

التحديات الأمنية لأنترنت الأشياء

مقراني قدور*، عطايث الله ربيع، شربي محمد الامين³

¹ طالب دكتوراه جامعة ورقلة الجزائر

² طالب دكتوراه جامعة ورقلة الجزائر

³ استاذ جامعة ورقلة الجزائر

تاريخ الاستلام: 2021/07/01 ؛ تاريخ القبول: 2021/08/30

ملخص: أدى التطور المتسارع لتكنولوجيا المعلومات والاتصال إلى ظهور مفاهيم جديدة في عالمنا، فبعد انتشار الانترنت في نهاية القرن الماضي والتي أحدثت طفرة في مجال الاتصالات، ظهر مفهوم انترنت الأشياء مبني على القواعد الهيكلية لهذه الشبكة، حيث أنتقل مفهوم الاتصال بين فردين أو أكثر ليصبح بالإمكان اتصال مجموعة من الأجهزة ببعضها البعض بتدخل أو بدون تدخل الإنسان، لتتشارك فيما بينها معلومات مجمعة تستخدم لأغراض مختلفة.

تتكون أنترنت الأشياء من مجموعة من الأجهزة غير المتجانسة سواء من ناحية تكنولوجيا التصنيع أو البرامج المسيرة لها تتفاعل فيما بينها من أجل تقديم خدمات في مجالات مختلفة، ويعتبر الأمن المعلوماتي من المتطلبات الأساسية لهذه الشبكة من أجل المحافظة على خصوصية الأفراد المتصلين عن طريقها، يتطرق هذا البحث إلى مفهوم هذه الشبكة واستكشاف أهم التحديات التي تواجهها مع اقتراح بعض الحلول في هذا المجال .

الكلمات المفتاحية : أنترنت أشياء، أمن ، مجسات ، الخصوصية

*مقراني قدور mokrani623@gmail.com

Security challenges of Internet of Things

MEGRANI GADOUR^{*}, ATAITE ELLAH ELRABIE², CHERBI MOHAMED ELAMINE³

Received: 01/07/2021 ; **Accepted:** 30/08/2021

Summary: the accelerated development of information and communication technologies led to the release of new concepts in our world, since the proliferation of the Internet at the end of the last century, another notion was appeared, based on Internet Infrastructure, Internet of Thing permit connexion between two or more objects with/out humans , it shares collected information for different uses.

Internet of things composed of many heterogeneous components in terms of hardware or software interact with each other to provide services in different fields, Information security is one of the basic requirements of this network in order to maintain the privacy of the individuals connected through it. This research deals with the concept of this network and explores the most important challenges faced by proposing some solutions in this area.

Keywords : Internet of Things (IoT), security, sensors , privacy

1. مقدمة: تهدف إنترنت الأشياء إلى جعل العالم عبارة عن شبكة واحدة متصلة ببعضها البعض ، ويقوم بربط الأجهزة المختلفة عن طريق شبكة

الإنترنت ، لتتمكن من التفاعل مع بعضها البعض دون تدخل الإنسان أحيانا، وفي أحيانا آخر من أجل تقديم المعلومات اللازمة له لإخاذ قرارات مناسبة ، أو لتنفيذ قرارات المستعمل.

لقد أحدثت إنترنت الأشياء ثورة في عالمنا ، حيث أصبح بالإمكان التحكم في مختلف أجهزة البيت مثلا من خلال تطبيق ، أو حتى يمكنها أن تتفاعل هذه الأجهزة دون تدخل الإنسان ، بقدر ما قدمت هذه التكنولوجيا الإضافة إلى حياتنا إلى أنها لا تزال تعتبر جديدة وغير مستعملة على نطاق واسع ، من هنا تأتي إشكالية هذا البحث والمتمثلة في :

ماهي أهم التحديات الأمنية التي تواجه تطبيق إنترنت الأشياء ؟

1. الاطار النظري:

1.1 أنترنت الأشياء :

يعتبر Kevin Ashton أول من قدم مفهوم أنترنت الأشياء سنة 1999، حين بين إمكانية توصيل الأشياء من خلال تقنية RFID (radio-frequency identification)¹، حينها كان الناس يظنون أن الكاتب يتكلم على فيلم من أفلام الخيال العلمي، ليتطور المفهوم بعد ذلك ويشمل جميع الكائنات المتصلة عبر الإنترنت.

