مجلة جامعة ام القرى للعلوم التربوية والنفسية

الموقع الإلكتروني: https://uqu.edu.sa/jep

تقييم حلول التحديات الأمنية السيبرانية للمدن الذكية السعودية من وجهة نظر المتخصصين

فهد صالح العتيبي[1*]، حسنين محمد البرهمتوشي[1]، فارس أنور كاتب[1]، ريان هشام أحمد موصلي[1]

[1]كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، جدة، المملكة العربية السعودية.

تاريخ التقديم: 2022/9/29 تاريخ القبول:2022/12/14

الملخص:

يُعد الأمن السيبراني أحد الركائز الرئيسة للمدن الذكية السعودية وفق رؤية المملكة 2030م. ولذلك سعي البحث إلى تقييم مدى مناسبة بعض الحلول التشريعية، والتثقيفية، والأخلاقية في مواجهة التحديات الأمنية السيبرانية المهددة لأمن المدن الذكية من وجهة نظر المتخصصين .واستهدف البحث تحديد تلك التحديات، وبيان الحلول المقترحة لمواجهتها، والرؤى التقييمية لها من وجهة نظر المتخصصين، والمساهمة في مواجهتها باقتراح مشروع تثقيفي في هذا المجال. واتبع البحث المنهج الوصفي التحليلي، حيث أعدت استبانة لتعرف الآراء التقييمية للحلول التشريعية، والتثقيفية، والأخلاقية لمواجهة التحديات السيبرانية المهددة لأمن المدن الذكية من وجهة نظر المتخصصين. ووزعت على عينة شملت (40) من أعضاء هيئة التدريس. منهم (25) من الذكور و (15) من الإناث. وأظهرت النتائج التقييمية مناسبة الحلول بمتوسط نسبي بلغ 95.7٪7، وكانت نسبة الحلول الأخلاقية 96.0٪. تلتها الحلول التثقيفية بنسبة 95.92٪، ثم الحلول التشريعية بنسبة 95.3٪. وللمساهمة الإجرائية في مواجهة تلك التحديات؛ تم تقديم (13) توصية إجرائية، كما تم وضع إطار تنفيذيا لمشروع تثقيفي مقترح وفقا لتوجهات الرؤية الاستراتيجية لجامعة الملك عبد العزيز، ورؤية المملكة العربية السعودية 2030م.

الكلمات المفتاحية: التقييم، التحديات، الأمن السيبراني، المدن الذكية.

Assessment Solutions to Cyber Security Challenges for Saudi Smart Cities from the Point of View of Specialists

Fahd S. Alotaibi[1*], Hassanin M. Al-Barhamtoshy[1], Faris A. Kateb[1], Rayan H. Mosli[1]

[1]Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

Received:29/9/2022 Accepted: 14/12/2022

Abstract:

Cybersecurity is one of the main pillars of Saudi smart cities, according to the Kingdom's Vision 2030. Therefore, the research sought to assess the appropriateness of some legislative, educational, and ethical solutions in facing cybersecurity challenges that threaten the security of smart cities from the perspective of specialists. The research aimed to identify these challenges, indicate the proposed solutions to confront them, evaluate them from the viewpoint of specialists, and contribute to facing them by proposing an educational project in this field. The research followed an analytical descriptive approach, as a questionnaire was prepared to identify the evaluative opinions of the legislative, educational, and ethical solutions to face cyber challenges threatening the security of smart cities from the specialists' point of view. It was distributed to a sample of 40 faculty members, 25 males and 15 females. The evaluation results showed the appropriateness of the solutions with a relative average of 95.77%, and the percentage of ethical solutions was 96.0%. This was followed by educational solutions with a percentage of 95.92%, then legislative solutions with a percentage of 95.3%. Regarding the procedural contribution to facing these challenges, 13 procedural recommendations were presented, and an executive framework for a proposed educational project was developed in accordance with the directions of the strategic vision of King Abdulaziz University and the Vision of the Kingdom of Saudi Arabia for 2030.

Keywords: Assessment, Challenges, Cyber Security, Smart Cities.

Doi: https://doi.org/10.54940/ep31011619

*معلومات التواصل : د. فهد بن صالح العتيبي

البريد الالكتروني الرسمي : fsalotaibi@kau.edu.sa

الإطار العام للبحث

تتزايد تهديد الهجمات السيبرانية للمدن الذكية في ظل اتصال مليارات الأفراد حول العالم بشبكة الإنترنت، عبر منصات الخدمات والأجهزة الجوالة، وقد نوقشت هذه التهديدات في مجالس المستقبل العالمية؛ التي نظمتها بعض دول الخليج بالشراكة مع منتدى "دافوس" الاقتصادي العالمي؛ وما ترتب عليها من انعكاسات تأثيرية في عصر الثورة الاصطناعية للذكاء، وكيف يمكن للأمن السيبراني أن يكون عاملاً أساسياً في رسم ملامح هذه المرحلة من مستقبل الإنسان. وأكدت التوصيات أهمية الأتمتة للحفاظ على سلامة البيانات، وثقة المستخدمين للتكنولوجيا في العصر الرقمي. حيث تلحق التهديدات السيبرانية أضراراً كبيرة في البيانات الرقمية التشغيلية لإدارة المرافق الخدمية للمدن الذكية، ويشمل ذلك: الكهرباء، والخطوط الجوية، التي يتسع نطاق تهديداتها بفعل إنترنت الأشياء، حيث يستخدمه القراصنة في إطلاق هجمات أشد ضراوة وتهديدا للمعلومات الشخصية المخزنة في الفضاء الإلكتروني، وانتهاك الخصوصية، والحقوق، والحريات. ولذا فإن تحديات الأمن السيبراني تستوجب رفع مستوى الوعي التشاركي بين الشركات والحكومات، وعدم قصر ذلك على قطاع تكنولوجيا المعلومات. وتضمنت توصيات مؤتمر "كوالس الأمني" حلولاً مقترحة لأمن معلومات المدن الذكية، كان من أبرزها توفير قاعدة أمنية فعالة وحلول امتثالية.

مقدمة

ودمج تقنية حماية التهديدات Protect Threat في بنية المنصات السحابية للمدن الذكية. (دنيا الوطن، 2016).

وتتزايد تحديات الأمن الإلكتروني السيبراني وتهديداته بتزايد اعتماد الأشخاص على التكنولوجيا الحديثة، حيث ترتب على ذلك زيادة معدلات اختراق أمن الشركات، والتصيّد الاحتيالي، وممارسة الابتزاز، والنصب والاحتيال عبر وسائل التواصل الاجتماعي، وتوزيع المواد الإباحية للأطفال والأحداث ومؤامرات استغلالهم، كما تزايدت أضرار التعطيل والتدمير المهددة للبنية التحتية الأساسية الحيوية، مما ينعكس أثره على سلامة كل مناحي الحياة (باسم، 2018).

وثمة إرشادات خاصة بالأمن السيبراني لتحديد البيانات والعمليات الحرجة الأكثر أهمية اللازم حمايتها، والتهديدات التي تواجهها، والمخاطر والأضرار المحتملة. وتعدد الإجراءات والحلول الوقائية للتخفيف من أضرار هذه التهديدات الأمنية الإلكترونية (مجتمع تكنولوجيا المعلومات، 2019).

كما تتنوع تحديات الأمن الإلكتروني الشائعة والتهديدات السيبرانية للمدن الذكية، ويشمل ذلك: البرمجيات الخبيثة، والتصيد Phishing، وحصان طروادة Trojans، وهجمات الفدية Ransomware، وهجوم رفض الخدمة الموزع (DDoS)، والهجمات على أجهزة إنترنت الأشياء (IoT)، وخروقات البيانات، والبرامج الضارة بتطبيقات الهواتف المحمولة (مجتمع تكنولوجيا المعلومات، 2019).

ويُعد تأمين إدارة سيل البيانات المتولدة من التحديات التي تواجه أمن المدن الذكية، حيث يلزم إجراء تحليلات فعالة لبياناتها الضخمة، لمعرفة السلوك وتفاعلاته، وسلامة الأنظمة الفيزيائية السيبرانية (CPS) وموثوقيتها. وذلك لتوفير وظائف جديدة، وخدمات متعددة منها: الرعاية الصحية الشخصية، والاستجابة لحالات الطوارئ، وإدارة تدفق حركة المرور، والتصنيع الذكي، والأمن الداخلي، وإدارة إمدادات الطاقة، لتحسين نوعية الحياة، وتوفير السلامة التأمينية العامة لمشاريع المدن الذكية (أمن المدن الذكية،2020; UCLG, 2020).

وتناولت دراسة Chen (2021) المكونات الأربعة الرئيسة للمدينة الذكية، وهي: الشبكة الذكية، والمباني الذكية، ونظام النقل الذكي، والرعاية الصحية الذكية. وناقشت طريقتين من طرق التعلم العميق، وبرامج الأمن السيبراني، وأوضحت أن العديد من المدن حول العالم تميل إلى استخدام التقنيات الجديدة لتصبح مدينة ذكية لتحسين جودة حياة المواطنين إلا أن استخدام أي تقنية يثير قضايا وتحديات جديدة، حيث يمكن أن تتعرض المدينة بأكملها للخطر؛ نظرًا لاعتمادها الكبير على تكنولوجيا المعلومات والاتصالات، مما يعرضها لتحديات الأمن السيبراني (مثل تسرب المعلومات، والهجمات السيبرانية الخبيثة). وأظهرت الدراسة الحلول الوظيفية الفعالة في الحفاظ على الأمن السيبراني وخصوصية المستخدم في المدن الذكية، وكان من أهمها وجوب مواجهة التحديات السيبرانية بالعمل الجاد للحكومات، ومطوري البرمجيات والشركات التي تقدم خدمات الأمن المعلوماتي التكنولوجي للمدن الذكية.

إن التقنيات الحديثة لديها إمكانات عالية في مجال الحوسبة الكمية، لحل المشاكل المعقدة من خلال ما يسمى بالذكاء الاصطناعي وإنترنت الأشياء. ومن ثم الاهتمام بالبنية التحتية في المدن الذكية. في الواقع، تعد المدن الذكية حقيقة يقوم على أساسها استخدام بنى تحتية تقنية لتقليل استهلاك الطاقة وتقليل انبعاثات ثاني أكسيد الكربون وزيادة جودة حياة السكان. فالمعايير التي تعمل على تأهيل المدينة كمدينة ذكية هي التزامها بالبيئة، وتخطيطها الحضري، وإدارتها العامة، وآليات النقل والتنقل، وجهودها لتسهيل الاستثمارات البشرية والاقتصادية لتحسين جودة الحياة فيها. باتباع مفهوم المدينة الذكية، ولقد تم تقديم فكرة المنزل الذكي على أنها تتضمن نظامًا يسمح بأتمتة العديد من المهام، بالإضافة إلى التحكم الكامل والمباشر فيما يحدث في هذا المنزل (Kaluarachchi, 2022; Desouza et al., 2020).

لقد ساهم اتساع نطاق الفضاء الإلكتروني في تزايد التحديات التصميمية والتشغيلية المهددة للأمن الإلكتروني للمدن الذكية، وأسفر عن تهديدات

ومخاطر تدميرية متعددة، نجمت عن حرية السماح للمستخدمين بالوصول إلى كافة موارد بيانات الشبكة الداخلية للمدن (الإنترانت)، أو دخولهم إلى النظم التقنية لإدارة خدماتها عبر الفضاء الإلكتروني الخارجي (الإنترنت). مما ترتب عليه العديد من التحديات والتهديدات الأمنية الإلكترونية منها: الانتحال، والتلاعب، وتجاوز الصلاحيات، والتصيد الاحتيالي، والاحتيال المصرفي. وثمة تزايد لحجم تحديات الأمن للمدن الذكية بتزايد أعداد الأجهزة المتصلة بالشبكات الداخلية والخارجية، وتستمر هذه التهديدات في خطورتها نظرا لمواصلة مجرمي الإنترنت ابتكار أساليب جديدة، يسيئون بها استخدام تكنولوجيا المعلومات، ويتحايلون باحترافية على اختراق ثغرات النظم الإلكترونية.

