مجلة الرواق للدراسات الاجتماعية والإنسانية | ISSN: 2437 - 0363 EISSN 2602-6767 | المجلد 08 / العـدد: 02 (2022)، ص 339- 359

أنظمة الأمن المنزلية بين تعزيز الحماية ومواجهة التهديدات

Home Security Systems between enhancing protection and confronting threats

مهملي بن علي*

جامعة أحمد زبانة غليزان (الجزائر)، mehamlidz@gmail.com

تاريخ الاستلام: 2022/03/26 تاريخ القبول: 2022/12/19 تاريخ النشر: 2022/12/28

ملخص:

يمثل المنزل الذكي ذلك الإطار الرقمي الذي تتفاعل من خلاله التكنولوجيا الحديثة وتنسجم مع كل الأشياء داخل المنزل وخارجه، ويتضمن نظام أمان المنزل مجموعة من المعدات والأجهزة التي تطلق إشارات الإنذار عند اختراق نقطة الدخول، يجب أن تتواصل أجهزة الاستشعار مع لوحة التحكم لتأمين المنزل، وعلى الرغم من التطور الكبير في مجال تكنولوجيا المعلومات تبقى المنازل الذكية مُعرّضة لخطر القرصنة والتشويش والاختراق الأمني، مما يتوجب تعزيز أنظمة الحماية المنزلية بأحدث الإبتكارات التكنولوجية، مع ضرورة التعامل مع مؤسسات وشركات عالمية رائدة ومعروفة في هذا المجال، تقوم بتوفير تحديثات البرامج والأمان بصورة تلقائية ومنتظمة.

كلمات مفتاحية: المنزل الذكي، الذكاء الإصطناعي، أنظمة الأمن المنزلية

Abstract:

The smart home represents that digital framework through which modern technology interacts and harmonizes with all things inside and outside the house. The home security system includes a set of equipment and devices that fire alarm signals when the entry point is breached, the sensors must communicate with the control panel to secure the house, although From the great development in the field of information technology, smart homes remain exposed to the risk of piracy and security breaches, which requires strengthening home protection systems with the latest technological innovations, and to deal with leading and well-known international institutions and companies in this field, which provide regular updates for software and systems.

Keywords: Smart home, artificial intelligence, home security systems.

*المؤلف المرسل

1. مقدمة:

أصبح مصطلح المنزل الذكي Smart Home من أحدث مفاهيم التكنولوجيا في الوقت الراهن، فهو الضامن الأساسي لتعزيز الأمن والأمان وتوفير الراحة والرفاهية ، حيث يتم على أساسه ربط مختلف الأجهزة والأنظمة المختلفة في المنزل عبر برامج وتطبيقات ومستشعرات وتكنولوجيات الذكاء الإصطناعي، بحيث يمكن التحكم فيها جميعاً من أي مكان في العالم بواسطة شبكة الإنترنت، بحيث تصبح الأشياء قابلة للاتصال بالإنترنت أو ببعضها البعض لإرسال و استقبال البيانات لأداء وظائفها المختلفة بكل فعالية، كما يتوفر المسكن الذكي على أنظمة صديقة للبيئة يمكن من خلالها توفير الطاقة والمحافظة على البيئة، هذا بالإضافة إلى أنظمة ذكية للتشغيل والتحكم والمراقبة، ولكي يتعزز هذا الأمن وتتحقق هذه الرفاهية لابد من ضمان التأمين الكامل لخصوصية بيانات المستخدم وحمايتها من التهديدات والمخاطر الأمنية المختلفة كالقرصنة والإختراق الأمني والتشويش وغيرها.

تطرح الأسواق في الوقت الراهن عددًا كبيرا من أنظمة الأمن والحماية الخاصة بالمنازل، والتي لا تتطلب معرفة أو مهارات خاصة لتركيبها أو حتى تشغيلها، مما جعلها محل طلب الكثير من المهتمين، ولكن في نفس الوقت لا يمكن لنا أن ننكر بعض الصعوبات التي يمكن مواجهتها، قد لا يمكنك الدخول إلى منزلك في أية لحظة، كوجود خطأ فني أو تقني أو تبلل أصابع اليدين أو اتساخها أو إصابتها مما يسبب اضطرابا لماسح البصمة، وغير قادر على إلغاء القفل بسهولة وسرعة، أو بعض أخطاء الإنذار كأن ينطلق جرس الإنذار في أية لحظة لسبب من الأسباب، وتتلقى رسالة من نظام الأمن على هاتفك وأنت بعيد عن المنزل، هذا ناهيك عن مشكل نفاذ بطارية الهاتف مثلا أو مشكل غياب تغطية شبكة المحمول والتي بواسطتها نتلقى رسائل الإنذار على الهواتف النقالة، قد تكون في مكان خارج مجال التغطية مما يصعب المأمورية على نظام الأمن بإيصال رسائل الإنذار إليك، أو

مشكل القرصنة مثلا، وغيرها من المشاكل التقنية والمخاطر الأمنية الأخرى، لكن على العموم تبقى تكنولوجية تأمين المنازل من بين الأولويات الرئيسية في الوقت الراهن لضمان تحصين المنازل وحمايتها، وتحقيق الرفاهية المنشودة للبشر.

مما سبق ذكره نطرح الإشكالية التالية :"ما المقصود بأنظمة الأمن المنزلية، وما هو الدور الذي تلعبه في تعزيز مستوى الحماية ؟"

يتفرع عن هذه الإشكالية الأسئلة الفرعية التالية:

1. ما المقصود بالمنزل الذكي؟ وماهي مميزاته وعيوبه؟
2. ما هي أنواع أنظمة الأمن والحماية المنزلية؟
3. هل يمكن لنظم الأمان المنزلية تأمين المنزل بالكامل من جميع المخاطر والتهديدات الأمنية؟
4. كيف نقيم واقع سوق المنازل الذكية في العالم؟

على ضوء ما سبق ذكره قمنا بصياغة الفرضيات التالية:

1. كلما كان نظام الحماية الداخلي والخارجي للمنزل قويا كلما كانت حماية المنزل أكثر فعالية.
2. يبقى نظام الأمن والحماية الداخلي والخارجي للمنزل غير كاف نظرا لإمكانية تعرضه للإختراق الأمني والتشويش من طرف المتطفلين.