يعرفها الاتحاد الدولي للاتصالات بأنها عبارة عن بنية تحتية عالمية لمجتمع المعلومات، تتيح خدمات متطورة من خلال ربط الأشياء المادية و الافتراضية المستندة على تكنولوجيا المعلومات والاتصالات²، ويدخل ضمن هذه الأشياء المكونات الصغيرة، مثل الرقاقات الالكترونية ، والساعات الذكية ، أو حتى الأجهزة المنزلية ووسائل النقل الذكية المرتبطة بالإنترنت.

2.1 مكونات أنترنت الأشياء :

من خلال معناها فإن أنترنت الأشياء عبارة عن مجموعة من المكونات التي تشكل هذا المعنى ، ويمكن تقسيم مكوناتها إلى:

1.2.1 الكائنات : هي جميع الكائنات التي تمتلك إمكانية الاتصال بالإنترنت ، بدءا من أجهزة صغيرة ، إلى شاحنات أو سيارات ، أو آلات كهر ومنزلية ، أو حتى مصباح في منزل .

2.2.1 المجسات (المستشعرات) : وهي عبارة عن أجهزة لها القدرة على اكتشاف التغيرات التي تطرأ على البيئة المحيطة بها ، قد تكون هذه المستشعرات لقياس درجة الحرارة مثلا، أو مستشعرات لقياس الضغط الجوي أو الرطوبة ، أو مستشعرات ضوئية ، تعتبر هذه الأجهزة ذات أهمية كبيرة في إنترنت الأشياء .

3.2.1 المستقبلات : وهي الأجهزة التي تضمن إرسال واستقبال المعلومات بين الأجهزة من خلال شبكة الاتصال المستعملة .

4.2.1 الشبكة : وهي البنية التي ترتبط من خلالها هذه الأجهزة فيما بينها ، قد تكون الشبكة سلكية أو لا سلكية ، وبإمكانها أن تستعمل مختلف التكنولوجيات المتوفرة للاتصال فيما بينها .

5.2.1 مستودع البيانات : خلال اتصال الأجهزة فيما بينها يتم جمع كم من المعلومات، التي تخزن في قواعد معطيات ، هذه المعطيات قد تكون بيانات عادية ، أو مقاطع فيديو ، أو صور ، يتم تحليلها والاستفادة منها، قد تكون قواعد المعطيات مخزنة ضمن سحابة إلكترونية .

6.2.1 واجهة المستخدم : وهو الجزء الذي يتدخل فيه المستعمل من أجل إعطاء الأوامر، أو قراءة مخرجات عمليات أنترنت الأشياء، ويكون عبارة على تطبيق مثبت على جهاز تحكم ، أو هاتف ذكي أو كمبيوتر منزلي ، أو أي جهاز آخر يملك واجهة مرئية .

3.1 خصائص أنترنت الأشياء : تتميز أنترنت الأشياء بمجموعة من الخصائص هي ³:

1.3.1 الربط البيئي: يمكن ربط أي مكون جديد بالبنية التحتية لأنترنت الأشياء.

2.3.1 الخدمات المتعلقة بالأشياء: يمكن لأنترنت الأشياء أن توفر مجموعة من الخدمات ، معتمدة على الأجهزة والكائنات المتصلة بها .

3.3.1 عدم التجانس: إن من أهم خصائص أنترنت الأشياء أنه تضمن اتصالات بين أجهزة غير متجانسة سواء من ناحية النظم التي تسيروها ، أو مكوناتها المادية.

4.3.1 مرونة التغييرات: تمتاز أجهزة أنترنت الأشياء بأنها مرنة وتتغير ديناميكيا حسب الحالة ، فقد يكون الجهاز في حالة خمول ، ثم ينشط بناء على تغييرات حصلت ، أو ربما يكون في حالة عدم اتصال ثم يصبح متصلا بناء على معطيات، مثال ذلك كاميرا مراقبة تقوم بالتسجيل فقط في حالة الصورة متحركة أما إذا كانت الصورة الملتقطة ثابتة فإنها لا تقوم بالتسجيل ، تساعد هذه الخاصية في الاستعمال الأمثل لموارد أنترنت الأشياء.

5.3.1 السعة : عدد كبير جدا من أجهزة يمكنها أن تكون على اتصال فيما بينها، مما ينتج عنه كم هائل من البيانات التي يتم جمعها وبالتالي تحليلها واستغلالها حسب الغرض المخصص لها .

