Un aperçu sur la sécurité de l'internet des objets (IOT)

Younes Abbassi, Habib Benlahmer

Un aperçu sur la sécurité de l'internet des objets (IOT)

Younes ABBASSI[1], Habib BENLAHMER[2]
Laboratoire de Technologie de l'Information et Modélisation, Faculté des Sciences Ben M'sik, Université Hassan II– Casablanca, BP 7955 Sidi Othman Casablanca, Maroc
Younes.abbassi@univh2c.ma, h.benlahmer@gmail.com

RESUME : L'Internet of things (IoT) est l'une des technologies les plus prometteuses qui vise pour améliorer la qualité de vie de l'être humain (QoL). L'IoT joue un rôle important dans plusieurs domaines tels que les services de santé, l'industrie automobile, l'agriculture, l'éducation et de nombreuses applications commerciales transversales. Il est essentiel de traiter et d'analyser les problèmes de sécurité dans l'IoT car les modalités de fonctionnement des applications IoT varient en raison de l'hétérogénéité des environnements IoT. Par conséquent, la discussion sur les préoccupations en matière de sécurité des IoT, en plus des solutions disponibles et potentielles, aideraient les développeurs et les chercheurs à trouver des solutions appropriées et opportunes pour faire face à des menaces spécifiques, en fournissant les meilleurs services possibles basés sur l'IoT. Ce document fournit une étude sur quelques problèmes (vulnérabilités) de sécurité de l'IoT, ses limites et ses exigences, et les solutions actuelles et potentielles. Le document s'appuie sur une taxonomie qui s'appuie sur l'architecture à trois couches de l'IoT comme référence pour identifier les propriétés et les exigences de sécurité. De là, les défis et les solutions de sécurité de l'IoT sont regroupés par l'architecture en couches pour permettre aux lecteurs de mieux comprendre examiner et adopter les meilleures pratiques pour éviter les menaces actuelles à la sécurité de l'IoT sur chaque couche.

Mots clés : Objet connecté, IOT, Architecture, Sécurité, Contre-mesure de sécurité, Cloud Computing.

1 INTRODUCTION

Le paradigme de l'Internet des objets (IoT) a attiré l'attention de fournisseurs de services, d'entreprises et d'industries massives comme les services de santé, les véhicules autonomes, les réseaux intelligents, l'agriculture numérique, et bien d'autres. L'IoT permet aux objets d'entendre, d'écouter, de parler et d'agir de manière intelligente et cela dans le cadre de la révolution de l'industrie 4.0.

Il existe de nombreuses expressions concernant le concept d'IOT. Actuellement, la définition la plus acceptée est la suivante : il s'agit d'un réseau, grâce à l'identification par radiofréquence (RFID)[1], aux capteurs infrarouges, au système de positionnement global, au scanner laser, aux équipements de détection d'informations, tout objet connecté à Internet peut échanger des informations et communiquer, selon l'accord, pour réaliser la reconnaissance intelligente des objets, la localisation, le suivi et la surveillance et la gestion.

Cet article est structuré comme suit. La section 2 ouvre la voie en explorant l'architecture en couche des Iot et la technologie d'identification par radio-fréquences, ainsi que les défis et les vulnérabilités du système IoT. La section 3 examine les exigences de sécurité posé par l'écosystème de l'internet des objets, de plus en plus dynamique et surpeuplé et en deuxième partie quelques solution pour évoluer l'aspect sécurité des IoT. La section 4 est la conclusion montrant l'évolution et la présence des objets connectés dans notre vie actuelle et futurs.

2 L'ECOSYSTEME IOT

2.1 Architecture en couche

Bien que nous ne puissions pas couvrir toutes les possibilités et permutations, le groupe d'architectures suivant devrait vous permettre de mieux comprendre les considérations de conception de base et les couches fonctionnelles[2] primaires typiques dans une pile IoT de bout en bout.

Couche de perception : le fonctionnement principal de l'IOT, c'est-à-dire la collecte d'informations se fait au niveau de la couche de perception à l'aide de différents appareils tels que la carte à puce, l'étiquette RFID, les réseaux de lecteurs et de capteurs, etc. Il a une fonction de détection complète à travers le Système RFID pour obtenir des informations sur les objets à tout moment et n'importe où. Chaque étiquette électronique RFID a un identifiant unique appelé code de produit électronique (EPC) qui est le seul identifiant de recherche attribué à chaque cible physique. Des informations supplémentaires sur le produit sont données par une suite de chiffres qui lui sont imposés tels que le fabricant et la catégorie de produit avec sa date de fabrication et sa date d'expiration, etc.

Couche réseau : les données collectées par les capteurs étaient envoyées à Internet via la couche réseau avec l'aide d'ordinateurs, de réseau sans fil / filaire et d'autres composants. Par conséquent, la couche réseau est principalement responsable de transmettre des informations avec la caractéristique de livraison fiable, par conséquent cette couche comprend également la fonctionnalité de la couche de transport.

