الجمهورية الجزائرية الديموقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE 20 AOUT 1955 SKIKDA
FACULTE DES SCIENCES
DEPARTEMENT D'INFORMATIQUE

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du diplôme de Master
Filière : Informatique
Spécialité : Génie Logiciel Avancé et Application

Thème :

Modèle cloud basé sur l'IOT et la blockchain pour une transmission sécurisée des données pour les villes intelligentes

---

Présenté par :
Mr. KHELFA SAHEL Mohamed salah.
Mr. MEDIOUNI Yacine

Encadré par :
Ms. ALIGUECHI Farida UNIVERSITE 20 AOUT 1955 Skikda Encadreur

2023 - 2024

Remerciement

Nous tenons tout d'abord à remercier Dieu le tout puissant et miséricordieux qui nous a donné la force et la patience d'accomplir ce Modeste travail. En second lieu, nous tenons à remercier notre encadreur Mme: « ALIGUECHI FARIDA » pour ses précieux conseils et son aide durant toute la période du travail. Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions. Nous tenons à exprimer nos sincères remerciements à tous les enseignants qui nous ont enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.

Enfin, nous tenons également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

DEDICACE

Je dédie cet humble travail C'est arrivé à mes chers parents, car Tout leur amour, leur tendresse, eux Soutien et prières tout au long De mes études.

En premier lieu, je déduis tout ce que j'ai Travaillez pour la femme qui a souffert pour moi , qui ne dit jamais non Mes exigences et qui n'a épargné personne Effort pour me rendre heureux : MON La merveilleuse maman Naima.

A l'homme, ma précieuse offrande De Dieu qui doit ma vie et ma réussite Avec tout le respect que je vous dois : Mon cher père est généreux.

Sans oublier Bynum, **Yacine** lui doit Soutien moral, patience et soutien Comprendre à travers cela projet.

Mohamed Salah

DEDICACE

Je tien a dédier ce modeste travail à tous ceux qui m’ont encouragédurant toute la période de réalisation de ce travail. En particulier :

A mes chers parents qui se sacrifient pour me voir réussir.

A ma soeur et mon frère qui m'ont toujours soutenu.

À mon ami, que je considère comme mon frère, mon plus grand supporter et mon meilleur partenaire dans mes études **Khelfa Sahel Mohamed Salah** , et deux autres à qui je remercie et leur souhaite beaucoup de succès.

A mes amis, merci à tous mes amis avec qui je partage des momentsde ma vie au fil du temps.

Yacine

Résumé : L'utilisation répandue de la technologie de l'Internet des Objets (IoT) présente à la fois des avantages et des inconvénients. Il est essentiel de disposer d'un système de sécurité complet et fiable pour que l'Internet des Objets fonctionne de manière sûre et empêche les intrusions. De nombreuses méthodes ont été développées pour renforcer la sécurité de l'IoT grâce à des systèmes de détection. Dans ce mémoire, un modèle de sécurité basé sur la blockchain et le cloud ; proposé récemment ; a été réalisé. Ce modèle assure la transmission sécurisée des données sur l'IoT.
Mots-clés: *internet des objets, vie privée, sécurit.*

ملخص: الاستخدام الواسع النطاق لتكنولوجيا إنترنت الأشياء (IoT) له مزايا وعيوب. يعد وجود نظام أمان شامل وموثوق أمرًا ضروريًا لكي يعمل إنترنت الأشياء بشكل آمن ويمنع التطفل. تم تطوير العديد من الأساليب لتعزيز أمان إنترنت الأشياء من خلال أنظمة الكشف. في هذه الأطروحة، نموذج أمني يعتمد على blockchain وCloud؛ تم اقتراحه مؤخرًا. يضمن هذا النموذج النقل الآمن للبيانات عبر إنترنت الأشياء.
كلمات مفتاحية : *انترنت الأشياء , الخصوصية , الحماية .*

Abstract: The widespread use of Internet of Things (IoT) technology presents both advantages and disadvantages. Having a comprehensive and reliable security system is essential for the Internet of Things to operate securely and prevent intrusions. Many methods have been developed to enhance IoT security through detection systems. In this dissertation, a security model based on blockchain and the cloud; recently proposed; Have been realised. This model ensures the secure transmission of data over the IoT.
Keywords: *Internet of things, privacy, security.*

Table des matières

Table des figures

Introduction générale

L’Internet des objets (IoT), la blockchain et le cloud sont des technologies innovantes qui promettent de révolutionner de nombreux secteurs. L'Internet des objets permet la connexion d'appareils intelligents pour les communications et l'automatisation dans les villes intelligentes, les soins de santé, l'automobile et l'industrie. La blockchain assure la sécurité et la transparence des transactions. Le cloud computing est un élément essentiel de l'architecture IoT, car il fournit l'infrastructure nécessaire pour établir des communications sécurisées et efficaces entre différents appareils et gérer les données qu'ils génèrent. Les systèmes de détection d'intrusion (IDS) dans l'Internet des objets (IoT) jouent également un rôle crucial dans la sécurisation des réseaux et des appareils connectés. Sa fonction principale est de surveiller en temps réel les activités suspectes ou anormales au sein du réseau IoT. Leur combinaison offre des solutions puissantes pour un avenir technologique sûr et efficace. Cette thèse explore leur développement, leurs fonctions et applications, ainsi que les enjeux de leur intégration.

Le présent mémoire est organisé en 4 chapitres :

Chapitre 1 est consacré à définir l'internet des objets, citer L'évolution d'internet des objets , ses fonctionnalités, ses différents domaines d’applications, et enfin mentionner ses avantages et ses inconvénients.

Chapitre 2 nous avons parlé des attaques contre les données IoT et nous avons présenté l'une des solutions, qui est le système de détection d'intrusion et son travail de protection des données IoT, en plus de son principe et enfin de ses types.