6.3.1 السلامة: يعتبر معيار السلامة من أهم المعايير في الأنترنت بصفة عامة وفي أنترنت الأشياء بالأخص، كون هذه الأجهزة تجمع معلومات عن حياتنا الخاصة ، وأي اختراق لها قد يشكل تهديد حقيقي للأفراد أو الكيانات، ومع التطور المتسارع للتكنولوجيا فإن السلامة تبقى من بين أهم التحديات التكنولوجية .

4.1 مجالات تطبيق أنترنت الأشياء : نظرا لكون تكنولوجيا المعلومات، أصبحت تمثل جزءا من حياة البشر في جميع المجالات ، أدى ذلك إلى ظهور إبتكارات تكنولوجيا تساعد الإنسان في حياته اليومية ، تعددت هذه الابتكارات وأصبح من السهل ربطها ببعضها البعض مع توافر شبكة الانترنت ، من بين هذه المجالات التي تطبق فيها أنترنت الأشياء نجد⁴:

1.4.1 المدن الذكية : سيكون بإمكان أنترنت الأشياء التحكم في إضاءة المدن من أجل اقتصاد الطاقة أو تسيير التزود بالمياه كما يمكنها التحكم بحركة السير وأمن المواطنين من خلال الكاميرات وأجهزة الملاحة العالمية GPS، وتسيير جمع النفايات من خلال الحاويات الذكية، في جانب آخر بإمكانها ومن خلال المستشعرات مراقبة الانبعاثات السامة و الغازات الدفينة، وتستطيع كذلك التحكم بمواقف السيارات ، سيكون بإمكانها التحكم بكل ما له علاقة بتسيير هذه المدن حتى حركة المواطنين في الشوارع .

2.4.1 المنازل الذكية : من خلال طبيعتها عملها تستطيع المستشعرات أن تجمع مختلف البيانات عن البنية المزروعة داخلها ، فعند استعمالها داخل المنزل ، سيكون بالإمكان التحكم بالإضاءة الداخلية ، ودرجة الحرارة للمنزل، سيكون بمقدور ثلاجة المنزل مراقبة موجوداتها وطلب التزود بالموونة من فضاءات التسوق دون تدخل البشر، التحكم بالمنزل يتم من خلال تطبيق هاتف يسمح بمراقبة الغلق المحكم للأبواب ، أو التعرف على من قام بزيارة المنزل أثناء غياب العائلة.

3.4.1 قطاع التصنيع : بما يحتويه من آلات وروبوتات كان من السهل ربط هذه الأجهزة فيما بينها، من أجل التحكم بسلسلة الإنتاج ، أو سلسلة التوريد من خلال التحكم في المخازن أليا، أو أن يقوم عميل بطلب طلبيته وتتبع مختلف مراحل تقدم تصنيعها داخل المصنع .

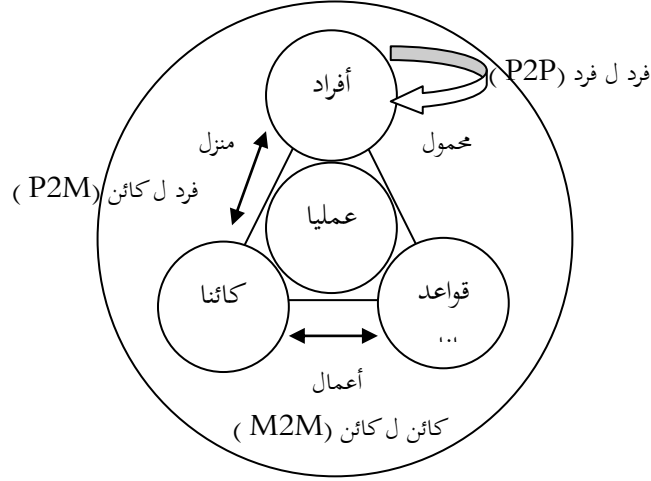
4.4.1 الصحة : تعتبر المستشعرات البشرية لضغط الدم ودرجة الحرارة وغيرها من المستشعرات من أهم مجالات تطبيق انترنت الأشياء، ومع ظهور تكنولوجيا النانو أصبح بإمكان زراعة روبوتات متناهية الصغر داخل جسم الانسان يمكن أن تتصل بأجهزة أخرى لتعطي نظرة على حالة مستعمل تلك الأجهزة ، كذلك يمكن لأنترنت الأشياء أن تساعد في تسيير المستشفيات والآلات المتواجدة بها من خلال دمجها داخل هذه الشبكة.