تهدف هذه الدراسة إلى إبراز أهمية أنظمة الحماية المنزلية في توفير الأمان والحماية والرفاهية ، فمن خلالها يمكن مراقبة كل ما يحدث داخل المنزل وخارجه، والتحكم بجميع الأجهزة المنزلية المتصلة بهذه الأنظمة، بالإضافة إلى مكافحة المتطفلين والمتسللين، وتمكين هذه الأجهزة الذكية من الإتصال مباشرة بالطوارئ أو الشرطة في حالة وجود حركة غير عادية في المنزل.

نعالج إشكالية الدراسة من خلال التطرق للمحاور التالية:

المحور الأول: الإطار النظري العام لمفهوم أنظمة الأمن المنزلية.

المحور الثاني: الإنفاق العالمي على المنازل الذكية.

2. الإطار النظري العام لمفهوم أنظمة الأمن المنزلية.

تركز أغلب تكنولوجيات المنزل الذكي بشكل أكبر على تحقيق الأمان والطمأنينة ، حيث توفر هذه الأخيرة حماية متكاملة لكل ما يحدث داخل المنزل وخارجه، كما تساهم أنظمة الأمان والحماية المنزلية في خفض تكاليف استهلاك الطاقة والحفاظ على البيئة، كما أن التكنولوجيا التي تستخدمها غالبا صديقة للبيئة، بالإضافة إلى تبسيط وتسهيل حياة المسنين و أصحاب الاحتياجات الخاصة و المصابين بأمراض معينة أو الذين تعرضوا لحوادث أدت لتعطيل بعض حواسهم.

1.2 مفهوم أنظمة الأمن المنزلية.

1.1.2 تعريف المنزل الذكي:

يعرف المنزل الذكي بأنه ذلك المسكن الذي يحتوي على أجهزة تحكّم متطورة وهي شاشات لمسية ثابتة بالحائط أو متحركة، بالإضافة إلى أزرار تحكّم قابلة للبرمجة والتي باستطاعتها التحكُّم ومراقبة جميع الأجهزة الكهربائية والإلكترونية «الأشياء»، مثل الإضاءة والستائر الكهربائية والتكييف والتلفزيون والنظام الصوتي والكاميرات والأبواب الكهربائية ونظام السرقة والحريق وإنارة المسبح والنوافير، لمزيد من الراحة والأمان. (ثابت، 2020)

يمكن للمنزل أو البيت الذكي أن يتنبأ بحدوث عاصفة حيث سيلتقط التنبؤ الجوي من شبكة الإنترنت وسيقوم بالإجراءات الضرورية مثل رفع درجة الحرارة مثلا، فالمنزل الذكي أشبه بالممرضة الآلية التي تشخص الحالة بدقة وترسل المعلومات آليا إلى الطبيب. (بيزان، 2017، صفحة 69)

سيكون المنزل الذكي مجهزاً بأدوات ذكية، كآلة غسل الأواني الذكية، الفرن الذكي، والشاحن الكهربائي للسيارة، فكل هذه الأجهزة ستنتج بيانات وستتواصل فيما بينها. لذلك سنحتاج للغة مشتركة للتعامل مع هذه البيانات، وتحسين أعمال هذه الأجهزة الموجودة في المنزل الذكي". (Chacra, 2018)

يُعَبر المنزل الذكي عن تلك الحالة الشبكية التي ترتبط ضمنها الأشياء الموجودة في محيطنا ببعضها البعض، سواء تعلق الأمر بالآلات والأجهزة المنزلية وغيرها...الخ، ويتم ذلك عبر برمجيات ومستشعرات وتكنولوجيات الذكاء الإصطناعي، والكمبيوترات العملاقة، بحيث تحدث عمليات كثيفة من تبادل البيانات وتلقي الأوامر والتخاطب بين الأشياء المتصلة بصورة مستقلة. (عبود، 2016، صفحة 214)

2.1.2 بعض المفاهيم المرتبطة به.

- **أتمتة المنازل:** يقصد بها التحكم الآلي في الأجهزة الإلكترونية الموجودة في المنزل. حيث أن هذه الأجهزة تكون متصلة بالإنترنت، فيسمح لك هذا الأمر بالتحكم بها عن بعد، كما يمكنك عن طريق أتمتة المنزل برمجة الأجهزة أيضاً لتشغيل بعضها البعض بشكل أوتوماتيكي، دون الحاجة للتحكم بها بشكل يدوي عبر تطبيق أو مساعد صوتي أو جهاز تحكم. (ما هي أتمتة المنازل؟ كيف تعمل وكيف يمكن تطبيقها؟، 2021)
- **إنترنت الأشياء** (بالانجليزية : Internet of Things - IoT)، مصطلح برز حديثا ، يُقصد به الجيل الجديد من الإنترنت (الشبكة) الذي يتيح التفاهم بين الأجهزة المترابطة مع بعضها (عبر بروتوكول الانترنت). وتشمل هذه الأجهزة الأدوات و المستشعرات ، والحساسات وأدوات الذكاء الاصطناعي المختلفة وغيرها. ويتخطى هذا التعريف المفهوم التقليدي وهو تواصل الأشخاص مع الحواسب والهواتف الذكية عبر شبكة عالمية واحدة ومن خلال بروتوكول الإنترنت التقليدي المعروف. وما يميز إنترنت الأشياء أنها تتيح للإنسان

التحرر من المكان، أي أن الشخص يستطيع التحكم في الأدوات من دون الحاجة إلى التواجد في مكان محدّد للتعامل مع جهاز معين. (الشريف، 2022، ص 9)

تعبر أنترنت الأشياء عن ذلك الشكل المتطور لشبكة الإنترنت بحيث تمتلك الأشياء في حياتنا قابلية الاتصال بالإنترنت أو ببعضها البعض لإرسال و استقبال البيانات لأداء وظائف محددة من خلال الشبكة، ويمكن أن تشير هذه الأشياء إلى مجموعة واسعة من الأجهزة مثل رقاقات الاستجابة الطبية الحيوية على حيوانات المزارع، الكاميرات المباشرة المزروعة في حيوانات البرية وفي المياه العميقة .....إلخ. (موسى وداسي، 2020، صفحة 525)

مما سبق ذكره نستنتج أن المنزل الذكي هو منزل رقمي تفاعلي تنسجم من خلاله التقنية الحديثة مع كل ما هو موجود في المنزل، فهو البيت الذي تحكمه وتديره التكنولوجيا الحديثة بالكامل عن طريق مجموعة من التطبيقات التي يتم تنزيلها على الهواتف الذكية المزودة بخدمة الإنترنت، كما أن هذه الأنظمة تتيح لمختلف الأجهزة المنزلية التواصل مع الأجهزة الالكترونية الذكية كالهواتف والحواسيب اللوحية وأجهزة التلفاز الذكية في سبيل تسهيل الحياة وتبسيطها جعلها أكثر أمنا ورفاهية.