مشكلة البحث وأسئلته

تواجه المدن الذكية السعودية العديد من التحديات الأمنية السيبرانية التي تهدد أمنها وسلامتها، مما يترتب عليه تهديدات ومخاطر وتحديات أمنية متعددة تضر بالفرد والمجتمع. ويتطلب مواجهة تلك التحديات إجراء تقييم للحلول المتعددة لمواجهتها، من وجهة نظر المتخصصين. ومن ثم؛ تحددت مشكلة البحث في السؤال الرئيس التالي:

كيف يمكن تقييم التحديات الأمنية السيبرانية للمدن الذكية السعودية والحلول المناسبة لها من وجهة نظر المتخصصين؟

وتتطلب الإجابة عن هذا السؤال الرئيس إجابة الأسئلة الفرعية التالية:

1- ما التحديات السيبرانية التي تهدد أمن وسلامة الأفراد في المدن الذكية؟

2- ما الحلول المقترحة للتحديات السيبرانية المهددة لأمن وسلامة الأفراد في المدن الذكية؟

3- ما الرؤى التقييمية لحلول تحديات الأمن السيبراني للمدن الذكية من وجهة نظر المتخصصين؟

4- ما التصور المقترح لمشروع تثقيفي للمساهمة في مواجهة تحديات الأمن السيبراني للمدن الذكية؟

أهداف البحث

يتمثل الهدف الرئيس للبحث في تقييم التحديات الأمنية السيبرانية للمدن الذكية السعودية وحلولها من وجهة نظر المتخصصين، ويمكن أن يتحقق ذلك بتحقق الأهداف التالية:

1- تحديد التحديات السيبرانية التي تهدد أمن وسلامة الأفراد في المدن الذكية.

2- بيان الحلول المقترحة للتحديات السيبرانية المهددة لأمن وسلامة الأفراد في المدن الذكية.

3- توضيح الرؤى التقييمية لحلول تحديات الأمن السيبراني للمدن الذكية من وجهة نظر المتخصصين.

4- تقديم تصورا مقترحاً لمشروع تثقيفي للمساهمة في مواجهة تحديات الأمن السيبراني للمدن الذكية.

أهمية البحث

نظراً لما تحظى به التحولات التكنولوجية للمدن العربية من اهتمامات لتكون مدنا ذكية تتسق مع توجهات التنمية المستدامة الآنية والمستقبلية، فإن تدارس التحديات الأمنية السيبرانية التي تهدد أمن المدن الذكية أصبح من أولويات التخطيط الاستراتيجي للمستقبل، ويكتسب ÷ذا البحث أهميته من هذا التوجه الاستراتيجي. مما يستدعى بذل المزيد من الجهد للمساهمة في تحقيق ما يلي:

1- تعزيز جهود الشراكات المجتمعية الداعمة للخطط الاستراتيجية والتنفيذية، استشرافا لمستقبل واعد لمدن ذكية تتوافر فيها مقومات التنمية المستدامة، والقدرة على مواجهة التحديات والتهديدات الأمنية السيبرانية.

2- تزويد المسئولين عن التخطيط الاستراتيجي للمدن الذكية بأنسب الحلول لمواجهة التحديات الأمنية السيبرانية التي تهدد الأفراد في المدن الذكية.

3- التوعية المجتمعية للأفراد بالسبل المناسبة لمواجهة التحديات الأمنية السيبرانية لمدنهم، والحد من تعرض نظمها لاختراق المتسللين.

3- إفادة الباحثين في مجال الأمن السيبراني للمدن الذكية بنتائج دراسة علمية لتفعيل آليات مواجهة تحدياتها وتهديداتها.

4- تزويد المهتمين بدراسة المدن الذكية والمخاطر المهددة لأمنها السيبراني بأداة علمية مضبوطة، لتقييم أنسب الحلول التكنولوجية المقترحة لمواجهة التحديات السيبرانية المهددة لسلامة المدن الذكية.

مصطلحات البحث.

التقييم Assessment

يقصد به وصف شيء ما ثم الحكم على قبوله أو ملاءمته لإصدار أحكام بشأنه (Thorndike & Hagen, 1990)، وهو عملية للحصول على معلومات تفيد في اتخاذ القرارات وإصدار الأحكام (Terry & Tanbnnk, 1994).

التحديات Challenges

يقصد بالتحديات تلك العراقيل والصعوبات المعوقة لتحقيق الهدف، وتحول دون النهوض بالمجتمع (عبد الفتاح، 2016). وتعرف التحديات بأنها العراقيل التي تعترض الطريق وتمنع الفعل أو الحركة أو النجاح. وتشمل التحديات المشكلات الضار المزعجة problems plaguing وظيفياً وبنائياً، والصعوبات Difficulties أو العوائق Barriers والتي تقف حائلاً أمام إشباع الاحتياجات الإنسانية الأساسية (محمد، 2017). كما عرفت التحديات Challenge بأنها: "المشكلات أو الصعوبات التي تواجه الأفراد والمجتمعات والدول، وتحد أو تعوق من تقدمها، وتشكل حجرة عثرة أمام تحقيق أمنها واستقرارها ومصالحها الحيوية، ويصعب تجنبها أو تجاهلها، وقد تبدأ أو تنتهي بزوال أسباب بلوغ التحدي، دون الوصول إلى مستوى التهديد" (باله، 2020).

الأمن Security

يعرف الأَمْن بأنه حالة من الاطمئنان يشعر بها الفرد لاتباعه تدابير تحقق الحماية لنفسِه ومالِه وممتلكاته، وتجنبه التعرض لفقد ما يخاف عليه. (الدويكات، 2018). والأمن والاستقرار مصطلحان مترافِقان معاً، وانعدام الأمن يسبب الخَوف والجَزَع وعدم الاستقرار (Wordfly, 2018).

الأمن السيبراني Cybersecurity

يعرف بأنه مجموعة ممارسات لحماية الشبكات والبرامج والأجهزة والبيانات من الاختراق أو التلف أو الوصول غير المسموح به. وتشمل عناصر الأمن الإلكتروني (السيبراني) الفعال بتحقق أمن البنى التحتية، والأجهزة، والشبكات، وبرامج التطبيقات، وقواعد البيانات، والحوسبة السحابية. (مجتمع تكنولوجيا المعلومات، 2019). ويهدف إلى تأمين البيانات المتاحة على النظم الإلكترونية والأجهزة المتصلة بالشبكة العنكبوتية لحمايتها من ضرر مهاجمة المشغلين المخادعين. وتشمل عناصر تحقيقه تأمين الشبكات، والأجهزة، والتطبيقات، والبيانات، والبنى التحتية، والأنظمة السحابية، ويتطلب خطط للتعافي من كوارث الهجمات السيبرانية.

التهديدات والتحديات الأمنية الإلكترونية CybersecurityThreats and Challenges of Electronic security

التهديد كلمة مشتقة من الفعل "هدد"، ويرتبط التهديد بكل ما من شأنه أن يعرقل تحقيق الأمن، أو يؤدي إلى إنقاص الشعور به. والتهديدات الأمنية يقصد بها كل ما يهدد الأمن القومي من أعمال، أو أحداث تقلل من نوعية جودة حياة المواطنين، وتستوجب تدخل الحكومات أو الهيئات أو المنظمات غير الحكومية لمواجهتها، والحد من آثارها. ويستلزم ذلك تحديد مصادر التهديد بالخطر الأمني، واتخاذ كافة الإجراءات لتحقيق الأمن، ودرء المخاطر أو التهديدات الأمنية الفعلية أو المحتملة. ويقصد بالتحديات بها تلك العراقيل والصعوبات التي تهدد نظم الأمن الإلكتروني للشبكات، والأجهزة، والبرامج، والبيانات، ويترتب عليها تهديدات ومخاطر، نتيجة وجود ثغرات أمنية بالنظم الرقمية، يتسلل منها المهاجمون ببرمجياتهم الخبيثة، مما يلحق أضرارا متعددة بالنظم الإلكترونية. (باله، 2020)

المدينة الذكية Smart city

المدينة الذكية هي مدينة خدماتها معززة بالتكنولوجيا في سياقات من الحداثة والاستشراف، لتحقيق التنمية المستدامة والازدهار في شتى المجالات، ويتوافر فيها التنوع البيئي الرقمي المحفز للإبداع. واستخدم مصطلح المدينة الرقمية أو الذكية Digital or Smart city للمرة الأولى في المؤتمر الأوروبي للمدينة الرقمية في عام 1994م. وتتميز بجودة الحياة فيها واستدامتها. ويشمل ذلك ابتكارات تطبيقية، وتخطيطا أفضل، واستخداما ذكيا لتكنولوجيا المعلومات والاتصالات، لتحقيق جودة الأداء لجميع مجالاتها، من خلال الحوكمة، وتفاعل مشترك بين القطاع الاقتصادي، والنقل والبيئة (عنتر ومعمر، 2019). وتستخدم المدينة الذكية المعلومات وتكنولوجيا الاتصالات لتعزيز قدرتها العملية واستدامة الحياة بطريقة آمنة، من خلال: جمع معلومات عن نفسها بأجهزة استشعار وأجهزة ونظم تقنية أخرى، ونقل بياناتها عبر الشبكات السلكية واللاسلكية وتبادلها، وتحلل بياناتها ومعالجتها لتفهم ما يحدث الآن وما يحتمل حدوثه في المستقبل. (Smart city, 2020).

الحلول التكنولوجية الأمنية Technical security solutions

يقصد بها مجموعة المعالجات التقنية، والوسائل المبتكرة المقترحة لاتخاذ التدابير الأمنية، وذلك لتجاوز الثغرات المهددة لأمن النظم المعلوماتية، والحماية من المخاطر التهديدية للمتسللين إليها. ويشمل ذلك إجراء عمليات البحث الاستكشافي المستمر، لتعرف التهديدات، واتخاذ ما يلزم من إجراءات في الوقت المناسب، ويشمل ذلك كافة التدابير الأمنية اللازم اتخاذها لتجاوز الثغرات المهددة لأمن النظم المعلوماتية للحفاظ عليها من اختراق المتسللين، بإجراء عملية البحث الاستكشافي المستمر، لتعرف التحديات والتهديدات ذات الأولوية، واتخاذ الإجراءات المناسبة لحماية النظم من التعرض لتأثيرات الثغرات الأمنية (دنيا الوطن، 2016).

أدبيات البحث

صنفت أدبيات البحث تبعا لمتغيراته في مبحثين رئيسين، يتناول المبحث الأول تحديات الأمن السيبراني للمدن الذكية وتهديداتها للفرد والمجتمع. أما المبحث الثاني فيتناول حلول مقترحة لتحديات الأمن الإلكتروني للمدن الذكية وتهديداتها.

المبحث الأول: تحديات الأمن السيبراني للمدن الذكية وتهديداتها للفرد والمجتمع

سعت الدول المتقدمة إلى استحداث نظما إلكترونية لتأمين مدنها الذكية، فاستخدمت شبكات SCADA لتأمين نظم تسيير الحركة المرورية للمركبات خلال ساعات الذروة، كما وظفت الأجهزة المرتبطة بإنترنت الأشياء لتشغيل المصاعد الكهربية، وتسيير وسائل الانتقال المختلفة. واستحدثت وزارة الأمن الداخلي الأمريكية نظام "آينشتاين" لاكتشاف الهجمات الإلكترونية على النظم الإلكترونية لمدنها الذكية واختراق المتسللين لها، حيث وظفت تقنيات الذكاء الاصطناعي وخوارزمياته التطبيقية لحماية البروتوكولات المؤتمتة وعناوين IP للمستخدمين من أضرار البرمجيات الخبيثة (Jackson, 2013). وخلص مؤتمر "كوالس الأمني" المنعقد بدبي إلى أن المعضلة التي تواجه التحديات والحلول التأمينية للمدن الذكية تكمن في غياب الرؤية الشمولية والتحكم الكامل، للحفاظ على أمن نظم وبيانات المدن الذكية (دنيا الوطن، 2016).

وتتعدد تحديات الأمن السيبراني للمدن الذكية، ويشمل ذلك تعقيد

البيانات نتيجة زيادة حجم الاتصالات بين المستخدمين الذين تتزايد أعدادهم بسرعة، وتنوع التطبيقات نتيجة زيادة مستوى استخدام الذكاء الاصطناعي، مما يزيد من تعقد التحديات التأمينية للشبكات (Weiner, 2017).

كما تتعدد المخاطر المهددة للأمن الإلكتروني للمدن الذكية، ويمتد أثرها ليشمل الضوابط الآلية لحماية البنية التحتية للمدينة الذكية، حيث ساهمت الآلات التقنية المستحدثة وأنظمة الذكاء الاصطناعي وتطبيقاته في زيادة معدلات العمليات بالمدن الذكية، حيث لم تعد قاصرة على وأنظمة النقل، والشبكات الكهربائية، وأنظمة المياه والصرف الصحي، وتوزيع الغاز الطبيعي في المباني والمنازل فحسب، بل امتدت لتشمل استخدام سيارات بدون سائق، واللقاحات الذكية، وعلاج الحمض النووي لمكافحة الأمراض وأصبح من المرجح أن يكون كل شيء في العقدين المقبلين "ذكيًا" (Lee, 2017).