Chapitre 3 Il était consacré à la définition de la blockchain et du cloud, en mentionnant leurs fonctionnalités et leurs utilisations, en plus d'expliquer le modèle de système permettant d'assurer un transfert sécurisé de données sur l'Internet des objets (IoT).

Chapitre 4 est dédié à la réalisation d'un système Parking, dans ce chapitre nous expliquerons les langages de programmation utilisés ainsi que les outils utilisés pour la conception, la programmation et le développement. Nous présenterons également les interfaces interactives du système et, enfin, nous soulignerons l'importance de ce travail et la raison pour laquelle nous avons choisi la technologie utilisée.

Chapitre I

L'Internet des objets

(IOT)

L'Internet des objets (IoT) est une révolution technologique en informatique et en communication qui a mobilisé le domaine de l'industrie ces dernières années. Dans ce premier chapitre, nous allons survoler la notion d'Internet des objets.

1. Définition d'internet des objets

L'Internet des objets (IoT) désigne l'interconnexion de millions d'appareils et de capteurs intelligents connectés à Internet. Ces capteurs et ces appareils connectés collectent et partagent des données qui seront utilisées et analysées par plusieurs organismes, dont des entreprises, des villes, des gouvernements, des hôpitaux et des particuliers. Il faut savoir que : L'Internet des Objets est un réseau des 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 [01].

Figure 1.1: Internet des objets.

2. L'évolution d'internet des objets

En 1990, le premier objet de connexion a été reformulé. Ce sont des grille-pain, Machine à café ou autres objets du quotidien. En 2000, le fabricant coréen LG a lancé un industriel qui parle sérieusement d'électroménager connecté à Internet et La même année verra les premières expérimentations d'appareils connectés à Internet pour rechercher automatiquement des informations.

En 2003, la population mondiale atteignait environ 6,3 milliards et 500 millions d'appareil connecté à Internet [02]. Le résultat de la division du nombre d'appareils par La population mondiale (0,08) indique un faible nombre d'appareils connectés par habitant. Selon la définition Cisco IBSG, l'Internet des objets n'existait pas en 2003 en raison du nombre d'objets la connexion est faible. En raison de l'explosion des smartphones et des tablettes, le nombre d'appareils et le nombre de personnes connectées à Internet a atteint 12,5 milliards en 2010, alors que la population mondiale 6,8 milliards.

C'est pourquoi il y a plus d'un appareil connecté par personne (1.84) pour la première fois dans l'histoire. Cisco explique l'évolution du nombre d'objets dans son livre blanc IoT [03]. Aujourd'hui, il dépasse largement le nombre d'habitants sur Terre, et Comme indiqué, il devrait continuer à croître pour atteindre 50 milliard.

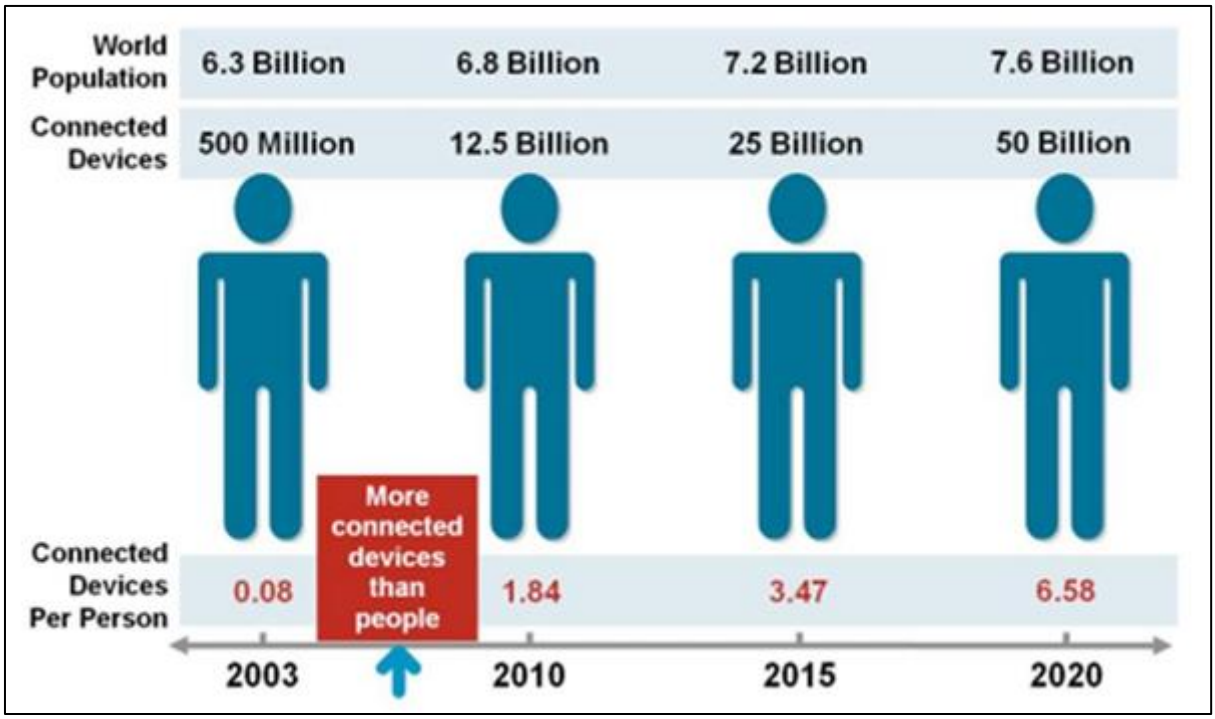

Figure 1.2: L'évolution d'internet des objets.[07]

3. La fonctionnalité de l'internet des objets

L'écosystème internet des objets il intègre divers technologies et domaines de compétences. Un système IDO constitué généralement, du hardware, du software, des protocoles de communication, du Cloud et du mobile.