5.4.1 الزراعة : تعتمد الزراعة الحديثة على التكنولوجيا بشكل كبير، فقد أصبح تسيير البيوت الزجاجية أو البلاستيكية من الأمور الضرورية في الزراعة ، إن عملية التحكم بدرجة حرارة هذه البيوت ودرجة الرطوبة داخلها نسبة الإضاءة ونسبة الأسمدة من العوامل المساعدة على تحسين الإنتاج ، تتيح أنترنت الأشياء ربط أجهزة التحكم هذه ببعضها البعض عبر شبكة الأنترنت ، وتسمح كذلك بالتحكم بها .

5.1 نحو أنترنت كل شي :

إن الجمع بين شبكات الأشخاص ، الإجراءات، قواعد المعطيات، والكائنات ينتج إنتقال مفهوم أنترنت الأشياء التي تعتمد فقط على اتصال الكائنات فيما بينها إلى مفهوم جديد أنترنت كل شيء⁵ ، حسب ما يوضحه الشكل التالي :

الشكل رقم (01): أنترنت كل شيء



المرجع: <https://www.cisco.com>

حيث سيتمكن الأفراد من الاتصال بالانترنت عبر طرق لا حصر لها بخلاف ماهو سائد اليوم ، إذ تقتصر أجهزة الاتصال عبر الحاسوب أو الهاتف أو حتى الساعة الذكية ، حيث سيكون بإمكان زراعة مجسات داخل جسم الانسان أو على الجلد ، أو أن يقوم بابتلاع قرص دوائي يحتوي على مجسات ، وسيكون بإمكان الأفراد الاتصال مباشرة فيما بينهم وتسمى هذه العلاقة فرد لفرد، أو الاتصال عن طريق قواعد المعطيات ، وهذه التقنية المستعملة في المحمول، كما أن الاتصال الناشئ بين الفرد والكائن يسمى فرد لكائن ويغلب استعماله في تسيير المنازل ، وأخيرا فإن اتصال الكائنات فيما بينها أو عن طريق قواعد المعطيات هي اتصال كائن لكائن ويستعمل بكثرة في الصناعة والأعمال .

6.1 خطوات إدماج وتثبيت الكائنات :

تعتبر الكائنات محور أنترنت الأشياء ، وحتى يكون بالإمكان استغلالها ضمن هذه الشبكة هناك مجموعة من المراحل التي تمر بها من أجل إدماجها⁶:

1.6.1 تعريف الكائن : يتم في هذه المرحلة تمكين الكائن من التعرف على باقي الكائنات من خلال بروتوكولات مثل IPV4, IPV6.

2.6.1 الإستشعار : ويتم ذلك من خلال تثبيت المجسات مثل مجسات قياس درجة الحرارة أو الرطوبة .

3.6.1 الإتصال : وهي العملية التي تقوم الكائنات بالاتصال فيما بينها عن طريق بروتوكولات خاصة مثل LoRA.

4.6.1 الإدماج : وهو إمتلاك وسيلة إتصال تسمح بربط الكائنات بالعالم الخارجي مثل NFC ، WIFI, RFID ،... الخ .

7.1 التحديات الأمنية لأنترنت الأشياء:

وجدت دراسة قامت بها مؤسسة تيليكونم أنتيليجنس ، أن أمن المعلومات يعتبر أكبر و أهم عقبة أمام تطور أنترنت الأشياء⁷، ويعتمد مفهوم أمن المعلومات في كيفية الحفاظ على المعلومة من التخريب والتجسس وإتاحتها في الوقت المناسب والمكان المناسب، وفق دلال صادق و حميد ناصر القتال فإن أمن المعلومات هو "مجموع الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية (من أجهزة وبرمجيات وبيانات وأفراد) من التجاوزات والتدخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل أو كنتيجة لإجراءات خاطئة أو غير الوافية المستخدمة من إدارة هذه المصادر"⁸، يمكن أن يضاف إلى هذا التعريف تأمين الشبكات والعمليات المالية المتعلقة بالتحويلات أثناء القيام بإتمام صفقات التخليص على أجهزة أنترنت الأشياء .