إن غياب السياسات الأمنية الضابطة للسلوكيات السلبية، ونقص الوعي بأساليب حماية المعلومات وتأمينها لمن أبرز التحديات التي تواجه أمن المعلومات في المدن الذكية، وتقلل من مقدرتها على حماية بياناتها. فعلى الرغم مما تتيحه الشبكات الرقمية من تيسير لأنماط التعامل في المدن الذكية، وسهولة الوصول الرقمي للخدمات، والفرص الحضرية المتطورة في مجالات متعددة منها: التعليم، والرعاية الصحية، والنقل، والطاقة والأمن على المستويات المحلية والعالمية؛ إلا أنها في الوقت ذاته تعرض السكان لمخاطر شتى ناتجة عن اختراق الحسابات وقرصنتها من المتسللين عبر الإنترنت، وتزايد المخاوف المهددة للخصوصية، والتوظيف (Pelton & Singh, 2019).

وقد ناقش مؤتمر دبي لأمن المعلومات التحديات التي تواجه المدن الذكية في الحاضر والمستقبل. وكان من أبرزها مشكلة اختراق البيانات، وتأثر مستوى الثقة لدى مستخدمي الشبكات في المدن الذكية (غاوي، 2019).

كما تشمل التحديات والتهديدات لأمنية الإلكترونية في المدن الذكية، تحديات خصوصية المستخدم وجمع البيانات، وضيق نطاق التحكم التكنوقراطي، خصخصة إدارة المدينة (عمر وريمي، 2019).

مما تقدم يتضح تعدد تحديات الأمن الإلكتروني السيبراني للمدن الذكية وتهديداتها الضارة بالفرد والمجتمع، وتم استخلاص وإيجاز أبرزها للإجابة عن السؤال الثالث للدراسة الحالية.

المبحث الثاني: إنترنت الأشياء واكتشاف الخدمات العدائية

أمن إنترنت الأشياء هو مجال تقني معني بحماية الأجهزة والشبكات والتطبيقات التقنية المتصلة في الإنترنت. تتضمن إنترنت الأشياء (IoT) عملية اتصال أجهزة الحوسبة، والآلات الميكانيكية والرقمية، والأشياء، والحيوانات، أو الأشخاص بالإنترنت. ويتم توفير معرّف فريد لكل "شيء" والقدرة على نقل البيانات تلقائيًا عبر الشبكة. يؤدي السماح للأجهزة بالاتصال بالإنترنت إلى فتحها أمام عدد من نقاط الضعف الخطيرة والتهديدات المحتملة إن لم تكن محمية بشكل صحيح. يستخدم هذا البحث، هندسة أمان ومبدئ الخصوصية لتصميم نظام بيئي آمن لإنترنت الأشياء وذلك لتنفيذ أمن سيبراني في المدن الذكية. سيركز هذا المبحث على فهم مشكلات الأمان في التقنيات التي تدعم إنترنت الأشياء وكيف يمكن تطبيقها في جوانب مختلفة. كما يؤكد على طريقة التعامل مع التحديات الأمنية لتطوير بنية تحتية آمنة لأجهزة إنترنت الأشياء. يساعد هذا البحث الباحثين والممارسين على فهم بنية الأمن السيبراني من خلال إنترنت الأشياء وأحدث ما توصلت إليه الإجراءات المضادة. كما أنه يميز التهديدات الأمنية في البنية التحتية التي تدعم إنترنت الأشياء عن شبكات البنية التحتية التقليدية أو المخصصة. كما يوفر هذا المبحث مناقشة شاملة حول التحديات الأمنية والحلول في تحديد هوية الترددات الراديوية (RFID) وشبكات الاستشعار اللاسلكية (WSNs) في إنترنت الأشياء.

استكشاف الخدمات العدائية

يؤدي الاستخدام المتزايد للإنترنت، سواء في الحياة العملية التطبيقية في المدن الذكية أو خدماتها التقنية، إلى تغيير طريقة تعلم الناس وعملهم تمامًا. ومع ذلك، فإن عدد الهجمات الإلكترونية يتزايد بنفس الطريقة. في فترة التحول الرقمي، يمكن لحادث تكنولوجي من هذا النوع أن يضع حدًا لاستمرارية هذه الخدمات التقنية. لهذا السبب، ينشأ الأمن السيبراني كمجموعة من التقنيات والعمليات المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجمات والتهديدات المحتملة.

تُستخدم خوارزميات التعلم الآلي والتعلم العميق لتحليل البرامج الضارة واكتشاف التسلل والوقاية منها (في الأمن السيبراني بشكل أساسي). لذا فإن تطوير هذه الخوارزميات مدفوع بالحاجة إلى توقع هجوم إلكتروني وتقييد الوصول إلى الملفات أو البرامج المصابة. وقد يكون خادم مقدم الخدمة DNS مصدرًا غنيًا للمعلومات حول تقنيات المدينة الذكية وخدماتها. غالبًا ما يتم تسمية إدخالات خادم (DNS) بطرق توحي بالغرض من عنوان جهاز محدد، مثل mail.example.com. يمكن أن يوفر تحليل هذه الإدخالات نظرة ثاقبة على بنية شبكة المدينة الذكية دون الحاجة إلى فحص المنافذ بشكل تدخلي وواضح للغاية. ومن ثم؛ يجب إجراء عمليات البحث واستكشاف هذه التدخلات العدائية.

فقد قام فريق البحث ببناء وبرمجة آلية تقنية للبحث في سجلات خادم المجال (DNS) عبر بروتوكولات عناوين الإنترنت IP Address لاستكشاف واستطلاع أي هجوم عدائي، من خلال الاستعلام في قائمة المشتركين في المجال (DNS). فنتج عن عملية البحث في السجلات استكشاف عنوان IP المرتبط باسم المجال. لتحديد المجالات المطلوب

الاستعلام عنها، في قائمة المضيفين المشتركين مع المجال الأساسي (مثال تطبيقي على google.com). يوضح ناتج تنفيذ هذه الآلية المخرجات التالية قائمة من عناوين المستخدمين (الشكل 1).

الشكل (1): اكتشاف مجموعة من قائمة المستخدمين

من عينة الإخراج في الشكل (1)، حددت الآلية المقترحة –بنجاح– العديد من أسماء مضيفي Google النشطة، بما في ذلك www وmail وblog وns، الخ. ومن هذا المنطلق أثبتنا من كيفية استفادة المهاجم من البنية التحتية لنظام أسماء النطاقات المقدمة في تطبيقات خدمات المدن الذكية. يتمثل أحد الحلول لهذه المشكلة في عدم وضع معلومات يحتمل أن تكون حساسة في استكشاف DNS، وكشف الخدمات التقنية التي تريد أن تكون مرئية للعامة في هذه المدن الذكية. ويمكننا تحديد طريقة بديلة أو خياراً آخر وهو الانخراط بنشاط في خداع DNS. فالهدف من هذه الآلية هو توفير استجابات صحيحة للنطاقات الفرعية الحقيقية من خلال خادم (DNS) عن طريق الاستعلام الخاص بالمجالات الفرعية الدخيلة.

الحصول على حق الوصول المبدئي

في الشرح السابق، ناقشنا كيف يمكن للمهاجم القيام بالاستطلاع وتطوير الموارد المطلوبة لتنفيذ هجومه. بعد التخطيط للهجوم ووضع تلك الموارد في مكانها الصحيح، فإن الخطوة التالية هي محاولة الوصول إلى البيئة المستهدفة. فالمهاجم يستخدم بروتوكول الوصول ويحاول اعتماد صحة المصادقة عليها عن بعد (بعد الاستيلاء على اسم المستخدم وكلمة المرور)، ومن ثم اختراق البيانات والتلاعب فيها أو اتلافها. ومن هنا يمكننا معالجة هذا التحدي باستخدام بروتوكول تشفير يطلق عليه Secure Shell، لتشفير عملية الاتصال بين مقدم الخدمة ومتلقي الخدمة (Client/Server) باستخدام مفتاح التشفير RSA الموثوق من قبل مقدم الخدمة.

تم وصف هذا الهدف في تكتيك الوصول، يتضمن هذا التكتيك تقنيتين توضحان بالتفصيل الطرق المختلفة التي يمكن للمهاجم من خلالها تحقيق الوصول لبيانات المدن الذكية. سنركز على أساليب: الحسابات الصالحة والنسخ المتماثل عبر الوسائط القابلة للإزالة. فالحسابات الصالحة هي التي يخول لها التعامل مع بيانات المدن الذكية، ومن ثم حرمان المهاجم من الولوج أو الدخول للتعامل مع خدمات المدن الذكية. أما النسخ المتماثل فيتمثل بحماية البيانات المهمة وحفظها في مكان آمن وتشفيرها ضد أي هجمات محتملة.

اكتشاف الحسابات الافتراضية

يمكن إجراء اختبارات الحسابات الصالحة والافتراضية بشكل أفضل عبر الشبكة. تسمح عدة بروتوكولات مختلفة بالوصول عن بُعد إلى جهاز كمبيوتر، بما في ذلك RDP وSSH وTelnet. تتطلب FTP وSMTP والعديد من مواقع الويب مصادقة المستخدم للوصول إلى الوظائف المحمية. باستخدام بوابة المصادقة لهذه الأنظمة، يمكن للمهاجم اختبار ما إذا كانت مجموعة بيانات الاعتماد صالحة لجهاز معين. أخيرًا، لدينا تقنية تمكننا من تحسين الأمن السيبراني ومراقبة جودة الخدمات التقنية في المدن. وهي أن كلاً من المستشعرات والكاميرات تساعد في تحديد الجوانب التي ستكون حاسمة لتصنيف هذه التقنيات بناءً على السمات المقاسة لتلك الجودة.

تستخدم غالبية الشركات في العالم تقنية تعليم الآلة في التصنيع واستثمار الملايين في التطورات التقنية ذات الصلة. بل إن بعضهم قام برقمنة المصانع والمباني لسنوات عديدة. على الرغم من أن هذا المفهوم يبدو طليعيًا للغاية، إلا أن الحقيقة هي أنه موجود منذ فترة طويلة. في الواقع، ما نقترحه في تقنيات تعليم الآلة هو نقل الشركة إلى مستوى أكثر تقدمًا من الرقمنة.

حقيقة أن المدن الذكية تقوم على أساس استخدام بنى تقنية تحتية ابتكارية لتقليل استهلاك الطاقة وتقليل انبعاثات ثاني أكسيد الكربون وزيادة جودة حياة الناس ورفاهية السكان. فالمعايير التي تعمل على تأهيل المدينة كمدينة ذكية هي التزامها بالبيئة، وتخطيطها الحضري، وإدارتها العامة، وجودة التعليم والصحة، وظروف التنقل والنقل، وجهودها لتسهيل التماسك الاجتماعي، والاستثمارات البشرية والاقتصادية لتحسين عملها. وفقًا لمفهوم المدينة الذكية، تم تقديم فكرة المدينة الذكية على أنها تلك التي تتضمن نظامًا يسمح بأتمتة العديد من المهام، فضلاً عن التحكم الكامل والمباشر فيما يحدث فيها.

المبحث الثالث: حلول مقترحة لتحديات الأمن الإلكتروني للمدن الذكية وتهديداتها

قدمت وزارة الأمن الأمريكية حلولاً لتحديات المدن الذكية ومخاطرها، شملت تأمين نقاط الضعف في الأنظمة الرقمية، واختبار الأنظمة والأجهزة قبل تشغيلها لكشف ثغراتها الأمنية، والاعتماد على قائمة مرجعية لعمليات التشفير، والمصادقة، وتحديثات البرمجيات، وإلزام الشركات المزودة للمدن بالخدمات التكنولوجية بضوابط تشفير المعلومات وتأمينها، وبحث سبل الإفادة من النظم التقنية لتحقيق صالح المواطنين وفقا لأسس ومبادئ أخلاقية (وزارة الأمن الداخلي الأمريكية، 2016).

ناقش مؤتمر "أمن المعلومات" التحديات الأمنية للمدن الذكية، وما تضمنته من فرص متعددة للارتقاء بمستوى كفاءة الأعمال وتحسين مستوى جودة الحياة. وأكدت التوصيات أهمية الربط بين البنى التحتية لتقنية المعلومات والاتصالات وخدمات أجهزة الاستشعار والتحكم، وبين عمليات التحليل المتطورة لمواجهة التحديات الأمنية السيبرانية للمدن الذكية (البيان، 2016). ويرى شركاء المجموعة المركزية للمدن الذكية أن مبادرة نيويورك العالمية للأمن الإلكتروني للمدن الذكية سوف تساعد بكفاءة على تبادل المعرفة لتحقيق الأمن الإلكتروني للمدن الحديثة الذكية، من خلال ما يلي (مبادرة نيويورك، 2016):

1- توعية مخططي المدن الذكية ومزودي خدماتها بأهمية الحماية الإلكترونية.

2- التعاون مع الشركاء لتبادل الأفكار والمنهجيات.

3- المصادقة على أهمية إدخال وسائل الأمن في وقت مبكر قبل وأثناء تنفيذ المشروعات.

4- تعزيز الشراكات بين المدن ومقدمي الخدمات والمجموعات الأمنية.

5- وضع المعايير والمبادئ التوجيهية، والموارد للمساعدة لتحسين الأمن الإلكتروني.