3.1. Collecter / Actionner

On est à la première couche au niveau des objets connectés. Qui peuvent être des capteurs qui captent des mesures de l'environnement physique (température, humidité) et des actionneurs qui ont le pouvoir d'agir sur l'environnement (des moteurs pour fermer ou ouvrir le volet de la chambre). Certains objets sont dotés de capacités et de ressources matérielles nécessaires qui leur permettent de se connecter directement à Internet. Mais généralement, ayant des contraintes matérielles, les objets connectés implémentent des protocoles de communication à basse énergie / bas débit et utilisent une Gateway pour pouvoir se connecter a internet cette Gateway peut être un Smartphone, une arduino ou une Raspberry … [04].

3.2. Communiquer

À cette étape que se passe l'envoi des données du LAN vers le Cloud. Et on peut distinguer deux modèles de protocoles pour transporter la donnée : Le modèle Publish / Subscribe avec des protocoles de type MQTT et le modèle REST avec des protocoles comme HTTP ou encore CoAP [04].

3.3. Exécuter

Cette étape s'occupe du stockage et du traitement des données. À cette étape que rentre en jeux la Plate-forme IoT qui est une solution Cloud qui a pour fonction de connecter plusieurs objets connectés, de traiter et de stocker leurs données, les analyser et les exposer à travers les différentes applications. Les plateformes IoT permettent aussi de faire communiquer des objets qui utilisent des protocoles différents [04].

3.4. Visualiser

Cette étape a pour tache d'afficher les services des objets connectés à travers différentes applications dédiées. Un utilisateur, à travers une application mobile, peut communiquer avec ses objets en consultant leurs données ou bien en envoyant des actions vers ses objets [04].

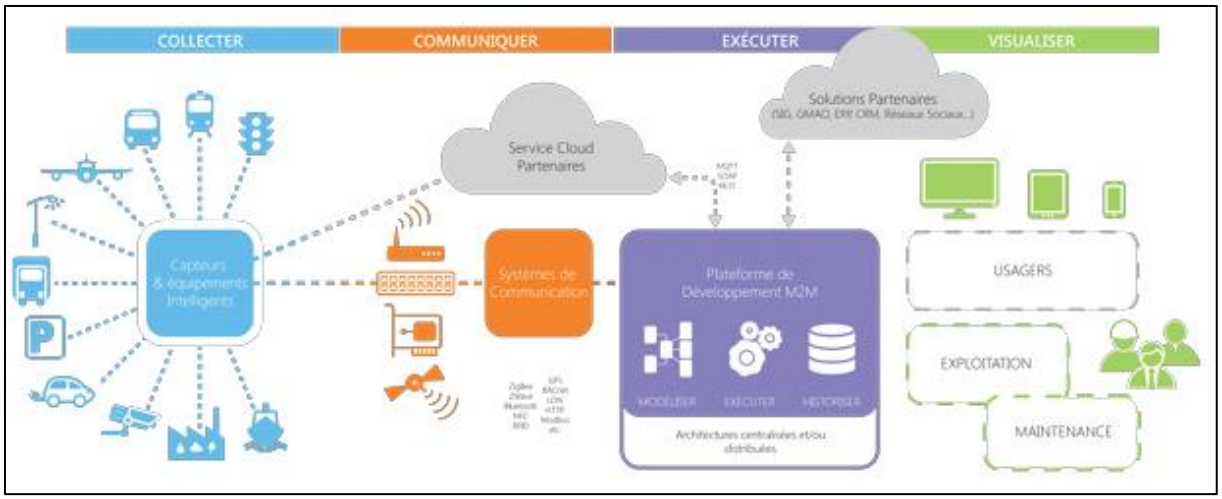

Figure 1.3: les fonctionnalités d'un écosystème IOT.[08]

4. Domaines d'applications

Dans nos jours l'importance de l'internet des objets augmente jour par jour, les chercheurs estiment : "que 3 millions de nouveaux terminaux se connecter à l'Internet chaque mois, dans les prochaines années ce chiffre devrait atteindre les 30 milliards appareils connectées dans le monde entier". L'utilisation de l'IOT permettra le développement de plusieurs applications intelligentes qui affecteront principalement les domaines abordés dans ce qui suit, avec un bref d'exemples de ses applications [05].

4.1. Les villes intelligentes

Beaucoup de grandes villes ont été soutenues par des projets intelligents, comme Séoul, New York, Tokyo, Shanghai, Singapour, Amsterdam et Dubaï. Les villes intelligentes (voir Figure 1.4) peuvent encore être considérées comme des villes de l'avenir et la vie intelligente, et par le taux d'innovation de la création de villes intelligentes d'aujourd'hui, il sera devenu très faisable pour entrer la technologie IoT dans le développement des villes.

La demande exige une planification minutieuse à chaque étape, avec l'appui de l'accord des gouvernements, citoyens à mettre en œuvre la technologie d'Internet des objets dans tous les aspects. Par l'IoT, les villes peuvent être améliorées à plusieurs niveaux, en améliorant les infrastructures, en améliorant les transports.

