرق القسم الراهن إلى المقارنة التفسيرية ؛ وفيها يتم عقد مقارنة بين حالات المقارنة ؛ بهدف الوقوف على أوجه التشابه وأوجه الاختلاف بينهم ، وتفسير ذلك في ضوء مجموعة من مفاهيم العلوم الاجتماعية ذات العلاقة ، وذلك وفقا للمحاور التي تم الإشارة إليها في حدود الدراسة ، وينبغي التأكيد في هذا السياق أن الوصول إلى أوجه التشابه والاختلاف ليس غاية في ذاته ؛ فالأهم من ذلك هو تفسير تلك الأوجه ؛ بهدف تقديم أطر علمية للإجابة على أسئلة مؤداها : لماذا تلك التشابهات؟ وفي المقابل لماذا تلك الاختلافات ؟ ومن ثم الخروج بمنطلقات عامة ؛ يمكن من خلالها طرح مقترحات لتمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا وجامعة طوكيو باليابان .

أولا : أوجه التشابه والاختلاف بين الجامعة الوطنية باستراليا وجامعة طوكيو باليابان :

وذلك علي النحو التالي :

١- نظام الكشف التلقائي للاختراق Intrusion Detection System (IDS):

يعد نظام الكشف التلقائي للاختراق أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعتين كما سلف بيانه في الإطار النظري للدراسة .

أ- أوجه التشابه :

هناك تشابه واضح بين الجامعة الوطنية باستراليا وجامعة طوكيو باليابان في مجال نظام الكشف التلقائي للاختراق وتمكين الأمن السيبراني ويظهر هذا التشابه في اعتماد الجامعتين على نظم أمنية متطورة لحماية البيانات الأكاديمية والبحثية للطلاب ولأعضاء هيئة التدريس وحماية الجامعة من القرصنة السيبرانية ، كما تتشابه الجامعتين في تبني اتجاه واضح نحو تطبيق تقنيات وحلول والأنظمة الأمنية للذكاء الاصطناعي وتعلم الآلة على نطاق واسع في كلتا الجامعتين ، كما تشترك الجامعتين في تبني هدف واضح ، وهو حماية أنظمة المعلومات والتكنولوجيا من الاختراق ويمكن تفسير هذا التشابة في ضوء مفهوم الأمن القوميNational Security والذي يقصد به : تأمين مصالحها الحيوية، وتهيئة الأوضاع الملائمة لتحقيق أهدافها وغاياتها والتي يحددها الاستقرار السياسي والتماسك الاجتماعي والتنمية الشاملة(على الدين هلال ، ١٩٨٤م ، ص١٣).

وهناك تشابه واضح بين الجامعتين أيضا في المنهجية المستخدمة في الكشف والتحليل والتصدي للاختراقات وهي: الافتراض الدائم لوجود ثغرات في نظام الأمن السيبراني، وتحديث الأنظمة بشكل مستمر، والتحليل الدقيق لسجلات النشاطات لرصد أي نشاطات غير مألوفة أو مشبوهة، وتدريب العاملين على اتباع إجراءات الأمن السيبراني بشكل دوري ، ويمكن تفسير هذا التشابة في ضوء مفهوم الأمن الفكري Intellectual Security والذي يقصد به : يعنى الحفاظ على المكونات الثقافية الأصيلة للمجتمع في مواجهة التيارات الثقافية الوافدة أو الأجنبية المشبوهة بما يسهم في حماية وصيانة الهوية الثقافية للمجتمع من الاختراق أو الاحتواء من الخارج كما يعني أيضاً الحفاظ على العقل الجمعي من الاحتواء الخارجي وصيانة المؤسسات الثقافية في الداخل من الإنحراف (محمد بن عبدالرحمن الفريدي ، ٢٠١٦م ، ص ١٨).

ب - أوجه الاختلاف :

تختلف الجامعة الوطنية باستراليا وجامعة طوكيو باليابان في طبيعة الثقافة التنظيمية السائدة بكل جامعة ، كما أن هناك إختلاف بين الجامعتين في طريقة التعامل مع قضايا الأمن السيبراني ، وفي الممارسات والاستراتيجيات المتبعة ويمكن تفسير هذا الاختلاف في ضوء مفهوم الثقافة التنظيمية Organizational Culture والتي يقصد بها : إطار معرفي مكون من الاتجاهات والقيم ومعايير السلوك والتوقعات التي يتقاسمها العاملون في المنظمة، وتتأصل أي ثقافة على مجموعة من الخصائص الأساسية التي يثمنها العاملون في المنظمة(جرينبرج و بارون، ٢٠١٠م ، ص ١٢٧) ، والتي تنعكس علي طبيعة الممارسات ، ويمكن تفسير هذا الاختلاف في ضوء مفهوم الممارسات التنظيمية الإدارية Management Organizational Practices والتي يقصد بها: هي مجموعة اللوائح والخدمات الإدارية التي تسعى إلى تحسين بيئة الأعمال التي أصدرها مجلس الدولة، بهدف التحسين المستمر لبيئة ممارسة الأعمال وتحديث أنظمة وقدرات المؤسسات، ودفع عجلة تطوير الجودة ، ومعالجة القضايا الرئيسية على الفور من خلال التنسيق ، وتعزيز العمل على تحسين بيئة الأعمال والإشراف على تنفيذ الإجراءات(Berg, 2013 ,p.11) ، حيث يمكن أن تؤثر تلك الاختلافات وفقا لنوع الثقافة التنظيمية Organizational Culture ، الممارسات التنظيمية الإدارية Management Organizational Practices بين الدول على نهج الجامعتين في التعامل مع بعض القضايا ذات العلاقة بتمكين الأمن السيبراني.

قد توجد صعوبات في فهم تقنيات الأمن السيبراني الجديدة إذا كانت مصطلحاتها مختلفة بين كل من الجامعتين، وقد تختلف الجامعتان في بنيتهما التحتية للتكنولوجيا ويمكن تفسير هذا الاختلاف في ضوء مفهوم البنية التحتية لتكنولوجيا المعلومات IT Infrastructure والتي يقصد بها : هي مجموعة الوسائل والتقنيات والقدرات التي يتم تنسيقها بواسطة منظمة مركزية للمعلومات وتشمل جميع الأنظمة التي تسهل تلك العمليات (محمد أبو القاسم الرتيمي ، ٢٠٠٢م ، ص٩٤) .

٢- نظام الجدار الناري المتقدم Next Generation Fire Walls (NGFW):

يعد نظام الجدار الناري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي والتي تساهم في تمكين الأمن السيبراني بالجامعتين كما سلف بيانه في الإطار النظري للدراسة.

أ- أوجه التشابه :

هناك تشابه واضح بين الجامعتين في مجال نظام الجدار الناري المتقدم وتمكين الأمن السيبراني ويظهر هذا التشابه في محاولة الجامعتين في تحقيق أهداف مماثلة من خلال تطوير تقنيات وأدوات فعالة لحماية البيانات والمعلومات الدقيقة ضد التهديدات السيبرانية، ويمكن تفسير ذلك في ضوء مفهوم خصوصية البيانات وخاصة الشخصية ، ويمكن تفسير ذلك في ضوء مفهوم **خصوصية البيانات الشخصية Data Privacy of personal** والتي يقصد بها :

مطالبة الأشخاص بأن لا تكون البيانات الخاصة عنهم متوفرة تلقائياً لغيرهم من الأفراد أو المنظمات، حتى في حالة أن تكون البيانات مملوكة من طرف آخر، فلهم القدرة على ممارسة قدر كبير من السيطرة أو التحكم بتلك البيانات وطريقة استخدامها ، كما أنها رغبة الشخص بالتحكم ،أو على الأقل التأثير بشكل كبير في كيفية التعامل مع بياناته الشخصية (Roger Clarke, 2008,p.7)

ب- أوجه الاختلاف :

تختلف الجامعة الوطنية باستراليا وجامعة طوكيو باليابان في الخبرة التقنية بين الجامعتين في مجال الأمن السيبراني، حيث يمكن أن تكون جامعة طوكيو أكثر تقدماً في هذا المجال لتاريخها الطويل في تكنولوجيا المعلومات والاتصالات عن الجامعة الوطنية الأسترالية ، ويمكن تفسير ذلك في ضوء مفهوم الخبرة Experience والتي يقصد بها : المعرفة ببواطن الأمور ، وهو مفهوم المعرفة أو المهارة أو قدرة الملاحظة لكن بأسلوب فطري عفوي عميق، عادة يتم اكتساب الخبرة من خلال المشاركة في عمل معين أو حدث معين، وغالبا ما يؤدي تكرار هذا العمل أو الحدث إلى تعميق هذه الخبرة وإكسابها عمقا أكبر وعفوية أكبر. لذلك تترافق كلمة خبرة غالبا مع كلمة تجربة.(معجم الجرجاني ، ٨١٦ هـ ، ص٦٠) ، كما هناك بعض الاختلافات في مجال القوانين المتعلقة بالأمن السيبراني بين الدولتين وبالتالي الجامعتين، مما يؤثر على أساليب وأدوات الجدار الناري المتقدم وتمكين الأمن السيبراني المستخدمة في الجامعتين.

ويمكن تفسير ذلك في ضوء مفهوم القانون The Lawوالذي يقصد به : مجموعة من القواعد التي تنظم العيش في جماعة، والتي يجب على الكافة احترامها احتراماً تفرضه السلطة العامة بالقوة عند الاقتضاء. أي هو بمثابة نظام اجتماعي ملزم يعكس التطور الذي يهدف باستمرار إلى تحقيق المصالح الاجتماعية المشتركة، عن طريق تنظيم شامل وطموح للأنشطة الإنسانية، بهدف تحقيق الأهداف وترجمة الأماني الاجتماعية(عبدالرازق السنهوري ، ١٩٥٠ ، ص ٢١٢)، وأيضا هناك بعض الاختلافات في النهج الثقافي والتقني بين الجامعتين التي تؤثر على اتخاذ القرارات والتي تتعلق بالتهديدات المتغيرة باستمرار ، ويمكن تفسير ذلك في ضوء مفهوم **اتخاذ** القرار Decision Making والذي يقصد به : اختيار نهج أو طريق أو آليّة للسلوك من بين عدد من البدائل والخيارات الممكنة أو المتاحة، أو هو الرأي عند من يملك اختياره وتصديره .(معجم المعاني ، ص٣٢١).