3.1.2 تعريف أنظمة الأمن المنزلية:

تعرف الأنظمة الأمنية بأنها وسيلة أو طريقة يتم من خلالها تأمين شيء ما من خلال نظام من مكونات وأجهزة تعمل مع بعضها البعض، كما تعمل أنظمة أمن المنازل على مفهوم بسيط هو تأمين نقاط الدخول إلى المنزل استخدام مستشعرات تتصل بلوحة تحكم أو مركز قيادة مثبت في مكان مناسب في مكان ما بالمنزل. وعادة ما يتم وضع أجهزة الاستشعار في الأبواب التي تؤدي من وإلى المنزل، بالإضافة إلى النوافذ التي يسهل الوصول إليها ، وفتحها ، خاصة تلك الموجودة على مستوى الأرض، كما يمكن تأمين المساحات المفتوحة داخل المنازل بأجهزة استشعار الحركة، ولقد تم تصميم أنظمة الأمان لأداء مهام معينة عند اختراق منطقة آمنة. (V KHANAA , P 255، 2018)

فنظام أمن المنزل، في أبسط المستويات، هو المعدات (أجهزة الاستشعار) التي تطلق إنذارًا عند اختراق نقطة دخول، بالطبع يجب أن تتواصل المستشعرات مع لوحة التحكم لتأمين المنزل، فإلى جانب المستشعرات، يمكن أن تتكامل العديد من الأجهزة الأخرى مع لوحة التحكم أو المحور المركزي للنظام (Home Security Systems: Your Options for 2022).

2.2 أنواع أنظمة الأمن والحماية المنزلية:

تنقسم أنظمة الحماية المنزلية إلى:

أ. **نظام الحماية الخارجي:** يعمل هذا النظام على ترهيب اللّص قبل الدخول إلى المنزل عن طريق استخدام موصلات الأبواب والنوافذ وكواشف كسر الزجاج، ففي اللحظة التي يفتح الباب أو النافذة شخص ما، أو يكسر الزجاج، يتم تفعيل أجهزة الإنذار، ومن المعروف أن معظم اللصوص يفضلون الابتعاد عن مكامن الخطر، ومن بينها: تلك البيوت التي تشتمل على أنظمة إنذار خارجية، لذلك فإن احتمالات عودة اللّص تبدو ضئيلة للغاية (السداوي، 2019).

ب. **نظام الحماية الداخلي:** يهدف هذا النوع من أنظمة الحماية إلى جعل منزلك فخاً للّص خلافاً لنظام الحماية المحيطة بكل ما لديها من موصلات للأبواب والنوافذ، ويعتمد النظام الداخلي أساساً على استخدام كواشف الحركة، وكما يوحي الاسم، فإن اللص يجب أن يكون داخل المبنى قبل أي إنذار (السداوي، 2019).

ج. **أنظمة الحماية المدمجة:** وهي الأنظمة التي تجمع بين نظام الحماية الداخلي والخارجي.

3.2 مكونات أنظمة الأمن المنزلية:

يتكون نظام أمن المنزل من مجموعة من المكونات الإلكترونية المادية التي تعمل جميعها معًا لحماية المنزل، غالبًا ما يتكون نظام أمان المنزل من العناصر التالية: (Aliza Vigderman، 2022)

أ. كاميرات الأمان: تتصل كاميرات الأمان الذكية بشبكة Wi-Fi ، مما يسمح ببث لقطات حية عن بُعد وتلقي الإشعارات عندما تكتشف هذه الكاميرات الحركة أو الأشخاص أو الطرود. كما تشتمل العديد من الكاميرات على الرؤية الليلية بالأشعة تحت الحمراء أو الملونة ، أو التخزين السحابي أو المحلي ، والصوت ثنائي الاتجاه ، مما يسمح لنا بالتحدث إلى أي شخص أمام الكاميرا. تحتوي بعض الكاميرات أيضًا على تكامل الأنظمة الأساسية الذكية مثل Amazon Alexa أو Google Assistant.

ب. مستشعر الحركة: يجب وضع مستشعرات الحركة في المدخل الرئيسي أو الردهة في الطابق الأرضي من المنزل حتى يتمكنوا من اكتشاف الحركة وتنبيهنا عندما يكون نظامنا مسلحًا، كما أن بعض مستشعرات الحركة حساسة للحيوانات الأليفة.

ج. مستشعر الدخول: المعروف أيضًا باسم مستشعرات الاتصال، تتكون مستشعرات الدخول من جزأين: أحدهما يكون على النافذة أو الباب والآخر على الإطار، كما تستخدم هذه المستشعرات المغناطيس لتحديد وقت فتح أو إغلاق أحد هذه المداخل، فإذا اعتقد المستشعر أن نقطة دخول مفتوحة، فإنه يقوم بتنبيهنا فورا. كما تعمل الغالبية بالبطاريات، بل إن العديد منها مزودة بدعامات لاصقة لسهولة التركيب.

د. مستشعر كسر الزجاج: في بعض الأحيان، بدلاً من فتح النوافذ بالطريقة القديمة، يقوم المتسللون ببساطة بفتحها لتجنب تشغيل مستشعرات الدخول. ومع ذلك، يكتشف مستشعر كسر الزجاج أيضًا صوت انكسار الزجاج ويقوم بتنبيهنا فورا عبر إشعار الهاتف المحمول.