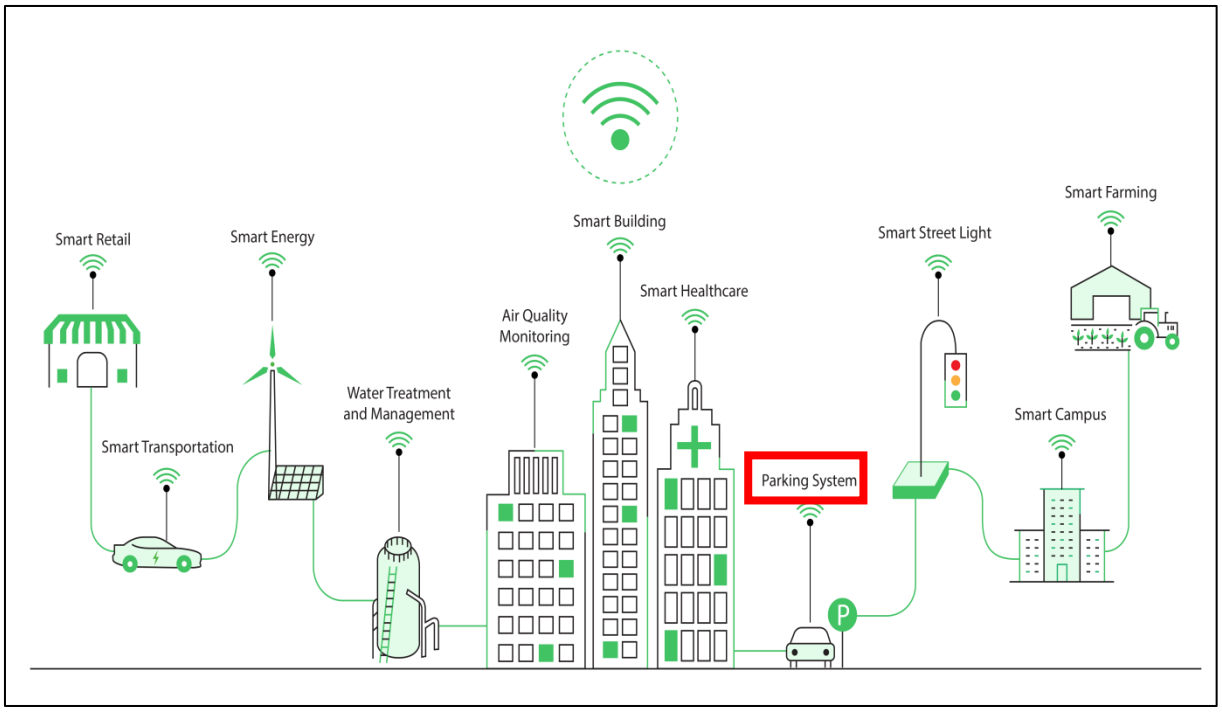

Figure 1.4: Les Villes Intelligentes IoT Solutions.[09]

4.2. Le smart grid

L'un des domaines d'application de l'IoT est le secteur de la distribution d'énergie intelligente, dit « Smart Grid » (voir figure 1.5). En France, ERDF est très actif dans le développement de ce domaine, où un besoin clair en récupération d'information à différents points du réseau électrique est devenue nécessaire pour une 15 meilleure intégration des différentes sources d'énergies et une meilleure gestion de la distribution jusqu'aux utilisateurs finaux [06].

Figure 1.5: Smart Grid

4.3. L'internet des objets dans le domaine de L'automobile

Le marché des transports à déjà anticipé l'arrivée des objets connectés. Parmi les enjeux les plus fréquents que ce domaine fait naitre on retrouve la réduction des accidents et des embouteillages, le partage entres voitures, le développement des offres de VTC et de TAX ou encore la gestion de flotte d'automobile.

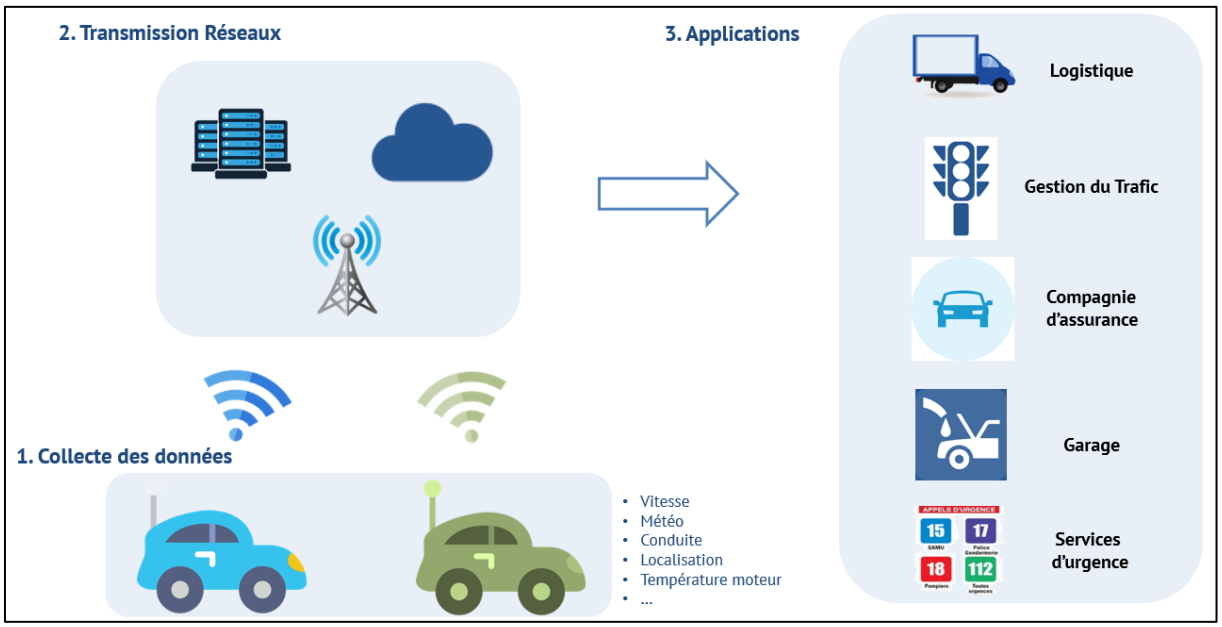

Figure 1.6: iot dans le domaine de L'automobile

4.4. Le système de santé electronique

L'internet des objets a rapidement transformé la prestation de soins. Les équipements et les capteurs sont de plus en plus « intelligents » et génèrent toujours plus de données nécessaires aux équipements médicaux, aux professionnels et profitant ainsi aux patients, en réduisant les coûts et en améliorant leur satisfaction. Les données ainsi collectées facilitent, adaptent, améliorent, anticipent ou réorganisent les soins des patients. Dans le contexte de généralisation du traitement médical électronique, l'Internet des objets est fondamental. En effet, la conception d'un système intelligent de prise de décision clinique, matérialisé par le stockage des données collectées sur les patients et leur accessibilité universelle, procurerait au médecin un excellent appui durant la phase de traitement (voir figure 1.7). L'internet des objets trouve donc tout son intérêt dans le domaine médical, et qui aussi peut améliorer le développement dans ce dernier.