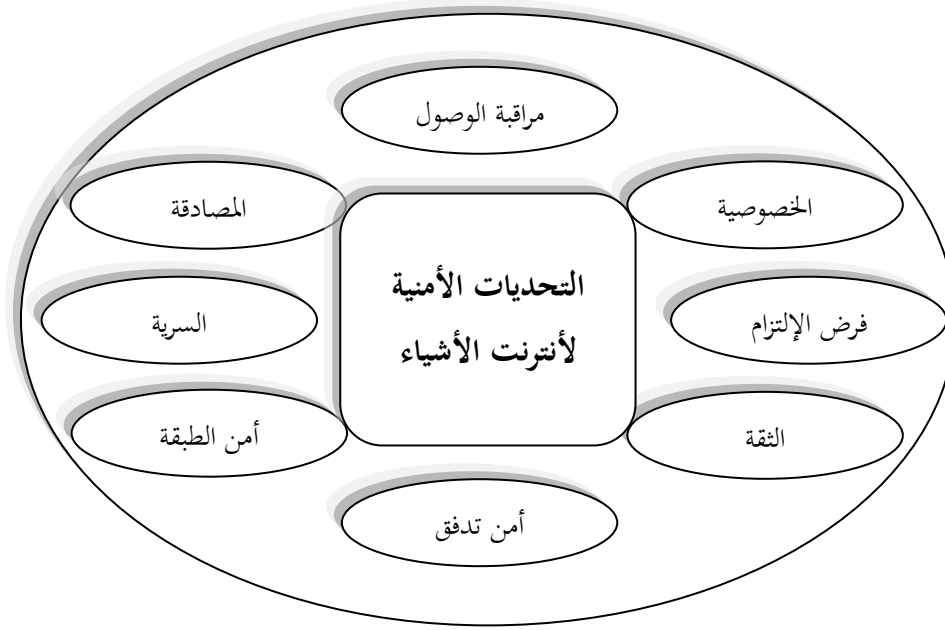
1.7.1 عناصر أمن المعلومات :

- هناك مجموعة من العناصر يجب توفرها من أجل توثيق مفهوم أمن المعلومات داخل أي نظام، تتشكل هذه العناصر من :
- السرية: وهي منع الأشخاص غير المخولين والذين لا علاقة لهم بالمعلومة من الوصول إليها⁹؛
- التكاملية: وهي القابلية لحماية المعلومات من أي تغيير غير مصرح به أو غير مرغوب فيه، أو العبث بالمعلومات سواء من خلال حذف معلومات ، تغييرها ، أو إضافة معلومات ملفقة¹⁰؛
- الاستمرارية: التأكد من استمرار الوصول إلى المعلومة و القدرة على التفاعل معها وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها¹¹.

2.7.1 تحديات أمن أنترنت الأشياء :

إن الكم الهائل من المعلومات التي يتم جمعها في بيئة أنترنت الأشياء تجعلها مستهدفة من طرف المتطفلين من أجل الحصول على تلك المعلومات بأشكال وطرق مختلفة واستعمالها أغراض غير التي جمعت من أجلها، تتعدد التهديدات التي هذه البيئة والتي يمكن توضيحها في الشكل التالي :

الشكل رقم (02): التحديات الأمنية لأنترنت الأشياء



Source :S. Sicari et al, Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, Elsevier, Vol. 76, 2015, P 147.

يعبر الشكل السابق على أهم التحديات الأمنية التي تواجه أنترنت الأشياء والتي تتلخص في مالي :

- **أمن تدفق المعلومات:** ويهتم هذا العنصر بتوفير أمن حركة المعلومات بين الأجهزة، ذلك أن خلال هذه الحركية يمكن أن يحدث تسلل أو تصنت على المعلومة أو حتى هجوم، وبالتالي ضمان إدارة تنقل آمن للمعلومات داخل شبكة أنترنت الأشياء.
- **المصادقة:** وهي العملية التي تضمن شرعية طلب الوصول لجهاز ما للسماح له بالدخول إلى معلومات وموارد النظام ، سواء كان هذا الطلب من طرف بشري أو كائن آخر ضمن شبكة أنترنت الأشياء من خلال التحقق من تعريف هوية المتصل، حيث أن كل كيان (بشري أو مادي) له إعدادات تحكم خاصة تمكنه من الوصول إلى مستوى محدد داخل الجهاز .
- **السرية:** تضمن للمخولين سواء كيانات مادية وأجهزة أو أشخاص الوصول إلى المعلومات وتعديلها، وتشمل هذه الألية مفهوم تحديد آلية التحكم في الوصول و عملية المصادقة عليها.
- **أمن الطبقة الوسيطة:** تختلف الأجهزة المنتجة من حيث التجانس كون كل منتج لديه تقنيات الإنتاج الخاصة به، لهذا وحتى تتمكن الأجهزة من الاتصال فيما بينها تستعمل برامج وسيطة باستخدام بروتوكولات محددة، تسمح هذه البرامج بتمكين الأجهزة من التخاطب بلغة مشتركة .
- **فرض الالتزام بالسياسات :** وهي ما تطبيق مجموعة الإجراءات والقوانين التي من شأنها أن تضمن الحفاظ على النظام وبالتالي المحافظة على البيانات ، من بين هذه الإجراءات استخدام المصادقة التشفير وبرامج مكافحة الفيروسات، والجدران النارية .