هـ. صفارات الإنذار: توجد صفارات الإنذار في أنظمة أمان المنزل سواء بمفردها أو كجزء من الأجهزة الأخرى، مثل المحطة الأساسية، فغالبًا ما تنطلق أجهزة الإنذار في نفس الوقت الذي تنطلق فيه أجهزة الإنذار الأخرى وتهدف إلى إخافة المتسللين بعيدًا أو تنبيه الجيران.

و. مفتاح فوب: تسمح لنا سلاسل المفاتيح بنزع سلاح أو تسليح نظام الأمان لدينا دون الحاجة إلى استخدام لوحة المفاتيح.

ز. زر الذعر: إذا حدث خطأ ما، فإن زر الذعر هو وسيلة سهلة وسريعة لتنبيه خدمات الطوارئ، سواء كانت الشرطة أو المستشفى أو حتى قسم الإطفاء.

ح. المحطة الأساسية: تقوم المحطات الأساسية بمزامنة جميع الأجهزة المتصلة مع تطبيق الهاتف المحمول الخاص بنا حتى نتمكن من تلقي تلك الإشعارات التي ذكرناها سابقًا.

ط. علامة الفناء و / أو ملصقات النوافذ: تقدم العديد من أنظمة الأمان أيضًا لافتات في الفناء أو ملصقات نافذة تسمح لنا بالإعلان عن وجود نظام أمان. في كثير من الأحيان، يستدير اللصوص إذا رأوا نظامًا أمنيًا ، لذلك من الجيد وجود هذه العلامات.

ي. كاشفات الدخان وأول أكسيد الكربون: يوصى بأن يكون في كل منزل كاشف للدخان وأول أكسيد الكربون. باستخدام هذه الأداة البسيطة، يتم تنبيهنا إذا أصبح الهواء في منزلنا غير آمن للتنفس.

4.2 عيوب المنازل الذكية.

على الرغم من التطور الكبير والهائل في مجال تقنيات الإعلام والإتصال، لا تزال المنازل الذكية معرضة لخطر القرصنة والإختراق والتشويش، مما قد يجعل إمكانية إختراق أنظمة التّحكم ممكنا جدا، أو حتى التحكم في كاميرات المراقبة، الإضاءة ، درجات الحرارة وغلق النوافذ والأبواب وغيرها من طرف غرباء.

ما يعاب على المنازل الذكية هو التكلفة المضافة للتكنولوجيا، فعادةً ما يكلف الجهاز الذكي ما بين 2 إلى 20 ضعف سعر الجهاز المكافئ، بالإضافة إلى ذلك، تتطلب بعض

الأجهزة اشتراكات مستمرة للوصول إلى جميع الميزات. هذا شائع جدًا مع الأجهزة الأمنية مثل أجراس باب الفيديو والكاميرات الأمنية التي تتطلب خطط تخزين سحابية مدفوعة للاستفادة من جميع ميزاتها.(Kieren, 2021)

أما عن عيوب الكاميرات وعلى الرّغم من أنّها تُعلمك مُباشرةً عند اكتشاف حركة ما إلّا أنّه يوجد تأخير يصلُ إلى 2.5 ثانية، ما يعني أنّ التّواصل الصوتي قد يكون مُربكاً نوعاً ما. (يوسف، 2018)

لكن ما يعاب على أنظمة الإستشعار الذكي بوجود حركة غير عادية مثلا، أن هناك ثغرة أمنية مع الجوال الآمن، بحيث يوجد هناك أجهزة خاصة بالتشويش على شبكات الجوال، Cellular Signal Blocker، والتي أثبتت فعاليتها على حظر جميع الإشارات المحددة داخل النطاق بما في ذلك CDMA / GSM، DCS / PCS، 3G، 4G LTE، 4G Wimax، WIFI، GPS، حيث تقوم أجهزة التشويش بمنع موجات وإشارات الإرسال من العبور في منطقة معيّنة، مما يعطي الفرصة للمتطفلين باستخدام هذه الأجهزة للتشويش على شبكات الإتصال الخاصة بالجوال لفترة مؤقتة، مما يتسبب في قطع العلاقة بين مالك المنزل ونظام الحماية في المنزل.

تواجه أنظمة الحماية المنزلية خطر الإختراق الأمني وإيجاد ثغرات أمنية، ونقصد هنا بالثغرات: " نقاط الضعف الموجودة في نظام المعلومات ككل أو في شبكة المعلومات أو الأجهزة التي تعمل ضمن الشبكة أو حتى البرمجيات التي يتم إتاحتها على شبكة المعلومات، ويمكن أن تكون هذه الثغرات في تصميم شبكة المعلومات Network Design أو في تهيئة الشبكة Network Configuration أو البرمجيات Software أو قواعد البيانات Data Bases التي تحتويها الشبكة، ومن خلال هذه الثغرات يمكن للمهاجمين أن يخترقوا شبكات المعلومات ويحدثوا فيها الأضرار أو حتى الاستيلاء على ما يريدوا منها". (حسنين، 2012)

3. الإنفاق العالمي على تكنولوجيا المنازل الذكية.

أصبح الاتجاه العالمي نحو الإنفاق على تكنولوجيا المعلومات في سوق المنازل الذكية يزداد ويتوسع يوما بعد يوم، كما تطورت أنظمة الأمن والحماية المنزلية بشكل كبير جدا، مما دفع العديد من الشركات العالمية المختصة في هذا المجال إلى تطوير برامجها بما يضمن توفير أعلى مستويات الأمان والموثوقية.

تشير الدراسات إلى أنه مع حلول سنة 2025، سيكون في العالم أكثر من 21 مليار جهاز متصل. وبحلول ذلك الوقت، وحتى ذلك الحين، سينمو سوق إنترنت الأشياء العالمي بنسبة 35٪ سنويًا في المتوسط والخدمات (Chavanne, 2018) .