6- التنسيق بين موردي معدات التشغيل الآلي والباحثين لمواجهة التحديات الأمنية.

7- استدامة تطوير عمليات دمج التقنيات في البنية التحتية، والإفادة من إنترنت الأشياء.

8- التعاون المشترك بين مخططي المدينة وبناة أنظمتها، لرفع مستوى الوعي.

كما يلزم لمواجهة تحديات الأمن الإلكتروني للمدن الذكية ما يلي (البيانات الذكية، 2017):

1- مراعاة عوامل السلامة ذات الأثر في الخدمات المتطورة التي تقدمها المدن الذكية.

2- توازن نشاط البنية التحتية ذات الأثر في الهيكل الحضري والتصميم الاجتماعي.

3- تشغيل العمالة في مجالات الأمن الإلكتروني للبيانات.

4- الإفادة من تحليل البيانات الذكية ومعالجتها بالاستخدام الرشيد لتطبيقات للذكاء الاصطناعي، وتكنولوجيا المعلومات والاتصالات الرقمية.

كما يلزم لتأمين سكان المدن الذكية ضد الهجوم السيبراني، ما يلي (Lee, 2017):

1- البحث عن أفضل طرق الدفاع عن هذه الأنظمة من الهجمات الإلكترونية.

2- تطوير الطرق الأمنية للإبلاغ عن التدخلات، ومعرفة هويات المتسللين.

3- تطبيق أساليب محسنة للتعافي السريع من الاعتداءات السيبرانية.

4- تصميم أنظمة تحكم صناعية آلية مؤتمتة فعالة وآمنة الاستخدام مثل نظام شبكات SCADA.

وللتعامل مع تحديات الأمن الإلكتروني للمدن الذكية وإيجاد حلول لها يلزم اتباع استراتيجيات حمايتها من الهجوم السيبراني تعتمد على (Weiner, 2017):

1- تقليل نقاط الضعف في الشبكات والنظم لزيادة القدرة على مكافحة التسلل والحماية من الفيروسات.

2- تفعيل قوة القانون لردع المجرمين والحد من هجماتهم الإرهابية الإلكترونية.

3- تعقب متخصصو الدفاع السيبراني وخبراء الطب الشرعي للمجرمين الإلكترونيين المنظمين.

4- مراجعة ثغرات خدمات الهاتف المحمول ذات النطاق العريض.

5- استكشاف مشكلات الويب المظلم ووضع الاستراتيجيات المناسبة للتعامل معها.

6- استكشاف استراتيجيات وأنظمة جديدة للدفاع الإلكتروني للتعامل مع إنترنت الأشياء (IoT).

7- توظيف الخدمات المساندة عبر الحوسبة السحابية لتعزيز ممارسات الأمن السيبراني للمدن الذكية.

8- تأمين أنظمة التحكم الصناعية (ICS) وخاصة أنظمة SCADA المستخدمة على نطاق واسع.

9- تفعيل الإجراءات الوقائية لدعم أنظمة التطبيقات الخاصة بالأقمار الصناعية والمراقبة على نطاق واسع.

10- تطوير أنظمة التشخيص لاكتشاف نقاط الضعف السيبرانية.

كما توجد حلول تأمينية مقترحة لحماية البنية التحتية الحيوية للمدن الذكية من الهجمات والتهديدات السيبرانية، ويشمل ذلك (باسم، 2018):

1- استعداد مديرو المخاطر والأزمات لتوفير نسخ احتياطية لإدارة الشبكات والنظم المتضررة.

2- توفير برامج حماية ذاتية تتيح لمسؤولي إدارة الأنظمة اتخاذ الإجراءات الفورية لحمايتها.

3- تفعيل الخدمات السحابية من خارج المواقع الإلكترونية للنظم لحماية بياناتها.

4- المراقبة المستمرة للأشخاص الذين يسجلون دخولهم إلى النظم والمواقع الإلكترونية.

5- استخدام نظام مخصص للبحث السريع عن أي ثغرات في البرامج والنظم.

6- استخدام تطبيقات منع التسلل وحجب المتسللين.

7- استخدام خدمات مكافحة البرامج الضارة التي يمكنها تحديد مواقع التصيد المعروفة.

8- استخدام جدران نارية للحماية والتشفير، وبرامج مكافحة الفيروسات،

ومراقبة سلامة الملفات.

9- الفصل المناسب للمعدات غير الضرورية لزيادة مستوى تأمين الشبكات.

10- تعزيز الأمن الشخصي للمستخدمين، بتحديث طرق مصادقة المصرح لهم.

11- تبادل أفضل الممارسات والأدوات لمواجهة تحديات للأمن الإلكتروني للمدن الذكية وتهديداتها.

13- إعطاء أولوية التوظيف والتدريب للخبراء التقنيين في مجالات الأمن السيبراني.

14- سرعة استجابة المحققون الجنائيون وخبراء أمن الشبكات للحوادث السيبرانية.

15- انجاز بعض الوزارات بتحقيقات سريعة، لردع مجرمي الإنترنت.

ومن الحلول التي يمكن تطبيقها للحد من التحديات والتهديدات لأمن معلومات المدن الذكية (Chen, 2021):

1- عدم الخلط بين الاستخدامات الشخصية والاستخدامات العملية الوظيفية للشبكات والبيانات.

2- وضع سياسات أمنية واضحة والمحافظة عليها لتحديد متطلبات أمن المعلومات بوضوح.

3- زيادة الوعي بأهمية أمن المعلومات للمحافظة على سريتها وتجنب اختراقها والعبث بها.

4- تأمين المعلومات ببرامج الحماية المتخصصة لإدارتها بشكل آمن من هجمات المتسللين.

5- الفحص الدوري للشبكات والأجهزة والبرامج لاكتشاف الاختراقات الأمنية والتعامل معها.

لذا نحتاج إلى برنامج فعالة لحماية المعلومات وتأمينها (مثال Password Manager Pro). كما يمكننا استخدام نظام أجهزة حواسيب الخدمة المدمجة الموثوقة للغاية (Thenic system) لمجموعة أعمال مركز البيانات (DCG) المزودة ببرمجيات البنية التحتية فائقة التقارب (HCI)، مما يساعد على سرعة التعامل مع البيانات، ومرونة أعلى لتوفير حماية أفضل للأجهزة الطرفية الموزعة مركزيًا. ويتوفر حاليًا بعض حلول أمن المدن الذكية المتعلقة بإنترنت الأشياء، وحواسيب محطة العمل، وأجهزة الواقع المعزز والواقع الافتراضي والحلول المنزلية والمكتبية الذكية. بتوفير السحابة المختلطة الذكية، لضمان الأمن والمرونة والبساطة على نطاق واسع لخدمات الأعمال ذات المهام الحرجة، بأتمتة إدارة التطبيقات وإزالة انقطاعات الخدمة غير المخطط لها، والتقليل من تكلفة البنية التحتية التقليدية لتكنولوجيا المعلومات بمقدار النصف أو أكثر، وتوفير الأداء الرائد لقطاع الاتصال، سعيا لتحقيق الريادة الفكرية لمستقبل أكثر ذكاء يتحقق فيه الازدهار للجميع. (لينوفو وبيفوت، 2018).

وتعددت الإرشادات الخاصة بالأمن السيبراني، ومنها ما يلي (مجتمع تكنولوجيا المعلومات، 2019):

1- تفعيل استخدام برامج مكافحة الفيروسات، والجدران النارية، وأنظمة كشف الاختراق.

2- تكثيف سبل حماية العمليات والبيانات الأكثر أهمية، باكتشاف الحوادث الأمنية، وسرعة التعامل معها.

3- رسم خطط للعمليات التشغيلية التنفيذية لبرامج الأمن السيبراني، والتحقق من نجاحها، وتقويم نتائجها.

4- تطوير استراتيجيات أمن السيبراني لاستيعاب الهجمات المتطورة والمتزايدة للمهاجمين.

5- نشر الوعي الأمني السيبراني وتوفير مقاييسه وأدواته، ومناقشة أفضل السبل والأفكار الأمنية ضد مجرمي الإنترنت الذين يحاولون اختراق الشبكات، والعبث بالبيانات.

كما تضمنت توصيات مؤتمر أمن المعلومات بعض الحلول لمواجهة تحديات الأمن الإلكتروني للمدن الذكية، ومنها ما يلي (غاوي، 2019):

1- إنشاء منصة عالمية لتبادل المعلومات وتسهيل تحليلها.

2- توفير البيئة الآمنة للاتصال بإنترنت الأشياء لزيادة ثقة السكان في بالتكنولوجيا الحديثة.

3- التدخل الحكومي لضمان مصالح المستخدمين، وإتاحة استخدامها الشخصي لكل فرد.

4- تطوير البيئة التشريعية بصورة تحمي خصوصية البيانات وسن تشريعات لقوانين تبادلها.

كما تتطلب مواجهة تحديات الأمن الإلكتروني وتهديداتها (أمن المدن الذكية،2020):

1- الالتزام بأخلاقيات جمع البيانات وتحليلها.

2- إجراء تقييمات منتظمة للمخاطر، لتحديد المجالات التي قد تتغير فيها بسرعة أكبر.

3- التوثق من مصدر البيانات والقرارات الصادرة عنها، لتجنب الحوادث واهتزاز ثقة العملاء.

4- حوكمة معايير السلامة والموثوقية، والتوافر، وإعطاء الأولوية للقدرة على التكيف.

5- تهيئة المنظمات لنقاش تكنولوجي بشأن التشريعات المحققة للأمن السيبراني CPS في ظل استخدام IoT.

6- إجراء تحديثات مستمرة للسياسات والتشريعات الأمنية وفقا لمعايير تكنولوجيا المعلومات وضوابطها.

7- تحديد حدود واضحة لحماية المعلومات، ومدى استخدامها المباشر من مصدرها.

وتعتمد المدن الذكية اعتمادًا كبيرًا على جمع البيانات ومعالجتها، من أجل

زيادة كفاءة الخدمة، ويجب أن تتوافر في البيانات الموثوقية، والوفرة، والسرية، للإفادة منها في اتخاذ القرار. كما يجب أن تعالج بسرية للحفاظ على ثقة سكان المدينة المستفيدون من خدماتها. ويتطلب ذلك توظيفا لتطبيقات الذكاء الاصطناعي لتحقيق مستوى مناسب من الأمن السيبراني، ووضع خطط احتياطية لضمان تحقق الأمن السيبراني، مما يستلزم إعداد نسخا احتياطية للبيانات، ونظم الإدارة التكنولوجية المعرضة للهجوم، مع تأكيد ضرورة الالتزام بالمبادئ التوجيهية والقانونية والأخلاقية لتحقيقه (تحديات الأمن السيبراني للمدن الذكية، 2020).

ويقدم الذكاء الاصطناعي حلولا تكنولوجية لإشكاليات التأمين السيبراني للمدن الذكية، من خلال المراقبة، والتحليل، وتعزيز قدرات اتخاذ القرار. حيث تجمع بيانات المدينة عبر الأجهزة المتصلة بشبكاتها، مثل الكاميرات، وأجهزة الاستشعار، ومن ثم؛ يمكن توظيف تطبيقات الذكاء الاصطناعي لتزويد المسؤولين بالمعلومات المطلوبة في وقت قصير، ليتمكنوا من اتخاذ القرار السريعة والمناسبة لإدارة كافة مرافق البنية التحتية بالمدينة، مما يقلل الهدر، ويزيد جودة الخدمات. كما يساعد الذكاء الاصطناعي على دمج البيانات من كاميرات التتبع، والمقاييس الذكية، وأجهزة الاستشعار وأجهزة المراقبة بكل أنواعها لبناء صورة أكثر دقة عن كيفية استخدام الناس للمدن. وذلك من خلاله قراءة اللوحات، والتعرف على الوجوه، وتتبع الحركات والتفاعلات الحضرية في المدينة لتقليل تأثيرها البيئي. وقد أطلقت "حكومة دبي الذكية" أول مختبر من نوعه لعلوم البيانات، يعمل مع شبكة متنامية من الشركاء من مختلف القطاعات الحكومية والخاصة. حيث تحلل أدوات ومنصات البيانات باستخدام تقنيات الذكاء الاصطناعي، والاستفادة من البيانات لتنفيذ حالات الاستخدام، والتنسيق، وبناء القدرات، للوصول إلى مدينة ذكية وآمنة للجميع. وقد أطلقت الإمارات "الاستراتيجية الوطنية للأمن السيبراني"، التي استهدفت خلق بيئة سيبرانية آمنة ومرنة، تساعد على تعزيز الأمان الإلكتروني، وتمكين الشركات من التطور والنمو. وتعمل هذه الاستراتيجية على تعزيز المنظومة المتكاملة للأمن السيبراني من خلال تنفيذ (60) مبادرة في محاور خمسة رئيسة، هي (عودة، 2020):

1- سن قوانين ولوائح الأمن السيبراني، لرفع جاهزية أمان الشركات.