- **الثقة :** ويقصد بها العلاقة المتبادلة بين الأجهزة المترابطة فيما بينها والتي تتبادل المعلومات والإشارات والأوامر. تتحكم في هذه العلاقة المبنية بين الجهازين المتصلين .
- **مراقبة الوصول :** وهي العملية التي تبني على قدرة الأجهزة للتعرف على المتصلين بها، وما إذا كان لديهم الترخيص المناسب للوصول إلى بيانات محددة، إن حجم البيانات الكبيرة المتدفقة خلال هذه الشبكة تمثل تحديا للمستخدمين الذين يسعون إلى الوصول للبيانات في أوقات محددة وبسرعات آنية.
- **الخصوصية :** أثناء عملية جمع البيانات داخل شبكة أنترنت الأشياء، يحتاج المستخدم أن يحصل على ضمان لعدم انتهاك خصوصيته، ذلك أن تلك البيانات قد تكون متعلقة بالحالة المرضية للمستخدم ، أو معلومات بنكية ، أو معلومات حول مسكنه وعمله.

2. الدراسة الميدانية:

1.2 تحليل أمن انترنت الأشياء :

تطور عدد الأجهزة المتصلة بشبكة أنترنت الأشياء من 17 مليار جهاز سنة 2016 إلى 23 مليار جهاز سنة 2018 ومن المتوقع أن يصل إلى حوالي 36 مليار جهاز بحلول سنة 2021¹²، يوضح الجدول التالي عدد الأجهزة :

الجدول رقم 2 : تطور عدد الأجهزة المتصلة بشبكة انترنت الأشياء

السنة	2016	2017	2018	2019	2020	2021
العدد (مليار جهاز)	17.68	20.35	23.14	26.66	30.73	35.82

Source : stista par, <https://dzone.com/articles/iot-security-challenges-and-5-effective-ways-to-ha-1>

يبين الجدول أعلاه تطور عدد الأجهزة والمتوقع أن يحدث إنفجار في عددها بحلول سنة 2021، حيث سيتضاعف بنحو 100 بالمئة على ما هو عليه سنة 2016، عبر زيادة سنة تراوح 15 بالمئة ، هذا العدد الهائل من الأجهزة المتصلة سيكون أمام تحدي أمني كبير من أجل أن توفر أفضل خدمة لمستخدميها، في هذا الصدد تقوم مؤسسات تكنولوجيا المعلومات بإنفاق مبالغ ضخمة من أجل حماية البنية التحتية والأجهزة المتعلقة بها لأنترنت الأشياء، حيث بلغت الاستثمارات في هذا القطاع حسب تقرير لمكتب الدراسات gartner 1.5 مليار دولار سنة 2018 ومن المتوقع أن تصل إلى حوالي 2.5 مليار دولار بحلول عام 2021 ، يبين الجدول التالي حجم الاستثمارات في ميدا أنترنت الأشياء من سنة 2016 إلى 2021:

جدول رقم (01) : تطور إستثمارات أمن أنترنت الأشياء (الوحدة مليون دولار)

2021	2020	2019	2018	2017	2016	
631	541	459	373	302	240	أمن الأجهزة الطرفية
415	327	251	186	138	102	أمن أجهزة الشبكات
2.071	1.589	1.221	946	734	570	الخدمات
3.118	2.457	1.931	1.506	1.174	912	المجموع

Source : <https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018>

يبين الجدول السابق تطور الإنفاق على أمن أنترنت الأشياء منذ سنة 2016 على مستوى على محاور وهي أمن الأجهزة الطرفية والتي تكون في متناول المستعمل ، وأمن أجهزة الشبكات بما فيها المحولات الرقمية ، والموجهات ، وأخيرا الخدمات الأمنية الأخرى، حيث بلغت نسبة التطور في النفقات 28 % ، وبنفس النسبة من المتوقع أن ترتفع النفقات حتى عام 2021 لتبلغ 3.118 مليار دولار، حيث يتركز أكثر من 64 % من هذه الاستثمارات الأمنية حول الخدمات، و 23 % تخصص إلى أمن الأجهزة الطرفية ، والنسبة بالباقية 13 % ستخصص لأمن أجهزة الشبكات ذلك خلال كامل الفترة .