يشهد سوق المنازل الذكية ازدهارًا حقيقيًا ، حيث استفاد مؤخرًا من جاذبية المعدات المنزلية مع الاحتواء. وفقًا لآخر التوقعات من توقعات السوق الرقمية ، حيث توقع المختصون وصول حجم التداول العالمي للقطاع إلى 88 مليار يورو خلال سنة 2021 (مقارنة بـ 69 مليارًا في عام 2020) ومن المتوقع أن يصل حجم التداول إلى 150 مليار يورو بحلول عام 2025. كما يتوافق سوق "المنزل الذكي" مع بيع معدات التشغيل الآلي للمنزل المتصلة بالإنترنت والتي تشمل استخداماتها التحكم في الوظائف المختلفة وإدارتها في المنزل (الطاقة والإضاءة) وكذلك الترفيه (التلفزيون الذكي). (Gaudiaut، 2021)

أما في فرنسا فيعتبر المتخصصون في الترقية العقارية أن 100٪ من العقارات المباعة اعتبارًا من عام 2021 ستكون متصلة ببعضها البعض، بحيث يظل الأمن أحد الأسباب الرئيسية لجعل الفرنسيين يتجهون نحو تجهيز منازلهم بالأشياء المتصلة، حيث تعد شركة Netatmoالفرنسية واحدة من الشركات المتخصصة في أمن المنازل، ومن بين أحدث منتجاتها على سبيل المثال، جرس الباب الذكي بالفيديو والذي يسمح للمستخدم بالرد من خلال هاتفه الذكي من أي مكان. (Dictionnaire de l'IoT، 2020)

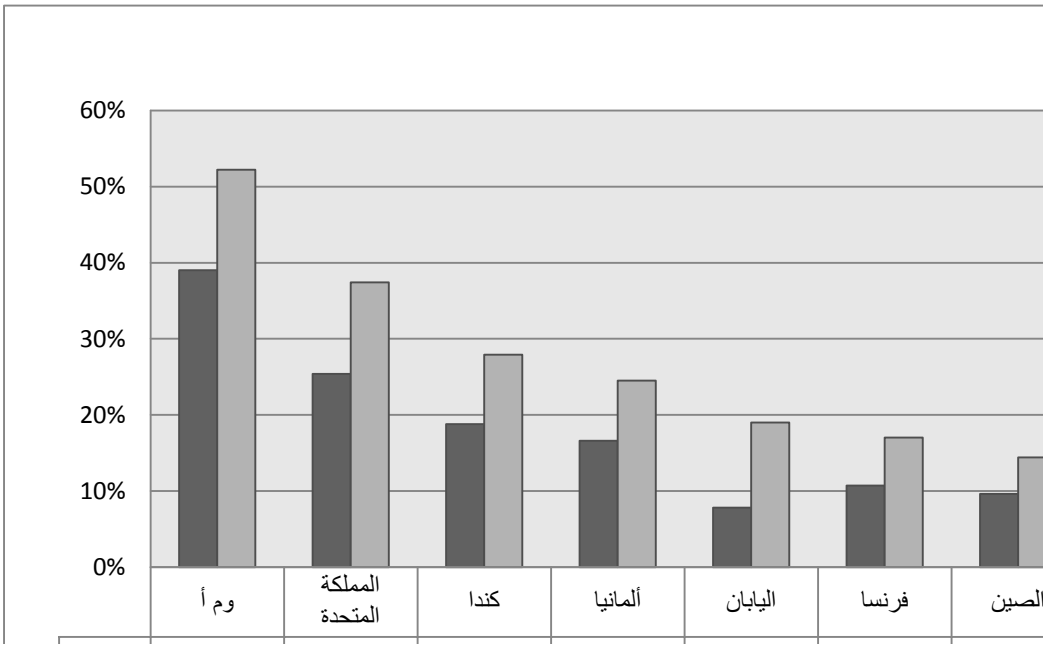
وفقًا للتوقعات المنشورة في تقرير Smart Home 2020 ، من المتوقع أن يرتفع حجم التداول العالمي للقطاع من حوالي 74 مليار دولار في عام 2019 إلى أكثر من 157 مليار دولار بحلول عام 2024. ووفقًا لدراسة أجرتها شركة Statista ، فإن السوق الأمريكية هي الأكثر تطورا، بحيث تشير الإحصائيات إلى أن نسبة 27.5 ٪ من الأسر لديها معدات التشغيل الآلي للمنزل، على سبيل المقارنة، فقد بلغ معدل المعدات للأسر الألمانية 16.5٪ في عام 2019، و 11.5٪ في فرنسا و 7.4٪ في إيطاليا. (Dictionnaire de l'IoT، 2020)

مع زيادة الاتصال بشبكة الويب العالمية، تسعى العديد من الصناعات إلى دمج منتجاتها وخدماتها في العصر الرقمي الجديد، وتسمى هذه العملية بالرقمنة، والصين من بين الدول الرائدة في هذا المجال، بحيث توفر نسبة اختراق عالية للإنترنت، وانفتاح المستهلكين على التقنيات الجديدة ، وصناعة التكنولوجيا المبتكرة ، فهي تمثل بذلك تلك الأرضية المثالية لانتقال الصين إلى العالم الرقمي، حيث تستخدم أكثر من 68 مليون أسرة صينية منتجات المنزل الذكي، كما أن العديد من كبار منتجي المنتجات الإلكترونية في الصين يقومون برقمنة منتجاتهم وتوفير برامج الهواتف الذكية المتوافقة، فعلى سبيل المثال يقدم منتج الأجهزة المنزلية Haier Smart Home وشركة الإلكترونيات الاستهلاكية Xiaomi إصدارات رقمية من منتجاتهما. من الغسالة إلى جهاز تنقية الهواء ، حيث يمكن توصيل جميع منتجات المنزل الذكي تقريبًا بالهاتف الذكي للمستخدم ، مما يتيح التحكم المركزي في المنزل . (Slotta، 2021)

كما يوفر قطاع التحكم والاتصال البنية التحتية لتوصيل أجهزة Smart Home IoT (إنترنت الأشياء)، حيث تتيح المنتجات من هذا الجزء الاتصال بين الأجهزة وكذلك بين البشر والأجهزة، ومن المتوقع أن تزيد الإيرادات العالمية البالغة 15.6 مليار دولار أمريكي في عام 2020 إلى 43.0 مليار دولار أمريكي بحلول عام 2026. (statista, 2021)

أما في سنة 2019 قدر بنحو 182 مليون جهاز متصل بالإنترنت في المنازل الأسترالية. وكان من المتوقع أن يصل هذا الرقم إلى 371 مليون بحلول عام 2024. ووفقًا للمصدر كانت أقوى القطاعات نموًا هي الأمن الذكي والمنافذ الذكية وأجهزة الحدائق الذكية. (L. Granwal, 2021)