4.5. L’internet des objets dans le domaine de l’industrie

Le déploiement de L’IoT dans l’industrie sera certainement un grand support pour le développement de l’économie et le secteur des services, puisque L’IDO permettra d’assurer un suivi total des produits, de la chaine de production, jusqu'à la chaine de distribution en supervisant les conditions d’approvisionnements. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transnationaux.

5. Avantages et inconvénients

5.1. Avantage

Les objets connectés offrent, sans conteste, de nombreux avantages aux utilisateurs. Notamment, dans certains domaines comme la santé, les objets connectés vont faire des économies aux patients, en ce que ces derniers évitent certains déplacements vers les établissements de santé, en se servant des objets connectés pour transmettre des éléments permettant de diagnostiquer leurs états.

Dans le domaine de la domotique, les objets connectés améliorent considérablement la sécurisation et le contrôle des habitats, tout on restant sur son canapé la personne peut faire plein d’action (Controller la température de sa chaudière et sa climatisation , préparer un café à partir du salon ,allumer ou éteindre les lampes non utilisées, du coup implique un gain d’énergie) et en multipliant les détecteurs d’anomalie dans un domaine, et en automatisant l’envoi d’alerte vers les autorités, en cas d’intrusion.

Dans le domaine du stationnement dans les villes intelligentes offre d’énormes opportunités pour améliorer l’expérience des conducteurs et gérer les installations plus efficacement. La technologie Internet des objets (IoT) peut être utilisée pour fournir des solutions avancées aux problèmes de stationnement, telles que la recherche de places disponibles et une meilleure gestion de la capacité.

5.2. Inconvénient

L’IoT gère nos données personnelles, en effet, les objets connectés produisent de grandes quantités d’information et le traitement de cette masse de données implique de nouvelle préoccupation notamment autour de la confidentialité et de la sécurité.

Bien que les capteurs IoT accomplissent des tâches simples, ils servent principalement à compter ou à mesurer des métriques, leur implémentation se révèle compliquée. En effet, un capteur n'est qu'un maillon d'une chaîne complexe mêlant micrologiciels, plateformes matérielles, équipements réseau, espaces de stockage et de calcul, middleware d'intégration, gestionnaire de terminaux, outil analytique et autres capacités de machine learning.

Dès lors, le déploiement de dispositifs IoT peut impliquer une courbe d'apprentissage importante. Il est judicieux de développer une stratégie sur la façon et les raisons de les déployer avant de les acheter. Il s'agit d'anticiper les problèmes qui pourraient survenir lors de leur implémentation dans un système IT/OT existant.

De nombreux appareils dépendent d'une alimentation continue ou d'une connectivité Internet pour fonctionner correctement. Si l'un ou l'autre tombe en panne, il en va de même pour l'appareil et tout ce qui y est connecté. Étant donné l'imbrication des systèmes IoT, tout peut alors s'arrêter.

6. Conclusion

L'IoT comme le permet l'évolution de internet actuel notre mode de vie et les objets intelligent se sont considérablement améliorés Le milieu environnement interagit les uns avec les autres.

Dans ce chapitre, nous avons expliqué les concepts qui composent l'internet des objets L'avenir de plusieurs domaines. Nous avons brièvement mentionné les domaines d'application d'Internet des objets.

Chapitre II

Sécurité des donnée IOT.

Dans ce chapitre, nous parlerons des risques qui menacent les données dans l'IoT et mettrons en évidence l'un des types de protection les plus importants contre ces menaces, à savoir l'IDS, où nous parlerons de son fonctionnement et de ses types.

1. La Sécurité dant l'Internet des objets

L'évolution rapide des objets connectés a fait l'objet de préoccupations du fait du manque déconsidération des enjeux en matière de sécurité et de modifications réglementaires qui pourraient se révéler nécessaire d'effectuer. En effet, selon l'Insider Business Intelligence Survey , une enquête réalisée au dernier trimestre de 2014 montre que 39 % des personnes interrogées pensent que la sécurité est leur principale préoccupation au moment d'adopter l'Internet des objets. Elles redoutent en particulier les cyberattaques, susceptibles de devenir une menace de plus en plus physique et non plus seulement virtuelle face à l'évolution des objets connectés90.[10]

Dans un article de janvier 2014 publié dans Forbes, un chroniqueur en cyber sécurité, Joseph Steinberg a répertorié plusieurs appareils connectés à l'Internet qui peuvent déjà « espionner les gens dans leur propre maison » à savoir, les téléviseurs, les appareils de cuisine, les caméras et les thermostats.[27] Le 21 octobre 2016, ces appareils ont été détournés de leur fonction et piratés afin de voler de nombreuses informations. En effet, les sites les plus fréquentés de la planète on tété piratés et rendus inaccessibles pendant plusieurs heures dont Amazon, eBay, Airbnb, PayPal, Spotify, Twitter ou encore les services de jeux en ligne de PlayStation et Xbox.[28]

Les dispositifs commandés par ordinateur dans les automobiles tels que les freins, le moteur, les serrures, la chaleur et le tableau de bord seraient considérés comme vulnérables face aux hackers qui ont accès à l'ordinateur de bord du véhicule. Dans certains cas, les systèmes informatiques du véhicule sont connectés à l'Internet, leur permettant d'être contrôlés à distance.