٣- نظام الأمن السحابي Cloud Security:

يعد نظام الأمن السحابي أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعتين كما سلف بيانه في الإطار النظري للدراسة .

أ- أوجه التشابه :

تتشابه الجامعتين في تعزيز الوعي الأمني لدى الطلاب والعاملين في الجامعة، وذلك عن طريق توعية المستخدمين بأهمية تأمين بياناتهم وتجنب الخروج عن السياسات الأمنية المعتمدة ، ويمكن تفسير ذلك في ضوء مفهوم الوعي الأمني Security Awareness والذي يقصد به : قناعة وإدراك الفرد بمدي خطورة الجرائم وأثارها السلبية على الفرد والمجتمع، وأهمية التعاون مع الأجهزة الأمنية للوقاية من أخطارها والتصدي لها ومقاومتها فكراً ومنهجاً وسلوكاً (تركي بن عيد البقمي، ٢٠١٢م ، ص ٢٩).

كما تتشابه الجامعتين في السعي الدائم نحو إيجاد الحلول الفعالة لمواجهة التحديات الأمنية في العصر الرقمي ، ويمكن تفسير ذلك أيضا في ضوء مفهوم العصر الرقمي The Digital Age والذي يقصد به : هو اسم يطلق على الفترة التي تلت العصر الصناعي وهو عبارة عن تطبيق على الزمن الذي تكون فيه المعلومات هي المحور الذي يتحكم في السياسة والاقتصاد والحياة الاجتماعية.(محمد

محمود مكاوي ، ٢٠٠٥م ، ص٢٠) ، عبر الاعتماد على تقنيات الذكاء الاصطناعي والتحليل الضخم للبيانات، والإشراف الدائم على أنظمة الأمان السحابية والتحقق من تحديثها بانتظام.

ب- أوجه الاختلاف :

تختلف الجامعتين في مجال الأمن السحابي حيث يمكن القول إن الجامعة الوطنية باستراليا تمتلك تقنيات أكثر تطوراً في الحوسبة السحابية مقارنة بجامعة طوكيو باليابان، في حين أن الأخيرة تمتلك مصداقية واسعة في مجال الأمن السيبراني على المستوى الدولي ، ويمكن تفسير ذلك في ضوء مفهوم الحوسبة السحابية Cloud Computing والتي يقصد بها : المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة والتى تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم، وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية، كما تشمل قدرات معالجة برمجية وجدولة للمهام ودفع البريد الإلكتروني والطباعة عن بعد (محمود شريف زكريا ،٢٠١٧م ، ص١٩٦٨م)

٤- نظام التعرف علي السلوك غير العادي(UEBA) User and Entity Behavior Analytics:

يعد نظام التعرف علي السلوك غير العادي أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعة الوطنية باستراليا، بالجامعتين كما سلف بيانه في الإطار النظري للدراسة .

أ- أوجه التشابه :

تتشابه الجامعتين في نظام السلوك غير العادي حيث تولي الجامعتان اهتماما ملحوظا بدراسة مظاهر السلوك غير العادي وفهمها بشكل أفضل. فضلا عن اتباع المناهج التعليمية المحدثة وبخاصة في مجال السلوك البشري واضطراباته، ويمكن تفسير ذلك في ضوء مفهوم علم السلوك البشري والذي يقصد به : دراسة سلوك الإنسان ، ويُعتبر علم السلوك كتخصص عام فرعًا لعلم الأحياء(hinde ,Robert A, 2012,p2) كما تتشابه الجامعتين في التعاون في بناء إستراتيجيات للوقاية من السلوك الغير العادي وتحديد أفضل الحلول التي تساهم في التغلب على هذه المشكلة ، ويمكن تفسير ذلك في ضوء مفهوم الوقاية Protection والتي يقصد بها :إجراء أو تدبير يتخذ للتخلص من شيء أو تطوير عملية ما وذلك لمنع احتمال أي حوادث مستقبلية قد لا تطابق المواصفات (الجمعية الأمريكية للجودة ، ٢٠٢٢م ص٣).

ب-أوجه الاختلاف :

تختلف الجامعتين في مجال نظام السلوك غير العادي ، حيث تهتم الجامعة الوطنية في استراليا بتطوير سياسات الأمن السيبراني، بينما تهتم جامعة طوكيو بتطويرالعمليات الأمنية الفعالة . كما تختلف الجامعتين من حيث العمليات التعليمية حيث تزود الجامعة الوطنية باستراليا الدارسين بالمعرفة اللازمة والتدريب المستمر في مجال في تكنولوجيا الأمن السيبراني، في حين أن جامعة طوكيو تركز على الجانب الأساسي للأمن السيبراني بشكلٍ عام. كما تختلف الجامعتين في طبيعة موضوعات البحث العلمي، حيث تركز الجامعة الوطنية باستراليا على البحث وتحليل التهديدات المختلفة، بينما تتمحور بحوث جامعة طوكيو حول تحليل الهجمات الإلكترونية وتصميم الحلول الفعالة لها.

٥ - نظام الإدارة التلقائية للأمن : Automated Security Management(ASM)

يعد نظام الإدارة التلقائية للأمن أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعتين كما سلف بيانه في الإطار النظري للدراسة .

أ- أوجه التشابه :

تتشابه الجامعتين في التقديم المتواصل لسلسلة تدريبات في مجال الأمن السيبراني والإدارة التلقائية للأمن ، كما تتمتع كلا الجامعتين بخبرات مماثلة في مجال البحث والتطوير في هذه المجالات. كما تتشابه الجامعتين في الإيمان بالذات (الثقة بالذات): حيث أن الثقة بالذات هي مفتاح تجنب الهجمات في العالم الافتراضي، وفي الوقت الذي تشجع فيه الجامعة الوطنية بأستراليا على تعزيز ثقة الفرد

بذاته من أجل الابتعاد عن الأخطار السيبرانية، بينما تستند الجامعة في طوكيو إلى المسؤولية المتبادلة بين الفرد والمجتمع لتحقيق الأمن السيبراني.

ب-أوجه الاختلاف :

تختلف الجامعتين في المفهوم الاجتماعي للأمن السيبراني: حيث تختلف مفاهيم الأمن السيبراني بين الثقافات والمجتمعات المختلفة، وتعتبر الجامعة الوطنية باستراليا تعتبر الخصوصية هي المفهوم الأساسي للأمن السيبراني، بينما في اليابان، يتم التركيز بشكل أساسي على الانضباط الذاتي، الذي يندرج تحته التزام الفرد تجاه التدابير الأمنية في الحفاظ على الأمن السيبراني. كما يوجد اختلاف بين كلتا الجامعتين في الاعتماد على الحلول التقنية: حيث تعتمد الجامعة الوطنية بأستراليا بشكل أساسي على التقنيات الحديثة والحلول التقنية المبتكرة للحفاظ على الأمن السيبراني، بينما تعمل جامعة طوكيو على تعزيز الإدارة المستدامة للأمن السيبراني عن طريق المعالجة المستمرة للنظام والتعاون بين الأفراد والمجتمع . بشكل عام، يمكن القول أن هناك اختلافات في الطريقة التي يتم بها النظر إلى الأمن السيبراني وتمكينه بين الجامعة الوطنية باستراليا وجامعة طوكيو باليابان، ويرجع ذلك جزئيًا إلى الفروقات الثقافية والاجتماعية بين البلدين .يعد نظام الأمن الاداري المتقدم أحد أهم الأنظمة الأمنية للذكاء الاصطناعي التي تستهدف تمكين الأمن السيبراني بالجامعتين كما سلف بيانه في الإطار النظري للدراسة .

أ- أوجه التشابه :

تتشابه الجامعتين في الحاجة إلى الابتكار المستمر والتطوير الدائم للتكنولوجيا والممارسات المشتركة المتعلقة بالأمن، كما يسعي كلاهما نحو الإدارة الفعالة والتخطيط الاستراتيجي لتحديد الأولويات والتحديات المرتبطة بالأمن، كما تحرص كلا الجامعتين على تمكين الأمن السيبراني والحفاظ على بيانات الطلاب والموظفين بشكل آمن،بالإضافة إلي تمتع كلا الجامعتين بخبراء ومختصين في مجال الأمن الإداري المتقدم، كما تعمل الجامعتان على تعزيز التعاون بين القطاع الحكومي والقطاع الخاص لتعزيز الأمن السيبراني، كما تتشابه الجامعتين في الاهتمام بأهمية توعية الموظفين والطلاب بخطورة التهديدات الإلكترونية والتدريب على كيفية استخدام الأدوات الأمنية المتاحة. كما تتشابه الجامعتان في السعي الدائم نحو التنسيق الدولي وتبادل المعلومات حول الهجمات السيبرانية والأدوات المستخدمة للدفاع عن أمن البيانات.

ب- أوجه الاختلاف :

تختلف الجامعتين في الطرق والأدوات المستخدمة لتعزيز الأمن. ففي الجامعة الوطنية باستراليا، تتمحور الجهود المتعلقة بالأمن السيبراني حول حماية البيانات والمعلومات الحساسة وتطوير سياسات وإجراءات الأمان. بينما في جامعة طوكيو باليابان، يتركز تمكين الأمن السيبراني على توسيع استخدام التكنولوجيا للحد من التهديدات السيبرانية. كما تختلف الجامعتان في طرق تنفيذ الأمن السيبراني، فالجامعة الوطنية باستراليا تستخدم نظامًا مركزيًا لإدارة الأمن، بينما تستخدم جامعة طوكيو في اليابان تقنيات مضادة للاختراق، وإجراءات تحليل النشاطات غير العادية. كما تختلف تقنيات الأمان في كلا الجامعتين من حيث البرمجيات المستخدمة وتقنيات التشفير والتشخيص، بالإضافة إلي اختلاف الجامعتين في طبيعة المناهج الدراسة والأبحاث الخاصة بالأمن الإداري المتقدم في الجامعتين.