الشكل رقم 01: معدل اختراق المنازل الذكية للسوق ما بين 2018 و 2021



المصدر:

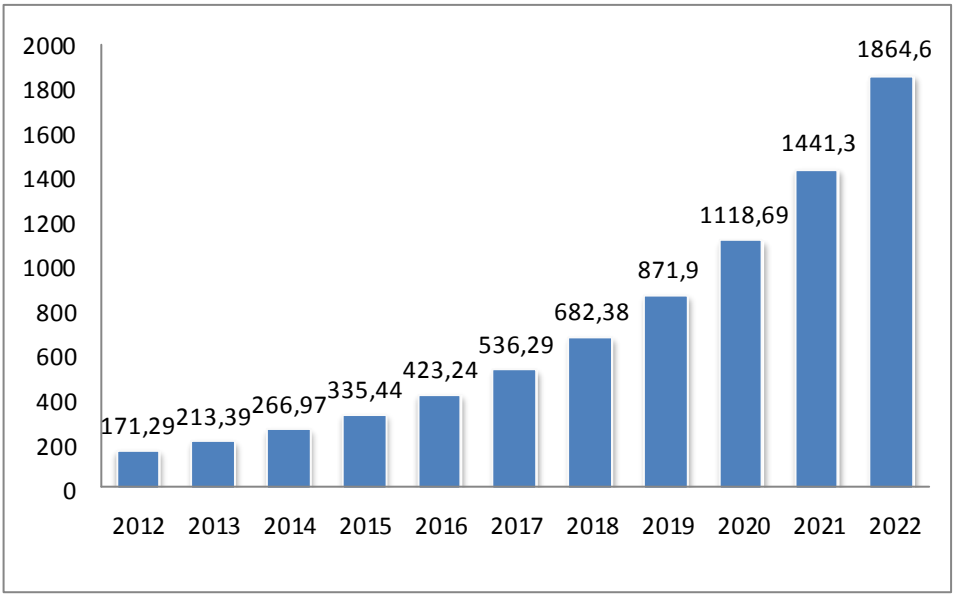
Tristan Gaudiaut (2021), Home Smart Home , https://fr.statista.com/infographie/11832/part-logements-equipes-appareils-intelligents-smart-home/ , (consulté le 09/03/2022) .

ملاحظة: معدل الاختراق (يُدعى أيضًا بالاختراق، أو اختراق العلامة التجارية، أو اختراق السوق حسب الضرورة) فهو مصطلح يشير إلى البيع الناجح للخدمات أو السلع في سوق معين. يُقاس بكمية حجم مبيعات سلعة أو خدمة موجودة بالمقارنة مع السوق المستهدف الكلي لهذه السلعة أو الخدمة.

نلاحظ من خلال الشكل رقم 01 أن سوق المنازل الذكية في الولايات المتحدة الأمريكية هو الأكثر تطورًا إلى حد بعيد، حيث نلاحظ أن معدل الإختراق في الولايات المتحدة الأمريكية انتقل من نسبة 39 % في سنة 2018 إلى نسبة 52,20 % في 2021، أما معدل الإختراق في كندا فقد بلغ نسبة 18,80% في سنة 2018، ليصل إلى نسبة 27,90% في سنة 2021، أما في أوروبا فنلاحظ أن معدل الاختراق أقل نسبيًا مقارنة بالولايات المتحدة الأمريكية، حيث تشير الإحصائيات إلى أن معدل الاختراق في المملكة المتحدة بلغ نسبة 25,40% في سنة 2018، ليصل إلى نسبة 37,40% في سنة 2021، أما في ألمانيا فقد بلغ نسبة 16,60% في سنة 2018، ليصل إلى نسبة 24,50% في 2021، ثم فرنسا بنسبة 10,70% في سنة 2018، ليصل المعدل إلى نسبة 17,00% في سنة 2021، ثم إسبانيا بنسبة 07,10% في سنة 2018، لتبلغ النسبة 10,90% في سنة 2021، أما الصين فقد بلغ معدل الإختراق نسبة 09,60% في سنة 2018، ليبلغ نسبة 14,40% في سنة 2021، أما اليابان فقد بلغ معدل الإختراق نسبة 07,80% في سنة 2018، ليبلغ نسبة 19,00% في سنة 2021.

احتلت أبوظبي ودبي الصدارة في منطقة الشرق الأوسط وشمال أفريقيا في مؤشر المدن الذكية للعام 2021، يصدر هذا التصنيف عن المعهد الدولي للتنمية الإدارية، بالشراكة مع جامعة سنغافورة للتكنولوجيا والتصميم، ويُقيّم تصور المقيمين في كلّ مدينة حول الخدمات الذكية المُتاحة والبُنى التحتية، ويغطي المؤشر خمسة محاور رئيسية، وهي: الصحة والسلامة، والتنقل، والأنشطة، الفرص، والحوكمة. (المدن الذكية المستدامة، 2021)

الشكل رقم 02: حجم سوق المنازل الذكية في الشرق الأوسط ما بين 2012 إلى 2022 (بالمليون دولار أمريكي).



المصدر:

Amna Puri-Mirza, (2020), Market size of smart homes in the Middle East 2012-2022, https://www.statista.com/statistics/806612/middle-east-smart-homes-market-size/ , (consulté le 17/03/2022)

أما إذا تحدثنا عن حجم سوق المنازل الذكية في الشرق الأوسط ما بين سنتي 2012 إلى غاية سنة 2022، فتشير الإحصائيات إلى أن حجم سوق المنازل الذكية بلغ في سنة 2012 171,29 مليون دولار، ليصل إلى 423,24 مليون دولار في سنة 2016، وصولا إلى 1.86 مليار دولار أمريكي بحلول سنة 2022، وهذا ما يبينه الشكل رقم 02 (Puri-Mirza، 2020)، كما تشهد دول مجلس التعاون اعتماد تقنيات جديدة وناشئة بشكل متزايد، مثل الذكاء الاصطناعي والتعلم الآلي وإنترنت الأشياء، حيث أصبح بإمكان المؤسسات والأفراد تولي إدارة ومتابعة وصيانة المنازل الذكية بشكل أفضل بداية من نواحي الأمان وحتى استخدام المرافق العامة (ALAMIN، 2019).