Il existe de nombreux autres exemples et événements survenus qui peuvent être étudiés pour comprendre la gravité de l'affaire.

2. Les attaques dans l'Internet des objets :

Les attaques les plus critiques sont décrites ci-dessous. Elles interviennent lors des transferts de données et plus particulièrement au niveau de la couche réseau [11,12] :

- Déni de service (DoS) :

Cette menace consiste essentiellement en une forme d'attaque par déni de service (DoS). Plutôt qu'écouter les communications, l'intrus peut essayer de les perturber en envoyant des données qui peuvent être valides ou en tentant de bloquer le canal de transmission.

- Hello flood :

Congestion du canal de transmission avec un nombre infini de messages inutiles créant un trafic important. Il s'agit d'une attaque équivalente au déni de service.

- Spoofing (usurpation d'identité ou d'adresse IP) :

Renvoi ou modification erronés du trafic dans l'objectif de dérober des données, de diffuser un logiciel malveillant ou de passer à travers les contrôles d'accès.L'intrus peut compromettre une partie du signal radio avec un module externe qui va exécuter du code malveillant.

- Selective forwarding :

Un nœud compromis envoie les données à certains autres nœuds du réseau (sélectionnés par l'attaquant) au lieu de les envoyer à tous comme prévu. En conséquence, certains modules ne transmettent pas correctement ou pas du tout les paquets de données.

- Sybil :

L'intrus réplique un simple nœud du réseau et le configure avec de multiples identités par rapport aux autres nœuds du réseau. Cette opération s'effectue en introduisant un autre nœud ou un morceau de programme qui est transmis dans le réseau.

- Wormhole (trou noir) :

Cette attaque provoque dans le réseau une modification de position dans les paquets de données, ce qui entraîne un retard dans la transmission.

- Acknowledgement flooding :

Les réceptions d'acquittement synchronisées sont requises dans les réseaux de capteurs quand les algorithmes de routage sont utilisés. Dans ce type d'attaque, un nœud malveillant envoie de façon erronée des acquittements et de fausses informations aux nœuds adjacents ou définis comme destinataires.

- Man-in-the-middle (homme du milieu) :

Il s'agit d'un type d'interception et d'altération de données. L'intrus agit entre deux modules du réseau en captant la communication de façon à récupérer et à altérer l'information en cours de transfert. La troisième partie agit comme un relais de transmission. Naturellement, les deux parties autorisées et concernées ne sont pas informées de la présence de l'intercepteur. Pour éviter cette menace, les périphériques pairs de transmissions actif-passif. Cela signifie, en mode continu, qu'un en service doivent constituer un module émet de l'information et l'autre la reçoit.

- Attaque par relais :

Dans ce cas, l'attaquant fraude le périphérique de réception local et redirige la communication vers un périphérique à distance et sans contact. De façon simple, c'est une attaque 31 man-in-the-middle appliquée aux périphériques NFC. Ce type d'attaque devient un problème de plus en plus critique suite à l'introduction des cartes à puce sans contact.

- Protocol Stack Fuzzing (collecte dans la pile de protocoles) :

Une autre catégorie d'attaque concernant la technologie NFC est basée sur les techniques de pêche ou fuzzing dans la pile de protocoles. Un intrus peut, lors d'un transfert, capter et analyser le logiciel de transmission. Il peut alors forcer un appareil mobile à collecter et à analyser des images, des contacts, des documents ou n'importe quel autre contenu à l'insu de l'utilisateur. Il utilise une technologie de récupération d'informations ou de capture de données (antenne, matériel)..

- Rogue Access Points (points d'accès illicites) :

Il s'agit des matériels réseaux connectés illégalement au réseau. Ils peuvent servir de relais lors de la transmission de données.

3. Les solutions

3.1. Le Chiffrement homomorphique

En cryptographie, un algorithme de **chiffrement homomorphe** est un système possédant des caractéristiques algébriques qui lui permettent de commuter avec certaines opérations mathématiques, c'est-à-dire qu'il permet d'effectuer lesdites opérations sur des données chiffrées sans avoir à les déchiffrer d'abord.

Le déchiffrement du résultat desdites opérations sur des données chiffrées donnera ainsi le même résultat qu'en ayant effectué ces opérations sur les données non chiffrées ; cette propriété permet de confier des calculs à un agent externe, sans que les données ni les résultats soient accessibles à cet agent. [13]

3.2. La Blockchain

La Blockchain une technologie numérique de stockage et de transmission d'informations sans autorité centrale. Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en « blocs », formant ainsi une chaîne. L'ensemble est sécurisé par cryptographie. [14]

3.3. Preuve à divulgation nulle de connaissance

Est un protocole cryptographique permettant l'authentification sécurisée d'informations. Dans le cadre de ce protocole, une entité, nommée « fournisseur de preuve », prouve mathématiquement à une autre entité, le « vérificateur », qu'une proposition est vraie sans révéler d'autres informations que la véracité de la proposition. [15]

3.4. Les systèmes de détection d'intrusion

On appelle système de détection d'intrusion, en anglais **I**ntrusion **D**etection **S**ystem ou (IDS), toutsystème combinant logiciel et matériel, qui permet d'écouter le trafic du réseau de manière furtive et en temps réel afin de repérer les tentatives d'intrusion sur un réseau interne ou sur un ordinateur hôte pour permettre une prévention contre les intrusions qui visent à compromettre la ***confidentialité*** (Pour chaque information, on définit l'ensemble

d'utilisateurs autorisés à y accéder), l'***intégrité*** des données (Les données n'ont pas été modifiées) et la ***disponibilité*** (les services du système doivent êtreopérationnels et accessibles) [16].

Certains termes sont souvent employés quand on parle d'IDS :

-Faux positif : une alerte provenant d'un IDS, mais qui ne correspond pas à une attaque réelle (Fausse alerte).