القسم السادس للدراسة : تمكين الأمن السيبراني بالجامعات المصرية في ضوء مدخل الذكاء الاصطناعي: دراسة وصفية تحليلية.

يعد إطلاق إستراتيجية موحدة في مجال الأمن السيبراني عام ٢٠١٥م بعنوان "الأمن السيبراني آفاق وتحديات"، وذلك على هامش المؤتمر السنوي لتطوير الصناعة ، بمثابة أحد أهم الجهود المصرية في مجال تقليص مخاطر الهجمات السيبرانية ، وتجدر الإشارة إلى أن الإستراتيجية قد ركزت على ، تأمين الخدمات الإلكترونية وشبكات البنية التحتية وتطبيقات التحكم الصناعي . (أحمد جلال محمود ، ٢٠٢٠م ، ص ص ٧٠-٧١)

وهذا يؤكد علي أن مصر تشهد حراكًا قويا في مجال تمكين الأمن السيبراني، والذي ظهر أيضاً في، إنشاء المجلس الأعلى للأمن السيبراني ، بالإضافة إلى انضمام مصر للاتفاقية العربية لمكافحة جرائم الإنترنت والإرهاب الإلكتروني، علاوة علي إنشاء مركز سيرت المصري، حيث يقدم المركز الدعم لمختلف الجهات عبر قطاعات تكنولوجيا المعلومات والاتصالات والخدمات المصرفية والحكومية؛ من أجل مساعدتها على مواجهة تهديدات الأمن السيبراني ؛ وذلك لتأمين ميكنة الخدمات الإلكترونية وللحد من آثار اختراق أمن المعلومات وللمساهمة في تأمين الأمن القومي للدول . (عمار ياسر البابلي ، ٢٠٢٠م ص٨). ومن أبرز الجهود المصرية تفعيل برنامج التعليم عن بعد، والذي ازداد استخدامه بشكل واضح خلال أزمة كورونا ، والذي يستهدف تمكين معظم الجامعات من إجراء المحاضرات عن بعد باستخدام تكنولوجيا الاتصالات والمعلومات ، لإثراء المعرفة وتطوير مهارات الإبداع، وتعزيز التدريس والتدريب الذاتي والعمل في مجموعات والانفتاح على العالم والثقافات الأخرى ، وذلك بهدف تعزيز التعليم الرقمي والتكنولوجيا الرقمية بالعمل مع العديد من الجهات التعليمية والجامعات والأكاديميات

كما تم تطبيق برنامج التعليم عن بعد لدى العديد من الجامعات المصرية، تم تفعيل المنصات الإلكترونية باعتبارها فصولا افتراضية تقدم خبرات ومواقف تعليمية متعددة، لتوفير الخدمات المساعدة للتعليم عن بعد للجامعات. (شيرين عيد مرسي، ٢٠٢١م ، ص ٤٤٠) شيرين عيد مرسي : سيناريوهات مستقبلية لمواجهة مظاهر الفاقد التعليمي في إطار جائحة كورونا ، مجلة كلية التربية ، جامعة بني سويف، ع١٠، ج ٢، ٢٠٢١م. واتساقا مع ما سلف بيانه قامت مصر بإطلاق القمر الصناعي ، لأغراض الاتصالات وحماية الأمن القومي الإلكتروني طيبة - ١"،وبهدف دعم جهود الدولة في مكافحة الجريمة والإرهاب وتأمين البنية التحتية المعلوماتية من الأخطار السيبرانية التي باتت ظاهرة تهدد أمن الشعوب واستقرارها كما يسهم في توفير خدمات الإنترنت عريض النطاق للأغراض الحكومية والتجارية (هيئة الاستعلامات المصرية "إطلاق القمر الصناعي طيبة ١) .ويغطي مصر بالكامل فيما يخص الاتصالات والإنترنت، والقمر الصناعي طيبة ١ هو الأول في سلسلة "طيبة سات"، والتي ستحدث نقلة نوعية في خدمات الاتصالات في مصر وأفريقيا، ويشمل مجال تغطية القمر الصناعي مصر وبعض دول شمال أفريقيا ودول حوض النيل.

وتظهر جهود جمهورية مصر العربية في إطلاق الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧ - ٢٠٢١م) والتي أطلقها المجلس الأعلى للأمن السيبراني، من أجل تأمين البنى التحتية للاتصالات والمعلومات بشكل متكامل لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، ورفع مستوى الوعي بالأمن السيبراني، وتجنب المخاطر والتهديدات السيبرانية وتقليل آثارها وذلك في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري، وبما يدعم التحول نحو اقتصاد رقمي متكامل. (الإستراتيجية الوطنية للأمن السيبرانى (٢٠١٧/٢٠٢١م) ، ص٣). وفي عام ٢٠١٧م أصدر الاتحاد الدولي للاتصالات تقرير مؤشر قياس استعداد الدول في هذا الأمن السيبراني؛ من أجل دفع المزيد من الجهود في مجال تمكين الأمن السيبراني ومواكبته عالمياً . وتجدر الإشارة إلى أن هذا التقرير قد أكد علي أن مصر لديها استعداد قوي في مجال الأمن السيبراني، من خلال هيكلة بنية تحتية وتبنيها إستراتيجيات وطنية في هذا المجال، كما عقدت اتفاقيات عديدة دعت من خلالها لتبادل الخبرات ونشر ثقافة الوعي بالأمن السيبراني، من خلال تبنيها سياسات وطنية، كما قدمت الكثير من المبادرات والملتقيات والمنتديات، وعقدت مؤتمرات واتفاقيات في مجال تمكين الأمن السيبراني، وبذلك قد عبرت مصر أزمات الثقة التي تهدد انتشار ثقافة الأمن السيبراني محليا وعالميا

وفي نفس العام وقعت مصر في ٢٠١٧م اتفاقية التعاون بين المعهد القومي للاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات وشركة سيسكو العالمية؛ بهدف إطلاق أول أكاديمية للأمن السيبراني، تهدف إلى تطبيق المهارات اللازمة لمواجهة تحديات الأمن السيبراني(إيمان علاء الدين سليمان ، ٢٠٢١م ، ص٣٩). وتأتي مصر في المرتبة ٢٣ عالميًّا والرابعة عربيًّا في المؤشر العالمي للأمن السيبراني Global Cybersecurity Index (GCI)K لعام ٢٠١٩م ، والذي يصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة، كما جاءت مصر في المرتبة الرابعة عشرة من بين ١٩٣ دولة من دول أعضاء الاتحاد وكذلك جاءت في المرتبة الثانية عربيًّا فيما يتعلق بمستويات الالتزام بالأمن السيبراني بعد سلطنة عمان التي جاءت في المركز الرابع

عالميًا والأول عربيًا .(أسماء أحمد أبوزيد ، ٢٠٢١م ، ص١٢). وتعتبر مصر واحدة من الدول الناشئة التي تهتم بالتطور التكنولوجي وتعزيز الحماية السيبرانية. في الآونة الأخيرة (Ahmadian, A., & Zawoad, S. ,2021,72-73)، وخاصة بعد أن أصبحت الجامعات المصرية محورا مهما لنشر الوعي السيبراني وتأهيل الكوادر اللازمة في هذا المجال المهم .

(Elbashir, M. Z., & Abdel-Aziz, A. H. M. ,2020,p. 76)

وتجدر الإشارة إلى أن هناك حاجة ملحة لبذل مزيد من الجهود في هذا المجال، خاصةً في ظل التهديدات السيبرانية المتزايدة التي تواجهها مصر والعالم. (Zhang, Y., Chen, D., & Yu, H. ,2019,p. 531). وتجدر الإشارة إلى أن تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي يشكل تحدياً كبيراً في الجامعات المصرية، إلا أن هناك العديد من التحديات التي لا تزال تعاني منها الجامعات المصرية في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي والتي من أهمها على النحو التالي:

١- ضعف الوعي الأمني وقلة المعرفة بين الطلاب وأعضاء هيئة التدريس ، وأن هناك حاجة ماسة لتعزيز الوعي بأهمية الأمن السيبراني وتوفير التدريبات وورش العمل المتخصصة لتعزيز المهارات الفنية والوقاية من الهجمات السيبرانية.

٢- تواجه الجامعات المصرية تحديات في مجال إدارة وحماية البيانات ، لذا يستوجب الأمر بذل المزيد من الجهود التي تستهدف تطوير سياسات وإجراءات فعالة لحماية البيانات، بما في ذلك تشفير البيانات الحساسة وتطبيق تقنيات الوصول المحدود والتحقق من الهوية ، بالإضافة إلى ضرورة توفير آليات الإبلاغ عن الاختراقات والتعامل معها بشكل سريع وفعّال.

(Hassan, A., Ahmed, M., & Ali, M. ,2021, p.1215).

٣- يعتبر اكتشاف التهديدات والهجمات السيبرانية التي تتعرض لها الجامعات تحديًا رئيسيًا ، لذلك يعد من الضروري توفير نظم متقدمة للكشف عن التهديدات وتحليل سلوك المستخدمين وتتبع الأنشطة الغريبة، مع توفير فرق متخصصة للتعامل مع الهجمات والتحقيق فيها وتطبيق التدابير الوقائية المناسبة.

٤- يتطلب تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية مواجهة تحديات تتعلق بالبنية التحتية التقنية والتمويل ، وذلك بتوفير التجهيزات والتقنيات المتطورة التي تدعم الأنظمة الأمنية للذكاء الاصطناعي مثل تطوير الشبكات وتحسين أنظمة التخزين وزيادة قدرة المعالجة. (Ali, S. A., & Elhoseny, M. ,2020, p.85)

٥- تواجه الجامعات المصرية تحديات في مجال توظيف الكوادر المؤهلة والخبراء في مجال تمكين الأمن السيبراني ، لذلك هناك حاجة ملحة لتوفير برامج تدريب وتأهيل للطلاب والباحثين في هذا المجال، فضلاً عن تعزيز التعاون بين الجامعات والشركات والمؤسسات ذات الصلة لتبادل الخبرات والمعرفة.