من خلال الجدولين السابقين يتبين أنه في سنة 2016، كان الإنفاق على أمن الأجهزة المرتبطة بأنترنت الأشياء بلغ 51.58 دولار على كل جهاز 57.69 دولار للجهاز سنة 2017، أما سنة 2018 فقد بلغ الإنفاق الأمني على كل جهاز متصل 65.08 دولار و من المتوقع أن يصل إلى 72.43، 79.95 و 87.04 دولار لكل جهاز لسنوات 2019، 2020 و 2021 على التوالي.

توضح هذه النتائج حجم التحديات المنتظرة في بيئة أنترنت الأشياء ، حيث كلما زادت أعداد الأجهزة المتصلة زاد حجم الإنفاق الأمني النسبي لكل جهاز ، ويرجع ذلك للمخاطر التي تهدد هذه التكنولوجيا ، كون أن التطور التكنولوجي لهذه الشبكة ليتوافق مع التطور في طرق التحسس والتخريب والإحتيال ، فحسب تقرير لشركة F-secure المختصة في الأمن فإنه تم تسجيل 2.9 مليار هجوم على الأجهزة المتصلة بأنترنت الأشياء في النصف الأول من عام 2019 بزيادة قدرها 300 بالمئة بمقارنة نفس الفترة لعام 2018¹³، أي بمعدل 186 هجوم في كل ثانية ، وهو رقم ضخم ومع ذلك سيتزايد مستقبلا أكثر بكثير.

في دراسة لشركة bitdefender¹⁴ حول سلوكيات الأفراد اتجاه أمن المعلومات أظهرت أن 50 بالمئة من أجهزة التلفاز الذكية لم يتم أصحابها بالتحديثات المناسبة لأكثر من شهر ، وأن 70 بالمئة من الأجهزة لم يتم تغيير كلمات المرور داخلها لفترة تزيد على 3 أشهر، كذلك

وجدت الدراسة أن 10 بالمئة من الأشخاص يستعملون نفس كلمة المرور لجميع الأجهزة لديهم، هذه الأرقام توضح مدى ضعف أمن المستخدمين النهائيين لدى الأفراد والتي تتسبب في سهولة اختراق أجهزتهم ، حيث يعتبرون هم الحلقة الأخيرة في سلسلة أنترنت الأشياء كونهم المستخدمين النهائيين لمخرجات هذه الشبكة.

2.2 الخاتمة :

تعتبر أنترنت الأشياء بيئة واسعة يمكن أن تشمل جميع الأجهزة التي لديها قابلية الاتصال بالشبكات وتتعدد مهام استعمالاتها لتغطي جميع مناحي الحياة، حيث ستصبح في المستقبل القريب موردا أساسيا للمعلومات وبإمكانها التأثير على جميع قراراتنا ، ولكن تعترى هذه الشبكة تهديدات أمنية كثيرة و حتى تتمكن من الانتشار والتوسع يجب الأخذ بعين الاعتبار مستويات الأمن عبر هذه الشبكة من أجل التغلب على التهديدات المتنامية والتي بإمكانها اختراق الخصوصية والوصول إلى معلومات غير مرخص بها خاصة في ظل التعقيد التكنولوجي الذي يتنامى بطريقة متسارعة.