2- إلزام موردي الخدمات التكنولوجية للجهات الحكومية بحيازة شهادة تطبيق الأمن السيبراني.

3- تطوير بوابة موحدة للشركات لتمكينها من تنفيذ المعايير والمواصفات اللازمة لتطبيق الأمن السيبراني.

4- تأسيس بيئة حيوية تتضمن الحماية الأمنية السيبرانية للتكنولوجيا الحالية والناشئة.

5- تحديث خطة الوقاية من الحوادث السيبرانية.

مما تقدم يتضح تعدد الحلول المقترحة لتحديات الأمن الإلكتروني للمدن الذكية وتهديداتها، وتم استخلاص أبرزها وتصنيفها في خمس مجالات رئيسة للحلول، شملت الحلول: التكنولوجية، والأمنية، والتثقيفية، والتشريعية، والأخلاقية، وذلك للإجابة عن السؤال الرابع للدراسة الحالية.

وتجدر الإشارة إلى أن المحور التكنولوجي والمحور الأمني مضمنان في بحث أعده فريق البحث الحالي (العتيبي وآخرون، 2022). ومن ثم فإن البحث الحالي ركز على تناول ثلاثة محاور للحلول، وهي: الحلول التشريعية، والتثقيفية، والأخلاقية.

تعقيب على الأدبيات

من العرض السابق للأدبيات المرتبطة بمتغيرات البحث، يتبين ما يلي:

1- أن المدن الذكية كيانات مطورة للمدن التقليدية، تعززها التطبيقات التكنولوجية في سياقات من الحداثة والاستشراف، لتحقيق التنمية المستدامة والازدهار في شتى المجالات. ويتوافر فيها التنوع البيئي الرقمي المحفز للإبداع. وتعتمد على التكنولوجيا الرقمية والمعلوماتية، وتوظف فيها تطبيقات تكنولوجيا المعلومات والاتصالات في إدارة خدماتها المتعددة؛ والتي تشمل: الصحة، والتعليم، والتخطيط العمراني، وإدارة الطاقة والأنظمة البيئة، وتنظيم تسيير المركبات، والرعاية الاجتماعية، وأمن البنية التحتية، ومكافحة الجريمة، وغيرها من التطبيقات التكنولوجية الخدمية لسكانها وزوارها. ومما يساعد على استدامة الحياة فيها بطريقة آمنة جمع معلوماتها عن نفسها بأجهزة استشعار وأجهزة أخرى وأنظمة، ونقل بياناتها عبر الشبكات السلكية واللاسلكية وتبادلها، وتحلل بياناتها ومعالجتها لتفهم ما يحدث آنيا، وما يحتمل حدوثه في المستقبل.

2- تواجه المدن الذكية تحديات أمنية إلكترونية تعترض مساراتها التنموية، وتتسبب في مشكلات ضارة مزعجة على المستويات البنائية والوظيفية، مما يهدد أمنها واستقرارها، ويحول دون تحقيق مصالحها الحيوية الذاتية والمشتركة، وجميعها تحديات يصعب تجنبها أو تجاهلها.

3- يترتب على التحديات الأمنية للمدن الذكية تهديدات تعرقل تحقيق أمنها الإلكتروني، مما ينعكس أثره على جودة الحياة فيها، ويستوجب ذلك تدخلا سريعا من الحكومات أو الهيئات أو المنظمات لمواجهتها، والحد من آثارها، واتخاذ كافة الإجراءات لدرء مخاطرها الفعلية أو المحتملة، وذلك ضماناً لتحقيق أمنها الإلكتروني السيبراني.

4- تعدد حلول مواجهة التحديات الأمنية السيبرانية المهددة لسلامة المدن الذكية لتشمل العديد من الحلول في المجالات التقنية، والأمنية، والتشريعية، والتثقيفية، والأخلاقية.

منهجية البحث وإجراءاته

اتبع البحث المنهج الوصفي (مطاوع والخليفة، 2017)، وذلك للإجابة عن بعض أسئلته، وإعداد مشروعه التثقيفي المقترح، وذلك باتباع الخطوات التالية:

1- روجعت الأدبيات ذات العلاقة بتحديات الأمن الإلكتروني للمدن الذكية، وتهديداتها الخطرة على الفرد والمجتمع، وذلك لاستقرائها،

واستخلاص الإجابات عن أسئلة البحث الأربعة الخاصة بـ: تحديد المقصود بالمدن الذكية، وماهية الأمن الإلكتروني (السيبراني) لها، وتحديات الأمن الإلكتروني للمدن الذكية وتهديداتها للفرد والمجتمع، واستخلاص حلول مقترحة لمواجهة تحديات الأمن الإلكتروني للمدن الذكية وتهديداتها.

2- أُعدت استبانة تقويمية لآراء المتخصصين حول الحلول المقترحة لمواجهة تحديات الأمن الإلكتروني للمدن الذكية العربية وتهديداتها، وذلك كما يلي:

أ- تحديد هدف الاستبانة المتمثل في تعرف الآراء التقويمية للمتخصصين في الحلول المقترحة لتحديات الأمن الإلكتروني للمدن الذكية العربية.

ب- تحديد صفحة عنوان الاستبانة، وبيانات المستجيب، وشملت: الاسم (اختياري)، والنوع (ذكر، أنثى)، ومجال التخصص (تكنولوجي/ تقني، تثقيفي/ تعليمي، وتشريعي، قانوني، وأمني، وأخلاقي). كما اشتملت صفحة التعليمات على التعريف بهدف الاستبانة، ومحاورها، وأسلوب الاستجابة على مفرداتها، وذلك بوضع علامة (√) في خلية أحد بدائل الموافقة على المفردة، وفق تقدير ليكرت؛ للموافقة بدرجة (كبيرة جدا، وكبيرة، ومتوسطة، وقليلة، وقليلة جداً).

ج- عرضت الاستبانة في صورتها الأولية على (10) من المحكمين لتعرف آرائهم التقويمية لها، وأجريت التعديلات المقترحة المناسبة التي اتفقت حولها أراء المحكمين بنسبة (90٪)، وتمركزت حول تعديل صياغة بعض المفردات. ثم أعيد عرض الاستبانة على المحكمين مرة ثانية لتحديد نسب اتفاق آرائهم حولها. وقد تراوحت بين (88- 94٪) بمتوسط مقداره (91٪) وهي نسبة مقبولة تشير إلى صدق الاستبانة. (Copper, 1981).

د- طبقت الاستبانة تطبيقا استطلاعيا على عينة من أعضاء هيئة التدريس بلغ عددهم (30) عضوا من المتخصصين في المجالات التكنولوجية، والتثقيفية، والتشريعية، بغرض التحقق من وضوح تعليماتها ومفرداتها. وتم حساب معامل ثباتها باستخدام معادلة "بيرسون"، وبلغت (0.86) وهي قيمة مقبولة لثبات الاستبانة. (السيد، 1978). وبذلك أصبحت الاستبانة في صورتها النهائية الصالحة للتطبيق على عينة البحث.

3- وزعت الاستبانة بصيغتيها الورقية والإلكترونية على (40) من المتخصصين، منهم (25) من الذكور، و (15) من الإناث من أعضاء هيئة التدريس بالجامعات.

4- رُصدت نتائج الاستبانات، وعولجت بالأساليب الإحصائية الوصفية، وشملت: التكرارات، والنسب المئوية، والمتوسطات الوزنية النسبية، لتحديد الرؤى التقييمية للحلول المقترحة لمواجهة التحديات الأمنية السيبرانية لسلامة المدن الذكية.

5- تم وضع تصور مشروع تثقيفي مقترح لتنمية الوعي بالتحديات الأمنية السيبرانية للمدن الذكية والحلول المناسبة لها.

6- تمت صياغة توصيات البحث ومقترحاته.

نتائج البحث (عرضها- تمثيلها- مناقشتها)

تمت الإجابة عن أسئلة البحث من خلال الاستقراء التحليلي لمضامين الأدبيات، واستخلاص إجابات الأسئلة من (الأول إلى الرابع)، وقد تمت الإجابة من خلال تحليل ومعالجة نتائج تطبيق الاستبانة على عينة البحث الميدانية.

أولا: إجابة السؤال الأول

الذي نص على: ما التحديات السيبرانية التي تهدد أمن وسلامة الأفراد في المدن الذكية؟

تم استخلاص الإجابة عنه من خلال مراجعة أدبيات المبحث الثالث، حيث تحددت أبرز تحديات الأمن الإلكتروني للمدن الذكية وتهديداتها للفرد والمجتمع فيما يلي:

1- يواجه الأمن الإلكتروني للمدن الذكية تحديات وتهديدات الاختراق للبروتوكولات، وعناوين IP لمستخدمي النظم، ولذا استحدثت وزارة الأمن الداخلي الأمريكية نظام "اينشتاين" واستخدمته بشبكات SCADA لتسيير المركبات في ساعات الذروة، كما وظفت الأجهزة المرتبطة بإنترنت الأشياء لتشغيل المصاعد الكهربية، ووسائل الانتقال

2- تتنوع تحديات الأمن الإلكتروني للمدن الذكية وتهديداتها، ويشمل ذلك: البرمجيات الخبيثة، والتصيد/ الخداع (Phishing)، وهجوم "رجل في الوسط" (MITM)، وحصان طروادة (Trojans)، وهجمات الفدية (Ransomware)، وهجوم رفض الخدمة الموزع (DDoS)، والهجمات على أجهزة إنترنت الأشياء (IoT)، وخروقات البيانات، والبرامج الضارة على تطبيقات الهواتف المحمولة.

3- تُعد غياب الرؤية الشمولية والتحكم في جميع الأصول من التحديات الكبرى التي تهدد الأمن السيبراني لبيانات المدن الذكية.

4- يواجه التأمين الإلكتروني للمدن الذكية تحديات مرتبطة بالبنية التحتية الذكية، ويشمل ذلك: التباينات بين مكونات البنى التحتية الحضرية والقديمة للقطاعات الخدمية، والتفاوت بين معدلات التحول إلى التقنيات الذكية للتباين بين الموارد مستويات المستهلكين، وما يحدث تقليص لمستويات التفاعل البشري بفعل التوسع في تطبيقات الأنظمة التقنية الذكية.

5- تتزايد تحديات الأمن السيبراني بتزايد الهجمات الإلكترونية للمدن الذكية، نظراً لتوظيف القراصنة لإنترنت الأشياء في إطلاق هجمات أشد ضراوة وتهديدا للمعلومات الشخصية المخزنة في الفضاء الإلكتروني.

6- تمثل انتهاك الخصوصية والحقوق والحريات تحديات مهددة للأمن السيبراني للمدن الذكية، وذلك في ظل اتصال مليارات الأفراد حول العالم بشبكة الإنترنت، عبر الأجهزة الجوالة. مما يوجب ضرورة أتمتة الأمن الإلكتروني للمدن، ورفع مستوى الوعي بين الشركات والحكومات وعدم جعل هذا المطلب حكراً على قطاع تكنولوجيا المعلومات فقط.

7- تتضاعف تحديات الأمن السيبراني للمدن الذكية نتيجة تعقيد شبكات البيانات، وزيادة حجم الاتصالات الرقمية لارتفاع نسبة مستخدمي تطبيقات الهاتف المحمول بتطبيقاته المتنوعة، التي تستخدم الذكاء

الاصطناعي في التواصل عبر الشبكات الرقمية وبين الأجهزة والآلات.

8- يواجه الأمن الإلكتروني للمدن الذكية إشكاليات منها: عدم تطبيق السياسات الأمنية للحد من السلوكيات السلبية.، ونقص الوعي في بأساليب حماية المعلومات وتأمينها.

9- تتزايد الفرص المحتملة للاختراق غير الآمن الذي يهدد حماية بيانات شبكات المدن الذكية ونظمها، ويزيد من معدلات الإرهاب، وما يترتب عليه من مخاوف تهديد الخصوصية، وغيرها من الأضرار الأخرى غير المتوقعة.

10- اختراق البيانات وما يترتب عليها من اهتزاز مستوى ثقة المستخدمين في المدن الذكية تعد من التحديات التي تواجه أمنها الإلكتروني في الحاضر والمستقبل.

11- تنعكس تحديات الأمن الإلكتروني للمدن الذكية وتهديداتها ومخاطرها على خصوصية المستخدم في جمع البيانات، وضيق نطاق التحكم التكنوقراطي، والخصخصة الإدارية.

12- يُعد التحدي التحليلي للبيانات الضخمة من التحديات التي تواجه الأمن السيبراني للمدن الذكية، الذي يلزم تنفيذه بفاعلية لمعرفة السلوك وتفاعلاته، وسلامة الأنظمة الفيزيائية السيبرانية (CPS) وموثوقيتها.