٦- هناك ضرورة لتبني إطار تشريعي وقوانين واضحة لتمكين الأمن السيبراني في الجامعات المصرية، بالإضافة إلى تنظيم حملات توعية ونشر المعلومات المتعلقة بأمان البيانات والتهديدات السيبرانية.

(Elragal, A., & Teixeira, N. M. 2021, p.3053)

واتساقا مع ما سلف بيانه فإن ضمان أمن المعلومات والحماية من التهديدات السيبرانية يعد أمرًا حيويًا في العصر الحديث، حيث تزايدت التهديدات الإلكترونية وأصبحت أكثر تعقيدًا وتطورًا. لذا، تحتاج مصر إلى الاستفادة من خبرات الجامعات الرائدة في مجال تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي ، والتي من أهمها كما سلف بيانه في الإطار النظري الجامعة الوطنية باستراليا ، وجامعة طوكيو باليابان ، حيث تتمتع تلك الجامعات علي وجه التحديد بمكانة مرموقة في هذا المجال ، وعند الاسترشاد بخبرات تلك الجامعات سيساهم ذلك في تعزيز القدرات السيبرانية لمصر وتمكينها من التصدي للتحديات الأمنية في العالم الرقمي.

حيث تمتاز الجامعة الوطنية باستراليا بأنها تعد واحدة من الجامعات الرائدة في مجال تمكين الأمن السيبراني حيث توفر الجامعة برامج تعليمية متخصصة تغطي مختلف جوانب أمن المعلومات، بداية من الأساسيات وصولاً إلى تحليل الهجمات السيبرانية المعقدة وتنفيذ استراتيجيات الدفاع المتقدمة. تعمل الجامعة الوطنية على تطوير أبحاث ومشاريع بحثية مبتكرة في هذا المجال، بما في ذلك تطوير أدوات وتقنيات جديدة لمكافحة التهديدات السيبرانية. كما تمتاز جامعة طوكيو باليابان بخبرتها الواسعة في مجال

تمكين الأمن السيبراني ، حيث تقدم الجامعة برامج دراسية شاملة في مجال التحقيق الرقمي والحماية من الهجمات السيبرانية واختبار الاختراق. تعمل الجامعة أيضًا على إجراء الأبحاث والتطوير في مجال تمكين الأمن السيبراني في ضوء الأنظمة الأمنية للذكاء الاصطناعي. وباستفادة مصر من خبرة الجامعة الوطنية باستراليا وجامعة طوكيو باليابان، ستكون قادرة على تحقيق تقدم ملحوظ في مجال تمكين الأمن السيبراني في ضوء الأنظمة الأمنية للذكاء الاصطناعي ، وبمكافحة التهديدات السيبرانية ستساهم استراتيجيات الدفاع المتقدمة وتقنيات التحقيق الرقمي والتدريب المتخصص في تمكين الكوادر البشرية في مجال الأمن السيبراني وتهيئتهم لمجابهة التهديدات القادمة.

ثانيا: أهم القوي والعوامل الثقافية المؤثرة علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات المصرية:

أولا : العوامل الجغرافية :

تعد العوامل الجغرافية أحد أهم العوامل التي لها أثر أكبر علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي ، حيث تعدّ الطبيعة الجغرافية لمصر مصدرًا للتحديات والصعوبات التي تواجهها فيما يتعلق بتمكين الأمن السيبراني واستخدام التكنولوجيا الحديثة، مثل الذكاء الاصطناعي، في الجامعات المصرية. حيث يتطلب الأمن السيبراني تبني استراتيجيات وسياسات فعالة للتصدي لتهديدات القرصنة والاختراقات الإلكترونية، وحماية البيانات الحساسة والأنظمة الحاسوبية المختلفة.

(El-Masry, A. A., Ghoneim, A., & Al-Tarawneh, H. ,2020,pp. 44-45)

من أجل تمكين الأمن السيبراني في الجامعات المصرية، تتطلب المسألة وعيًا تامًا وتعاونًا فعّالًا بين الجهات المعنية، بما في ذلك الحكومة والجامعات والشركات الخاصة. يجب زيادة الاستثمار في تجهيز الأجهزة والبرامج والموارد البشرية المتخصصة، بحيث يتم تطبيق أحدث التقنيات والأساليب في مجال الأمان السيبراني.

(Egyptian Ministry of Communications and Information Technology., 2019 ,pp.5-6)

بجانب التحديات الأمنية، تواجه الجامعات المصرية صعوبات في تمكين الذكاء الاصطناعي واستخدامه بشكل فعال في عمليات التعليم والبحث العلمي. يعد الذكاء الاصطناعي مجالًا متقدمًا يعتمد على تقنيات الحوسبة الذكية والتعلم الآلي لتمكين الأنظمة والروبوتات من أداء المهام المعقدة واتخاذ القرارات الذكية.

(Afify, A. I., Mashhour, A. S., & Hammad, S. E. ,2018,pp. 87-88)

لتمكين الذكاء الاصطناعي في الجامعات المصرية، يجب توفير بنية تحتية قوية وموارد مالية وبشرية للبحث والتطوير في هذا المجال. يعتبر التعليم والتدريب المتخصص للأطقم الأكاديمية والطلاب مهمة حاسمة، فضلًا عن ضرورة تعزيز التعاون مع الجامعات والمنظمات الدولية ذات الخبرة في مجال الذكاء الاصطناعي.

(Ezzat, H. A., & Sharaf, A. M. 2019,pp. 0578-0579).

ثانيا : العوامل الاقتصادية :

تعد العوامل الاقتصادية أحد أهم العوامل التي لها أثر أكبر علي تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي ، وتعتبر جمهورية مصر العربية دولة ذات طبيعة اقتصادية متنوعة . تمتلك مصر المزيد من الموارد الطبيعية والثروات البشرية والثقافية التي تعتبر قوة فريدة وقوية في منطقة الشرق الأوسط وشمال أفريقيا. يعتبر قطاع تكنولوجيا المعلومات والاتصالات من أهم القطاعات التي تساهم في الاقتصاد المصري .

مع التطور السريع للتكنولوجيا، تزايدت التحديات والصعوبات التي يواجهها الأمن السيبراني في مصر. فبينما يلتفت المجتمع إلى فوائد التكنولوجيا واستخداماتها الإيجابية، يتزايد أيضًا الوعي بأهمية حماية المعلومات الحساسة والبيانات الشخصية من الاختراق والاستغلال غير المشروع. يعد الامتناع عن اتخاذ تدابير الأمن السيبراني اللازمة تهديدًا جديًا لاقتصاد مصر واستقراره.

(عبد العال عبد الناصر طنطاوي ، وساميل المطراوي ، ٢٠٢٠ ، ص ص ١٥-١٦) . تعاني الجامعات المصرية من تحديات وصعوبات في مجال تمكين الذكاء الاصطناعي. الذكاء الاصطناعي عبارة عن تطبيقات تكنولوجية تعتمد على الحوسبة والتعلم الآلي لتحليل البيانات واتخاذ القرارات. ومع ذلك، تنتج الجامعات المصرية عادةً كميات كبيرة من البيانات ولكن يفتقر النظام التعليمي إلى البنية التحتية والموارد اللازمة لاستخدام فعال للذكاء الاصطناعي.(محمود محمد السيد ، فيروزمحمد ، فهد الرسين. ، ٢٠١٩، ص ص ٣٣-٣٤)

لمواجهة هذه التحديات، يجب أن تعمل الجامعات المصرية على تطوير بنية تحتية تكنولوجية قوية وزيادة الاستثمار في تحسين قدرات الأمن السيبراني. يجب أن يتم تدريس الطلاب وتوجيههم في مجال الأمن السيبراني وتكنولوجيا المعلومات والاتصالات بشكل أفضل في الجامعات. ينبغي أن تكون هناك تعاون وثيق بين الجامعات والقطاع الخاص لتوفير الفرص التعليمية والتدريبية المناسبة لتطوير المهارات اللازمة في مجال الأمن السيبراني والذكاء الاصطناعي. بالنهاية، تحظى مصر بمكانة استراتيجية هامة على الصعيدين الاقتصادي والتكنولوجي. من أجل الاستفادة الكاملة من إمكاناتها، يجب أن تعمل الحكومة والجامعات والقطاع الخاص بتعزيز الأمن السيبراني وترسيخ دور الذكاء الاصطناعي في التطوير الاقتصادي والتكنولوجي في البلاد.(علاء عفت،ومحمود بدوي ،٢٠٢١، ص ص ٥٥-٥٦)

القسم السابع للدراسة: نتائج الدراسة والاجراءات المقترحة:

في ضوء ما ورد في الإطار النظري واستناداً إلى ما تم عرضه عن تمكين الأمن السيبراني بالجامعة في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا وجامعة طوكيو باليابان يمكن توضيح أهم النتائج التي توصلت إليها الدراسة وتقديم بعض الإجراءات المقترحة للإستفادة من تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا وجامعة طوكيو باليابان بما يتفق مع طبيعة المجتمع المصري ويمكن توضيح ذلك من خلال مايلي:

أولا : نتائج الدراسة:

١- نتائج تتعلق بفلسفة بتمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي:

توصلت الدراسة إلي العديد النتائج التي تتعلق بفلسفة بتمكين الأمن السيبراني بالجامعات في ضوء مدخل الذكاء الاصطناعي والتي من أهمها علي النحو التالي :

أ- **دور الأنظمة الأمنية للذكاء الاصطناعي:** إن فلسفة تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات ترتكز على الأنظمة الأمنية ، والتقنية ، والإدارية في حماية البيانات والمعلومات المخزنة على الحواسيب والشبكات بالجامعات.