إن أي تطور مرتبط بأمن المعلومات سيقابله تقدم في الجهة المقابلة من ناحية طرق الاختراق، لذلك يجب إيلاء أهمية كبرى لهذا الميدان، أما بخصوص أهم توصيات هاته الدراسة فإننا نوجزها في النقاط التالية :

تنقسم مسؤولية المحافظة على أمن المعلومات داخل بيئة أنترنت الأشياء إلى مجموعة من المستويات :

المستوى الأول : على مستوى الأفراد (المستخدمين النهائيين) :

- يعتبر الفرد هو المستهلك النهائي لمخرجات أنترنت الأشياء، يجب عليه الالتزام بقواعد السياسات الأمنية، كالمحافظة على كلمات المرور وعدم تركها مهمة لأن لا تصل إلى طرف آخر؛
- الحرص على تغيير كلمات المرور دوريا، مع إعادة تشكيلها كل مرة بأحرف ورموز تزيد من تعقيدها؛
- الحرص على تثبيت مضادات الفيروسات الأصلية؛
- تفعيل جدار ناري يمنع محاولات الاختراق للأجهزة؛
- مراقبة دورية للمنافذ المفتوحة داخل الأجهزة من خلال برامج متخصصة؛
- الحرص على القيام بتحديثات المناسبة في الوقت المناسبة للتطبيقات التي يستعملها.

المستوى الثاني : على مستوى الشركات المقدمة للخدمة

- الحرص على تأمين مستودعات البيانات والسحابة الإلكترونية التابعة لها؛
- الحرص على استقطاب الكفاءات الأمنية للشركة؛
- الحرص على تفعيل خطة الإسترجاع في حالة تعرض البيانات إلى خطر؛
- ترصد بعض المؤسسات مكافآت للمستخدمين الذين يقومون باستكشاف نقاط الضعف داخل نظامها.

المستوى الثالث : على مستوى الشركات المصنعة

- ويندرج تحت هذا البند جميع أنواع المصنعين من الأجهزة إلى الشبكات
- الإستثمار في تطوير الأجهزة بشكل فعال يسمح بتوفير حماية أفضل لها؛
 - على شركات الشبكات أن تعمل على تطوير بروتوكولات اتصال أكثر أماناً؛
 - محاولة توحيد أنظمة التصنيع بين الشركات العملاقة لكي تقلص من استعمال البرامج الوسيطة والتي عادة ما تكون موردة من طرف ثالث.

3. الملاحق :

قائمة المختصرات المستعملة في البحث

- GPS : Global Positioning System ;
- http : Hypertext Transfer Protocol ;
- IoT : Internet of Things ;
- IPV4 : Internet Protocol version 4 ;
- IPV6 : Internet Protocol version 6 ;
- LoRA : Long Range Protocole ;
- M2M : Machine to Machine ;
- NFC : Nearfield communication ;
- P2M : Person to Machine ;
- P2P : Person to Person ;
- RFID : Radio Frequency Identification ;
- WIFI : Wireless Fidelity.

4. المراجع:

- ¹Ibrar Ahmed et al., Internet Of Things(IoT), Meaning , Application and challenges, IJSTRD Journal, V2, IS6, 2018.
- ²Mahmoud Elkhodr et al, The Internet of Things: Vision & Challenges, IEEE Tencon conference – Spring, 2013, P 218.
- ³Keyur K Patel and Sunil M Patel, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, IJES, Volume 6 Issue No. 5, 2016, P 6123.
- ⁴Yusuf Perwej et al., The Internet of Things (IoT) and its Application Domains, International Journal of Computer Applications, Volume 182 – No. 49, April 2019.
- ⁵https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/everything-for-cities.pdf, visited Sept, 19 nd 2019 at 17 :47.

⁶ Imad Saleh, Internet des Objets (IdO) : Concepts, Enjeux, Défis et Perspectives, ISTE OpenScience – Published by ISTE Ltd. London, UK, 2018, P4.

⁷ <https://aitnews.com/>, site visité le 20/09/2019 à 14h40.

⁸ دلال صادق و حميد ناصر الفتال ، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، الأردن ، 2008، ص ص: 11-12.

⁹ Jason Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Elsevier, 2011, P4.

¹⁰ المرجع السابق.

¹¹ قدايفة أمينة، استراتيجية أمن المعلومات، مجلة أبعاد إقتصادية – جامعة بومرداس، المجلد 6، العدد 1، سنة 2016، ص 166.

¹² <https://dzone.com/articles/iot-security-challenges-and-5-effective-ways-to-ha-1>, 20/09/2019 à 14h53

¹³ <https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/> <https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/>, visité le 20/09/2019 à 21h14

¹⁴ LuanaPascu, The IoT Threat Landscape and Top Smart Home Vulnerabilities in 2018, birdefender, 2018.

¹⁵ <https://www.gartner.com/>.

¹⁶ S. Sicari et al, Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, Elsevier, Vol. 76, 2015, P 147.

¹⁷ <https://www.cisco.com>.