وتتعدد التأثيرات الانعكاسية لتحديات الأمن السيبراني وتهديداته للفرد من خلال زيادة مشاعر عدم الثقة، والتعرض للإرهاب الإلكتروني، وزيادة المشاعر العدوانية والسلبية، والشعور بالانهزامية، والتمرد. كما تنعكس تأثيراتها على المجتمع لتشمل زيادة معدلات انتشار الجرائم، وانتشار الإرهاب الإلكتروني وغيره من الأعمال التخريبية الضارة بمستوى الخدمات المتعددة التي يمكن أن تقديمها لمجتمع سكان المدن الذكية. ويمكن بيان نموذج توضيحي لحماية أمن المعلومات بالمدن الذكية في الشكل (2) التالي.

الشكل (2) نموذج لأبعاد الحماية الأمنية بالمدن الذكية (العتيبي وآخرون، 2022)

ثانيا: إجابة السؤال الثاني

الذي نص على: ما الحلول المقترحة للتحديات السيبرانية المهددة لأمن وسلامة الأفراد في المدن الذكية؟

تم ذلك من خلال مراجعة أدبيات المبحث الثاني، وتم تحديد أبرز الحلول المقترحة وصنفت في محاور تشريعية، وتثقيفية، وأخلاقية، وذلك على النحو التالي:

أ) الحلول التشريعية: وتشمل ما يلي:

1. سن قوانين ولوائح الأمن السيبراني، لرفع جاهزية أمان المدن الذكية.
2. تطوير البيئة التشريعية المحددة للأطر الأساسية لتبادل المعلومات حماية للخصوصية.
3. إلزام الشركات المزودة للمدن بالخدمات التكنولوجية بالضوابط الأمنية لتشفير المعلومات.
4. وضع المعايير والمبادئ التوجيهية للأمن الإلكتروني بجميع الخدمات في المدن الذكية.
5. تنفيذ لوائح ومعايير تأمينية لنقاط ضعف الأنظمة الرقمية المتحكمة في إدارة المدن الذكية.
6. إقرار وسائل التأمين الإلكتروني قبل وأثناء تنفيذ المشروعات التكنولوجية بالمدن الذكية.
7. التدخل الحكومي لضمان مصالح المستخدمين، واستخدامهم الموثوق للبيانات بالمدن الذكية.
8. تحديث مستمر للتشريعات والسياسات الأمنية تبعا للمستجدات التكنولوجية للمدن الذكية.

ب) الحلول التثقيفية: وتشمل ما يلي:

1. نشر ثقافة التعاون مع الشركاء لتبادل الأفكار والمنهجيات بين المخططين، وبناة الأنظمة، ومقدمي الخدمات، والمجموعات الأمنية للمدن المختلفة.
2. إعطاء أولوية التوظيف والتدريب للخبراء التقنيين في مجالات الأمن السيبراني، لحماية المعلومات والبيانات.
3. توعية مخططي المدن الذكية ومزودي خدماتها بأهمية الحماية الإلكترونية وفوائدها.
4. التوعية بوسائل أمن المعلومات للمحافظة على سريتها، وتجنب اختراقها والعبث بها.
5. نشر الوعي الأمني السيبراني وتوفير مقاييسه وأدواته.
6. تدارس أفضل الأفكار الأمنية ضد مجرمي الإنترنت الذين يحاولون اختراق الشبكات، والعبث بالبيانات.
7. تهيئة المنظمات لنقاش تكنولوجي يساهم في تعزيز الأمن السيبراني للمدن الذكية CPS في ظل اتساع نطاق استخدامات إنترنت الأشياء IoT.
8. التعريف بالمبادئ التوجيهية التشريعية والقانونية المحققة للأمن السيبراني للمدن الذكية وأدوار الأفراد ومؤسسات المجتمع نحوها.

ج) الحلول الأخلاقية: وتشمل ما يلي:

1. حوكمة المعايير والضوابط الأخلاقية لتكنولوجيا المعلومات في المدن الذكية.
2. تطبيق الأسس والمبادئ الأخلاقية لضمان تأمين مصالح سكان المدن الذكية.
3. الالتزام بأخلاقيات جمع البيانات وتحليلها لتطوير خدمات المدن الذكية.
4. التقيد بالضوابط الأخلاقية في تحديث التطبيقات التكنولوجية بالمدن الذكية.
5. الالتزام بالمبادئ الأخلاقية المحققة للأمن السيبراني لنظم وبرامج المدن الذكية.

ثالثا: إجابة السؤال الثالث

الذي نص على: ما الرؤى التقييمية لحلول تحديات الأمن السيبراني للمدن الذكية من وجهة نظر المتخصصين؟

تم ذلك من خلال معالجة نتائج استجابات الاستبانة، ورصدها في الجدول (1). يتبين من الجدول (1) أن المتوسط النسبي التقويمي العام للحلول التي تضمنتها الاستبانة بلغ 95.77٪، كما يتضح أيضا أن المتوسطات النسبية التقويمية للحلول كانت: 95.9٪ للحلول التشريعية، و95.3٪ للحلول التثقيفية، و96٪. للحلول الأخلاقية وتشير المتوسطات النسبية التقويمية إلى ارتفاع المعدل التقويمي لحلول تحديات الأمن الإلكتروني للمدن الذكية العربية وتهديداتها من وجهة نظر عينة البحث.

ومن خلال الجدول (1)، يمكننا الإشارة إلى الاستبانة وأسئلة البحث في محور الحلول التشريعية، وبنود تفاصيلها يبينها الشكل رقم (2). أما تفاصيل محور الحلول التثقيفية والحلول الأخلاقية فيوضحهما الشكلين (2)، و(3).

ومن الجدول (1) يمكن استخلاص محصلة النتائج التقويمية للحلول التقنية، والأمنية، والتشريعية، والتثقيفية، والأخلاقية لتحديات الأمن الإلكتروني وتهديداتها، وترتيبها تبعا لنسبها الوزنية التقويمية، كما هو مبين بجدول (2). الجدول (2): محصلة النتائج التقويمية للحلول التشريعية، والتثقيفية، والأخلاقية لتحديات الأمن الإلكتروني وتهديداتها وترتيبها تبعا لنسبها المئوية الوزنية التقويمية.

كما يمكن التمثيل البياني لمحصلة النتائج التقويمية للحلول التشريعية، والتثقيفية، والأخلاقية لتحديات الأمن الإلكتروني وتهديداتها وترتيبها تبعا لنسبها المئوية الوزنية التقويمية في الشكل (3) التالي. كما توضح الأشكال (4)، (5): التمثيل البياني للنتائج التقييمية للحلول التشريعية، والتثقيفية، والأخلاقية لتحديات الأمن السيبراني للمدن الذكية وترتيبها تبعا لنسبها المئوية.

يتضح من الجدول (2) والشكل (6) أن الحلول الأخلاقية احتلت الترتيب الأول بنسبة 96٪، ثم جاءت الحلول التشريعية في الترتيب الثاني بنسبة 95.9٪، وجاءت في الترتيب الثالث الحلول التثقيفية بنسبة 95.3٪.

رابعا: إجابة السؤال الرابع

الذي نص على: ما التصور المقترح لمشروع تثقيفي للمساهمة في مواجهة تحديات الأمن السيبراني للمدن الذكية؟

لتعميق الإفادة مما توصل إليه البحث الحالي من نتائج، وما قدمته من توصيات، يمكن تقديم مشروعا تطبيقيا مقترحا لتعزيز الوعي بالتحديات الأمنية السيبرانية وتهديداتها للمدن الذكية العربية والحلول الفاعلة لمواجهتها، للمساهمة في تفعيل الدور المجتمعي الاستشرافي لمواجهتها، وذلك بتنفيذ المشروع المقترح التالي:

أ) عنوان المشروع

(مشروع مقترح لتنمية الوعي بالتحديات الأمنية السيبرانية للمدن الذكية أو حلولها).

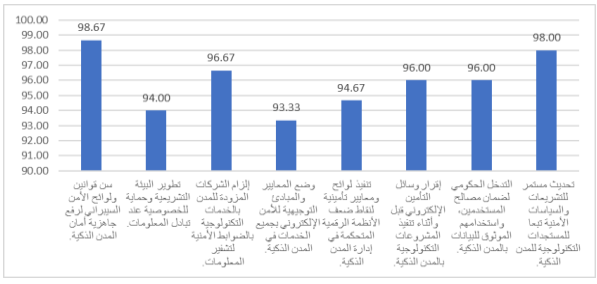
ب) المقدمة

على الرغم مما أضافته نظم التقنية من تيسيرات إدارية ذكية للخدمات المتعددة في المدن الذكية؛ إلا أنها نظمها المعلوماتية تتعرض لتحديات أمنية إلكترونية سيبرانية ذات آثار تهديدية ضارة للفرد والمجتمع، ويشمل ذلك اختراق المتسللين للشبكات والأجهزة والبرامج والعبث في البيانات، مما ترتب عليه أضراراً بالغة لحقت بالنظم التقنية لخدمات المدن في مجالات: الصحة، والتعليم، والتخطيط العمراني، وإدارة الطاقة والأنظمة البيئة، وتنظيم تسيير المركبات، والرعاية الاجتماعية، وأمن البنية التحتية، ومكافحة الجريمة. ولذا تكاتفت الجهود لوضع الحلول المقترحة لمواجهة تلك التحديات، وشملت حلولاً: تشريعية، وتثقيفية، وأخلاقية.

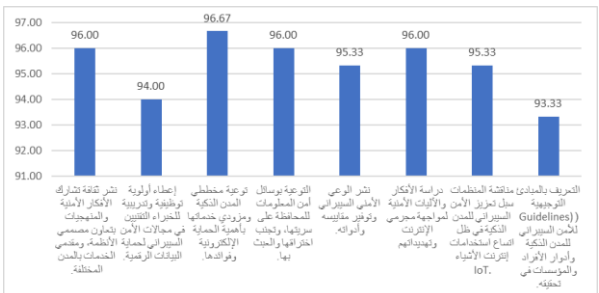
الجدول (1): الآراء التقييمية لبعض حلول التحديات السيبرانية المدن الذكية

م	المحاور والمفردات لحلول التحديات السيبرانية	النسبة %
	أ) محور الحلول التشريعية	
1	سن قوانين ولوائح الأمن السيبراني لرفع جاهزية أمان المدن الذكية.	%98.7
2	تطوير البيئة التشريعية المحددة للأطر الأساسية لتبادل المعلومات حماية للخصوصية.	%94
3	إلزام الشركات المزودة للمدن بالخدمات التكنولوجية بالضوابط الأمنية لتشفير المعلومات.	%96.6
4	وضع المعايير والمبادئ التوجيهية للأمن الإلكتروني بجميع الخدمات في المدن الذكية.	%93
5	تنفيذ لوائح ومعايير تأمينية لنقاط ضعف الأنظمة الرقمية المتحكمة في إدارة المدن الذكية.	%94.7
6	إقرار وسائل التأمين الإلكتروني قبل وأثناء تنفيذ المشروعات التكنولوجية بالمدن الذكية.	%96
7	التدخل الحكومي لضمان مصالح المستخدمين، واستخدامهم الموثوق للبيانات بالمدن الذكية.	%96

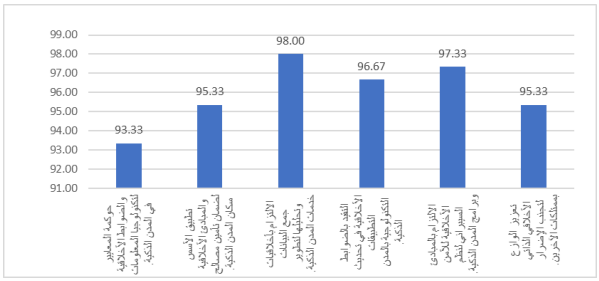
8	تحديث مستمر للتشريعات والسياسات الأمنية تبعا للمستجدات التكنولوجية للمدن الذكية.	%98
المتوسط التقويمي للمحور		%9.95
ب) محور الحلول التثقيفية		
1	نشر ثقافة تشارك الأفكار الأمنية والمنهجيات بتعاون مصممي الأنظمة، ومقدمي الخدمات بالمدن المختلفة.	%96
2	إعطاء أولوية توظيفية وتدريبية للخبراء التقنيين في مجالات الأمن السيبراني لحماية البيانات الرقمية.	%94
3	توعية مخططي المدن الذكية ومزودي خدماتها بأهمية الحماية الإلكترونية وفوائدها.	%96.7
4	التوعية بوسائل أمن المعلومات للمحافظة على سريتها، وتجنب اختراقها والعبث بها.	%96
5	نشر الوعي الأمني السيبراني وتوفير مقاييسه وأدواته.	%95
6	تدارس الأفكار والآليات الأمنية لمواجهة مجرمي الإنترنت وتهديداتهم عبثهم بالبيانات.	%96
7	مناقشة المنظمات سبل تعزيزي الأمن السيبراني للمدن الذكية في ظل اتساع استخدامات إنترنت الأشياء IoT.	%95
8	التعريف بالمبادئ التوجيهية للأمن السيبراني للمدن الذكية وأدوار الأفراد ومؤسسات المجتمع في تحقيقه.	%93
المتوسط التقويمي للمحور		%95.3
جـ) محور الحلول الأخلاقية		
1	حوكمة المعايير والضوابط الأخلاقية لتكنولوجيا المعلومات في المدن الذكية.	%93
2	تطبيق الأسس والمبادئ الأخلاقية لضمان تأمين مصالح سكان المدن الذكية.	%95
3	الالتزام بأخلاقيات جمع البيانات وتحليلها لتطوير خدمات المدن الذكية.	%98
4	التقيد بالضوابط الأخلاقية في تحديث التطبيقات التكنولوجية بالمدن الذكية.	%96.7
5	الالتزام بالمبادئ الأخلاقية للأمن السيبراني لنظم وبرامج المدن الذكية.	%97.33
6	تعزيز الوازع الأخلاقي الذاتي لتجنب الإضرار بممتلكات الآخرين.	%95.33
المتوسط التقويمي للمحور		%96
المتوسط النسبي التقويمي العام لكل محاور الاستبانة		%95.77