ب- **تفعيل الأنظمة الأمنية للذكاء الاصطناعي لتمكين الأمن السيبراني بالجامعات :** أشار الإطار النظري إلى أن توظيف الأنظمة الأمنية للذكاء الاصطناعي يساهم في تفعيل التعلم العميق ، وفي التحليل بالإضافة إلى التنبؤ بالسلوك غير العادي ، علاوة على رصد وتحجيم البرامج الضارة، كل هذه العوامل تساهم فى تمكين الأمن السيبراني بالجامعات.

ج- **بالنسبة للجانب الإداري :** ينبغي للجامعات تطوير سياسات وإجراءات تحمي البيانات الدقيقة ، والشبكات الداخلية والخارجية من الهجمات السيبرانية. يجب أيضاً اتخاذ إجراءات أمنية صارمة في التحقق من هوية المستخدمين وتحديد مستوى وصلاحية الدخول إلى البيانات والشبكات ، ومن ثم تمكين الأمن السيبراني.

د- **تعدد العوامل :** هناك العديد من العوامل التي تساهم في تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعات حيث أشار الإطار النظري للدراسة إلي أن هناك العديد من العوامل التي تساهم في تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي والتي من أهمها إقامة فرق الاحتواء ، والتدقيق المستمر للنظام ، وتحليل المخاطر وبناء خطط العمل ، وتدريب المستخدمين ونشر ثقافة الوعي السيبراني.

ه- **تشجيع التعاون :** نظراً لتعرض الحواسيب والشبكات المرتبطة بالجامعات باستمرار للهجمات السيبرانية ، فإن الجامعات يجب أن تشجع على التعاون وتبادل المعلومات فيما بينها والمشاركة في النقاش الوطني بشأن تمكين السيبراني.

٢ - نتائج تتعلق بتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بالجامعة الوطنية باستراليا:

يعد تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي من الموضوعات المهمة والحرجة في العالم المعاصر، حيث تشكل الهجمات الإلكترونية على الأنظمة الحيوية والتكنولوجية تهديدًا خطيرًا ومستمرًا على كل المؤسسات والمنظمات حول العالم. ومن هذا المنطلق أصبح من الضروري بالاهتمام بتمكين الأمن السيبراني وفي ضوء مدخل الذكاء الاصطناعي لدى الجامعات والمؤسسات الحكومية والخاصة.

وتتمثل أهم النتائج البحثية التي تتعلق بتمكين الأمن السيبراني في ضوء الذكاء الاصطناعي بالجامعة الوطنية باستراليا علي النحو التالي :

أ- تعتبر الجامعة الوطنية باستراليا واحدة من أفضل الجامعات في العالم التي تهتم بتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي وتهدف إلى تطويرهما من خلال برامج الدراسة والبحث.

ب- يتم توظيف الأنظمة الأمنية للذكاء الاصطناعي بهدف تمكين الأمن السيبراني بالجامعة الوطنية باستراليا بالإضافة إلى تحليل المخاطر وتحديد أفضل الحلول والتوصيات ، كما تم الإشارة لذلك عند تناول خبرة الجامعة الوطنية باستراليا في الجزء الخاص بالخبرات.

ج- يتم توظيف الذكاء الاصطناعي في تحليل البيانات والتنبؤ بالهجمات السيبرانية المحتملة ، والقرصنة ، وتطوير أساليب الوقاية منها بالجامعة الوطنية باستراليا علي أكمل وجه.

د- يوجد لدي الجامعة الوطنية باستراليا خطة عمل فعالة وشاملة تستهدف تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي كما تم الإشارة لذلك سالفا.

ه- تتميز الجامعة الوطنية باستراليا باستدامة تطوير برامج التدريب والتعليم والتوعية للطلاب والعاملين بمدي أهمية الأمن السيبراني وتحديثها باستمرار.

٣ - نتائج تتعلق بتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي بجامعة طوكيو باليابان :

الذكاء الاصطناعي وتقنيات الحوسبة السحابية هي من بين التكنولوجيات الحديثة التي تساهم في تحسين الأمن السيبراني. ومع ذلك ، تكمن التحديات في استخدام هذه التقنيات والتأكد من أنها تفي بمتطلبات الأمن السيبراني.

ومن جهة أخرى، قد حظيت جامعة طوكيو باليابان بانتباه العالم بفضل نتائجها المتميزة في الكثير من المجالات الرائدة، بما في ذلك مجال الأمن السيبراني. يتم اعتماد تقنيات الذكاء الاصطناعي في تطبيقات الأمن السيبراني لتوفير خوارزميات قادرة على رصد التهديدات ومعالجتها بشكل فعال وسريع.

ومن خلال تدشين المشاريع المختلفة ، يتم تمكين جامعة طوكيو من ترسيخ مكانتها كمدير تقني معتمد لتطوير مجال الأمن السيبراني. وقد اعتمدت الجامعة مختلف التقنيات المتعلقة بالذكاء الاصطناعي، بما في ذلك تقنيات التعلم الآلي والتعلم العميق، لتصميم وتطوير أنظمة الأمن السيبراني الفعالة التي تمكنها من مواجهة التحديات الحالية.

ثانيا : الإجراءات المقترحة لتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي وخبرة الجامعة الوطنية بأستراليا وجامعة طوكيو باليابان:

هناك العديد من الإجراءات المقترحة لتمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي والجامعة الوطنية بأستراليا وجامعة طوكيو باليابان أهمها على النحو التالي:

عند الحديث عن تمكين الأمن السيبراني في ضوء مدخل الذكاء الاصطناعي وخبرة الجامعة الوطنية بأستراليا وجامعة طوكيو باليابان، تعد الأجراءات المقترحة أمرًا حيويًا ، ويمكن تناول ذلك علي النحو التالي:

١. تعزيز التوعية الأمنية: يجب تعزيز الوعي بمدي أهمية الأمن السيبراني بين الأفراد وتوعيتهم حول التهديدات المحتملة وأفضل الممارسات للتحقق من سلامة المعلومات والتحكم في الوصول إلى البيانات الدقيقة.

٢. تطوير السياسات والإجراءات: ينبغي تطوير سياسات وإجراءات فعّالة للأمن السيبراني تتناسب مع تقنيات الذكاء الاصطناعي وتعتمد على الخبرات المكتسبة من الجامعة الوطنية بأستراليا وجامعة طوكيو باليابان ، ويتضمن ذلك إنشاء قواعد بيانات تتعامل مع تحليلات البيانات وتقنيات الكشف عن التهديدات السيبرانية.

٣. استخدام التكنولوجيا الحديثة: يمكن استخدام الأنظمة الأمنية للذكاء الاصطناعي وتحليل البيانات الضخمة لكشف الهجمات السيبرانية والتنبؤ بالتهديدات المستقبلية. يمكن أيضًا استخدام الأتمتة والتعلم الآلي في مجال الأمان السيبراني لتحسين فعالية استجابة النظام واعتراض الهجمات بشكل مباشر.

٤. إقامة التعاون الدولي: ينبغي تبني نهج التعاون بين الدول والمؤسسات الأكاديمية المتخصصة في مجال الأمن السيبراني، مثل الجامعة الوطنية بأستراليا وجامعة طوكيو باليابان، لتبادل المعرفة والخبرات والممارسات الجيدة في هذا المجال. يمكن تعزيز الشراكات وتنظيم ورش العمل والمؤتمرات المشتركة لتحقيق هذا الهدف.

٥. بناء فرق عمل لتمكين الأمن السيبراني: يجب أن تتمتع المؤسسات بفرق متخصصة في الأمن السيبراني تتولى مسؤولية حماية الأنظمة والبنية التحتية من التهديدات السيبرانية. يجب توفير التدريب والتثقيف المستمر لهذه الفرق للتأكد من قدرتها على التعامل مع التحديات الحديثة

المراجع العربية :

آبادي مجد الدين الفيروز (٢٠٠٨): القاموس المحيط دار الحديث للطبع والنشر والتوزيع - القاهرة .

أحمد جلال محمود (٢٠٢٠): إثر التهديدات غير التقليدية للأمن على العلاقات الدولية المعاصرة ، مؤتمر الأمن السيبراني في الشرق الأوسط، مركز بحوث الشرق الاوسط والدراسات المستقبلية ، جامعة عين شمس.

أسماء أحمد أبو زيد علام (٢٠٢١): استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني دراسة تحليلية مقارنة ، المجلة المصرية لبحوث الرأي العام، كلية الإعلام، مركز بحوث الرأي العام ، جامعة القاهرة ، مج ٢٠ ، ع٢.

أسماء أحمد خلف حسن (٢٠٢٠): السيناريوهات المقترحة لدور الذكاء الاصطناعي في دعم المجالات البحثية والمعلوماتية بالجامعات المصرية ،المركز العربي للتعليم والتنمية ، مستقبل التربية العربية ، مج ٢٧، ع١٢٥.

أمنية عثمانية (٢٠١٩): المفاهيم الأساسية للذكاء الاصطناعي: تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال، الطبعة الأولي المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية برلين ألمانيا.

إيمان علاء الدين سليمان (٢٠٢١): الأمن السيبراني: المفهوم والتداعيات في السياسة العالمية ، قضايا ونظرات تجديد الوعى بالعالم الإسلامي والتغيير الحضاري، تقرير ربع سنوي مركز الحضارة للدراسات والبحوث ، ع ٢١.

تركي بن عيد البقمي (٢٠١٢): دور الوعي الأمني في الوقاية من الجرائم الإرهابية. رسالة ماجستير قسم العلوم الشرطية كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية.

الجامعة الوطنية أستراليا (٢٠٢١): تقرير الأمن السيبراني.

جرينبرج و بارون (٢٠١٠): الثقافة التنظيمية.

الجمعية الأمريكية للجودة (٢٠٢٢): الوقاية من الجرائم.

حسين بن سليمان بن راشد الطيار (٢٠٢٠): الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية، مجلة جامعة الطائف للعلوم الإنسانية، جامعة الطائف السعودية، مج ٦، ع ٢١ .