Couche application : analyse des informations reçues et prise de décisions de contrôle pour atteindre sa fonction de traitement intelligent par connexion, identification et contrôle entre objets et appareils. Les moyens de renseignement utilisent une technologie informatique intelligente telle que le cloud computing et traitent les informations pour un contrôle intelligent, comme ce qu'il faut faire et quand faire les choses.

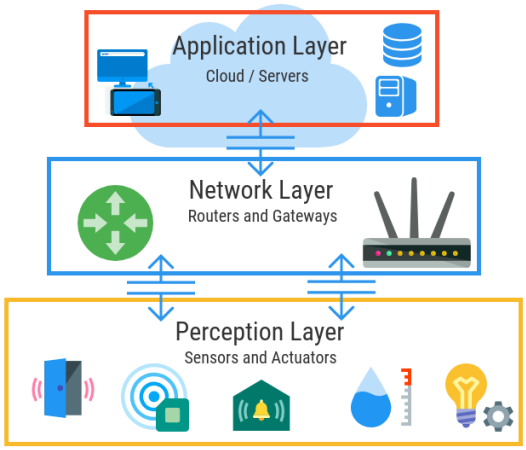

fig 1 : Architecture en 3 couche.

2.2 Notion technique de la RFID

L'IoT repose actuellement sur un certain nombre de technologies habilitantes différentes. Celles-ci comprennent les systèmes d'identification par radiofréquence (RFID) [1], ainsi que les réseaux de capteurs sans fil (WSN), les systèmes de machine à machine (M2M), les données volumineuses, les services en nuage et les applications intelligentes :

- un transpondeur (étiquette RFID), qui est attaché à une "chose" (qui peut être pratiquement n'importe quoi, d'un appareil informatique à un produit d'épicerie, même un animal ou un être humain) et sert de support de données, et
- un lecteur ou un dispositif d'enregistrement, qui lit les données du transpondeur. Dans une telle infrastructure, les "objets" sont des objets qui portent des étiquettes RFID avec un code produit électronique unique.

L'infrastructure peut offrir et interroger les services d'information EPC (EPCIS), tant localement qu'à distance, à destination et en provenance des abonnés. Au lieu d'enregistrer les informations sur une étiquette RFID, des serveurs distribués sur l'internet peuvent fournir les informations en les reliant et en les croisant à l'aide d'un service de dénomination des objets (ONS).

2.3 Vulnérabilité et risque

Le système IoT dispose d'une base de données en nuage qui est connectée à tous vos appareils. Ces appareils sont connectés à l'internet et les cybercriminels et les pirates informatiques peuvent y accéder. Plus le nombre d'appareils connectés augmente, plus les chances que des pirates informatiques violent le système de sécurité augmentent.
Examinons quelques-unes des vulnérabilités [4] auxquelles les systèmes IdO sont confrontés :

-Absence de cryptage des transports : De nombreux dispositifs IoT sont de simples "unités de traitement" et tous les dispositifs ont un coût, une taille et des contraintes de traitement (une puissance de traitement supplémentaire ajoute du coût). Cela signifie que la plupart des dispositifs ne supporteront pas la puissance de traitement requise pour des mesures de sécurité strictes et une communication sécurisée, comme le cryptage (par exemple, un microcontrôleur de 8 bits, dont la fonction est simplement d'allumer et d'éteindre des lumières, ne peut pas supporter le SSL, norme industrielle pour le cryptage des communications) et peuvent transmettre des données en texte clair.

-Authentification et autorisation insuffisantes : L'authentification et l'autorisation peuvent être insuffisantes en raison de la mauvaise qualité des mots de passe, de l'utilisation imprudente des mots de passe (fruit du hasard pour les pirates informatiques), de l'absence de réinitialisation périodique des mots de passe et de l'absence d'exigence de nouvelle authentification pour les données sensibles.

-Interface Web non sécurisée : Les problèmes de sécurité de l'interface web comprennent la persistance de scripts intersites, une mauvaise gestion des sessions et des identifiants par défaut faibles ou simples (qui peuvent être exploités en énumérant les comptes jusqu'à ce que l'accès soit accordé).

-Logiciels et micro-logiciels non sécurisés : en raison de contraintes de ressources, la plupart des dispositifs IoT sont conçus sans pouvoir accueillir des mises à jour de logiciels ou de micro-logiciels (ce qui entraînerait des coûts supplémentaires). Par conséquent, il est difficile de corriger les vulnérabilités. Cela est bien sûr problématique, car il est "virtuellement impossible " de concevoir des logiciels sans vulnérabilité.

-Attaques numériques [4] : Une autre grande vulnérabilité des systèmes IoT est la connexion sans fil qui est exposée pour les attaquants. Par exemple, les pirates peuvent brouiller la fonctionnalité d'une passerelle dans les systèmes IoT, ou carrément détruire un des composants de l'objet, ou encore des attaques de déni de service DDOS….

3 SECURITE

3.1 Exigence de la sécurité

Sur la base des problèmes de sécurité IOT, le besoin de sécurité est requis pour le système IOT. Par conséquent, en examinant les paramètres traditionnels de la demande de sécurité, il a besoin de construire un système Internet sûr des objets, qui sont les suivants [6] :

- Authenticité : les informations reçues par un lecteur doivent être visibles, qu'elles soient envoyées à partir d'une étiquette électronique authentifiée ou non.
- Confidentialité : les informations sensibles ne doivent pas être divulguées à un lecteur non autorisé en utilisant une étiquette électronique RFID.
- Intégrité : lors de la transmission des informations à l'IOT, l'intégrité des données peut garantir l'originalité des informations. Il doit garantir que les informations transmises ne sont pas fabriquées, c'est-à-dire non réécrites, copiées ou remplacées par l'attaquant.
- Confidentialité : la confidentialité telle que l'identité ou l'intérêt commercial d'un utilisateur individuel doit être protégée par le système IOT sécurisé.
- Disponibilité : un utilisateur autorisé peut utiliser divers services fournis par IOT et peut empêcher les attaques DOS pour la disponibilité des services. L'attaque DOS est une cause majeure de menace pour la disponibilité.

3.2 Solution de sécurité

Le Xu Xiaohui [7] a parlé des contre-mesures pour les problèmes de sécurité de l'IOT. Certaines d'entre elles, comme la certification, le contrôle d'accès, le cryptage des données et le Cloud Computing, sont abordées dans cette sous-section :
La certification : est un moyen sûr de confirmer la véritable identité des deux parties qui communiquent entre elles. D'où en utilisant l'infrastructure à clé publique (PKI), il est possible d'obtenir l'authentification forte par clé publique bidirectionnelle pour prévenir l'authenticité et la confidentialité du système IOT.

Sécurité des données : La sécurité des données et l'exploration des données doivent figurer en tête de la liste des caractéristiques de sécurité de l'IoT à travers la cryptographie. Il s'agit de la première étape pour empêcher tout accès non authentifié aux appareils du réseau IoT. Une architecture en couches doit être utilisée dans le système de sécurité des données. Par conséquent, toute violation du niveau de sécurité initial n'expose pas toutes les données. Elle doit plutôt alerter les autorités sur les menaces potentielles et la violation du niveau de sécurité initial.

Contrôle d'accès : Le contrôle d'accès est un autre mécanisme qui sécurise l'environnement de l'IoT en limitant le contrôle d'accès aux machines, objets ou personnes qui n'ont pas le droit d'accéder aux ressources.

Cloud Computing : Le "cloud" est un nom qui désigne une capacité de stockage de données énorme, des performances élevées à un coût abordable. Dans le fonctionnement essentiel de l'ITO, c'est-à-dire le grand nombre de nœuds de capteurs qui collectent et analysent une énorme quantité de données, le stockage et le traitement des données où l'informatique dans les nuages peut être utilisée très efficacement.

4 CONCLUSION

En résumé, nous pouvons dire que l'IoT est la technologie la plus intéressante et la plus récente de nos jours. L'Internet des objets est utilisé pour définir le réseau qui se compose d'un certain nombre d'appareils électroniques interconnectés avec une technologie intelligente. Les villes intelligentes, les voitures intelligentes, les appareils ménagers intelligents vont être les prochains grands projets qui révolutionneront notre façon de vivre, de travailler et d'interagir. Comme nous le savons, chaque pièce a deux faces. De même, l'IoT présente également certains risques et vulnérabilités. En surmontant ces menaces, nous pouvons profiter des services des systèmes IoT.

Bibliographie

[1] Rolf H. Weber, "Internet of Things – New Security and Privacy Challenges," Computer Law & Security Review 26, no. 1 (January 1, 2010): 23–30, http://www.sciencedirect.com/science/article/pii/S0267364909001939.

[2] Hamed HaddadPajouh, Ali Dehghantanha, Reza M. Parizi , "A Survey on Internet of Things Security: Requirements, Challenges, and Solutions - ScienceDirect," https://www.sciencedirect.com/science/article/pii/S2542660519302288.

[3] I.Saleh: Les enjeux et les défis de l'Internet des Objets (IdO). In: Internet des objets (2017).

[4] Weber, Rolf H., et Evelyne Studer. « Cybersecurity in the Internet of Things: Legal Aspects ». Computer Law & Security Review 32, no 5 (1 octobre 2016): 715-28. https://doi.org/10.1016/j.clsr.2016.07.002.

[5] D.Singh, G.Tripathi, & A. J. Jara: A survey of Internetof-Things: Future vision, architecture, challenges and services. In: In Internet of things (WF-IoT), world forum on IEEE (2014).

[6] A., Mayuri, et Sudhir T. « Internet of Things: Architecture, Security Issues and Countermeasures ». International Journal of Computer Applications 125, no 14 (17 septembre 2015): 1-4. https://doi.org/10.5120/ijca2015906251.

[7] Xu Xiaohui „" Study on Security Problems and Key Technologies of The Internet of Things", 2013 International Conference on Computational and Information Sciences