الشكل (3): الحلول التشريعية



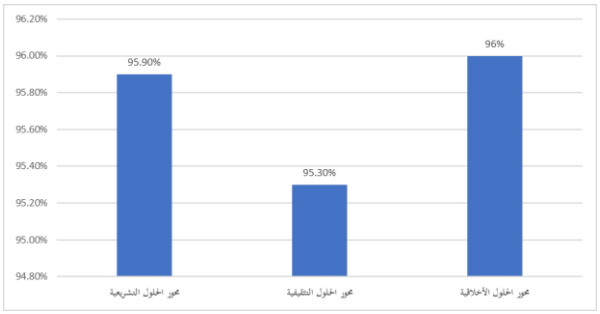
الشكل (4): الحلول التثقيفية



الشكل (5): الحلول الأخلاقية

الجدول (2): محصلة النتائج التقويمية للحلول التشريعية، والتثقيفية، والأخلاقية لتحديات الأمن الإلكتروني وتهديداتها وترتيبها تبعا لنسبها المئوية الوزنية التقويمية

م	المحصلات التقويمية الوزنية النسبية لمحاور حلول تحديات الأمن الإلكتروني وتهديداتها	النسبة % التقويمية	الترتيب
3	محور الحلول التشريعية	%95.9	2
4	محور الحلول التثقيفية	%95.3	3
5	محور الحلول الأخلاقية	%96	1
المتوسط النسبي للمحصلة التقويمية العامة لكل محاور الاستبانة		%93.4	



الشكل (6): التمثيل البياني للنتائج التقييمية للحلول التشريعية، والتثقيفية، والأخلاقية لتحديات الأمن السيبراني للمدن الذكية وترتيبها تبعا لنسبها المئوية

ونظرا لتنامي عناية الدول العربية الأسيوية والإفريقية بتطوير مدنها التقليدية لتتحول إلى مدن حضرية ذكية، فإن ثمة جهود ينبغي تكاملها للمساهمة في التوعية التثقيفية بالحلول المقترحة للتحديات الأمنية السيبرانية التي تواجه المدن الذكية العربية، ويُعد المشروع المقترح الحالي حلقة في سلسلة هذه الجهود.

ج) أهداف المشروع

يستهدف المشروع في مرحلته الأولى وضع تصورا مرناً لإطار برنامج مقترح، لتوعية مجموعة من المثقفين المسؤولين في المجتمع، ومنهم منتسبي التعليم العام والعالي، ورجال الإعلام، وعلماء الدين، وجميعهم ممن يمكنهم المشاركة في توعية أفراد المجتمع بالتحديات الأمنية السيبرانية وتهديداتها للمدن الذكية العربية وحلولها، وذلك لتحقيق الأهداف التالية:

1- التوظيف التطبيقي لمضامين البحث الحالي وتوصياته ومقترحاته لتحقيق مستهدفات مخرجاتها، لمواجهة تحديات الأمن السيبراني للمدن الذكية العربية، ومواجهة تهديداتها التأثيرية في الفرد والمجتمع.

2- تنمية قدرات بعض المسئولين من أفراد المجتمع، للقيام بمهام التوعية بتحديات الأمن السيبراني للمدن الذكية وتهديداتها، وحلولها.

3- تقديم أبرز الحلول المقترحة المناسبة لمواجهة تحديات المدن الذكية في ضوء المحصلة التقويمية لمدى مناسبتها من وجهة نظر المتخصصين.

4- إكساب مفاهيم ومهارات تفكير لحل المشكلات واتخاذ القرار بشأن التحديات التي تواجه الأمن السيبراني للمدن الذكية العربية، ومناسبة الحلول التقنية، والأمنية، والتشريعية، والتثقيفية، والأخلاقية المقترحة.

5- التكامل التنسيقي بين الجهود، لتعزيز الوعي التثقيفي بتحديات الأمن السيبراني للمدن الذكية العربية وتهديداتها، والمحصلة التقويمية لحلولها المقترحة.

د) أهمية المشروع

تبرز أهمية المشروع من خلال ارتباطه بموضوع الأمن السيبراني للمدن الذكية، الذي يحظى بعناية متزايدة على المستويين العالمي والعربي، نظرا لتعدد التحديات والتهديدات الأمنية الناجمة عن مهاجمة المتسللين لنظمها وأجهزتها وبرامجها. ويمكن إيجاز أبرز أوجه أهمية المشروع المقترح من خلال مساهمته في:

1- إفادة سكان المدن العربية وزوارها بأبرز التحديات الأمنية الإلكترونية وتهديداتها للمدن، ليكون لهم دور فاعل في المبادرة التنفيذية للحلول المقترحة لمواجهتها.

2- مساعدة المسؤولين عن تخطيط المدن الذكية والمشرفون على نظم إدارتها على تعرف الأدوار التثقيفية لمواجهة التحديات الإلكترونية الأمنية للمدن الذكية.

3- تزويد منتسبو التعليم العام والعالي، ورجال الإعلام، وعلماء الدين من الدعاة وأئمة المساجد، بحلول تطبيقية متعددة لمواجهة الهجمات السيبرانية الشرسة على المدن الذكية، لمساعدتهم على القيام بأدوارهم التثقيفية التوعوية للمجتمع في هذا المجال.

4- تزويد صناع السياسات على المستوى العربي بالتحديات والتهديدات السيبرانية للمدن الذكية، وما تتطلبه من اتخاذ إجراءات للحوكمة التشريعية والأمنية على المستويات الدولية لمواجهتها، والحلول ذات الأثر الفاعل في تحقيق ذلك.

5- إفادة الشركات التقنية والموردة لخدماتها للمدن الذكية بالآليات التنفيذية التي يمكنهم المشاركة فيها، لتعزيز الثقافة الأمنية السيبرانية للمدن الذكية.

هـ) مرحلة إعداد المشروع

ويمكن أن تتم وفق للخطوات التالية:

1- يُعقد اجتماع لفريق من المتخصصين الأكاديميين (خبراء تعليم – خبراء تقنية المعلومات- متخصصون في التشريعات القانونية- رجال أمن- علماء في التربية والإعلام، والاجتماع والدعوة، والأخلاقيات) لتحديد أهداف البرنامج المقترح ومحتواه، والموضوعات المراد تدارسها من منظور تقني، تثقيفي، تشريعي، أمني، أخلاقي، في إطار الثوابت العربية.

2- تحدد مصادر اشتقاق المعرفة اللازمة، وعناصرها، وموضوعاتها ومحدداتها وضوابط محتواها المحقق لأهداف البرنامج، والطرائق الملائمة لتدارسها، والأنشطة المصاحبة، وأساليب التقويم المناسبة لها.

3- يُناقش البرنامج في صورته الأولية للإثراء التفصيلي لهيكله المقترح، وذلك مع متخصصين من علماء التقنية، والتربية، والإعلام، والتشريع، ورجال الأمن، وعلماء الدين.

4- توضع خطة لقنوات التنفيذ التي يمكن أن يتم تنفيذ البرنامج من خلالها، وتشمل قنوات:

أ- تقنية: وتشمل أنشطة تنظمها كليات الحاسبات وتقنية المعلومات، ومراكز دعم القرار.

ب- أمنية: وتشمل: ندوات ونشرات تعريفية بالتحديات الأمنية السيبرانية، وعقوبات جرائمها.

ج- تعليمية وتشريعية: وتنظمها مراكز ووحدات خدمة المجتمع في الكليات التربوية، والتشريعية بالجامعات، وفي مراكز التدريب التابعة لإدارات التعليم.

د- إعلامية: وتشمل: المواقع التثقيفية عبر الإنترنت، والقنوات المرئية التي تعرض حوارات ومناقشات، ومناظرات، واستطلاعات للرأي، والقنوات المسموعة التي تطرح تحليلات وتفسيرات، والقنوات المقروءة التي تنشر مقالات، وكتب، ودراسات.

هـ- أخلاقية: وتشمل: خطب، ودروس، وكتيبات، ومواد مرئية ومسموعة، وما تقدمه مؤسسات الشئون الاجتماعية من أنشطة أخلاقية خلال مراكزها ووحداتها للأسر والأفراد.

5- تحدد كافة الاحتياجات اللازمة لتنفيذ البرنامج عبر كل قناة من القنوات السابقة.

و) مرحلة تنفيذ المشروع

يمكن أن يتم تنفذ برنامج المشروع بتكامل أنشطة القنوات التقنية، والتعليمية، والإعلامية، والتشريعية، والأمنية. حيث يعقد الفريق القائم بالتنفيذ لقاءات مع المثقفين المسؤولين في مؤسسات المجتمع، ويمكن تنظيم بعض اللقاءات عبر منصات زوم Zoom، وبعضها الآخر في لقاءات مباشرة، تشمل ما يلي:

1- محاضرات حول تحديات الأمن السيبراني وتهديداته، مع التركيز على أضرار تلك التحديات والتهديدات على الفرد والمجتمع في المدن الذكية.

2- مناقشات حول الحلول المقترحة للتحديات السيبرانية للمدن الذكية العربية، ومخاطرها، وتهديداتها، وقرائنها الدلالية وعقوباتها، وسبل ترسيخ القيم والضوابط الأخلاقية لمواجهتها.

3- عرض نماذج من التأثيرات المتباينة للهجمات السيبرانية الإلكترونية للمدن الذكية، وما ترتب عليها من جرائم، وتحليلها ومناقشتها، واستطلاع أراء المفكرين حولها.

4- تنظيم مؤتمرات ومنتديات نقاشية للبحوث والدراسات الخاصة

بالتحديات الأمنية السيبرانية وتهديداتها وحلولها.

ز) مرحلة تقويم المشروع

يمكن تقويم المشروع للوقوف على إيجابياته، ومعالجة سلبياته، من خلال ما يلي:

1- تطبيق اختبارات تقويمية لمضامين المشروع، وتحليل أنماط التفاعل مع موضوعاته في اللقاءات التثقيفية عبر المنصة الإلكترونية، واللقاءات المباشرة في المحاضرات.

2- تطبيق مقاييس الاتجاهات والقيم الخاصة بقياس مدى تأثير المشروع في التوعية التثقيفية بالتحديات السيبرانية للمدن الذكية العربية، والجوانب التفاعلية الوجدانية معها.

3- تقييم تقارير المشاركين، ومقترحاتهم لمواجهة تحديات وتهديدات الأمن السيبراني للمدن الذكية العربية، والآليات الفاعلة في التوعية للحد من مخاطرها.

4- تحدد إيجابيات برنامج المشروع المقترح وسلبياته، في ضوء ما تظهره نتائج تقويمه.

توصيات البحث

يتناول هذا القسم من البحث التوصيات والمقترحات لمواجهة التحديات الأمنية السيبرانية للمدن الذكية والسبل المناسبة لمواجهتها.

توصيات البحث ومقترحاته

من خلال مراجعة أدبيات البحث وما أسفر عنه من نتائج، يمكن تقديم التوصيات والمقترحات الاستشرافية للمساهمة في مواجهة التحديات الأمنية السيبرانية للمدن الذكية على النحو التالي:

1- تغليظ العقوبات التشريعية والقانونية للحماية الأمنية إلكترونية للمدن الذكية، لردع المجرمين، مما يتطلب تكاتف على المستوى الدولي بين الهيئات والمجالس لمحاربة الإرهاب السيبراني.

2- زيادة إعداد الكوادر المؤهلة للتأمين السيبراني للمدن الذكية من التعرض لجرائم العابثين مثل الهاكرز Hackers أو المهاجمين لأغراض غير قانونية مثل الكراكرز Crackers.