حليمة حسن الفقيه ، لينا أحمد القرني (٢٠٢٣): واقع استخدام طالبات كلية الدراسات العليا التربوية بجامعة الملك عبد العزيز لتطبيقات الذكاء الاصطناعي في ضوء بعض المتغيرات، مجلة العلوم التربوية والنفسية، المركز القومي للبحوث غزة، مج ٧، ع ١.

حنين جميل أبو حسين (٢٠٢١): الإطار القانوني لخدمات الأمن السيبراني: دراسة مقارنة ، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط ، عمان، الأردن.

خالد مخلف الحنفاوي (٢٠٢١): التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت، المجلة العربية للآداب والدراسات الإنسانية المؤسسة العربية للتربية والعلوم والآداب ،مصر ، ع ،١٩.

عبدالله الخالدي ، ونورة العضيبي (٢٠١٨): "أبعاد تكنولوجيا الذكاء الاصطناعي: الحالة الأسترالية."

رشا عبد القادر محمد الهندي (٢٠٢١) : تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول ، مجلة جامعة الفيوم للعلوم التربوية والنفسية ، كلية التربية ، جامعة الفيوم ،مج ١١ ، ع ١٥.

رمضان محمد السعودي (٢٠٢١): تقنيات الذكاء الاصطناعي ودورها في التحول التنظيمي للجامعات المصرية: دراسة تطبيقية على جامعة كفر الشيخ، سيناريوهات مقترحة، مجلة الإدارة التربوية، الجمعية المصرية للتربية المقارنة والإدارة التعليمية، ع٣٢.

رياض زروقي، ، أميرة فالتة (٢٠٢٠) : " دور الذكاء الاصطناعي في تحسين جودة التعليم العالي- المجلة العربية للتربية النوعية - مج (٤) - ع (١٢)- المؤسسة العربية للتربية والعلوم والآداب - دار المعارف المصرية – القاهرة.

سعيد عبد اللطيف حسن (٢٠١٧): اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت دار النهضة العربية للنشر والتوزيع ، القاهرة، ط ٤.

سلمان العتيبي (٢٠٢٢): "أمن البيانات الإدارية في الجامعات: الضرورة والتحديات والحلول"، دراسات الأعمال الإلكترونية والتطبيقية، المجلد ٨، العدد ٢.

سهام العايب (٢٠١٩): استخدام الخوارزميات الجينية كإحدى تقنيات الذكاء الاصطناعي في مجالي الاقتصاد وإدارة الأعمال. كتاب جماعي بعنوان : تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال، الطبعة الأولي، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية برلين، المانيا.

صلاح الدين محمد توفيق ، شيرين عيد مرسي (٢٠٢٣): متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمية من وجهة نظر أعضاء هيئة التدريس ، جامعة بنها أنموذجا ،المجله التربوية ، كلية التربية جامعة سوهاج ، ج١٠٥.

عادل عبد النور بن عبد النور (٢٠٠٥): مدخل إلى عالم الذكاء الاصطناعي ، مدينة الملك عبد العزيز للعلوم والتقنية - المملكة العربية السعودية .

عبد الجواد السيد بكر (٢٠٢٠): سياسات الذكاء الاصطناعي في نظم التعليم وجهة نظر في رأي - ورقة عمل مقدمة إلى المؤتمر العلمي السابع والعشرين نظم التعليم قبل الجامعي في الوطن العربي وإدارته الفرص والتحديات في يناير ٢٠٢٠ - الجمعية المصرية للتربية المقارنة والإدارة التعليمية - كلية التربية - جامعة عين شمس.

عبد الجواد السيد بكر ، محمود إبراهيم عبد العزيز طه (٢٠١٩) : الذكاء الاصطناعي: سياساته وبرامجه وتطبيقاته في التعليم العالي: منظور دولي ، جامعة الأزهر - مجلة كلية التربية، ج ٣ ، ع١٨٤.

عبد العال عبد الناصر طنطاوي ، وساميول المطراوي (٢٠٢٠): "تقنيات الذكاء الاصطناعي وتطبيقاتها في مجالات الحاسوب." مجلة بحوث العلوم الهندسية ٢.١٧.

عبد الكريم سلمان اللصاصمه ، فايز عبد القادر مناور (٢٠٢٢) : الأدوار الأكاديمية والتوعوية للجامعات الأردنية الرسمية نحو أمن المعلومات الإلكترونية من وجهة نظر أعضاء هيئة التدريس فيها، مجلة كلية الآداب ، جامعة عين شمس ، مج ٥٠.

عبدالرازق السنهوري (١٩٥٠): المدخل في دراسة القانون ، ١٩٥٠.

عبير أحمد علي كاعوه (٢٠٢٠): سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية مجلة كلية التربية، جامعة حلوان، مج ٢٦، ج٣.

علاء عفت،ومحمود بدوي (١٩٨٤): "أمن المعلومات وتحديات الأمن السيبراني." مجلة البحوث العلمية بجامعة بدر ١.٩.

على الدين هلال (١٩٨٤): الأمن القومي العربي القاهرة ، مجلة شئون عربية، العدد ٢٥ .

عمار ياسر البابلي (٢٠٢٠): أمن الفضاء الإلكتروني ، معهد الدراسات العربية، جامعة الدول العربية، القاهرة.

عهود أحمد الغامدي (٢٠٢١): الأمن السيبراني في تحقيق الميزة التنافسية دراسة ميدانية على موظفي مطار الملك عبد العزيز الدولي بجدة، مجلة العلوم الإقتصادية والإدارية والقانونية المركز القومي للبحوث غزة، مج ٥ ، ع ٩.

اللجنة الأمنية للجامعة الوطنية أستراليا (٢٠٢٠): خطة الأمن السيبرانيي.

لووران بروبست وآخرون (٢٠١٨): استشراف مستقبل المعرفة"- تقرير من خلال الشراكة بين مؤسسة محمد بن راشد آل مكتوم للمعرفة والمكتب الإقليمي للدول العربية / برنامج الأمم المتحدة الإنمائي – الإمارات.

المجلس الأعلى للأمن السيبراني (٢٠١٧): الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧ -٢٠٢١م)، رئاسة مجلس الوزراء القاهرة، جمهورية مصر العربية.

المجلس الأعلى للأمن السيبراني (٢٠١٧): الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧/٢٠٢١م)، رئاسة مجلس الوزراء القاهرة، جمهورية مصر العربية.

محمد أبو القاسم الرتيمي (٢٠٠٢): البنية التحية لتقنية المعلومات ومستقبل التعليم، قسم الحاسوب، جامعة السابع من أبريل. ج.م.ع.

محمد بن عبدالرحمن الفريدي (٢٠١٦): متطلبات تحقيق أبعاد الأمن الفكري.

محمد رفيق عمر (٢٠٢١): "الأمن السيبراني في الحياة الجامعية: خيارات واقعية لضمان الأمن والخصوصية"، المؤتمر الدولي للتعليم العالي المتميز للجيل السابع.

محمد عبدالله قاريزيكس (٢٠٢٢): "تحديات الأمن السيبراني في عصر المعلوماتية الرقمية" مجلة أمن المعلومات والأمن السيبراني. العدد ٢٢.

محمد علي العريان (٢٠١١): الجرائم المعلوماتية : انعكاساتها دورة المعلومات على قانون العقوبات ، دار الجامعة الجديدة ، الاسكندرية.

محمد محمود مكاوي (٢٠٠٥): البيئة الرقمية بين سلبيات الواقع وآمال المستقبل، مجلة المعلوماتية ، ع ، وكالة التطوير والتخطيط وزارة التربية والتعليم السعودية.

محمد محمود (٢٠١٩): "الذكاء الاصطناعي وأمن المعلومات"، مؤتمر الحوسبة والنظم.

محمود شريف زكريا (٢٠١٧): الحوسبة السحابية وبناء مجتمع المعرفة : رؤية استشرافية ورقة علمية منشورة ، أعمال المؤتمر الثالث والعشرون للإتحاد العربي للمكتبات والمعلومات (اعلم) بالتعاون مع وزارة الثقافة والفنون والتراث القطرية الحكومة والمجتمع والتكامل في بناء المجتماعات المعرفية العربية الدوحة - قطر ١٨ - ٢٠ نوفمبر.

محمود محمد السيد ، فيروز محمد ، فهد الرسين (٢٠١٩): "أمن المعلومات والسيبرانيات: الاتجاهات، نماذج الهجوم وتدابير الأمن." مجلة اقتصاد وتكنولوجيا المعلومات ٢.١١ .

المركز المصري للدراسات الاقتصادية (٢٠١٩): ندوة على أعتاب التغيير : التجارة والتنمية في عصر المعلومات.

معجم الجرجاني : كتاب التعريفات ٨١٦ هـ

معجم المعاني : معنى اتخاذ القرار .

المملكة العربية السعودية (٢٠٢٠): الاستراتيجية الوطنية للأمن السيبراني، نظرة عامة المركز الاعلامي للهيئة الوطنية للأمن السيبراني، الرياض، السعودية.

منال البلقاسي (٢٠١٩): الذكاء الاصطناعي صناعة المستقبل ، الحاسبات المتوازنة - التحكم الآلي ، البرمجة الوراثية ، لغة البرولوج ، الخلايا العصبية الاصطناعية - دار التعليم الجامعي – الإسكندرية.

المنظمة الدولية للمعايير (٢٠١٨): "متطلبات الأمن والخصوصية في تكنولوجيا الحوسبة السحابية"، الإصدار الثاني.

منى عبد الله السمحان (٢٠٢٠) : متطلبات" تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود " . مجلة كلية التربية ، جامعة المنصورة ، ع ١١١.

مني بنت عبد الله بن محمد البشر (٢٠٢٠): متطلبات توظيف تطبيقات الذكاء الاصطناعي في تدريس طلاب وطالبات الجامعات السعودية من وجهة نظر الخبراء مجلة كلية التربية ، جامعة كفر الشيخ - كلية التربية مج (٢٠) ، ع (٢).