-Faux négatif : une intrusion réelle qui n'a pas été détectée par l'IDS.

-Vrai négatif et Vrai positif : correspondent aux comportements souhaités.

3.4.1. Principe de détection d'intrusion

Deux méthodes sont principalement utilisées par les systèmes de détection d'intrusion lareconnaissance de signatures et la détection d'anomalies [17].

3.4.2. Le modèle architecture de base d'un système de détection d'intrusion

Le groupe IDWG (**I**ntrusion **D**etection exchange format **W**orking **G**roup) de l'IETF (**I**nternet **E**ngineering **T**ask **F**orce) [4] a proposé une architecture de base d'un système de détection d'intrusion.Cette architecture définit un format d'échange de message pour les IDS : *Intrusion Detection Message Exchange Format (IDMEF)*, qui contient implicitement un modèle de données.

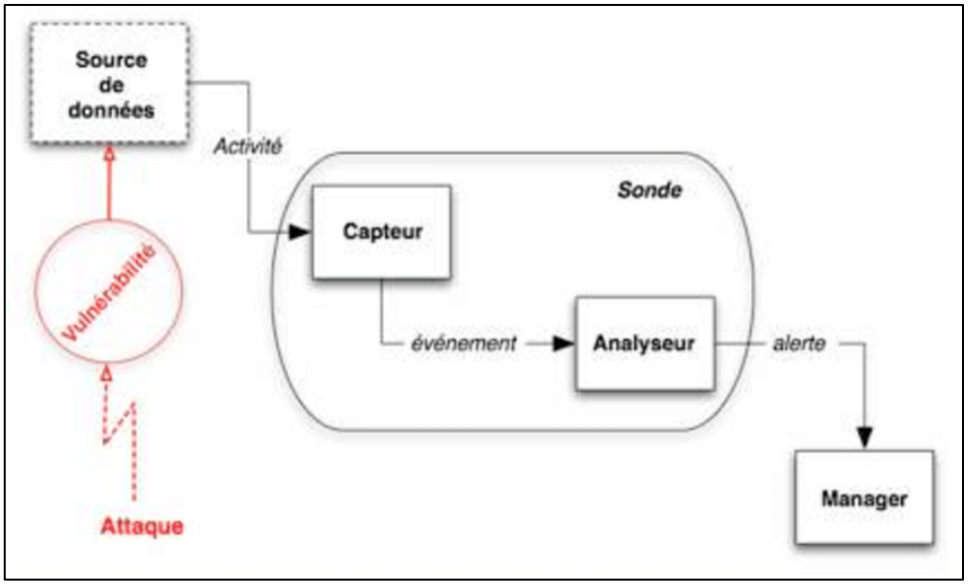

Figure 2.1 : Architecture de base d'un IDS [26] .

Cette architecture est composée des modules suivants :

Source de données : Appelée aussi sonde de capture, c'est l'interface entre le système surveillé et l'IDS, c'est la collecte d'informations sur les activités non autorisées du système. Sa position joue unrôle stratégique dans la détection des intrusions

Capteur : charge de collecter et filtrer les informations brutes envoyées par la source de données. Lerésultat de ce traitement sera un message formaté, appelé évènement, après il fait le transfert des évènements à l'analyseur

Analyseur : il est responsable de l'analyser des évènements générés par le capteur. Et en cas de détection d'une activité indésirable il le signale à l'administrateur de sécurité. Dans cette architecture,*le capteur* et *l'analyseur* forment ensemble *une sonde*.

Manager : en plus de la notification des alertes, il offre à l'administrateur la possibilité de configurerune sonde et de gérer des rapports.