4. خاتمة:

يمثل المنزل الذكي ذلك البيت الذي تحكمه وتديره التكنولوجيا الحديثة بالكامل عن طريق مجموعة من التطبيقات التي يتم تنزيلها في الهواتف الذكية المزودة بخدمة الإنترنت، وهذا ما يؤكد لنا أننا سنعيش مرحلة قادمة ستكون فيها الأجهزة الذكية والهواتف النقالة أكثر وقعا في حياتنا اليومية، وستجعلنا نتوجه أكثر إلى تكريس الجانب الأتوماتيكي في طرق عيشنا وجميع سلوكياتنا ، مما جعل الكثير من المؤسسات العالمية المختصة في هذا المجال تسعى جاهدة إلى تسويق منتجاتها وخدماتها التي تقدمها في مجال توفير الحماية الذكية للمنازل ومحاولة ضمان أعلى درجات الراحة والأمان والرفاهية للمستخدم، فأصبحت هذه الشركات تتسابق من أجل تطوير برامجها وأجهزتها المختلفة سواء تعلق الأمر بالحماية الداخلية أو الخارجية للمنزل، أو حتى تقديم خدمات مختلفة للزبائن.

لكن على الرغم من المزايا المتعددة التي توفرها أنظمة الحماية المنزلية تبقى ضحية التشويش والإختراقات والثغرات الأمنية التي تجعل التكنولوجيا في مواجهة مثل هذه الصعوبات التقنية، بحيث يوجد هناك أجهزة خاصة بالتشويش على شبكات الجوال، بحيث يمكنها حظر جميع الإشارات، وبالتالي تستطيع إعاقة عمل أنظمة الحماية المنزلية بالكامل وتجعلها غير قادر تماما على أداء مهامها، مما يعطي الفرصة للمتطفلين للتشويش على شبكات الإتصال الخاصة بالجوال وقطع العلاقة بين مالك المنزل ونظام الحماية المنزلي، هذا بالإضافة إلى معوقات تقنية أخرى كتواجد مالك المنزل في منطقة غير مغطاة بشبكة الجوال أو الأنترنت مما يصعب المهمة كثيرا على عمل هذه الأنظمة، أو يمكن أيضا لصاحب المنزل أن يتعطل هاتفه الجوال أو تنفذ بطاريته في أية لحظة ...الخ.

أبرز التوصيات التي يمكن تقديمها ما يلي:

- ضرورة تطوير أنظمة الحماية الداخلية والخارجية للمنازل، مع ضرورة تأمين خصوصية البيانات المقدمة من طرف المستخدم وتأمينها الكامل من القرصنة والإختراق الأمني، حيث يجد المستخدم نفسه في مواجهة من يتحكم في منزله.
- العمل من أجل تشجيع المؤسسات المختصة في مجال تطوير التكنولوجيا الحديثة لجعلها أكثر أمانا وقدرة على مواجهة المخاطر التقنية والأمنية، مع ضرورة تعزيز التعاون الدولي في هذا المجال، لما يحقق الراحة والأمان والرفاهية للمستخدم.
- ضرورة تطوير أنظمة الحماية بصورة تجعلها قادرة على مواجهة أجهزة التشويش المختلفة لمواجهة مشكل اختراق الشبكة والتشويش على شبكات الجوال أو تعطيل نظام الأمن وكاميرات المراقبة فيه.
- تعزيز الحماية الذكية للمنازل من خلال تطويرها بأحدث الإبتكارات التكنولوجية، بصورة تجعلها تعمل وفق نظام أمني خاص يتصل مباشرة بالمصالح الأمنية المختصة فور حدوث أي طارئ أو محاولة إختراق أمني من طرف المتطفلين.
- ضرورة التعامل مع مؤسسات وشركات عالمية رائدة ومعروفة في مجال توفير أنظمة الحماية المنزلية، لأن هذه الشركات توفر تحديثات البرامج بانتظام وتقوم أيضا بتنزيل تحديثات الأمان بصورة تلقائية، مما يصعب المهمة أمام المتطفلين لإيجاد ثغرات أمنية يتم من خلالها الوصول إلى بيانات المستخدم.
- ضرورة الإعتماد على أجهزة سيرفر خارجية يتم من خلالها تخزين بيانات المستخدم وبيانات الإعدادات وغيرها، بحيث يتوجب على أي مستخدم الوصول إلى سيرفر الشركات المقدمة للخدمة لإجراء أي إعدادات، كما يجب أن يصاحب في كل عملية من عمليات تدفق البيانات استعمال تقنية تشفير البيانات.

- إنشاء شبكة اتصالات خاصة بأنظمة الحماية المنزلية تعمل وفق نظام مستقل يعمل في نطاقات ترددية تختلف عن نظيره في مجال شبكات الجوال، مما يضمن تحصين الأنظمة المنزلية من الإختراقات الأمنية والتشويش عليها.
- تعزيز الجهود المبذولة لتطوير معايير المنزل الذكي، وضمان دعمها من قبل جميع الشركات العالمية الرائدة في هذا المجال، بالإضافة إلى شركات الإنترنت العملاقة، بما يضمن توفير مستويات أعلى من الأمان والموثوقية.
- يتعين على مديري الأنظمة والشبكات القيام بعمليات فحص مستمرة ومنتظمة لشبكة المعلومات للوقوف على الثغرات الأمنية التي يمكن أن تحدث، والعمل فورا على معالجتها وسدها تجنباً لاكتشافها من قبل بعض العابثين.

5. قائمة المراجع:

- **المؤلفات:**

1. هلال البياتي وأخرون. (2005). أساسيات نظم المعلومات الإدارية، عمان، دار المناهج للنشر.
2. محمد فتحي عبد الهادي. (1983). مقدمة في علم المعلومات. القاهرة، دار غريب للطباعة والنشر والتوزيع.
3. بيزان حنان الصادق. (2017). دراسات ورؤى معلوماتية في ادارة المعلومات والمعرفة. مصر، دار حميثرا للنشر والترجمة.
4. عبود رامي. (2016). ديجيتولوجيا الانترنت، اقتصاد المعرفة، الثورة الصناعية الرابعة ، المستقبل. القاهرة، دار العربي للنشر والتوزيع.
5. الشريف أيمن، (2022).الذكاء الإصطناعي وأنترنت الأشياء، مصر: مؤسسة Read Publisher للطباعة والنشر والتسويق .