منير البعلبكي (٢٠٠٤): المورد : قاموس إنجليزي - عربي دار العلم للملايين ، بيروت.

الهيئة الوطنية للأمن الإلكتروني (٢٠١٩): "تقرير الأمن السحابي والذكاء الاصطناعي في الشرق الأوسط وشمال أفريقيا"، الإصدار الأول.

وفاء حسن عبد الوهاب صائغ (٢٠١٨): وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية المجلة العربية للعلوم الاجتماعية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية ، مصر ، ع ١٤ ، ج ٣.

وفاء فواز المالكي (٢٠٢٣): دور تطبيقات الذكاء الاصطناعي في تعزيز الاستراتيجيات التعليمية في التعليم العالي: مراجعة الأدبيات ،مجلة العلوم التربوية والنفسية ، المركز القومي للبحوث غزة ،مج ٧، ع٥.

وليد عبد الرحيم جاب الله (٢٠٢١): الأمن السيبراني بين الاحتكار والاستثمار، مجلة الديمقراطية، مؤسسة الأهرام، القاهرة، مج ٢١ ، ع ٨٢،.

ياسر العمري، وياسين الشريف (٢٠٢٣): " تحديات وتوجهات أمن المعلومات في الجامعات السعودية"، دراسات الأعمال والإدارة، المجلد ٧، العدد ٢.

ياسمين الكريم (٢٠٢٣) (، "تحديات الأمن السيبراني في الجامعات في العصر الحديث"، المؤتمر الدولي لأمن المعلومات والتقنية الرقمية.

ثانيا: المراجع الأجنبية :

Alattas, A. (2018): A Review of Cybersecurity Behavioural Analytics Approaches. The Computer Journal, Vol. 61, No. 12.

Afify, A. I.; Mashhour, A. S. and Hammad, S. E. (2018): The future of artificial intelligence in Egypt. International Journal of Intelligent Computing and Applications, 11(2).

Ahmadian, A. and Zawoad, S (2021): Artificial Intelligence for Cybersecurity: Recent Advances, Challenges, and Future Directions. IEEE Security & Privacy, 19(2).

Ahmed, S. and Lee, D. (2023): A survey on the adoption of artificial intelligence in university cybersecurity programs. Proceedings of the International Conference on Cyber Security and Protection (ICCS&P 2023).

Aiyed S. A. (2020): The Future of Higher Education in the Light of Artificial Intelligence Transformations",International Journal of Higher Education, Vol. (9), No. (3).

Akbar, M. and Gao, J. (2019) :Artificial Intelligence in Cyber Security: A Review. Cybersecurity, 2(1).

Alfandi, O. O. and Alhaboby, Z. I. (2019): Cloud Computing Security and Privacy Challenges and Hindrances-Review and Analysis. Journal of Information Sciences and Computing Technologies, 2(2).

Ali, S. A. and Elhoseny, M. (2020): Artificial intelligence in cybersecurity: Challenges and solutions. Computers & Electrical Engineering, 85.

Aljohni, W.; Mohamed, N. E.; Jarajreh, M. and Gasmelsied, M. (2021): Cybersecurity Awareness Level: The Case of Saudi Arabia University Students, International Journal of Advanced Computer Science and Applications 12(3).

Alkhatani, N. (2021):Security awareness model for digital transformation in 96 Raqi high schools. Security Awareness Model for Digital Transformation in Saudi High Schools.

Al-Mayadhmi, M. S. and Al-Qudsi, H. A. (2021): Cybersecurity and advanced firewalls: Review. Iraqi Journal of Information Systems and Computing, 1(1).

Almorsy, M. (2018): Sitalakshmi Venkatraman, and Salmin Sultana.: "Automated Penetration Testing: A survey." arXiv preprint arXiv:1806.04927.

Alshammari, M. Kim, M. A. Al-Khasawneh and A. Al-Faries (2018): "Cloud computing security issues in Saudi Arabia: Systems, solutions and recommendations," Sixth International Conference on Digital Information, Networking, and Wireless Communications, Riyadh.

Artificial Intelligence and Its Impact on Employment and Economy in UAE, Saudi Arabia, and Australia: A Comparative Review" ،Proceedings of the International Conference on Future Networks and Distributed Systems, 2018

Asghar, S. H. and Rehman, H. U. (2019): Role of artificial intelligence in cyber security. Journal of Cyber Security Technology, 3(1).

Australian Computer Emergency Response Team ACERT (2021): "Automated Intrusion Detection and Prevention Systems.

Australian Computer Society (2018): Artificial Intelligence and Machine Learning: Principles. Sydney: Australian Computer Society.

Berg, S. V. (2019) : Best practices in regulating State-owned and municipal water utilities,2013

Beyond DLP: UEBA Comes of Age." Information Week.

Black, J. (2018): "The cyber risk landscape: how artificial intelligence could safeguard businesses against emerging threats." Cybersecurity: A Business Solution.

Bongs L. , and Hanan Tmouche (2023): The Impact of Artificial Intelligence On Higher Learning,Institutions,International Journal of Education, Teaching, and Social Science IJETS e-ISSN: 2809-0489,Vol 3 No 2.

Cai, Y. and Wang, T. (2020):Deep Coalesced Network for Intrusion Detection. IEEE Access.

Chen, H.; Ishigaki, K.; Fang, F. C. and Otsuka, A. (2017): Geographic Distribution of GigaPOP Nodes in Internet Service Providers. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) , IEEE.

Cheng-Jian L. and Shih-Jen H. (2021): "Application of artificial intelligence in university security", 1st International Conference on AI and Cloud Computing (AICCC).

Chen, A. and B. Mao (2017): "Security and privacy in cloud computing: A survey," Sixth International Conference on Measuring Technology and Mechatronics Automation, Zhangjiajie.

Choo, K.K. R. (2023): Artificial intelligence and cybersecurity in universities: challenges and opportunities. Journal of Cybersecurity Education, 3(1).

Chowdhury, N. and Abawajy, J. H. (2018):"Artificial intelligence-based cybersecurity for the Internet of Things: models, algorithms and evaluation." ACM Transactions on Privacy and Security (TOPS), 21(1).

Christopoulos, I.; Tsalamanis, D.; Kounelis, N. V.; Karadimas and S. A. Karkanis (2017): "Decision Making in Intrusion Detection Systems: Review and Research Trends," in IEEE Access, vol. 5

Deakin University (2021): Artificial Intelligence and Cyber Security. Retrieved from https://www.deakin.edu.au/research/story?story_id=2021/02/16/artificial-intelligence-and-cyber-security. DOI: 10.31695/IJERAT.2020.3612 E-ISSN: 2454-6135

Dumitru, G. C.; Ghiba, R. C. and Blaj, M. A. (2017): Cyber Security in Higher Education Institutions. Acta technica Napocensis: Academic Journal of Electrical Engineering, Electronics, and Computer Science.

Egyptian Ministry of Communications and Information Technology (2019): National Cyber Security Strategy 2019-2023.

Elana Z. (2019): Artificial Intelligence in Higher Education: Applications, Promise and Perils, and Ethical Questions, Imrsquid /Gtty Images, University School of Law, New York.

Elbashir, M. Z. and Abdel-Aziz, A. H. M. (2020): Cybersecurity Education and Awareness in Egyptian Universities: Challenges and Opportunities. International Journal of Computer Science and Network Security, 20(11).

El-Masry, A. A.; Ghoneim, A. and Al-Tarawneh, H. (2020): Cyber Security Education in Egyptian Higher Education Institutions. Journal of Information Security and Cybercrimes, 13(1).

Elragal, A. and Teixeira, N. M. (2021): A framework for cybersecurity practices in higher education institutions. Education and Information Technologies, 26(3).

Emilia B. (2018): A Short History of Artificial Intelligence, accessed date 8/8/2023 ,Intelligence, Future Horizons Journal, Vol. (20), No. (11).

Ezzat, H. A. and Sharaf, A. M. (2019): Artificial Intelligence for Sustainable Development in Egypt: Opportunities and Challenges. In 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0578-0583). IEEE.

Feng, Y., Shi, Q. and Zhang, Y. (2020): Design and Implementation of Honeypot Technology in Cloud Computing. Journal of Intelligent & Fuzzy Systems, 38(6).

Fouad Noran Shafik (2021) : Securing higher education against cyberthreats: from an institutional risk to a national policy challenge, Journal of Cyber Policy, 10.1080/23738871.2021.1973526 6:2.

Fujiwara, H. and Nakayama A. (2016): HSecurity Management for Cloud Environment at the University of Tokyo. 2016 15th IEEE/ACIS International Conference on Computer and Information Science (ICIS).

Ghorbani, M. A. Alazab, R. Acarman and M. Hayes (2019): "Cloud computing security: A systematic literature review," 2019 IEEE Conference on Information and Communication Technology, Istanbul.

Gupta, A. and Singh, P. (2023) :Machine learning-based anomaly detection for securing university networks against cyber threats. Journal of Information Assurance and Cybersecurity, 9(2).

Abeer, F. Zohair, and S. Hussam (2020): Deep Learning-Based Intrusion Detection System: A Comprehensive Review. IEEE Access, Vol. 8.

Takeuchi, M. Ohki, Y. Oda, and Y. Watanabe (2018): "AI-Assisted Automatic Vulnerability Detection Using Machine Learning." 2018 IEEE International Conference on Software Quality, Reliability and Security (QRS).

Hashim, H., Kasim, N. F. M.; Ibrahim, R. and Rahman, S. A. (2020): Developing Online Cybersecurity Training Course for Higher Education Institutions Employees. Journal of Physics: Conference Series.

Hassan, A.; Ahmed, M. and Ali, M. (2021): Cybersecurity challenges and potential countermeasures in educational institutions. Journal of Advanced Research in Dynamical and Control Systems, 13(3).

Hindawi, A. (2021):Cybersecurity Threats and Challenges: Emerging Trends and Countermeasures. Retrieved 15 August 2021, from https://www.hindawi.com/journals/scn/2021/9947569/.