3- التوعية الجادة بمخاطر الجرائم السيبرانية، بجهود تشاركية فاعلة لمؤسسات المجتمع ذات العلاقة، لمواجهة التحديات والتهديدات المؤثرة على الفرد والمجتمع في المدن الذكية.

4- بناءً على مراجعة ممارسات المدن الذكية المختارة في المملكة، وفقًا للفئات الرئيسة الثلاث للمدينة الذكية التي طورها هذا البحث؛ مدينة رقمية (الحوكمة الذكية وأبعاد الحياة الذكية)، وذكاء المدينة (بعد المواطنين الأذكياء)، والمدينة البيئية (الاقتصاد الذكي، والنقل الذكي، وأبعاد البيئة الذكية).

5- يكمن التغلب على تحديات المستقبل في الموارد البشرية للمملكة، والاستثمار في الناس من خلال التركيز على بُعد المواطنين الأذكياء سينتج عنه امتلاك مدينة ذكية حقًا تؤدي إلى مدينة ذكية كاملة.

6- نظرا للتزايد الملحوظ للتحديات والتهديدات السيبرانية للمدن الذكية، فإن ثمة حاجة إلى سياسات وإجراءات إدارية لتحقيق أفضل معدلات الاستقرار الشبكي، والاستدامة التأمينية للنظم الإلكترونية، وذلك بتوظيف تطبيقات الذكاء الاصطناعي في تحليل بياناتها الضخمة اللازمة لصناعة القرار، بالتبادل الفعال للبيانات عبر الأجهزة والشبكات، لخفض معدلات استهلاك الطاقة، وتنظيم السير وغيرها من الخدمات الأخرى المتعددة في المدن الذكية.

7- إن كفاءة خدمات المدن الذكية في المجالات المصرفية والمالية، والإمدادات الغذائية وغيرها؛ مرهون بكفاءة البني التحتية لنظمها التكنولوجية، ومستويات تأمينها. حيث يترتب على تعطلها أو تدميرها تأثيرات ومخاطر شتى على: للأمن والسلامة، والصحة، ورفاهية السكان، مما يوجب العناية بسبل الوصول الرقمي إلى مرافق المدن الذكية، وتأمينها من الهجمات السيبرانية.

8- لقد ساهم اتساع نطاق الفضاء الإلكتروني في تزايد التحديات التصميمية والتشغيلية المهددة للأمن الإلكتروني للمدن الذكية، وأسفر عن تهديدات ومخاطر تدميرية متعددة، نجمت عن حرية السماح للمستخدمين بالوصول إلى كافة موارد بيانات الشبكة الداخلية للمدن (الإنترانت)، أو دخولهم إلى النظم التقنية لإدارة خدماتها عبر الفضاء الإلكتروني الخارجي (الإنترنت). مما ترتب عليه العديد من التحديات والتهديدات الأمنية الإلكترونية منها: الانتحال، والتلاعب، وتجاوز الصلاحيات، والتصيد الاحتيالي، والاحتيال المصرفي. وثمة تزايد لحجم تحديات الأمن الإلكتروني للمدن الذكية بتزايد أعداد الأجهزة المتصلة بالشبكات الداخلية والخارجية، وتستمر هذه التهديدات في خطورتها نظرا لمواصلة مجرمي الإنترنت ابتكار طرق وأساليب جديدة، يسيئون بها استخدام تكنولوجيا المعلومات، ويتحايلون باحترافية على اختراق ثغرات النظم الإلكترونية.

الشكر Acknowledgement

تم تمويل هذا العمل البحثي من قبل مشاريع الصندوق المؤسسي تحت المنحة رقم (IFPAS-045-611-2020)، لذلك، يقدم المؤلفون شكرهم للدعم الفني والمالي من وزارة التربية والتعليم وجامعة الملك عبد العزيز، جدة، المملكة العربية السعودية.

الإفصاح و التصريحات

تضارب المصالح: ليس لدى المؤلفون أي مصالح مالية أو غير مالية ذات صلة للكشف عنها. المؤلفون يعلنون عن عدم وجود اي تضارب في المصالح.

قائمة المراجع:

الأمن السيبراني للمدن الذكية. (2020). مسترجع بتاريخ أغسطس 2،2021، من موقع https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html.

أمن المدينة الذكية. (2020). مسترجع بتاريخ مايو 17،2022، من موقع https://techcrunch.com/2015/09/12/building-smart-city-security/

الأمن في المدن الذكية. (2020). *الأمن السيبراني*. مسترجع بتاريخ ديسمبر 10،2021، من موقع https://www.arab-cio.org

باله، صباح. (2020). *الموسوعة السياسية*. مسترجع بتاريخ مايو 17،2022، من موقع https://political-encyclopedia.org/dictionary/

البيان. (2016). *التحديات الأمنية للمدن الذكية في مؤتمر أمن المعلومات*. مسترجع بتاريخ مايو 17،2022، من موقع https://www.albayan.ae/economy/local-market/2016-03-14-1.2594531

البيانات الذكية ما هي وكيف تختلف؟. (2017). مسترجع بتاريخ مايو 17،2022، من موقع https://mail.aol.com/webmail-std/en-us/suite

تحدي الأمن السيبراني في المدن الذكية. (2020). *دراسة حالة مشروع الأمة الذكية في سنغافورة*. مسترجع بتاريخ سبتمبر 10،2021، من موقع https://www.researchgate.net/

تحديات الأمن السيبراني للمدن الذكية. (2020). مسترجع بتاريخ مايو 17،2022، من موقع https://resources.infosecinstitute.com/top-cyber-security-challenges-smart-cities/#gref

تحديات المدن الذكية. (2020). مسترجع بتاريخ مايو 17،2022، من موقع https://blog.mobility.here.com/smart-city-challenges

تقرير الاتحاد الدولي للاتصالات. (2015). *المدن الذكية المستدامة*. الاتحاد الدولي للاتصالات ولجنة الأمم المتحدة الاقتصادية لأوروبا. https://www.itu.int/ar/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx

حسين، فاتن. (2020). *كيف تواجه المدن الذكية بالعالم العربي تحديات التمدن؟*. مسترجع بتاريخ مايو 17،2022، من موقع https://www.tech-mag.net

باسم، حسين. (2018). *تحديات الأمن السيبراني*. مسترجع بتاريخ مايو 17،2022، من موقع http://kerbalacss.uokerbala.edu.iq/wp/blog

دنيا الوطن. (2016). *مؤتمر كوالس الأمني" السنوي يكشف عن أحدث الحلول التكنولوجية الأمنية عالمية المستوى*. مسترجع بتاريخ مايو 12،2022، من موقع https://www.alwatanvoice.com/arabic/news/2016/05/12/916744.html

الدويكات، سناء. (2018) *تعريف الأمن*. مسترجع بتاريخ مايو 17،2022، من موقع https://mawdoo3.com

عبد الفتاح، محمد. (2016). *الاتجاهات التنموية الحديثة في ممارسة الخدمة الاجتماعية*. المكتب الجامعي الحديث الإسكندرية.

العتيبي، فهد، البرهمتوشي، حسنين، كاتب، فارس، وريان موصلي. (2022). واقع المدن الذكية السعودية وتحدياتها الأمنية السيبرانية وحلولها في ضوء رؤية المملكة 2030م. *مجلة الآداب والعلوم الإنسانية، 30*(6)، 113-73.

العلي، عماد. (2017). *مجالس المستقبل العالمية: تعزيز الأمن السيبراني ضرورة حيوية*. وكالة أنباء الإمارات http://wam.ae/ar/details/1395302646036

عمر، الأخضر، وريمي، عقبة. (2019). *المدن الذكية من المقاربة النظرية إلى التجارب العربية*، مؤتمر المدن الذكية في ظل التغيرات الراهنة واقع وآفاق، المركز الديمقراطي العربي بالتعاون مع مخبر اللغة العربية وآدابها، جامعة البليدة، برلين، ألمانيا.

عنتر، أسماء، ومعمر، حيتالة. (2019). *الحماية القانونية للمدن الذكية من الجرائم الإلكترونية*. مؤتمر المدن الذكية في ظل التغيرات الراهنة واقع وآفاق، المركز الديمقراطي العربي بالتعاون مع مخبر اللغة العربية وآدابها، جامعة البليدة، برلين، ألمانيا.

عوده، سليمان. (2020). *المنتدى الحضري العالمي: هكذا تصبح المدن ذكية، الدورة العاشرة في أبو ظبي تعرض تجارب عربية في استخدام الذكاء الاصطناعي*. مسترجع بتاريخ مايو 17،2022، من موقع https://www.awalan.com/Article

غاوي، ميشيل. (2019). *أمن المعلومات وتحديث البيئة التشريعية أبرز تحديات المدن الذكية*. مسترجع بتاريخ مايو 12،2022، من موقع https://www.alroeya.com/9-20/2041084

لينوفو وبيفوت. (2018). *شراكة لتحسين أمن المدينة الذكية*. مسترجع بتاريخ مايو 11،2022، من موقع https://aetoswire.com/ar/news

مبادرة نيويورك. (2016). *مبادرة عالمية لحماية المدن الذكية من الخروقات الأمنية*. مسترجع بتاريخ مايو 17،2022، من موقع https://webcache.googleusercontent.com

مجتمع تكنولوجيا المعلومات. (2019). *ما هو الأمن السيبراني (الأمن الإلكتروني)؟*. مسترجع بتاريخ مايو 17،2022، من موقع https://itcomunity.com/post/

محمد، أميمة. (2017). *التحديات المؤثرة على التنمية*. مسترجع بتاريخ مايو 17،2022، من موقع http://omeema90.blogspot.com/2017/01/blog-post_79.html

مطاوع، ضياء الدين، والخليفة، حسن. (2017). *مبادئ البحث ومهاراته*. دار المتنبي.

References

Al-Barhamtoshy, A., & Abd al-Latif, F. (2018). Intelligent Traffic Vehicles (ITV) and Road Sign Detection Systems. *JKAU: Comp. IT. Sci., 7* (1), 1 – 16. Doi: 10.4197/Comp. 7-1.1

Al-Barrak, I. (2011). *Al Ahsa Industrial City*. 2018 MODON. Saudi Authority for Industrial Cities and Technology Zones. Retrieved Febraury2,2022, from https://www.modon.gov.sa/en/

Chen, M. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations *Energy Reports, 7*. 7999- 8012. https://doi.org/10.1016/j.egyr.2021.08.124 .

Copper, J. (1981). *Measuring Behaviour*. Bell, H., & Columbus, Ohio.

Desouza, K., Hunter, M., Jacob, B., & Yigitcanlar, T. (2020). Pathways to the making of prosperous smart cities: An exploratory study on the best practice. *J. Urban Techno, 27*(3), 3–32. DOI: 10.1080/10630732.2020.1807251

Farag, A. (2019). The Story of NEOM City: Opportunities and Challenges. In S. Attia, Z. Shafik, & A. Ibrahim (Eds.), *New Cities and Community Extensions in Egypt and the Middle East* (pp. 35-49). Springer. https://doi.org/10.1007/978-3-319-77875-4_3

Jackson, W. (2013). "*Einstein 3 goes live with automated malware blocking" GNC blocking*. Retrieved Febraury15, 2022, from https://gcn.com/ articles/2013/07/24/einstein-3-automated-malware-blocking.aspx

Kaluarachchi, Y. (2022). Implementing Data-Driven Smart City Applications for Future Cities. *Smart Cities, 5*(2), 455-474. https://doi.org/10.3390/smartcities5020025

Kumar, H., Singh, M., & Gupta, M. (2016). *September Smart governance for smart cities: A conceptual framework from social media practices. In: Conference on e-Business, e-Services and e-Society*. Springer, Cham, 628-634. DOI: 10.1007/978-3-319-45234-0_56

Lee, K. (2017). *"The Real Threat of Artificial Intelligence*". Sunday Opinion Section. https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html

Pelton ،J., & Singh, I. (2019). *Smart Cities of Today and Tomorrow Better Technology ،Infrastructur*. Retrieved Febraury15,2022, from https://www.amazon.com/Smart-Cities-Today-Tomorrow-Infrastructure/dp/3319958216

Smart city. (2020). "Alcatel-Lucent Enterprise's Business Partner". Retrieved Febraury15, 2022, from https://rg.smartcitiescouncil.com/readiness-guide/article/definition-definition-smart-city

Smart City. (2021). *A Tool for Action, an Instrument for Better Lives for all Citizens, IMD World Competitiveness Centre*.file:///C:/Users/Lenovo/Downloads/smart_city_index2021%20(1).pdf.

Thorndike, R., & Hagen, E. (1990). *Measurement and Evaluation.* John Wiley & Sons.

UCLG. (2020). *Smart Cities Study, International Study on the Situation and Future Trends in Smart Governance*. UCLG Bilbao.

Weiner, R. (2017). "*Romanians Charged with Hacking*" Washington Post.

Wordfly. (2018). "The Importance of Security". Retrieved March12, 2022, from www.wordfly.com .