- المقالات:

1. داسي وهيبة، وموسى سهام. (2020، 10). مساهمة انترنت الأشياء في خلق القيمة - دراسة تحليلية -.
2. V KHANAA, M.Sundararajan , (2018) Smart Electronic Home Security System, Volume 118 No. 18.

- **مواقع الأنترنت:**

1. الأمين، أسماء .(23/12/2019) .المنازل الذكية في الشرق الأوسط ترفع حجم سوق تقنيات "واي فاي" لـ 16 مليار دولار بحلول 2022، https://entrepreneuralarabiya.com/2019/12/23/25131/. تم زيارة الموقع بتاريخ 17 مارس 2022.

2. إنترنت الأشياء، (27 نوفمبر 2020)، https://www.mcit.gov.sa/ar/iot، تم زيارة الموقع بتاريخ 10 مارس 2022.

3. ثابت، مناهل. (27 نوفمبر 2020). أتمتة المنازل. https://www.albayan.ae/opinions/articles/2020-11-27-1.4024159، تم معاينة الموقع بتاريخ 24 مارس 2022.

4. رجب ، عبد الحميد حسني . (30 ديسمبر 2012). أمن شبكات المعلومات الإلكترونية: المخاطر والحلول http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies&Itemid=94، تم زيارة الموقع بتاريخ 11 مارس 2022.

5. السداوي، مصطفى. (22 جوان 2019). أفضل الأنظمة الأمنية لحماية منزلك . https://www.sayidaty.net/node/662876/ ، تم زيارة الموقع بتاريخ 05 مارس 2022.

6. غومز ، جوليان ، و أبو شقرة، رندة ، (04 ديسمبر 2018)، المنزل الذكي هو منزل المستقبل ... أجهزته متصلة ويستهلك الطاقة وينتجها...، https://arabic.euronews.com/2018/12/03/smart-home-is-the-home-of-the-future، تم زيارة الموقع بتاريخ 08 أفريل 2022.

7. ما هو المنزل الذكي، (16 أفريل 2017)، https://alwaght.net/ar/News/94182 ، تم زيارة الموقع بتاريخ 04 مارس 2022.

8. ما هي أتمتة المنازل؟ كيف تعمل وكيف يمكن تطبيقها؟. (16 جوان 2021)، https://thaqafati.com/%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7/%D8%A3%D8%AA%D9%85%D8%AA%D8%A9-

/%D8%A7%D9%84%D9%85%D9%86%D8%A7%D8%B2%D9%84 ، تم زيارة الموقع بتاريخ 10 مارس 2022.

9. المدن الذكية المستدامة، (آخر تحديث في 25 أكتوبر 2022) البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة،https://u.ae/ar-ae/about-the-uae/digital-uae/smart-sustainable-cities، تم زيارة الموقع بتاريخ 17 نوفمبر 2022.

10. المنزل الذكي. رفاهية لا تخلو من المخاطر. (02 سبتمبر 2014) ، https://www.emaratalyoum.com/life/life-style/2014-09-02-1.705935، تم معاينة الموقع بتاريخ 08 مارس 2022.

11. يوسف، محمود. (26 مارس 2018). نظرة على المنزل الذكي وأبرز أجهزته. https://www.samma3a.com/tech/ar/best-smart-home-devices-2/، تم زيارة الموقع بتاريخ 07 مارس 2022.

12. Aliza Vigderman, G. T. (2022, 03 01). *What Is A Home Security System and How Does It Work?* Consulté le 03 07, 2022, sur security.org: https://www.security.org/home-security-systems/what-is-a-home-security-system/.

13. Chavanne, Y. (2018, 11 22). *Internet des objets: Le marché des objets connectés va croître de 35% par an jusqu'en 2025*. Consulté le 03 09, 2022, sur ictjournal: https://www.ictjournal.ch/etudes/2018-11-22/le-marche-des-objets-connectes-va-croitre-de-35-par-an-jusquen-2025

14. *Dictionnaire de l'IoT*. (2020, 09 21). Consulté le 03 09, 2022, sur journaldunet: https://www.journaldunet.fr/web-tech/dictionnaire-de-l-iot/1440702-smart-home-qu-est-ce-qu-une-maison-connectee-et-combien-ca-coute/.

15. Gaudiaut, T. (2021, 04 01). *Home Smart Home*. Consulté le 03 09, 2022, sur https://fr.statista.com/infographie/11832/part-logements-equipes-appareils-intelligents-smart-home/.

16. *Home Security Systems: Your Options for 2022*. (s.d.). Consulté le 03 04, 2022, sur https://www.safehome.org/security-systems/.

17. Kieren, (2021, 04 27). Consulté le 05 01, 2022, sur smarthomeinsider: https://smarthomeinsider.co.uk/advantages-and-disadvantages-of-smart-homes/ ,

18. L. Granwal. (2021, 02 17). *Number of internet-connected devices in households in Australia 2019-2024*. Consulté le 03 11, 2022, sur statista:

https://www.statista.com/statistics/1202832/australia-number-of-household-internet-connected-device/.

19. Puri-Mirza, A. (2020, 08 26). Market size of smart homes in the Middle East from 2012 to 2022. Consulté le 03 17, 2022, sur statista: https://www.statista.com/statistics/806612/middle-east-smart-homes-market-size/

20. Slotta, D. (2021, 12 07). *Smart homes in China - statistics & facts*. Consulté le 03 10, 2022, sur statista: https://www.statista.com/topics/7207/smart-homes-in-china/#topicHeader__wrapper.

21. *smartsecurityest*. (s.d.). Consulté le 03 06, 2022, sur smartsecurityest.com: http://www.smartsecurityest.com/ar/security.html.

22. *statista*. (2021, 12). Consulté le 03 09, 2022, sur Statista Digital Market Outlook: https://www.statista.com/study/38345/smart-home-report-control-and-connectivity/