Robert A. (2012): Individuals, relationships and culture: Links between ethology and the social sciences. CUP Archive.

Hu, Q.; Dinev, T.; Hart, P. and Cooke, D. (2012): Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4).

Hu, W. and Tan, C.C. (2015) : Intrusion Detection and Prevention. London, UK: Springer Science & Business Media.

Ilkka Tuomi (2018): "The Impact of Artificial Intelligence on Learning, Teaching, and Education", this publication is a Science for Policy report, the Joint Research Centre (JRC),the European Commission's.

Ishaq, A. M. (2020): Novateur Publicaion: International Journal of Innovations in Engineering Rrsearch and Technology [IJIERT]ISSN: 2394-3696 Website: ijiert.org V.7, ISS. 9, Sep.- ,ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY.

Izumida, T. and Tokuda, H. (2018): Security as a service: Implementing a complete virtual security operation center for an academic network. Future Generation Computer Systems, 88.

Hasegawa, S. Nakayama, and K. Sakurai (2019): "Visualization and Interpretation of Network Security Inspection Results with Convolutional Neural Networks." Proceedings of the 2019 IEEE Symposium Series on Computational Intelligence (SSCI).

Kankanamge, T. W. and Warren, M. (2018): Cybersecurity management in higher education institutions: A review of literature. The Journal of Enterprise Information Management, 31(5).

Kim, Y. and Park, S. (2023): Applications of natural language processing in enhancing university cybersecurity. Proceedings of the International Conference on Artificial Intelligence and Cybersecurity (AICS 2023).

Klutka Justin, Ackerly Nathan, Magda Andrew J. : Artificial intelligence in Higher Education Current Uses and Future Applications, Wiley brand, United States of America,2018.

Kourdi, M. and Alsaidan, S. (2020): Artificial intelligence and cyber security: challenges and opportunities. Journal of Information Security, 11(1).

Kriti K. (2018): Brian Stewart, Anshuman Khare: Artificial Intelligence and the Student Experience: AnInstitutional Perspective", IAFOR Journal of Education, Vol. 6 - Issue 3.

Kshetri, N. (2019): "Artificial intelligence initiatives in cybersecurity." Journal of Business Research, 98.

Lakshit Malhotra, Bharat Bhushan (2021):Artificial Intelligence and Deep Learning-based Solutions to Enhance Cyber Security,INTERNATIONAL CONFERENCE ON INNOVATIVE COMPUTING AND OMMUNICATION ,ICICC.

Li, X.; Shen, J. and He, W. (2020): "Anomaly detection in network security based on bidirectional long short-term memory for industrial Internet of Things." IEEE Access, 8.

Liu, J.; Shu, T.; Yang, W. and Ding, Y. A. (2018): Novel intrusion detection model based on machine learning algorithms in the Internet of Things system. Future Generation Computer Systems, 86.

Lo, K., Chandra, A. and Harris, S. (2021): Artificial intelligence in higher education: What can we learn from a review of AI applications in e-learning?. International Journal of Educational Technology in Higher Education, 18(1).

Okada and T. Miyajima (2019): "Security Improvement in Web Applications using Automatic Vulnerability Detection System." 2019 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN).

Matsuda, S. Goto, A. Kakei and H. Sato.(2019): Anomaly Detection in Intrusion Detection System using Machine Learning. Journal of Information Processing, 27.

Matthew N. (2020): Artificial Intelligence in Cyber Security International Journal of Engineering Research and Advanced Technology (IJERAT) Volume.6, Issue 5 .

Mirza, A. M. (2021): Abbas, H..: Cloud Computing Security Challenges and a Hybrid Encryption Technique. Future of Computing and Communications.

Mohanty, S. and Chaki, R. (2018): Cloud Computing Security: Challenges and Remedies. In Handbook of Research on Cloud Computing and Big Data Applications in IoT (pp. 52-73). IGI Global.

Mohamad et al. Machine Learning Techniques for Intrusion Detection System: A Comprehensive Survey. IEEE Access, vol. 7, 2019.

Mudit Verma (2018): Artificial intelligence and its scope in different areas with special reference to the field of education", International Journal of Advanced Educational Research, VOL (3), Issue (1), India.

Murakami, T. and Suga, Y. (2017) :Security Measures for Cloud at the University of Tokyo. IEICE Transactions on Information and Systems, E100.D(7).

Narumiya, M., Ishibashi, Y., and Tanabe, Y. (2020): Development of cyber security education and training system with a cyber range at the University of Tokyo. IEICE Transactions on Communications, 103(4).

Nils J. Nilsson (2008): The Quest for Artificial Intelligence: A History of Ideas and Achievements (Cambridge, UK: Cambridge University Press, 2010 Hamadoun.: Cyber security, Geneva: International Telecommunication Union (ITU).

Onuma, Y. and Akiyama, H. (2019): Detection of Bank Account Fraud with Ensemble Learning by Feature Importance Analysis. Mathematics, 7(9).

Peng, J.; Li, T.; Li, R.; Guo, Y.; Liu, Y. and Lai, X. (2019): Automated Penetration Testing for Web Applications: A Survey. Journal of Network and Computer Applications, 125.

Popenici Stefan A. D and Kerr Sharon (2017): "Exploring the impact of artificial intelligence on teaching and learning in higher education", Office of Learning and Teaching, Charles Darwin University, Australia.

Raghav Sandhane: Artificial Intelligence in Cyber Security ,July Journal of Physics Conference Series 1964(4):042072,DOI:10.1088/1742-6596/1964/4/042072,2021

Rastogi, M., and Mishra, P. (2016): Intrusion detection system based on deep-learning classifier. Procedia Computer Science.

Saxena, S. Raj and N. Agrawal, "Behavior-based cyber-attack detection," Computers & Security, vol. 57, 2016.

Saeed, N., Naeem, M. and Riaz, Z. (2018): Applications of artificial intelligence for cyber security: A review of trends from literature. Journal of Computer and Communications, 6(8).

Sahlin, R. K. (2018): The ethics of artificial intelligence in cyber security. Journal of Information Warfare, 17(1).

Samaniego, J. A. and Alfaro, E. (2019): "Intelligence and Security in Artificial Intelligence: A Survey." In 23rd International Conference on Information Fusion (FUSION), IEEE.

Sato, K. (2022): "The Role of Artificial Intelligence in Cybersecurity: A Case Study at the University of Tokyo." International Conference on Cybersecurity and Data Privacy.

Sato, N. and Seki, H. (2014): Evaluation of the Information Security Management System in the Cloud Computing Environment of a University. Journal of Information Processing, 22(2).

Seraj, A. (2018) Cyber attack detection using machine learning algorithms. Journal of Jomard Publishing.

Shabir, M. (2020): Cybersecurity and Privacy - An Enterprise Side Look. Journal of Philosophy, Culture and Religion, 29(3).

Smith, J. (2018): Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

Smith, J., and Johnson, R. (2023): Enhancing cybersecurity in universities through AI-based threat detection systems. International Journal of Information Security, 21(3).

Takahashi, M. (2021): "Economic Factors in Enhancing Cybersecurity: Lessons from University Cybersecurity Initiatives in Asia." Journal of Security Engineering, vol. 15, no. 4.

Takeuchi, Y.; Shibuya, M., and Fujisaki, Y. (2017): Artificial intelligence-based intrusion detection system using support vector machines. Future Generation Computer Systems, 76.

Tan, L. P. (2019): Cybersecurity challenges in Japan: Securing the 2020 Olympic Games. Journal of Asian Security and International Affairs, 3(1).

Taniguchi, M.; Inoshita, Y.; Eguchi, H. and Yamadai, M. (2017): Design of automatic vulnerability detection system with code reviews information. In 2017 19th International Conference on Advanced Communication Technology (ICACT) IEEE.

Thierry, K. (2019): Artificial intelligence in education. The Urgent need to prepare Teachers for Tomorrow's schools", Formation et profession, 27(1).

Tshilenge, D. M.; Abbas, H.; Hu, J. and Hao, Q. (2020): A survey of current trends and possible future directions in artificial intelligence with regards to cybersecurity. Security and Communication Networks.

Varshney, S. and Sharma, P. (2018): Anomaly detection in network traffic using machine learning algorithms. Journal of King Saud University-Computer and Information Sciences, 30(4).

Wang, X.; Tsai, S. B., and Lee, C. A. (2016): cybersecurity management framework for financial institutions in Taiwan. Journal of Cybersecurity and Mobility, 4(1).

Wang, Z.; Wang, G., Wang, T. and Song, W. (2021): Host-Based Intrusion Detection System Based on Kernel Principal Component Analysis and Support Vector Machine. IEEE Access.

Watts, T. and Hare (2019): RStrategies for effective higher education cybersecurity management. Journal of Cybersecurity Education, Research and Practice.

Whitty, A. and P. O'Shea (2019): "Behavioral anomaly detection for insider threat in software development activities," Journal of Empirical Software Engineering, Vol. 23, No. 2.

Yamada, T. (2023): "Cybersecurity Challenges in the Digital Economy." Journal of Cybersecurity and Artificial Intelligence, vol. 10, no. 2, 2023.

Yan, Z., Xue, Y., & Lou, Y. (2021): Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. Computers in Human Behavior, 121 (10).

Yaqoob, I., Ahmed, E., Imran, M., & Al-Qurishi, M. (2019):Cybersecurity of Internet of Things: The Role of Artificial Intelligence. IEEE Access.

Yusuke Saito (2020): "An Overview of Tokyo: University's Cyber Security Department," International Conference on Cyber Security and Information Protection.

Zhang, W., Wu, J., Jia, F. and Lv, Y.(2021): An Improved Intrusion Detection System Based on Random Forest Algorithm. IEEE Access.

Zhang, Y., Chen, D., & Yu, H.(2019): Artificial Intelligence for Cybersecurity: A Survey. Wirtschaftsin for matik, 61(5), 531-541.

Zhang, X. Zhang, Y. Yang and Y. Liu, (2020): "Anomaly Detection Method Based on Improved Convolutional Neural Network," 2020 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC).