REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed Khider – BISKRA
Faculté des Sciences Exactes, des Sciences de la Nature et de la Vie
Département d'informatique

N° d'ordre : RTIC 1/M2/2018

Mémoire

présenté pour obtenir le diplôme de master académique en

Informatique

Parcours : Réseaux et Technologies de l'Information et de la Communication

---

Système de détection d'intrusion pour maison intelligente

Par :

ELHAMEL SOHEIB

Soutenu le 24/06/2018, devant le jury composé de :

Mr Madi Med Nadjib	M C B	Président
Mme Boukhlouf Djemaa	M C B	Rapporteuse
Mr Mokhtari Bilal	M C B	Examinateur

Remerciements

Je remercie tout d'abord «Allah » le tout puissant, de m'avoir donné la santé, le courage et la patience pour mener à bien ce projet de fin d'études.

Je tiens à remercier le docteur **BOUKHLOUF DJEMAA** *pour son encadrement, sa disponibilité, son suivi, ses conseils et ses critiques constructives malgré ses occupations,* et je remercie vivement tous les membres de jures.

Je tiens à remercier toute personne ayant contribué de près ou de loin à la réalisation de ce travail.

Pour finir j'aimerais remercier toute ma famille pour leur soutien constant.

Une autre fois Je remercie beaucoup mon encadreur Mr.

BOUKHLOUF DJEMAA :

" جزاك الله عني كل خيـــــــر "

Dédicaces

Je remercie Dieu tout puissant de m'avoir donné la force et le courage de finir ce modeste travail, que je dédie :

A

Ma chère maman& mon cher papa

Vous êtes pour moi une source de vie car sans vos sacrifices, votre tendresse et votre affection je ne pourrais arriver jusqu'au bout. Je me réjouis de cet amour filial. Que Dieu vous garde afin que votre regard puisse suivre ma destinée.

A

Mes adorables frères et Yahya& Mes chères sœurs

Mon amour à votre égard est une grandeur non quantifiable.

A

Toute ma famille

A

Mon Encadreur BOUKHLOUF DJEMAA

A

Tous mes amis & mes camarades

En témoignage de notre amitié sincère

A

tous ceux que j'aime, et à tous ceux qui m'aiment…

Je dédie ce travail.

Résumé

Le but de notre projet est la conception et la réalisation d'un système de détection d'intrusion pour maison intelligente .

Notre travail se résume dans quatre chapitre, le premier « Internet des objets » consiste à présenter les caractéristiques et les architecture de l'IOT de ce dernier ainsi domaines d'application, le deuxième « IDS et Sécurité » présente le différents concepts et l'IDS, le troisième « Conception » explique la conception de notre système ainsi que l'architecture des différents globale du système, le quatrième chapitre présente l'environnement de travail (logiciel) et les interfaces qui illustrent notre système dans son état final.

Mots-Clés : IOT(internet des objets(ido)), IDS(Système de détection d'intrusion).

Table des matières

Liste des figures

Introduction générale

Dans la « société de l'information », la sécurité des systèmes informatiques constitue un enjeu crucial. Le contrôle de l'information traitée et partagée au sein de ces systèmes est un problème d'autant plus délicat que le nombre d'utilisateurs de ces systèmes est important**.** Avec plus de 24 milliards d'appareils connectés d'ici 2020**.**

Ce problème touchera presque tous les secteurs, notamment le transport, l'assurance, les medias, les télécommunications, la santé, les maisons intelligentes..etc

Dans le contexte de *Smart Home*, la fiabilité d'un système informatique repose en premier lieu sur la mise en place d'une politique de sécurité. Celle-ci peut être définie comme un ensemble de règles permettant d'assurer trois propriétés : [22]

- la confidentialité des données : seuls les utilisateurs autorisés peuvent consulter une information donnée.
- l'intégrité des données : seuls les utilisateurs autorisés peuvent modifier une information donnée.
- la disponibilité du système : le système doit être capable de rendre le service prévu en un temps borné.

Une fois le plan de sécurité définie, il convient de la mettre en œuvre au sein du système informatique. Deux approches non exclusives sont envisageables : la prévention des attaques et leur détection. La première approche, en appliquant un contrôle a priori sur les actions effectuées au sein du système, s'assure que les utilisateurs ne pourront violer la politique. Cette approche évite que le système ne se trouve dans un état corrompu, nécessitant une analyse et une correction. De ce fait, des mécanismes de prévention sont présents sur les systèmes informatiques ; il s'agit souvent de contrôle d'accès. Cependant, de tels mécanismes possèdent leurs propres limitations, qui peuvent porter sur des aspects théoriques des modèles sous-jacents ou sur leur implémentation. Ces limitations justifient le recours à des mécanismes et systèmes de détection d'Intrusion (IDS).

L'objectif de la détection d'intrusions est d'automatiser la tâche de contrôles et d'accès d'audit. Il s'agit bien, théoriquement, de détecter de manière automatique les violations de de sécurité, qu'on appelle intrusions. Dans la pratique, la relative de détection conduit à un nombre élevé d'alertes, dont une part significative est en fait constituée de fausses alertes (faux positifs). Enfin, certaines intrusions peuvent ne pas être détectées (faux négatifs).

Afin de qualifier un IDS, on s'intéresse à sa fiabilité, qui est sa capacité à émettre une alerte pour toute violation de la politique de sécurité, et à sa pertinence, qui est sa capacité à n'émettre une alerte qu'en cas d'un attaque.

Dans le contexte de ce domaine, notre travail s'articule autour le sujet dont il consiste à sécuriser un *Smart Home* avec un système de détection d'intrusion adéquat.

Pour cet objectif, ce document est organisé comme suit:

Le premier chapitre est un chapitre descriptif sur l'internet des objets, dans lequel on va défini le concept IoT, les caractéristiques principales et l'architecture, ainsi les domaines d'application de ses technologies.

Le second chapitre est consacré à présenter une architecture globale d'un IDS, la définition et le mode de fonctionnement de ce dernier. Ainsi les différentes classifications des IDS et par la suite les méthodes de détection d'une intrusion.

Le troisième chapitre est consacré pour la conception, qui va présenter une architecture globale du système les définitions UML et diagrammes utilisés.

Le dernier chapitre contient la partie de la réalisation de notre application (Système de détection d'intrusion pour maison intelligente), nous avons donc implémenté un système de détection d'intrusion avec une approche comportementale.

Chapitre 01

Internet des objets

1.1. Introduction

Notre quotidien s'enrichit d'une dimension étendue et virtuelle. Cette extension du réel par l'ajout de fonctionnalités de communication et de traitement donne à nos objets de tous les jours de nouvelles possibilités d'interactions. Notamment, des objets et des utilisateurs qui interagissent, des bâtiments qui guident leurs visiteurs et les renseignent, congruent leurs appareils électroniques portatifs, proposent des services contextualités ou encore des villes intelligentes gérant de façon autonome leurs ressources, sont quelques unes des promesses de l'Internet des objets.

Dans ce chapitre, on va présenter les concepts de base de l'internet des objets afin de comprendre par la suite les méthodes utilisées pour faire face aux intrusions détectées dans un "smart home".

1.2. Définition [1]

L'internet des objets ou bien IoT (*Internet of Things*) comme définition est un: « réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et sans fil, d'identifier et de communiquer numériquement avec des objets physiques afin de pouvoir mesurer et échanger des données entre les mondes physiques et virtuels ».

Certaines autres définitions insistent sur les aspects techniques de l'IoT portent sur les usages et les fonctionnalités: « des objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés ». Notant qu'il devient possible d'identifier de manière unifiée (adresses) des éléments d'information numérique et des éléments physiques.

Il est parfois suggéré que l'objet deviendra un acteur autonome de l'Internet, c'est-à-dire capable de percevoir, analyser et agir par lui-même dans les contextes des processus dans lesquels il sera engagé. Dans ce cas de figure, l'avènement de l'Internet des objets s'associe à celui des technologies ou méthodes de conception logicielle liées à l'Intelligence artificielle. Le couple "objet physique" / "Intelligence virtuelle associée", qu'elle soit embarquée, distribuée ou hébergée dans le Cloud (*Cloud computing*) y est alors mentionné sous l'appellation « cyberobjet ». Les cyberobjets sont des acteurs potentiels des chaines de valeurs qui agissent sous le contrôle des opérationnels ou en partenariat avec eux. En accédant ainsi au statut d'assistants, de conseillers, de décideurs ou encore d'organisateurs selon les cas.

Une définition plus synthétique est la suivante : « l'IoT est un réseau de réseaux qui permet via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant ».

La figure suivante montrer les différentes applications des IoT dans notre vue quotidienne.

Figure 1.1: Applications de l'Internet des objets [2].

1.3. Caractéristiques [3]

1.3.1. Connectivité:

Cela signifie que tous les dispositifs, capteurs, ils doivent être connectés à un objet à l'autre via l'internet ou un autre réseau.

1.3.2. Des Objets:

Le terme d'objet comporte tous types des dispositifs connecté (objets physiques, capteurs,…etc.). Certains ajoutent des mots "smart" ou "intelligent" aux objets. Disons qu'ils contiennent une technologie qui leur donne une capacité additionnelle de «faire quelque chose»: mesurer la température ou l'humidité, capturer des données de localisation, détecter des

mouvements ou toute autre forme d'action qui pouvant être traité et transformé en données (Data).

1.3.3. Les données:

Les données sont l'élément essentielle de l'Internet des objets, premier pas vers l'automatisation et l'intelligence. La quantité des données collectées est augmentée de façons très rapide et énorme, on parle alors sur le "Big data". Ces données peuvent être traitées et communiquées par la suite.

1.3.4. La communication:

Les objets sont connectés pour pouvoir collecter et communiquer les données via plusieurs canaux et protocole de communication, ces données peuvent être analysées afin de prendre une décision ou bien une action intelligente.

1.3.5. Intelligence:

L'aspect de l'intelligence dans les dispositifs IoT vient -réellement- à partir de la capacité d'analyse de données recueillies (également comme dans les outils de data mining). Qui peuvent être tiré des informations et des connaissances utiles, afin de résoudre les problèmes ou bien automatisé les processus et les solutions proposées.

1.3.6. Automatisation des Actions:

La conséquence d'une solution intelligente. Cela peut être une action manuelle et répétitive. L'automatisation dans ce cas est souvent la pièce la plus importante lorsque une action fondée sur des étapes bien définies.

1.3.7. Écosystème:

Avec plus de 24 milliards d'appareils connectés d'ici 2020, l'écosystème IoT touchera presque tous les secteurs, notamment le transport, l'assurance, les medias, les télécommunications, la santé, les maisons intelligentes (Smart Home)...etc.

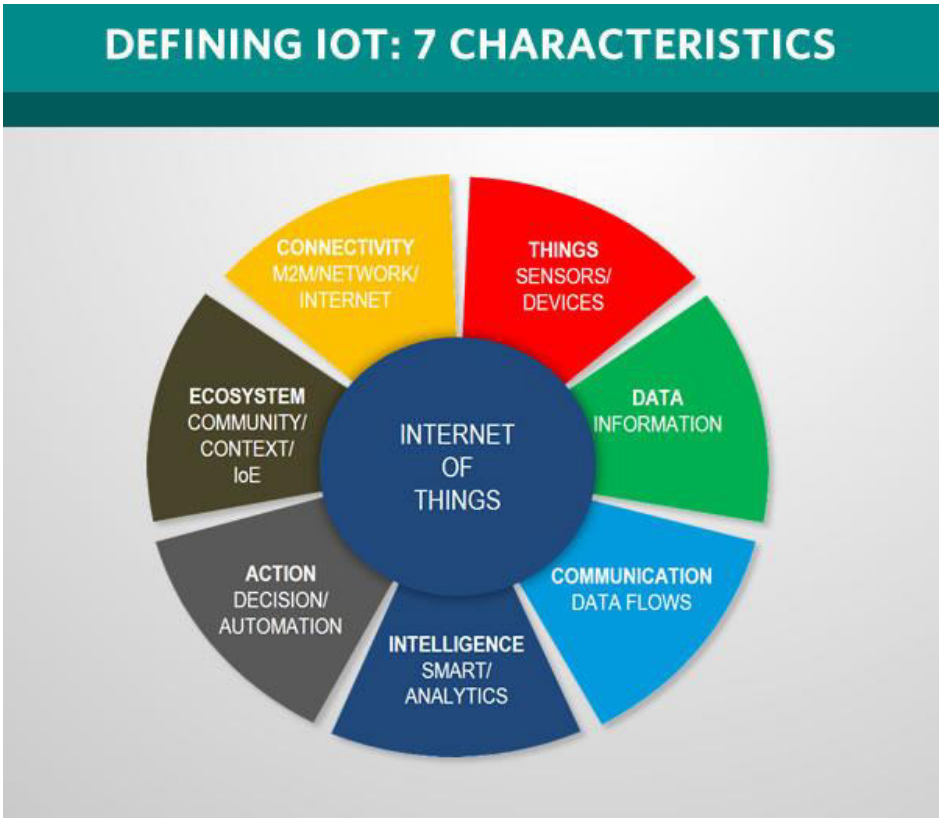


Figure 1.2 : Caractéristiques Internet des objets [3].

1.4. Architecture [4]

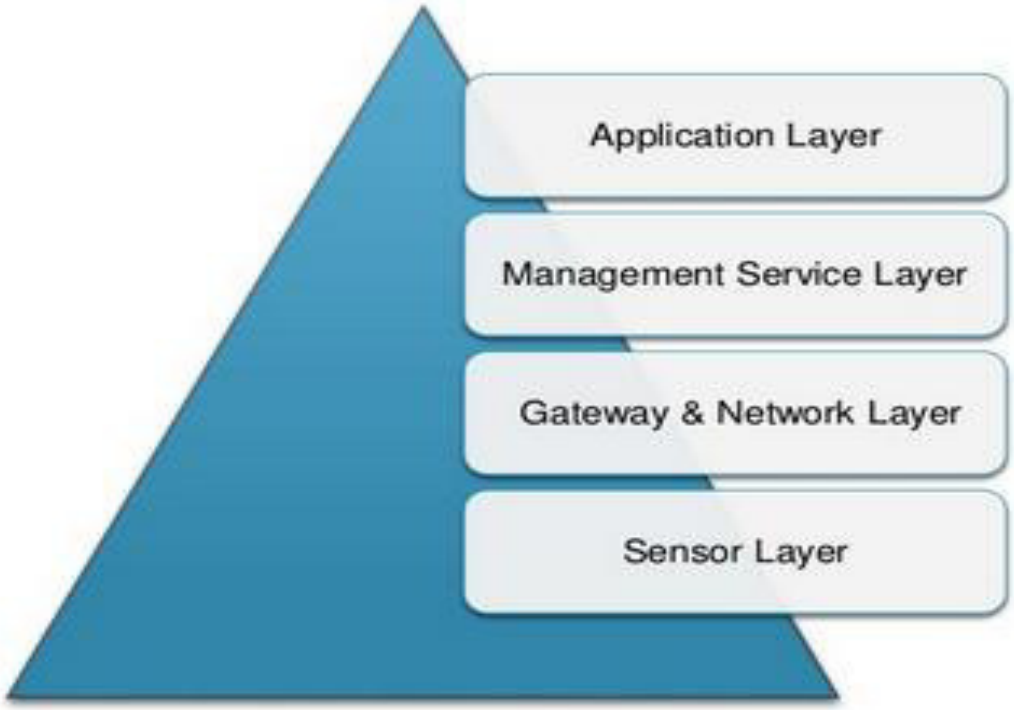


Figure 1.3: Architecture Internet des objets [4].

1.4.1 Couche des Capteurs

Cette couche est constituée des différents capteurs (température, humidité, mouvement, lumière, pression...etc.), ces capteurs sont chargés de collecter des données brutes. Ceux-ci forment la chose essentielle d'un système IoT.

Les capteurs sont actifs par la nature, ce qui signifie que les informations doivent être collectées et traitées en temps réel.

Cette couche est également responsable de la communication des données brutes à la couche suivante qui est la couche passerelle et réseau.

Les dispositifs connectés ont une capacité de stockage limitée, qui nécessite une bande passante suffisante et une vitesse de traitement acceptable.

Nous avons différents capteurs pour différentes applications (capteur thermique pour la collecte des données de température, capteur déduit pour l'examen de la qualité de l'eau, capteur spécialisé pour mesurer le degré d'humidité de l'atmosphère ou du sol, etc.).

Comme il est montré par la figure suivante, en haute de couche des capteurs nous avons trouvé les réseaux de communication.

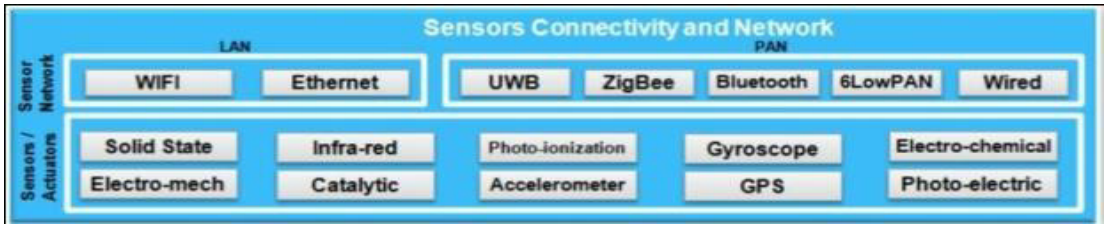


Figure 1.4: Couche des Capteurs [4].

1.4.2 Passerelles et couche réseau

Les passerelles sont rôle est le routage des données provenant des capteurs. la couche réseau et passez-le à la couche suivante qui est la couche de service de gestion.

Cette couche nécessite une grande capacité de stockage pour stocker l'énorme quantité de données collectées par les capteurs, etc. De plus, cette couche doit avoir une performance fiable en termes de réseaux publics, privés et hybrides.

La plupart des appareils IoT fonctionnent sur différents types de protocoles réseau. Tous ces protocoles doivent être assimilés en une seule couche. Cette couche est responsable de l'intégration de divers protocoles réseau.

À partir de la figure ci-dessous, en bas, nous avons la passerelle qui comprend les systèmes intégrés, processeurs de signal et modulateurs, microcontrôleurs, etc.. Au-dessus de la

passerelle, nous avons les réseaux de passerelle qui sont LAN (réseau local), WAN (réseau étendu) etc.

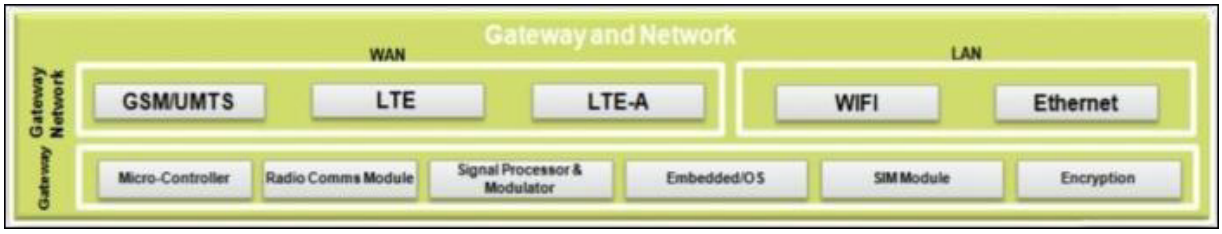


Figure 1.5: Passerelle et couche réseau [4].

1.4.3 Couche Service de gestion

Cette couche est utilisée pour gérer les services IoT. La couche Service de gestion est à l'origine de l'analyse des informations (Stream Analytics, Data Analytics) et de la gestion des périphériques.

La gestion des données est nécessaire pour extraire les informations a partir de l'énorme quantité de données brutes recueillies par les dispositifs connectés. Pour l'objectif de donner un résultat précieux de toutes les données collectées. Cette action est effectuée dans cette couche.

De plus, certaines situations exigent une réponse immédiate à la situation (en temps réel). Cette couche contribue à cela en traitant des données, en extrayant des informations et en gérant le flux de données.

À partir de la figure ci-dessous, nous pouvons voir que la couche de service de gestion dispose d'un service de support opérationnel (OSS) qui inclut la modélisation et la configuration du système. En outre, nous avons le système de support de facturation (BSS) qui prend en charge la facturation et les rapports. [6]

En outre, à partir de la figure, nous pouvons voir qu'il existe des services d'application IoT / M2M qui incluent la plate-forme Analytiques; Données - qui est la partie la plus importante; Sécurité qui inclut les contrôles d'accès, le cryptage, la gestion des accès d'identité, etc. Nous avons ensuite la gestion des règles métier (Business Rule Management, BRM) et la gestion des processus métier (BPM).

Figure 1.6: Couche de service de gestion [4].

1.4.4 Couche d'application

La couche d'application constitue la couche supérieure de l'architecture IoT, responsable de l'utilisation efficace des données collectées.

Diverses applications IoT comprennent la domotique, la cyber santé, le cyber gouvernement, etc.

De la figure ci-dessous, nous pouvons voir qu'il y a deux types d'applications qui est le marché horizontal qui inclut la gestion de flotte, la chaîne d'approvisionnement, …etc. et sur l'application sectorielle d'IoT, nous avons l'énergie, la santé, le transport, etc. [6]

Figure 1.7: Couche d'application [4].

1.5. Technologies

1.5.1 Capteurs

Les capteurs permettent d'en savoir plus sur l'environnement qui nous entoure. Ils sont importants pour l'internet des objets car ils permettent d'obtenir des informations essentielles. Les capteurs sont présents partout autour de nous : dans les téléphones portables, dans les GP et sur les feux de signalisation routière,... etc. Les capteurs permettent de « recueillir des informations présentes dans l'environnement pour enrichir les fonctionnalités du dispositif » [5].Ils sont de plus en plus petits et sont donc plus facilement intégrables au sein des objets. Ainsi, nous pouvons faire le lien avec la loi de Moore qui explique que les ordinateurs/les capteurs deviennent de moins en moins chers, ils sont également de plus en plus petits et environ tous les 18 mois, leur puissance se voit multipliée par deux. Cette miniaturisation permet aux capteurs de s'implanter plus facilement dans les objets afin que ceux-ci puissent donner davantage d'informations. En 2013, environ 3,5 milliards de capteurs partout dans le monde et ce chiffre pourrait atteindre 100.000 milliards de capteurs en 2030. [6]

Figure 1.8: quelques capteurs [6].

1.5.2 Connectivité [8]

1.5.1.1. Communication radio courte portée

Wifi: Il est le plus utilisé par les entreprises sur le marché. Par contre, à cause du grand nombre de périphériques connectés à un seul point d'accès, un nouveau standard a été implémenté, le IEEE Wifi 802.11ah utilisant une bande de 900 MHz qui peut connecter 8 000 périphériques à l'intérieure d'un périmètre de 1 km. En outre, ce standard permet une plus faible consommation d'énergie grâce à d'autres innovations établies autour du Wifi avec rétrodiffusion ou '*backscatter WiFi*' permettant une communication sans alimentation ou avec une consommation minime de batterie.

- Norme : basée sur 802.11n (actuellement la norme la plus utilisée pour un usage privé)
- Fréquences : bandes de 2,4 GHz et 5 GHz
- Portée : environ 50 m
- Vitesses de transmission : 600 Mbit/s maximum, mais les vitesses habituelles sont plus proches de 150 Mbit/s, en fonction de la fréquence de canal utilisée et du nombre d'antennes (la dernière norme 802.11-ac devrait permettre des vitesses pouvant atteindre 500 Mbit/s à 1 Gbit/s)

Z-wave: Un des protocoles les plus utilisés dans le domaine. Il permet la minimisation de la consommation d'énergie faisant de lui le protocole préféré pour les périphériques avec batteries. Quant à son fonctionnement, il utilise une technologie radio de faible puissance dans la bande de fréquence de 868.42 MHz. Il est optimisé pour les échanges à faible bande passante, entre 9 et 40 kbits/s. En ce qui concerne le protocole, il définit les couches radio et les couches applicatives permettant l'interopérabilité des équipements en précisant le type d'équipement à l'aide de la notion de classe. De plus, chaque nœud agit comme un répéteur dans un réseau de 232 appareils. Il est aussi important à noter qu'il est facile à intégrer dans les produits électroniques.

- Norme : Z-Wave Alliance ZAD12837/ITU-T G.9959
- Fréquence : 900MHz (ISM)
- Portée : 30 m
- Vitesses de transmission : 9,6 / 40 / 100 Kbit/s

ZigBee: Un des protocoles basé sur la norme IEEE 802.15.4 ayant une faible consommation d'énergie et un coût faible qui fonctionne dans un réseau maillé (Wireless Mesh Network). Ce type permet le routage des messages à deux niveaux, soit au niveau de la couche réseau et de la couche applicative.

- Norme : ZigBee 3.0 basé sur IEEE802.15.4
- Fréquence : 2,4 GHz
- Portée : 10-100 m
- Vitesses de transmission : 250 Kbit/s.

Bluetooth: Ce protocole est déjà connu via notre utilisation des appareils mobiles. Dans le domaine d'IoT, il est utilisé avec la même contrainte de proximité. Ce qui le diffère du ZigBee et Z-wave est son utilisation de bande passante plus élevée. La nouvelle version Bluetooth LE permet une faible consommation d'énergie en comparant avec le WiFi.

- Norme : la spécification fondamentale de Bluetooth 4.2
- Fréquence : 2,4 GHz (ISM)
- Portée : 50-150 m (Smart/BLE)
- Vitesses de transmission : 1 Mbit/s (Smart/BLE)

1.5.1.2. Communications radio mobiles longue

LoRa: Ce protocole permet la communication à bas débit basé sur LPWAN (Low-Power Wide Area Network). Il permet la communication machine à machine (M2M), et ce, particulièrement dans le secteur industriel et des villes intelligentes. Il est caractérisé par son pouvoir de couvrir un plus grand périmètre grâce à sa forte capacité et son réseau en étoile. Sa consommation d'énergie est aussi faible que celle du ZigBee et Z-wave. Il a plusieurs avantages dont sa facilité, la traçabilité des objets et la sécurité.

Figure 1.9: La technologie LoRa [8].

Sigfox: La technologie Sigfox s'est également spécialisée dans le M2M (Machine to Machine) à l'aide d'une connectivité cellulaire, dédiée aux réseaux à bas débit. Sigfox veut réinventer la transmission d'informations en baissant d'une manière importante la consommation d'énergie des périphériques connectés ainsi que le coût. On sait que le prix est un facteur clef de succès pour voir émerger durablement l'IoT. Sigfox a généré un réseau longue portée à bas débit permettant la communication de données de taille réduite entre les objets connectés.[8]

Figure 1.10: La technologie Sigfox [8].

1.6. Domaines d'application [9]

- Automobile:

Reliée à l'IoT, la voiture transforme les données en informations exploitables, à la fois dans le véhicule et dans le monde qui l'entoure.

Figure 1.11: Automobile [9].

- Énergie:

L'Internet des objets permet aux innombrables appareils qui composent le réseau électrique de partager des informations en temps réel pour une distribution et une gestion plus efficaces de l'énergie.

Figure 1.12: Énergie [9].

- Santé:

On trouve plusieurs genres d'équipements des soins utilise la technologie IoT, tels que les appareils médicaux *wearables* et tablettes de premiers secours...etc.

Figure 1.13: Santé [9].

- Industrie:

La technologie IoT permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production et d'assurer la sécurité des employés.

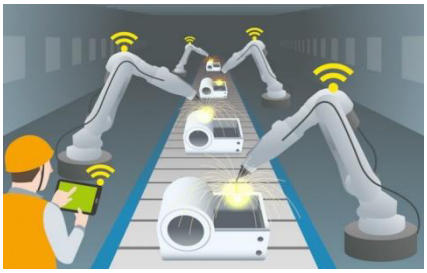


Figure 1.14: Industrie [9].

- Vente au détail:

L'IoT offre aux détaillants des possibilités illimitées d'améliorer l'efficacité des chaînes d'approvisionnement, de développer de nouveaux services et de proposer de nouvelles expériences aux clients.

Figure 1.15: Vente au détail [9].

- Bâtiments intelligents:

L'IoT résout les problèmes de l'augmentation des coûts énergétiques, de développement durable et de conformité au code en connectant, gérant et sécurisant les appareils qui collectent les données.

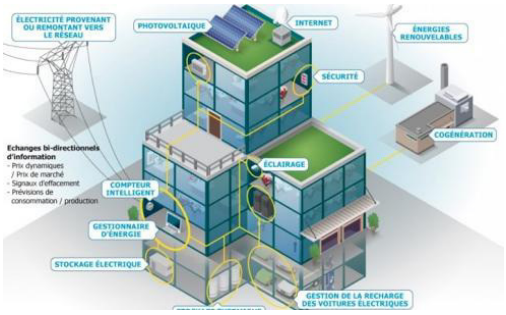


Figure 1.16: Bâtiments intelligents [9].

- Maisons intelligentes :

Parmis les application dans les Maisons intelligentes (Smart Home) on a la reconnaissance vocale à l'identification de la personne à la porte d'entrée, la technologie IoT donne vie au rêve d'une maison intelligente protégée.

Figure 1.17: Maisons intelligentes [9].

- Transports:

Dans un système logistique intelligent de transport, des voitures autonomes sera connectées les réseaux IoT peut sauver des vies, réduire le trafic et minimiser l'impact des véhicules sur l'environnement.

Figure 1.18: Transports [9].

1.7. Conclusion

Dans ce chapitre, on a vu les différents aspects de l'IoT, concernant les caractéristiques, l'architecture, les technologies et les domaines d'application. Par ailleurs, les objets connectés exposent un grand nombre de vulnérabilités et problèmes de sécurité. Dans ce stade, le deuxième chapitre est consacré à détailler ces points, ainsi les mécanismes de détection et de prévention.

Chapitre 02

Système de détection d'intrusion et Sécurité

2.1. Introduction

Une propriété de valeur doit être protégée contre le vol et la destruction. Certaines maisons sont équipées de systèmes d'alarme qui peuvent décourager des voleurs, prévenir les autorités dans le cas d'une effraction et même avertir les propriétaires que leur maison est en feu. De telles mesures sont nécessaires pour assurer l'intégrité des maisons et la sécurité de leurs propriétaires [10].

La même assurance d'intégrité et de sécurité devrait également être appliquée aux systèmes et données informatiques. L'internet a facilité le flux d'informations, personnelles, financières et autres. En même temps, il a également promu autant de dangers. Les utilisateurs malveillants et les craqueurs recherchent des proies vulnérables comme les systèmes sans correctifs, les systèmes affectés par des chevaux de Troie et les réseaux exécutant des services peu sûrs. Des alarmes sont nécessaires pour prévenir les administrateurs et les membres de l'équipe de sécurité qu'une effraction s'est produite afin qu'ils puissent répondre en temps réel au danger. Les systèmes de détection d'intrusions ont été conçus pour jouer le rôle d'un tel système d'alarme [11].

Deux approches ont été proposées à ce jour dans ce but: l'approche comportementale et l'approche par signatures. La première se base sur l'hypothèse que l'on peut définir un comportement « normal » de l'utilisateur et que toute déviation par rapport à celui-ci est potentiellement suspecte. La seconde s'appuie sur la connaissance des techniques employées par les attaquants : on tire des signatures d'attaque et on recherche dans les traces d'audit leur éventuelle survenue [12].

Dans ce chapitre nous présentons tout d'abord la notion de système de détection d'intrusions ainsi que son architecture. On présente également la classification des IDS, dans ce cadre plusieurs critères sont pris en compte. Commençant par la classification selon la méthode d'analyse qui découpe les IDS en deux approches (comportementale et par signatures), enfin on mettre le point sur la détection d'intrusions dans les maisons intelligents (*Smart Home*).

2.2. Concepts de base

2.2.1 Système de détection d'intrusion (IDS)

La détection des intrusions est le processus de surveillance des événements se trouvant dans un système des ordinateurs ou du réseau et les analysant pour détecter les signes des intrusions, défini comme des tentatives pour compromettre la confidentialité, l'intégrité, la disponibilité ou éviter des mécanismes de sécurité de l'ordinateur ou du réseau. L'intrusion est causée par les attaques accédant au système via l'Internet, autorisée l'utilisateur du système qui essaye de gagner les privilèges supplémentaires pour lesquels ils n'ont pas autorisés, et autorisé les utilisateurs qui abusent les privilèges donnés. Le système de détection des intrusions est un logiciel ou un matériel qui automatise des surveillances et les processus analysés [13].

Les IDS traditionnellement suivent deux critères :

- **Fiabilité :** toute intrusion doit effectivement donner lieu à une alerte. Une intrusion non signalée constitue une défaillance de l'IDS, appelée faux négatif. (voir Figure 2.1)
- **Pertinence des alertes :** toute alerte doit correspondre à une intrusion effective.

Toute « fausse alerte » (appelée également faux positif) diminue la pertinence de l'IDS. (voir Figure 2.1)

Un IDS est parfaitement fiable en absence de faux négatif ; il est parfaitement pertinent en l'absence de faux positif

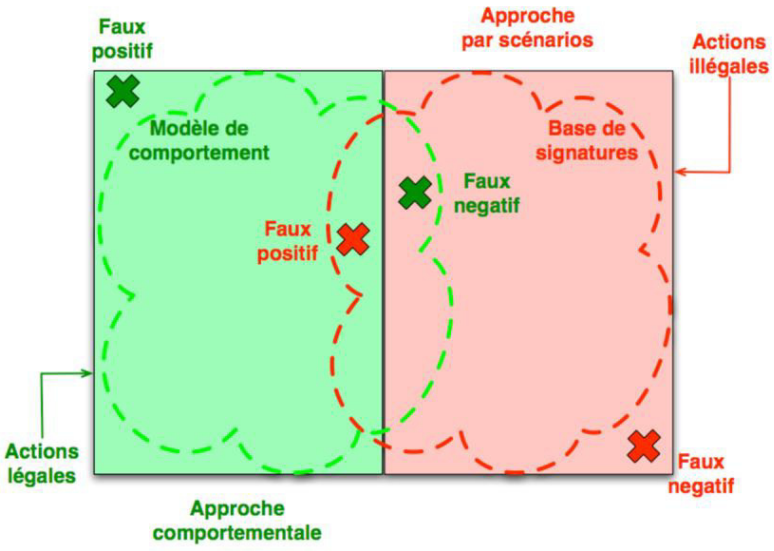


Figure 2.1: Critères des IDS [14].

Un IDS a quatre fonctions principales : l'analyse, la journalisation, la gestion et l'action [15].

- Analyse: Analyse des journaux du système pour identifier des intentions dans la masse de données recueillie par l'IDS. Il y a deux méthodes d'analyse : L'une basée sur les signatures d'attaques, et l'autre sur la détection d'anomalies.
- Journalisation: Enregistrement des évènements dans un fichier de log. Exemples d'évènements : arrivée d'un paquet, tentative de connexion.
- Gestion: Les IDS doivent être administrés de manière permanente. On peut assimiler un IDS à une caméra de sécurité.
- Action: Alerter l'administrateur quand une attaque dangereuse est détectée.

2.2.2 Attaque

Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système.
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- glaner des informations personnelles sur un utilisateur.
- récupérer des données bancaires.
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.).
- troubler le bon fonctionnement d'un service.
- utiliser le système de l'utilisateur comme « rebond » pour une attaque.
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

2.2.3 Intrusion

Opération qui consiste à accéder, sans autorisation, aux données d'un système informatique ou d'un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place.

2.3. Classes d' IDS

2.3.1 Network IDS

Le rôle essentiel d'un IDS basé sur le réseau (NIDS) est l'analyse et l'interprétation des paquets circulant sur ce réseau.

L'implantation d'un NIDS sur un réseau se fait de la façon suivante : des capteurs sont placés aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une attaque. Ces alertes sont envoyées à une console sécurisée, qui les analyse et les traitent éventuellement. Cette console est généralement située sur un réseau isolé, qui relie uniquement les capteurs et la console [28].

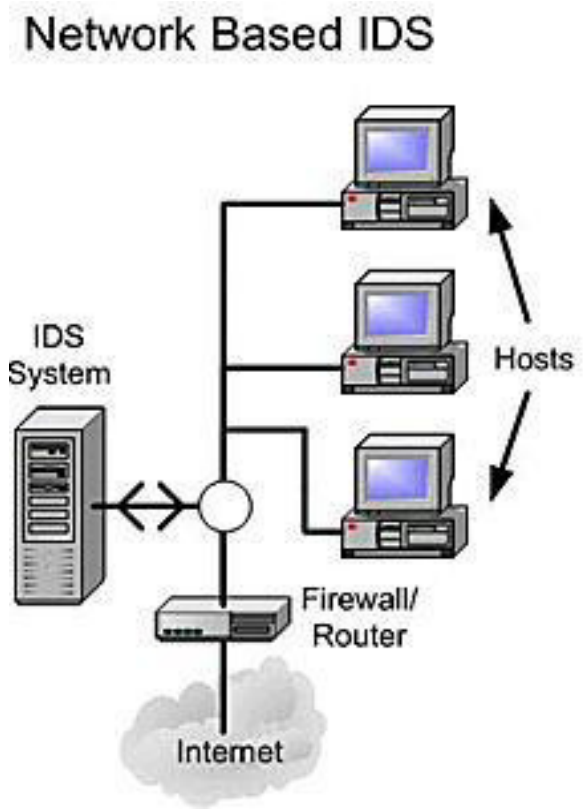


Figure 2.2 : Architecture d'un NIDS [19].

2.3.2 Host IDS

Les HIDS (Host IDS) analysent le fonctionnement et l'état des machines sur lesquelles ils sont installés. L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent êtres levées [19].

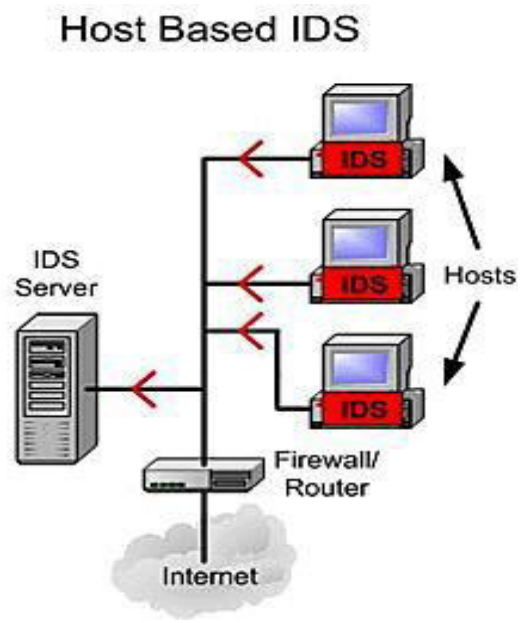


Figure 2.3: Architecture d'un HIDS [19].

2.3.3 IDS Hybride

Les IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, en un seul outil, de surveiller le réseau et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et agréger/lier les informations d'origines multiples. Ainsi, on comprend que les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi. Cela permet de communiquer et d'extraire des alertes plus pertinentes. Les avantages des IDS hybrides sont multiples : [19]

- Moins de faux positif.
- Meilleure corrélation (la corrélation permet de générer de nouvelles alertes à partir de celles existantes).
- Possibilité de réaction sur les analyseurs.

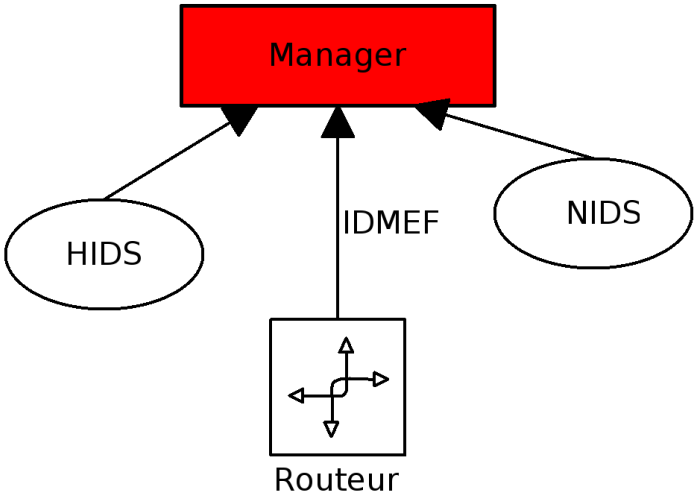


Figure 2.4: Architecture d'un IDS Hybride [19].

2.4. Architecture d'un IDS :

Cette section décrit les trois composants **(capteur, analyseur et manager)** qui constituent classiquement un système de détection d'intrusions. La Figure 2.5 illustre les interactions entre ces trois composants.

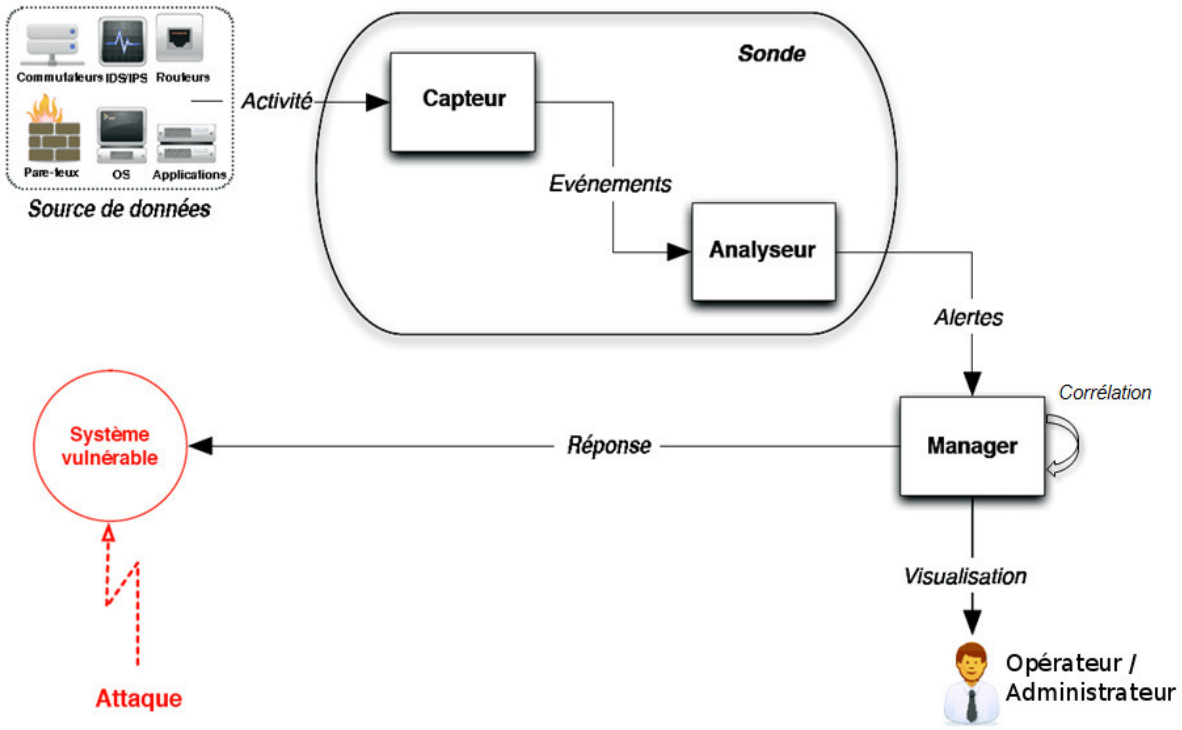


Figure 2.5: Architecture d'un IDS [14].

2.4.1 Capteur

Le capteur observe l'activité du système par le biais d'une source de données et fournit à l'analyseur une séquence d'événements qui renseignent de l'évolution de l'état du système. Le capteur peut se contenter de transmettre directement ces données brutes, mais en général un prétraitement est effectué. On distingue classiquement trois types de capteurs en fonction des sources de données utilisées pour observer l'activité du système : les capteurs système, les capteurs réseau et les capteurs applicatifs [14].

2.4.2 Analyseur

L'objectif de l'analyseur est de déterminer si le flux d'événements fourni par le capteur contient des éléments caractéristiques d'une activité malveillante [14].

2.4.3 Manager

Le manager collecte les alertes produites par le capteur, les met en forme et les présente à l'opérateur. Éventuellement, le manager est chargé de la réaction à adopter qui peut être : [14]

- Confinement de l'attaque, qui a pour but de limiter les effets de l'attaque
- Eradication de l'attaque, qui tente d'arrêter l'attaque ;
- Recouvrement, qui est l'étape de restauration du système dans un état sain
- Diagnostic, qui est la phase d'identification du problème.

Du fait du manque de fiabilité des systèmes de détection d'intrusions actuels, les réactions sont rarement automatisées, car elles peuvent se traduire par un déni de service en cas de faux positif.

2.5. Les approches d'IDS

Plusieurs critères permettent de classer les systèmes de détection d'intrusions, la méthode d'analyse étant le principal. Deux méthodes dérivant de cette dernière existent aujourd'hui : l'approche comportementale et l'approche par scénarios.

On peut citer aussi d'autres critères de classification des IDS: la fréquence d'utilisation, les sources de données à analyser, le comportement de l'IDS après intrusion [21].

2.5.1 Approche comportementale

L'approche comportementale est fondée sur une description statistique des sujets.

L'objectif est de détecter les actions anormales effectuées par ces sujets (par exemple, des heures de connexion anormales, un nombre anormal de fichiers supprimés ou un nombre anormal de mots de passe incorrects fournis au cours d'une connexion).

Le comportement normal des sujets est appris en observant le système pendant une période donnée appelée phase d'apprentissage (par exemple, un mois). Le comportement normal, appelé comportement sur le long terme, est enregistré dans la base de données et comparé avec le comportement présent des sujets, appelé comportement à court terme. Une alerte est générée si une déviation entre ces comportements est observée. Dans cette approche, le comportement sur le long terme est, en général, mis à jour périodiquement pour prendre en compte les évolutions possibles des comportements des sujets. Je considère traditionnellement que l'avantage principal de l'approche comportementale est de pouvoir être utilisée pour détecter de nouvelles attaques. Autrement dit, en signalant toute déviation par rapport au profil, il est possible de détecter a priori toute attaque qui viole ce profil, même dans le cas où cette attaque n'était pas connue au moment de la construction du profil [21].

Cependant, cette approche présente également plusieurs inconvénients. Tout d'abord, le diagnostic fournit par une alerte est souvent flou et nécessite une analyse complémentaire.

Ensuite, cette approche génère souvent de nombreux faux positifs car une déviation du comportement normal ne correspond pas toujours à l'occurrence d'une attaque. Citons à titre d'exemples, en cas de modifications subites de l'environnement de l'entité modélisée, cette entité changera sans doute brutalement de comportement. Des alarmes seront donc déclenchées. Pour autant, ce n'est peut-être qu'une réaction normale à la modification de l'environnement [21].

En outre, les données utilisées en apprentissage doivent être exemptes d'attaques, ce qui n'est pas toujours le cas. Enfin, un utilisateur malicieux peut habituer le système (soit pendant la phase d'apprentissage, soit en exploitation si l'apprentissage est continu) à des actions malveillantes, qui ne donneront donc plus lieu à des alertes. Le problème de la détection d'intrusions est couramment approché d'une façon radicalement différente qui est l'approche par scénario [21].

2.5.2 Approche par scénario

La détection d'intrusions peut également s'effectuer selon une approche par scénario. Il s'agit de recueillir des scénarios d'attaques pour alimenter une base d'attaques. Le principe commun à toutes les techniques de cette classe consiste à utiliser une base de données, contenant des spécifications de scénario d'attaques (on parle de signatures d'attaque et de base de signatures). Le détecteur d'intrusions compare le comportement observé du système à cette base et remonte une alerte si ce comportement correspond à une signature prédéfinie. Le principal avantage d'une approche par scénario est la précision des diagnostics qu'elle fournit par rapport à ceux avancés par l'approche comportementale. Il est bien entendu que l'inconvénient majeur de cette approche est qu'elle ne peut détecter que des attaques dont elle dispose de leur signature. Or, définir de façon exhaustive la base de signatures est une des principales difficultés à laquelle se heurte cette approche. La génération de faux négatifs est à craindre en présence des nouvelles attaques. En effet, contrairement à un système de détection d'anomalies, ce type de détecteur d'intrusions nécessite une maintenance active : puisque par nature il ne peut détecter que les attaques dont les signatures sont dans sa base de données, cette base doit être régulièrement (sans doute quotidiennement) mise à jour en fonction de la découverte de nouvelles attaques. Aucune nouvelle attaque ne peut par définition être détectée [21].

D’autre part, il existe de nombreuses attaques difficiles à détecter car elles nécessitent de corréler plusieurs événements. Dans la plupart des produits commerciaux, ces attaques élaborées sont décomposées en plusieurs signatures élémentaires. Cette décomposition peut générer de nombreux faux positifs si un mécanisme plus global n'est pas développé pour corréler les alertes correspondant à ces différentes signatures élémentaires. Chacune de ces deux approches peut conduire à des faux positifs (détection d’attaque en absence d’attaque) ou à des faux négatifs (absence de détection en présence d’attaque) [21].

2.6. IDS pour smart home

Le concept Smart Home vise à créer un écosystème cohérent constitué d'un nombre croissant d'appareils intelligents. L'utilisation courante des dispositifs intelligents encourage les attaquants potentiels à violer la confidentialité. Parfois, prendre le contrôle d'un appareil permet à l'attaquant d'obtenir des données secrètes (comme un mot de passe pour le réseau WiFi domestique).

Dans ce contexte, Le problème se pose lorsqu'un utilisateur non autorisé est capable d'utiliser des appareilles intelligents connectés dans un Smart Home a travers la transmission radio. L'attaquant peut facilement endommager ou utiliser les objets intelligents de manière inappropriée et ainsi influencer les systèmes Smart Home (par exemple, le chauffage, la surveillance, le système de santé etc.).

Généralement, un réseau local d'un *Smart Home* connecte trois types de périphériques (Figure 2.6): les dispositifs intelligents, les contrôleurs et les périphériques réseau chargés de connecter le *Smart Home* à Internet. Les appareils intelligents, qui agissent en tant qu'éléments actifs ou passifs, interagissent directement avec l'environnement. Les contrôleurs sont des passerelles dépendant de la technologie assurant la communication entre les appareils intelligents et les réseaux. Les passerelles résidentielles connues également sous le nom de routeurs résidentiels (*Home Gateway*) sont des dispositifs qui facilitent la communication entre le réseau local et l'opérateur d'internet (*ISP*).

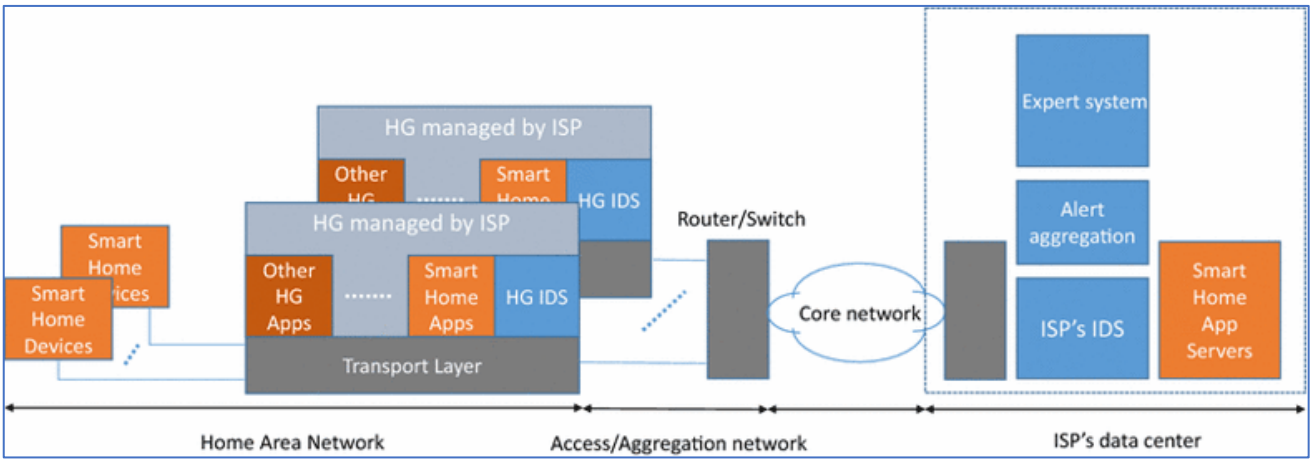


Figure 2.6: Architecture for IDS in Smart Home

2.7. Travaux connexes

Les environnements domestiques intelligents sont considérés comme un élément clé des applications IoT. L'adoption généralisée des appareils intelligents dans les maisons d'aujourd'hui (Smart Home) a conduit les chercheurs à se concentrer sur les propriétés de sécurité et de confidentialité. Dans cette section, on présente trois travaux connexes concernant le sujet du Système de détection d'intrusion pour maison intelligente (IDS for Smart Home).

Le travail intitulé "Smart Home Automation System for Intrusion Detection",[16] Ce travail a discuté la conception et la mise en œuvre d'un système domotique intelligent avec détection d'intrusion incorporée pour minimiser les dommages causés par l'attaque.

La Figure 2.7 présente le schéma fonctionnel de l'architecture du système proposé.

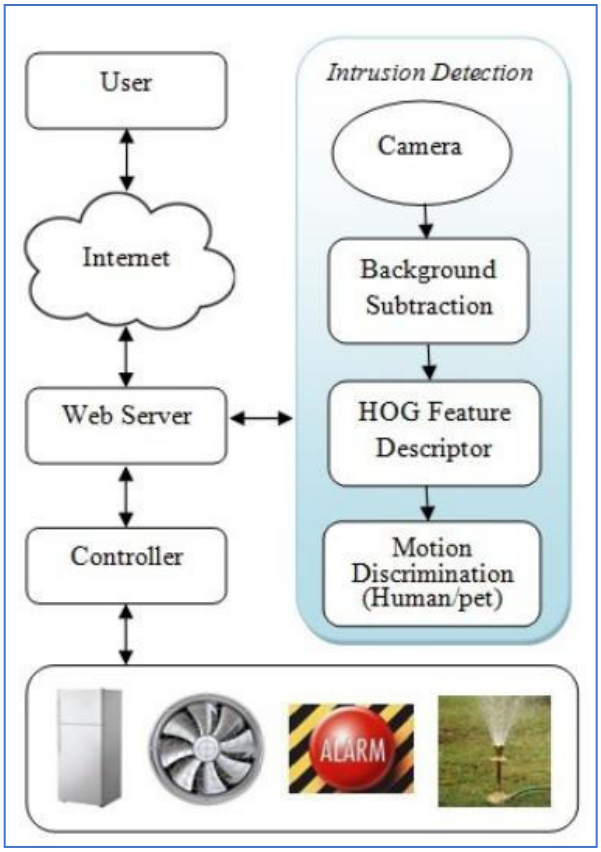


Figure 2.7: Schéma fonctionnel de l'architecture[16].

Le système de détection d'intrusion utilisé dans ce travail permet à l'utilisateur de détecter le mouvement humain à partir d'une séquence vidéo et de rejeter un mouvement non humain (animaux de compagnie par exemple, etc.). Les descripteurs utilisés dans cette section sont basés sur l'histogramme des dégradés orientés (HOG). Le système détecte d'abord la région de mouvement à l'aide de la soustraction d'arrière-plan (BGS), puis calcule les valeurs d'entités histogramme en superposant la normalisation de contraste locale. La discrimination de mouvement facilite enfin la détermination de la présence humaine au moyen d'un classificateur SVM (Support Vector Machine).

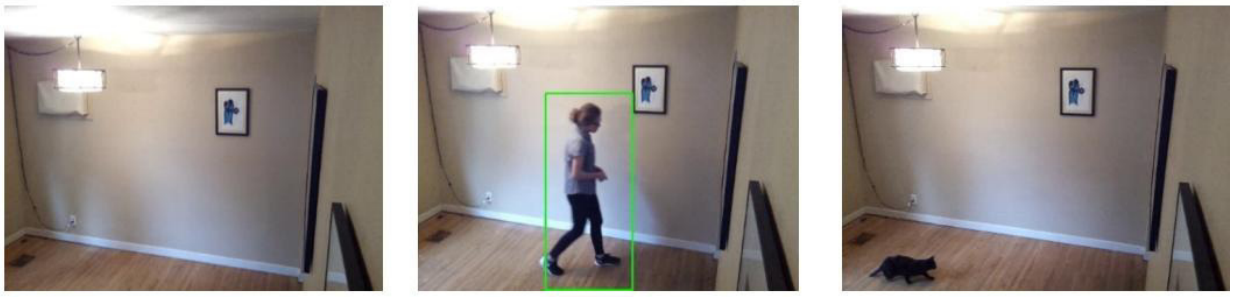


Figure 2.8: Exemple expérimentale [16].

La figure ci-dessus (**Figure 2.8**) montre trois cas possibles: (a) absence de mouvement ou bien arrière plan vide, (b) capture d'une intrusion d'une personne qui passe, et le dernier cas (c) présente un chat dans le plan et le système classifie ce comportement comme action nulle (mouvement non humain).

L'expérience de ce travail suggère qu'il est difficile d'obtenir un bon taux de détection dans des scénarios en temps réel. Par conséquence la détection d'intrusion rejette intelligemment les "fausses alarmes" possibles qui peuvent se produire en raison d'un mouvement non humain. Le système proposé est donc précis à 87,2% dans la détection et la classification de l'intrus en mouvement [16].

Un autre travail intitulé " Specification-based Intrusion Detection for Home Area Networks in Smart Grids " [17]. Ce papier présenter un IDS basé sur des spécifications en couches pour les réseaux domestiques.

Dans ce travail, le comportement normal du réseau est défini par le biais de spécifications prédéfini de l'IDS. Chaque déviation par rapport au comportement normal défini peuvent être le signaliser comme activités malveillantes.

L'IDS basé sur les signatures a des taux de "faux positifs" faibles, mais il est incapable de détecter les attaques inconnues et sa base de données doit être mise à jour très fréquemment. A l'inverse de l'IDS basé sur les comportements, qui souffre de taux élevés de "faux positifs" et de longs temps d'apprentissage et de mise au point, mais il est capable de détecter des nouvelles attaques et inconnues.

Les auteurs de ce papier proposent un IDS pour fonctionner dans un Smart Home,il permet de détecter les attaques contre les appareils a partir l'analyse de trafic de données (déférentes scenario exécuter). Ce système écoute le trafic vers et depuis les interfaces des objets connectés et extrait les propriétés de trafic.

Contrairement aux IDS basés sur les signatures, les IDS basés sur les comportements sont censés détecter les attaques connues et inconnues au même temps [17].

Le travail intitulé " A Host-based Intrusion Detection and Mitigation Framework for Smart Home IoT using OpenFlow " [23].

Dans ce travail, un cadre de détection et d'atténuation des intrusions est proposé, appelé IoT-IDM, pour fournir une protection au niveau du réseau pour les dispositifs intelligents déployés dans les environnements domestiques Smart Home.

Les auteurs de ce papier exploitent la technologie HIDS pour redessiner et intégrer le système de sécurité à l'intérieur des objets connectés. Cependant, une telle approche ne serait pas à l'échelle et ne serait pas abordable. Cela qu'ils lui motiver à proposer un cadre de travail (Framework) qui sera capable de détecter et d'atténuer les menaces de la sécurité dans les maisons intelligentes.

Toute on utilisant les capacités de l'architecture SDN (Software-Defined Networking) et en particulier le protocole OpenFlow pour réaliser ce framework.

Les applications SDN pour la sécurité réseau doivent idéalement pouvoir détecter et isoler les périphériques réseau qui ont été compromis.

Le point fort de cet article est d'utiliser des statistiques de flux pour détecter les anomalies, ce qui réduit les charges sur le contrôleur central. Cependant, cette approche est incapable de détecter d'autres types d'attaques telles qu'une insuffisance d'autorisation.

Les équipements Hardware dans les réseaux informatiques (comme commutateurs et routeurs) ont deux fonctionnalités principales. Le premier est le "plan de contrôle", qui est responsable de prendre des décisions sur l'endroit où le trafic est envoyé, et le second est le "plan de données" qui transmet le trafic à la destination sélectionnée. Par contre le système (SDN) est une nouvelle architecture prometteuse de la mise en réseau d'ordinateur au niveau du Software dans laquelle le "plan de contrôle" est découplé du "plan de données".

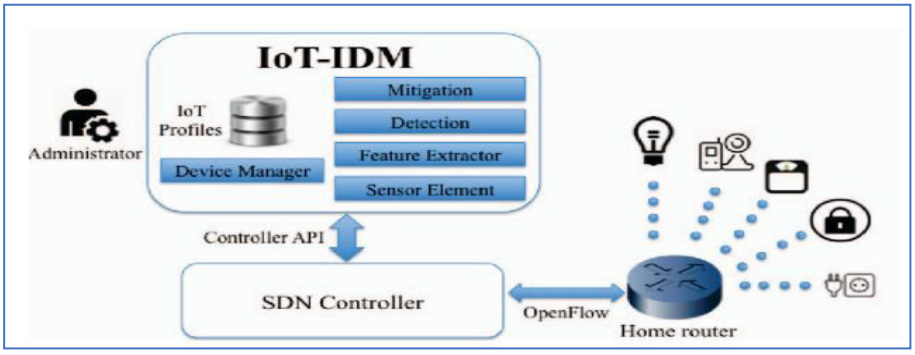


Figure 2.9: IoT-IDM Architecture [23].

Le système IoT-IDM crée un objet de capteur virtuel puis utilise les informations de localisation (adresse IP) du passerelle pour construire deux règles OpenFlow statiques afin de rediriger le trafic réseau allant et venant du passerelle vers les capteurs. Considérant les résultats obtenus, il s'est avéré que le système IoT-IDM a détecté l'intrusion de type "accès non autorisé" avec un taux de précision égale 94,25%.[23].

2.8. Conclusion

La plupart des IDS sont fiables, ce qui explique qu'ils sont souvent intégrés dans les solutions de sécurité. Les avantages qu'ils présentent face aux autres outils de sécurités les favorisent, mais d'un autre côté cela n'empêche pas que les meilleurs IDS présentent aussi des lacunes et quelques inconvénients. Nous comprenons donc bien qu'ils sont nécessaires mais ne peuvent pas se passer de l'utilisation d'autres outils de sécurité visant à combler leurs défauts.

Chapitre 03

Conception du système

3.1. Introduction

Ce chapitre présente la description d'une solution proposée dont le but est de sécuriser un smart home. Cette partie comprend deux étapes. La première étape consiste à décrire la réalisation en détail de cette smart home. La deuxième étape consiste à sécuriser smart home réalisée on se basant sur l'approche comportementale des IDS.

La conception est une phase très importante dans la création d'une application, cette dernière permet de tracer les grandes lignes avant le développement d'un logiciel. Dans notre conception on a utilisé le langage de modélisation unifié UML.

3.2. Architecture globale du système

Notre système a l'objectif de sécuriser un smart home, pour cela on a utilisé l'approche comportementale pour la détection d'intrusions.

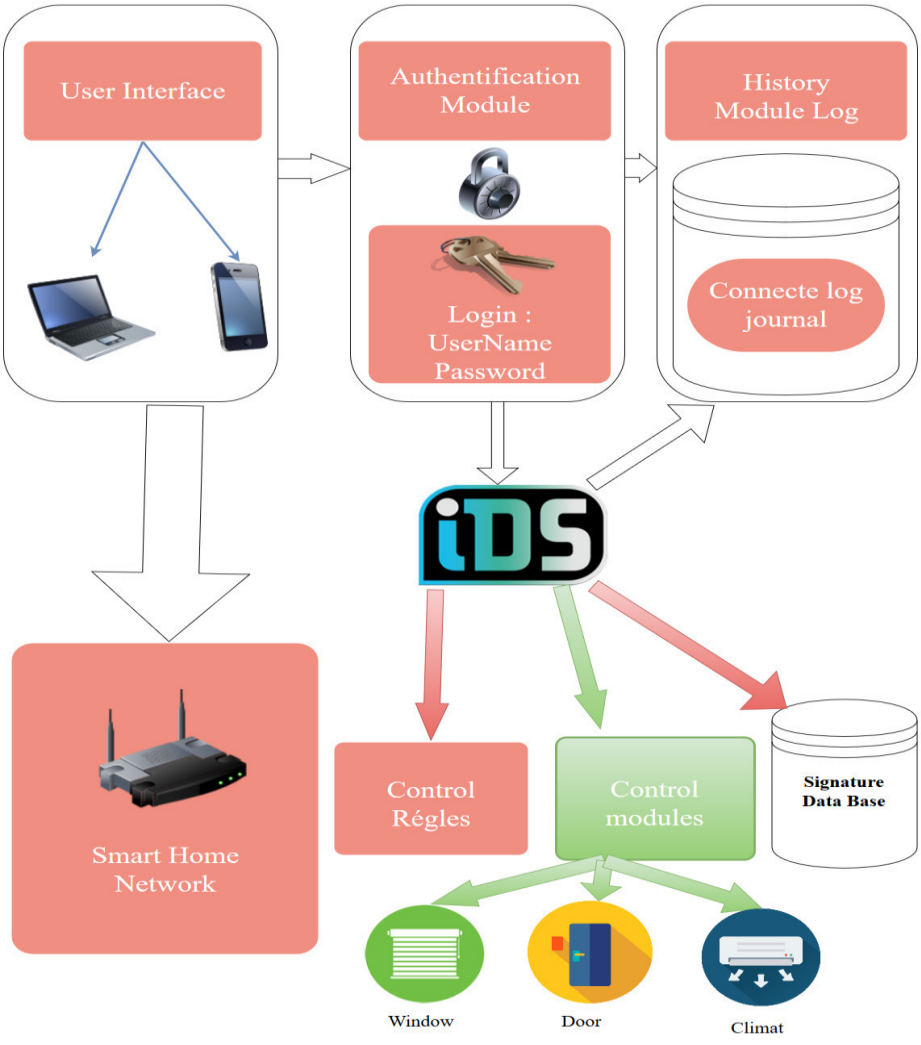


Figure 3.1: : Architecture générale du système.

3.3. Introduction à UML

UML (Unified Modeling Language, que l'on peut traduire par "langage de modélisation unifié) est une notation permettant de modéliser un problème de façon standard. Ce langage est né de la fusion de plusieurs méthodes existant auparavant, et est devenu désormais la référence en terme de modélisation objet, à un tel point que sa connaissance est souvent nécessaire pour obtenir un poste de développeur objet.

On peut voire UML comme un ensemble des diagrammes, on trouve parmis ces dernières :

- Le diagramme de cas d'utilisation : interactions entre le système et les utilisateurs (et autres systèmes externes). Il aide dans la visualisation des exigences / besoins.
- Le diagramme d'activité : séquence et parallélisme dans les activités du système, autrement dit, modélisation des processus métier avec les échanges de données
- Le diagramme de classes : classes, types, interfaces et relations entre eux.
- Le diagramme d'objets : instances de classes définissant une configuration importante du système.
- Machine à états : états des classes à travers leur cycle de vie (de la création / instanciation des objets à leur destruction) et les événements qui provoquent les transitions / changements d'états.
- Le diagramme d'interaction : qui se décline en deux types de diagrammes :

Le diagramme de séquence : interactions entre des objets pour lesquelles l'ordre des interactions est important

Le diagramme communications : interactions entre objets pour lesquels les connexions entre objets sont importantes.

- Le diagramme de composants : rassemblements de classes ou de composants tels que vus par l'équipe de développement pour décomposer le système en parties de logiciel gérables (du point de vue développement en gestion de projet).
- Le diagramme paquetages : rassemblement d'éléments de modélisation par exemple pour les distribuer entre membres de l'équipe de développement.
- Le diagramme déploiement : unités d'installation, de configuration et de déploiement du produit fini sur un parc de machines.

Dans notre travail on se limite sur l'utilisation de deux diagrammes qui sont :

- Diagramme de Cas d'utilisations
- Diagramme de séquence

3.4. Les diagrammes utilisés

3.4.1 Diagramme de Cas d'utilisations

Un diagramme de cas d'utilisation capture le comportement d'un système, d'un sous système, d'une classe ou d'un composant tel qu'un utilisateur extérieur le voit. Il scinde la fonctionnalité du système en unités cohérentes, les cas d'utilisation, ayant un sens pour les acteurs. Les cas d'utilisation permettent d'exprimer le besoin des utilisateurs d'un système, ils sont donc une vision orientée utilisateur de ce besoin au contraire d'une vision informatique.

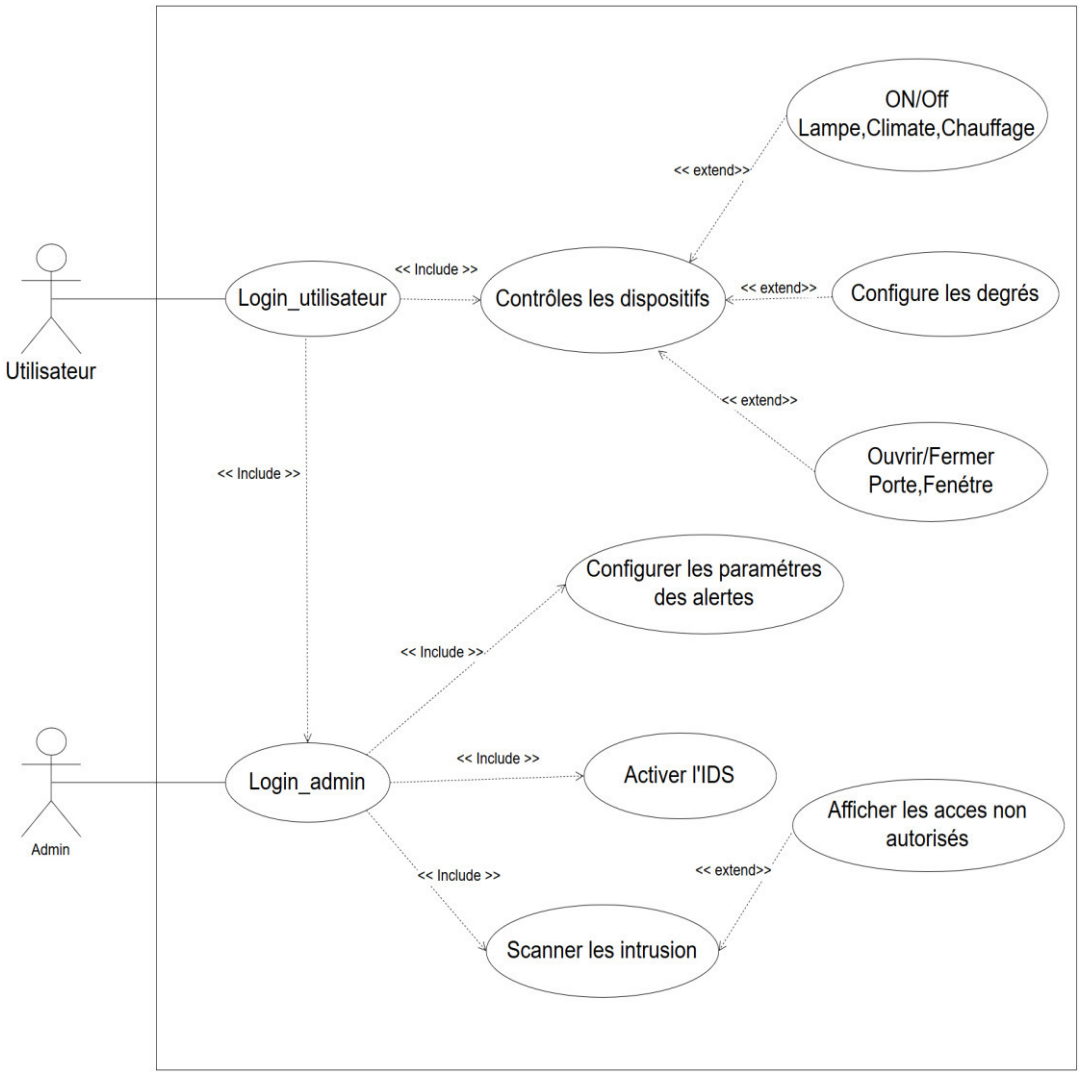


Figure 3.2 : Diagramme de Cas d'utilisations.

3.4.2 Le diagramme de séquence

Un diagramme de séquence qui représente la séquence de messages entre les objets au cours d'une interaction. Un diagramme de séquence comprend un groupe d'objets, représentés par des lignes de vie, et les messages que ces objets échangent lors de l'interaction.

- Diagramme de séquence : authentification

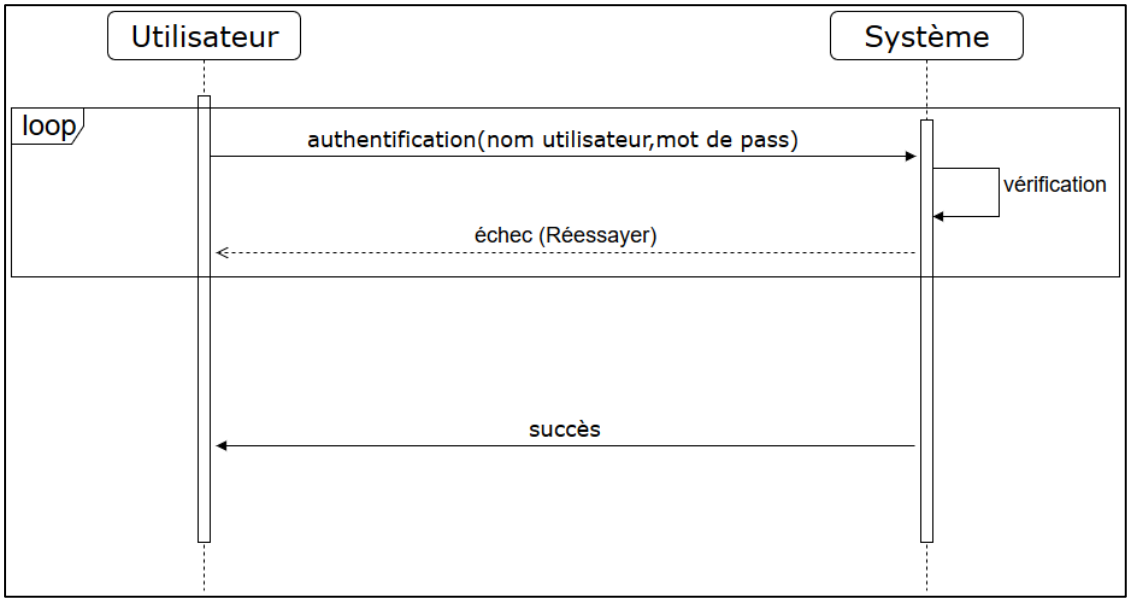


Figure 3.3 : Diagramme de séquence du scénario "authentification".

- Diagramme séquence : contrôle du dispositifs

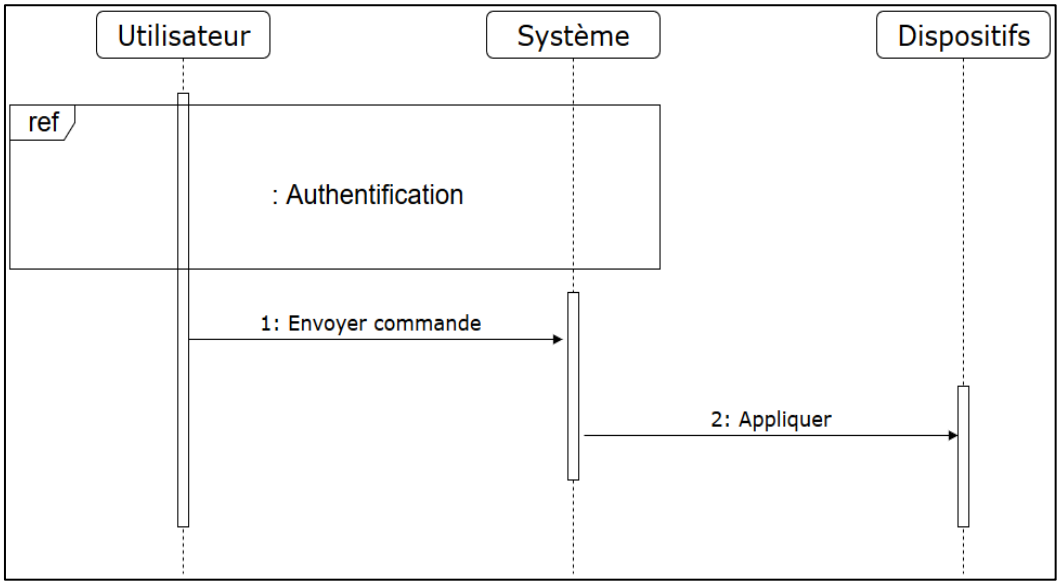


Figure 3.4 : Diagramme de séquence du scénario "contrôle du dispositifs".

- Diagramme séquence : configurer de l'admin

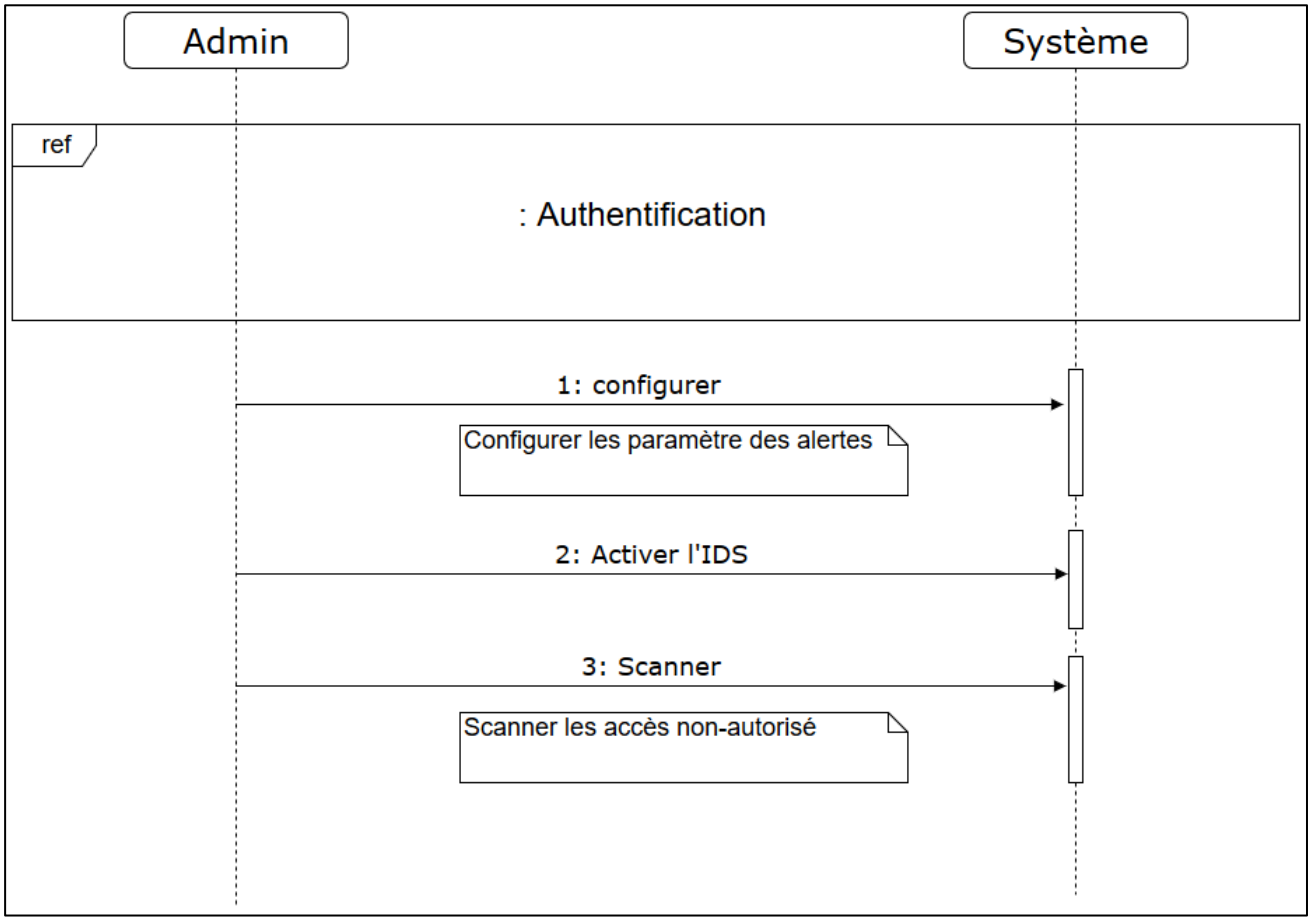


Figure 3.5 : Diagramme de séquence du scénario "configurer de l'admin".

3.5. Conclusion

Nous avons présenté dans cette partie les différentes phases pour aboutir à la réalisation de notre application et qui peuvent être schématisées par le schéma décrit ci-avant. En suite une interprétation de ses vues de conception, en terme des diagrammes et des schémas. Et les résultats et les implémentations de ces derniers sont donnés dans le chapitre suivant.

Chapitre 04

Mise en œuvre

4.1. Introduction

Ce dernier chapitre est réservé à la partie implémentation qui consiste à faire une présentation des différents outils utilisés lors du développement de notre application ainsi que la description de son fonctionnement par des images explicatifs. Nous avons principalement utilisé le langage JAVA et l'environnement de développement NetBeans.

4.2. Outils de développement utilisés

4.2.1 Langage java

Le langage Java est un langage de programmation informatique orienté objet et un environnement d'exécution informatique portable créé par James Gosling et Patrick Naughton employés de Sun Microsystems avec le soutien de Bill Joy (cofondateur de Sun Microsystems en 1982), présenté officiellement le 23 mai 1995 au SunWorld.

Nous avons choisi de développer notre système par le langage Java en vue de possibilités et les caractéristiques qu'il offert cette langage

- JAVA est un langage orienté objet simple.
- Est un langage facilement portable et peut s'exécuter sur les différents systèmes grâce a Java Virtuelle Machine (JVM)
- Java possède une importante bibliothèque de routines permettant de gérer les protocoles TCP/IP tels que HTTP et FTP. Les applications Java peuvent charger et accéder à des sur Internet via des URL avec la même facilité qu'elles accèdent à un fichier local sur le système.
- Java a été conçue pour être exploité dans des environnements serveur et distribués.
- Dans ce but, la sécurité n'a pas été négligée. Java permet la construction de systèmes inaltérables et sans virus
- Il permet un accès aux bases de données simplifié soit à travers la passerelle JDBCODBC ou à travers un pilote JDBC spécifique au SGBD.
- Il existe une API JAVA fournie avec l'éditeur d'ontologies Protégé 3.4.4 ce qui permet d'accéder à l'ontologie à partir de notre application.

- Il est doté d'une riche bibliothèque de classes, comprenant la gestion des exceptions, la gestion des interfaces graphiques (fenêtres, menus, graphismes, boites de dialogue, contrôles).

4.2.2 L' environnement NetBeans

NetBeans est un environnement de développement intégré (EDI), placé en open source par Sun en juin 2000 sous licence CDDL (Common Développement and Distribution License) et GPLv2. En plus de Java, NetBeans permet également de supporter différents autres langages, comme C, C++, JavaScript, PHP et HTML de façon native ainsi que bien d'autres (comme Python) par l'ajout de greffons. Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, éditeur graphique d'interfaces et de pages Web).

On a choisit NetBeans pour les raisons suivants :

- L'IDE NetBeans est un produit gratuit, sans aucune restriction quant à son usage, il est écrit en Java
- un outil pour les programmeurs pour écrire, compiler, déboguer et déployer les programmes Java
- NetBeans permet également de supporter différents autres langages, comme Python, C, C++, XML et HTML.
- Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, éditeur graphique d'interfaces et de pages web).
- NetBeans est disponible sous Windows, Linux, Solaris (sur x86 et SPARC), Mac OSX et Open VMS.
- Il ya également un grand nombre de modules pour étendre l'IDE NetBeans

4.2.3 SQLite

SQLite est un moteur de base de données relationnelle, son avantage par rapport à d'autres bases de données relationnelle est qu'elle est indépendante d'un système de gestion de base de données. Cela dit une base de données SQLite peut être intégrée facilement dans le code d'un programme, d'où l'usage récurrent de cette base dans le contexte des applications mobiles sous Android , IOS ou Windows Phone. Intégrer cette base dans les applications peut donc se faire dans un fichier appartenant au programme et indépendant de la plateforme en question. SQLite est open source et écrit en C.

4.2.4 Android studio

L'écosystème d'Android s'appuie sur deux piliers:

- le langage Java
- le SDK qui permet d'avoir un environnement de développement facilitant la tâche du développeur

Le kit de développement donne accès à des exemples, de la documentation mais surtout à l'API de programmation du système et à un émulateur pour tester ses applications.

Stratégiquement, Google utilise la licence Apache pour Android ce qui permet la redistribution du code sous forme libre ou non et d'en faire un usage commercial.

Le SDK était:

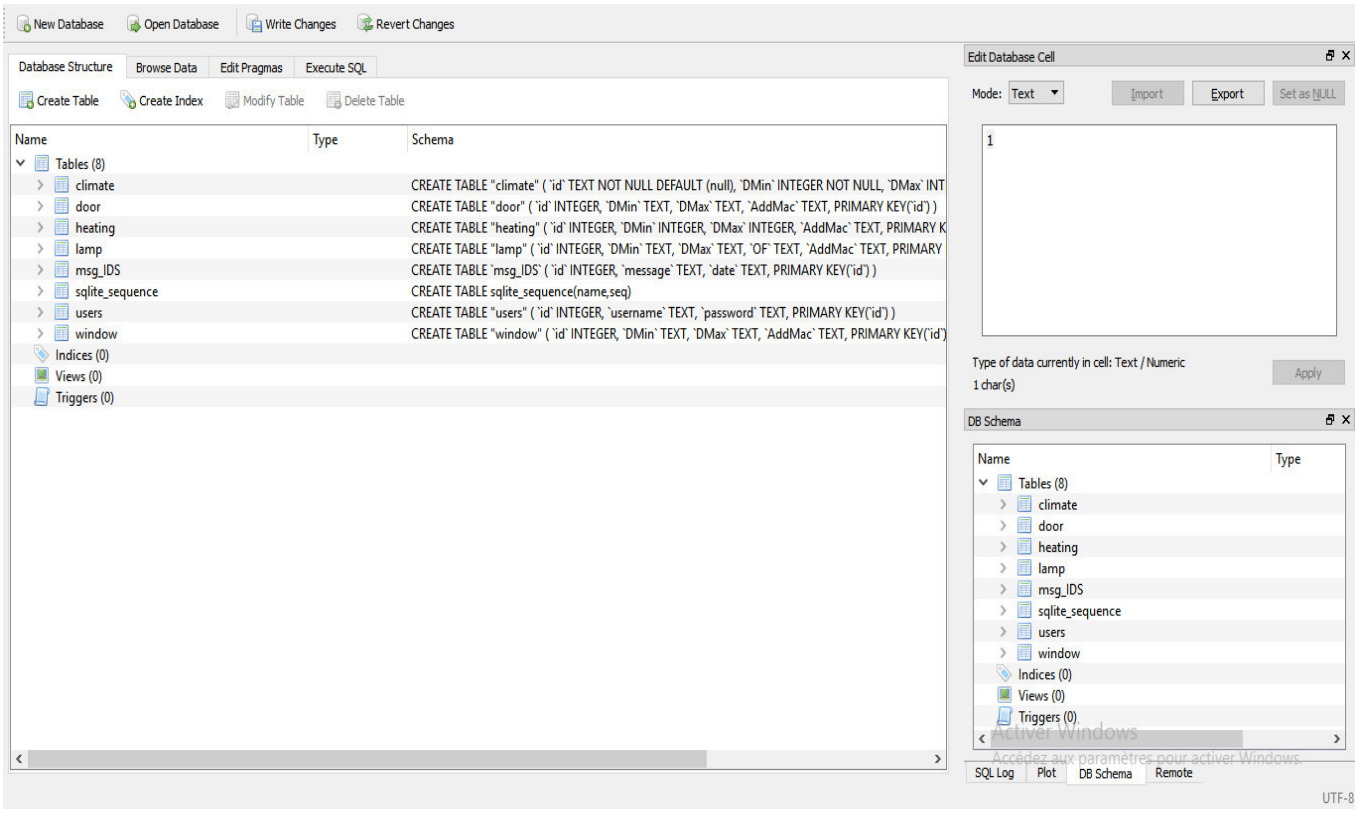
• anciennement manipulé par un plugin d'Eclipse (obsolète)

• maintenant intégré à Android Studio (IntelliJ)

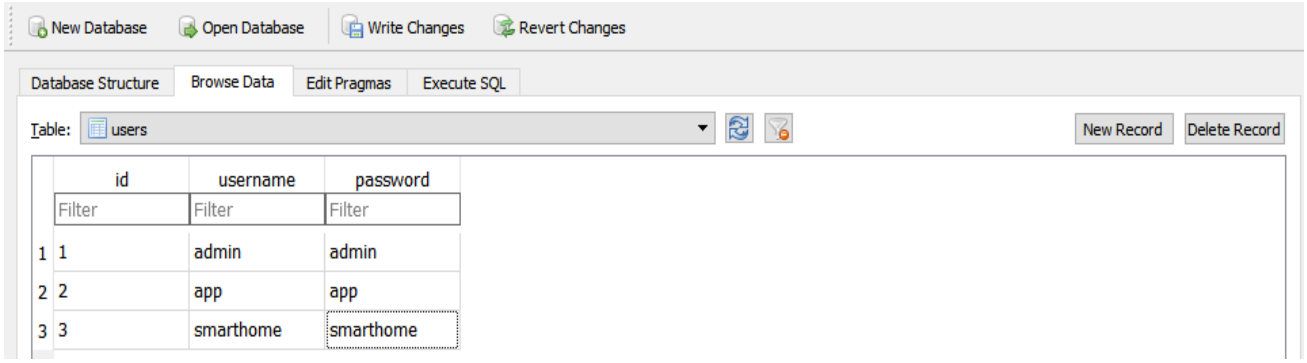
4.3. Etude de cas

4.3.1 Conception de la base de données

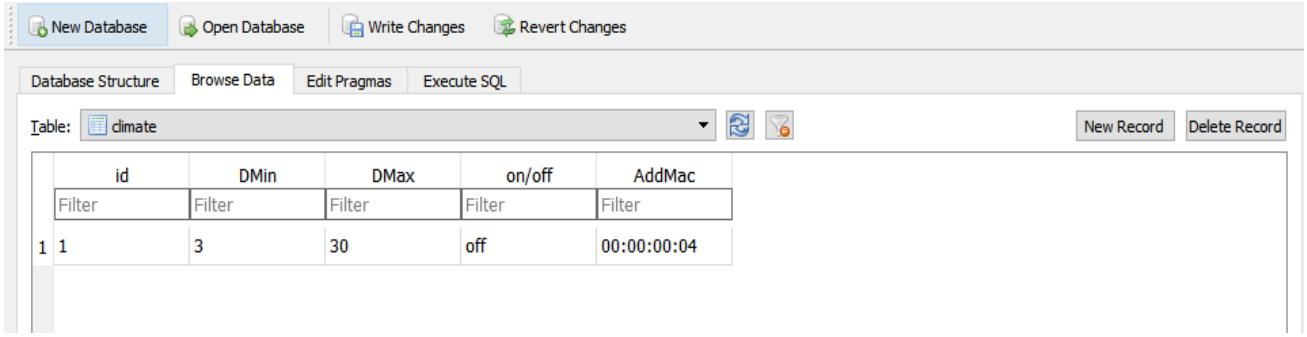
Les tables de la base de données : notre base de données contient 07 tables.



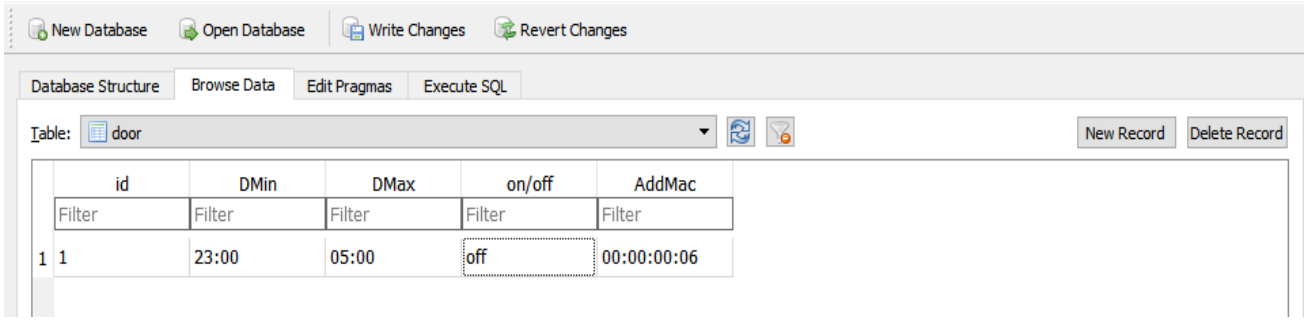
La table users : Cette table contient les informations des users inscris elle contient 03 champs avec **id** comme clé primaire.



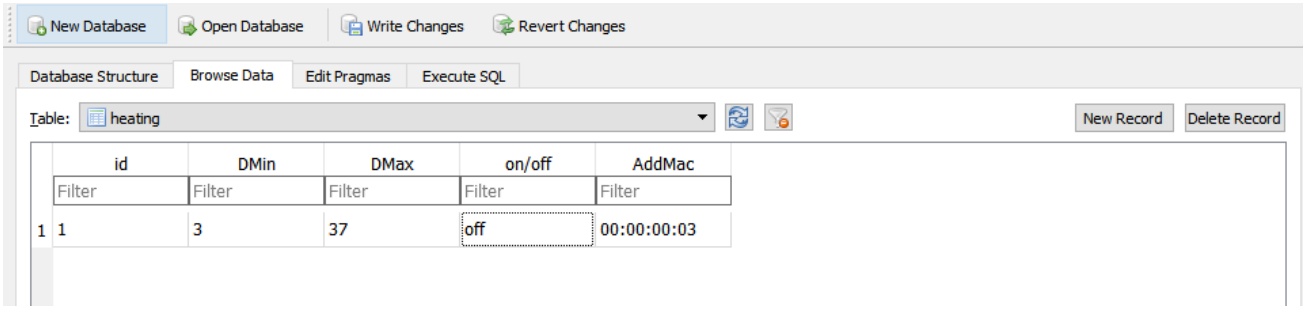
La table climate : Cette table contient les informations des climates elle contient 05 champs avec **id** comme clé primaire.



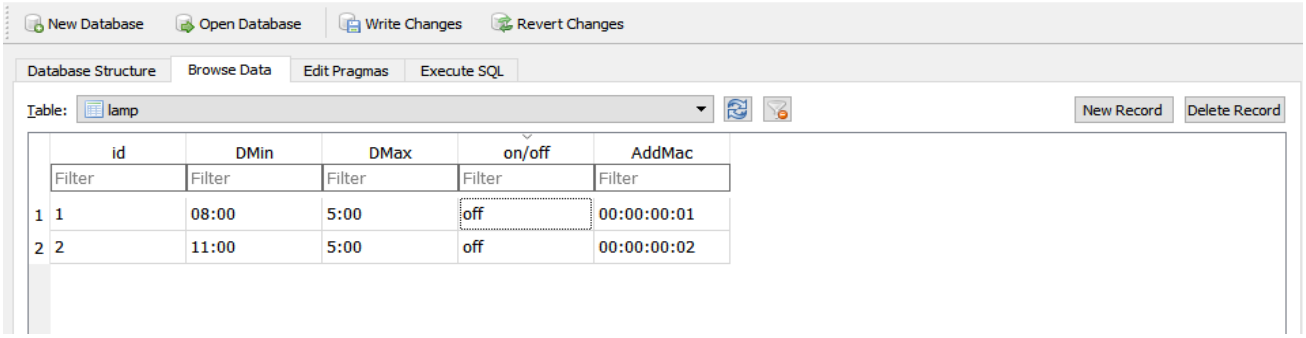
La table door : Cette table contient les informations des doors elle contient 05 champs avec **id** comme clé primaire.



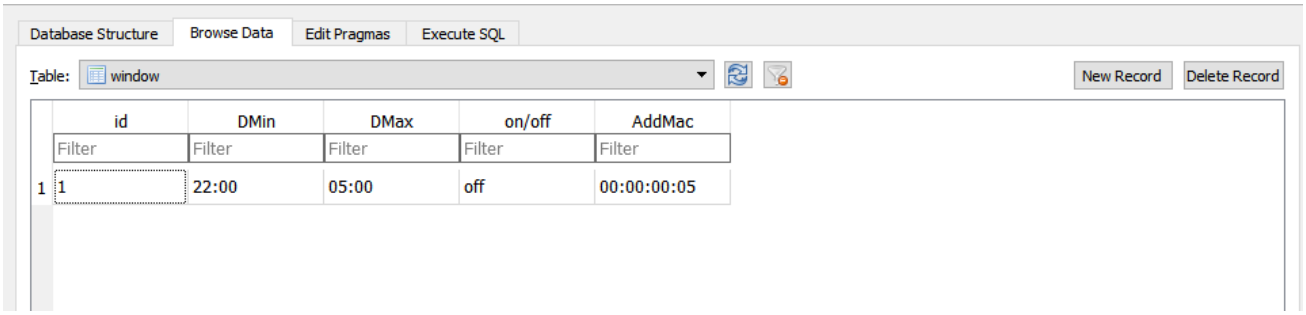
La table heating : Cette table contient les informations des heatings elle contient 05 champs avec **id** comme clé primaire.



La table lamp : Cette table contient les informations des lamps elle contient 05 champs avec **id** comme clé primaire.



La table window : Cette table contient les informations des **window** elle contient 05 champs avec **id** comme clé primaire.



4.3.2 Description de l'application

Notre application à une interface graphique " Smart home"est comme suit :

Figure 4.1: Interface smart home.

Cette interface login users pour commande les dispositifs :

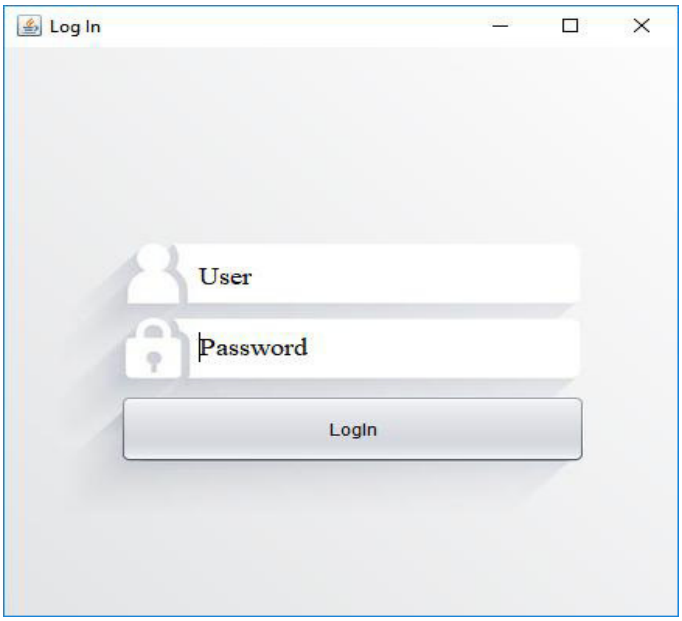


Figure 4.2: Interface Login User.

Cette interface sert à commande les dispositifs :

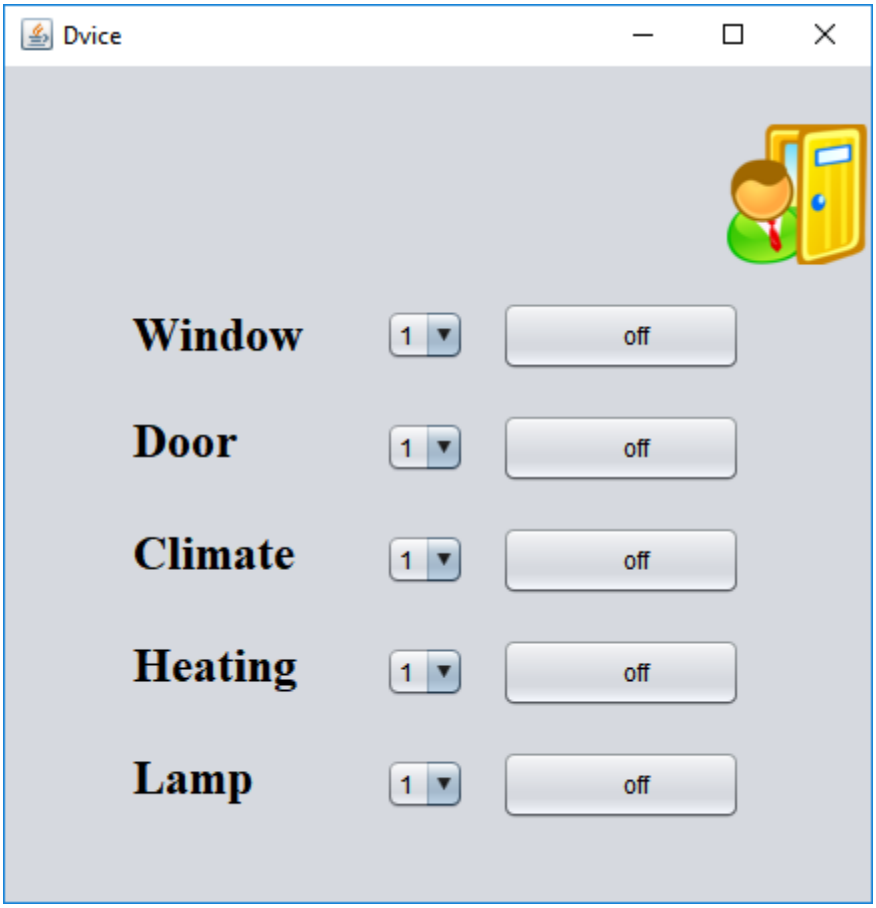


Figure 4.3: Interface commande les dispositifs.

Cette interface login admin pour configurer IDS et dispositifs :

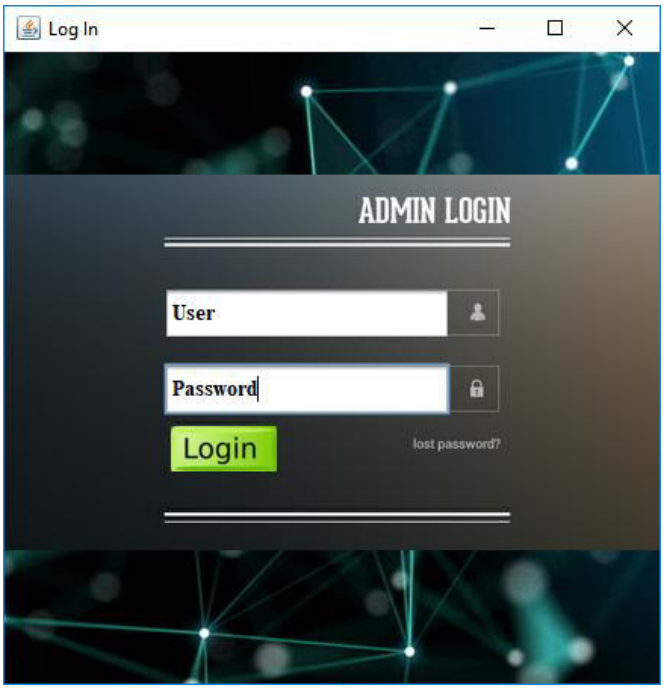


Figure 4.4: Interface Login pour admin.

Cette interface login admin pour configurer dispositifs :

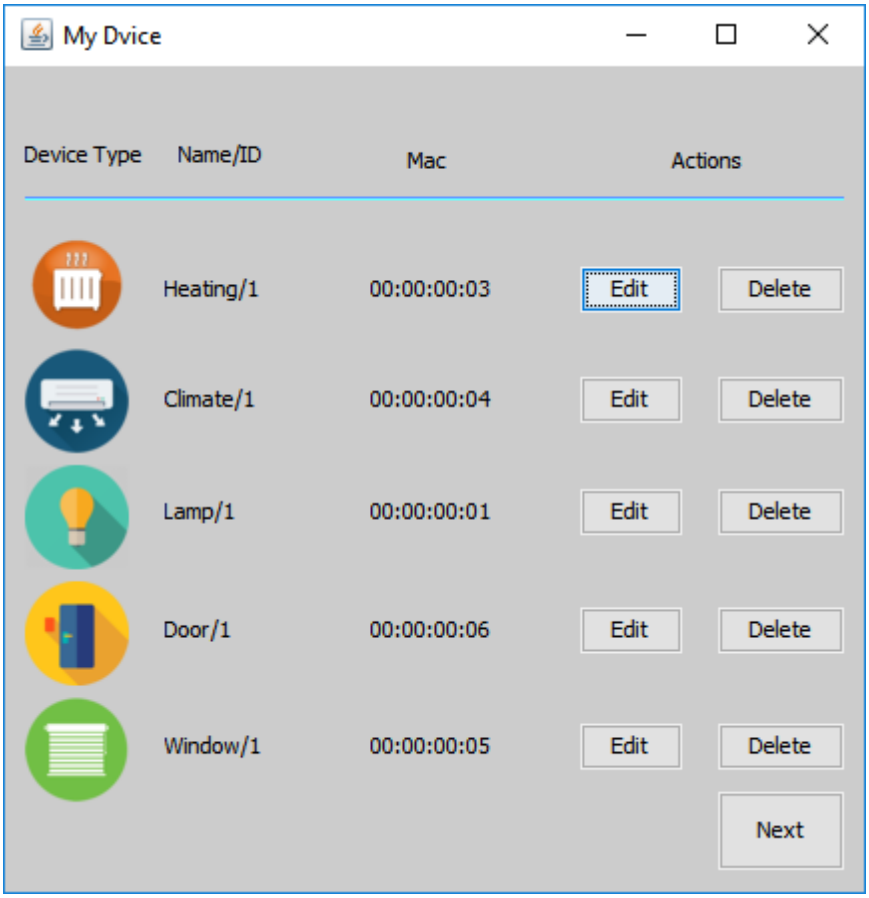


Figure 4.5: Interface configurer les dispositifs.

4.4. Conclusion

Dans ce chapitre on a décrire les détails d'implémentation de notre système de détection d'intrusions. Les résultats sont satisfaites.

Conclusion générale

Ce projet de fin d'étude consiste à proposer une solution au problème de sécurité informatique concernant le Système de détection d'intrusion appliquer pour les maisons intelligentes (*Smart Home*).

Au cours de ce mémoire, nous avons présenté une partie théorique autour de ce domaine, et une autre partie applicative sur les différentes étapes de la conception et la réalisation de notre application.

La réalisation de ce projet nous a permis d'explorer, d'apprendre et d'améliorer nos connaissances et nos compétences dans ce domaine. Nous avons appris à mieux manipuler les déférents outils de programmation, notamment: SQLite , Java ,Android studio et NetBeans.

En effet, et malgré toutes les difficultés que nous façons, ce travail me permit de découverte un nouveau domaine pour nous, c'est pourquoi nous restons besoin de recevoir toutes vos suggestions et remarques tendant à améliorer davantage cette initiative.

Bibliographie

[1] Site Web : "https://fr.wikipedia.org/ ", Consulté le : 10/04/2018.

[2] Site Web pour la ruée vers l'internet des objets: " https://www.horizons-decisionnels.fr/La-ruee-vers-l-internet-des-objets_a257.html ", Consulté le : 10/04/2018.

[3] Site Web pour la understanding internet of things: " https://learninternetgovernance.blogspot.com/p/internet-of-things-iot.html ", visité en 14/04/2018.

[4] Site Web pour la Internet of Things (IoT):" https://www.c-sharpcorner.com/UploadFile/f88748/internet-of-things-part-2/ ", visité en 14/05/2018.

[5] Benghozi et al. , «L'Internet des objets. Quels enjeux pour les Européens ? », Rapport de la chaire Orange "innovation and regulation", Ecole polytechnique et TELECOM Paris Tech. 2008, p. 9.

[6] Site Web pour la Liste des capteurs:" http://www.lafabriquediy.com/tutoriel/liste-des-capteurs-1-229/ ", visité en 20/05/2018.

[8] site Web pour la Internet of Things:" https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about ", visité en 20/05/2018.

[9] site Web pour la Applications M2M :" http://www.factorysystemes.fr/solutions/m2m/experiences-clients/ ", visité en 20/05/2018.

[10] http://stuff.mit.edu/afs/athena/project/rhel-doc/4/RH-DOCS/rhel-sg-fr-4/chdetection.html. Consulté le : 2018

[11] http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-fr-4/ch-detection.html ,consulté le: 2018.

[12] Aurobindo Sundaram, Met à jour le: Février 2005, « An introduction to intrusion detection », ACM Crossroads Student Magazine, disponible sur : http://www.acm.org/crossroads/xrds2-4/intrus.html , Consulté le : Mai 2018.

[13] Tran Van Tay, « Le systeme de detection des intrusions et le systeme d'empechement des intrusions », Rapport de stage de fin d'études, 2005.

[14] Jacob Zimmermann et al. , « Vers une détection d'intrusion à fiabilité et pertinence prouvable», Thèse de doctorat, Université de Technology, Australie, 2006.

[15] Fissale TCHAKALA, « Optimisation de la sécurité dans un environnement de travail bancaire», mémoire de fin d'étude pour l'obtention de Licence professionnelle, Université de Lomé, Togo, 2011.

[16] Danish Chowdhry et al , «Smart Home Automation System for Intrusion Detection», IEEE Canadian Workshop on Information Theory ,2015.

[17] Paria Jokar et al , « Specification-based Intrusion Detection for Home Area Networks in Smart Grids », Cyber and Physical Security and Privacy (IEEE SmartGridComm),2011.

[18] Nicolas Baudoin et Marion Karle, « NT Réseaux –IDS et IPS », 2000, support de cours, Enseignant Etienne Duris en 2003-2004.

[19] Michaël AMAND et Mohamed NSIRI , « Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire », Rapport de projet LENAC, 2011

[20] Lalaina KUHN, « VolP & Security :IPS» support de cours, Ecole d'Ingénieurs du Canton de Vaud.

[21] Jabou Chaouki, Schillings Michaël et Hantach Anis, « TER Détection d'anomalies sur le réseau », Rapport de projet, Université Paris Descartes, 2009

[22] Jacob Zimmermann et al. , « Vers une détection d'intrusion à fiabilité et pertinence prouvable», Thèse de doctorat, Université de Technology, Australie, 2006.

[23] Vijay Sivaraman et al , , « Network-Level Security and Privacy Control for Smart-Home IoT Devices », University of New South Wales, ∗IBM Research-Australia, ⋆NICTA, Australia