3.4.3 Classification du système de détection d'intrusion

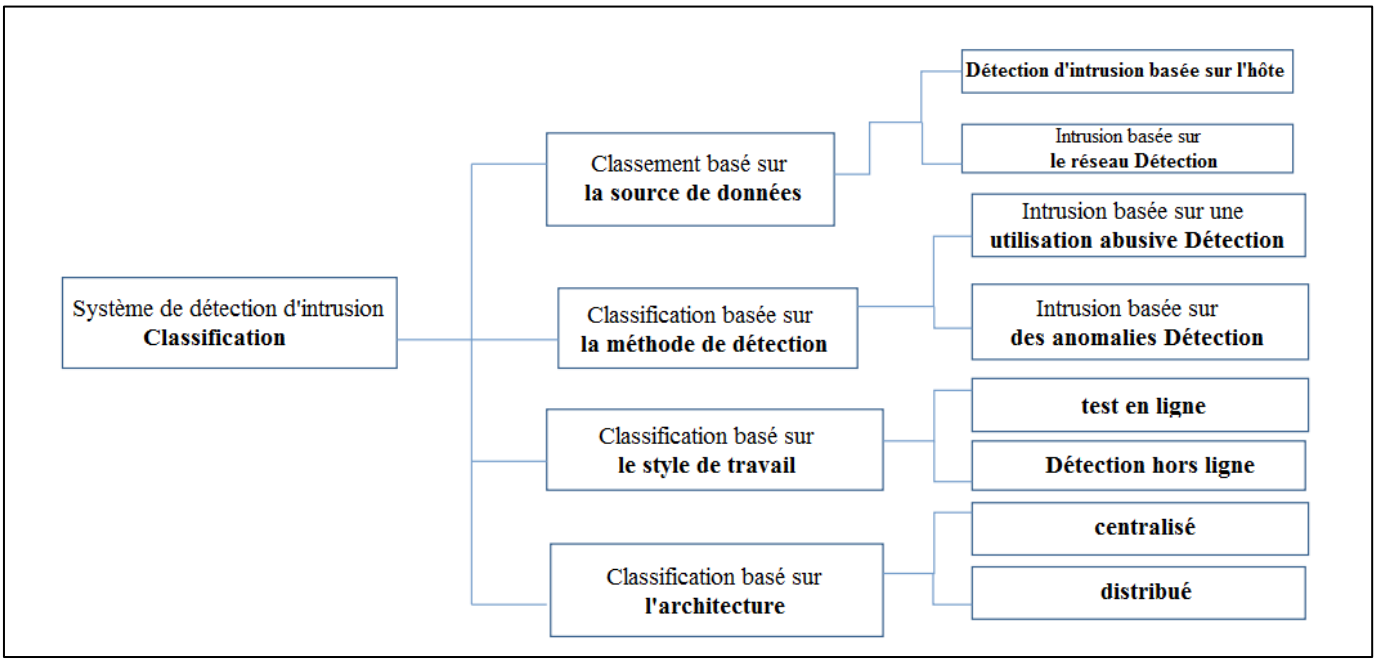

Figure 2.2 : Cadre de classification du système de détection d'intrusion.

- Classification basée sur les méthodes de détection

Du point de vue des méthodes de détection, les techniques de détection d'intrusion sont généralement divisées en techniques de détection d'abus et de détection d'anomalies.

- Basé sur la technologie de détection des abus

La technologie de détection des abus [18] est basée sur le principe de correspondance de modèles, collecte les caractéristiques du comportement d'attaque et établit une base de données de signatures pour celui-ci. Lorsque le comportement de l'utilisateur surveillé correspond aux enregistrements de la base de données de signatures, le système considère ce comportement comme une intrusion. La technologie de détection des abus peut réduire le taux de faux positifs. Néanmoins, le taux de faux négatifs augmentera également. Une fois que les caractéristiques de l'attaque changent, la technologie de détection des abus deviendra incompétente. Les techniques de détection d'abus existantes sont généralement divisées en méthodes de détection d'abus basées sur des systèmes experts [19], méthodes de détection d'abus basées sur une analyse de transition d'état [20], méthodes de détection d'abus basées sur la surveillance du clavier [12] et méthodes basées sur des probabilités conditionnelles.

- Basé sur la technologie de détection d'anomalies

Les techniques de détection d'anomalies [18] sont basées sur des principes d'analyse statistique. Premièrement, nous déterminons les caractéristiques du comportement normal et le décrivons à l'aide de méthodes quantitatives. Lorsque le comportement de l'utilisateur s'écarte du fonctionnement normal, il est défini comme un comportement agressif. L'efficacité des techniques de détection des anomalies dépend en grande partie de l'exhaustivité des caractéristiques typiques de l'utilisateur et de la fréquence de détection. Les attaques inconnues peuvent être détectées efficacement car chaque épisode n'a pas besoin d'être défini. Dans le même temps, le système peut également s'adapter aux changements de comportement des utilisateurs grâce à l'auto-évaluation.

- Classification basée sur la source de données.

Du point de vue des sources de données, les systèmes de détection d'intrusion peuvent généralement être divisés en systèmes de détection d'intrusion basés sur l'hôte (Host Intrusion Detection System, HIDS) et en détection d'intrusion basée sur le réseau (Network Intrusion Detection System, NIDS).

- Détection d'intrusion basée sur l'hôte.

Système hôte ou serveur les attaques sont la principale chose que HIDS [22, 23] recherche et répond à. Les personnes qui travaillent avec HIDS utilisent deux techniques,

nommément techniques de détection d'anomalies et techniques de détection des abus. En utilisant la technologie de détection des abus et la technologie de détection des anomalies, l'auteur [14] a trouvé un moyen de garder un œil sur les données que l'hôte recueille. Ce système utilisait l'analyse du fichier journal et le système neuronal BP. technologie de réseau pour garder un œil sur les données de l'hôte recueille. Par conséquent, cela peut contribuer à améliorer le taux de détection et l'exactitude de la recherche. L'auteur a proposé un système de détection d'intrusion de botnet basé sur l'hôte qui utilise une algorithme de technologie de détection d'anomalies pour examiner et traiter chaque paquet de données reçu pour voir s'il y a une tromperie causée par une attaque extérieure pour protéger le système.

- Détection d'intrusion basée sur le réseau.

Lorsque la carte réseau est en mode promiscuité, NIDS [24, 25] peut surveiller le service de communication sur l'ensemble du segment du réseau en temps réel. Peu importe que vous utilisiez la détection d'intrusion basée sur l'hôte ou la détection d'intrusion basée sur le réseau. Ils ont tous des problèmes, alors ils continuent de s'améliorer. Ils ont trouvé un meilleur moyen de détecter les intrusions sur le réseau. Tout d'abord, ils placent un nœud de serveur dans une partie spécifique du réseau, puis ils installent le système de détection d'intrusion sur le serveur avant que chaque paquet de données n'atteigne l'hôte de destination. L'hôte de destination ne peut pas recevoir de paquets de données provenant de l'extérieur du réseau. Même si certains paquets de données lui sont envoyés directement, ils doivent être envoyés au serveur pour être vérifiés avant de pouvoir continuer. Si le serveur constate que le paquet de données constitue une invasion, jetez-le immédiatement. Le système permet non seulement d'économiser de l'argent, mais il présente également de très bons taux de détection.

- Classification basée sur l'architecture.

Du point de vue architectural, les systèmes de détection d'intrusion peuvent être divisés en centralisés et distribués. Le moteur d'analyse centralisé des systèmes de détection d'intrusion et le centre de contrôle forment un seul système et ne peuvent pas fonctionner à distance. Cette architecture est simple, ne perdra pas la confidentialité en raison de la communication et n'affectera pas la bande passante du réseau. Cependant, cette méthode est peu évolutive et configurable. D'autre part, le moteur d'analyse et le système distribué de détection d'intrusion sont deux systèmes pouvant être exploités à distance via le réseau. À l'heure actuelle, la plupart des systèmes de détection d'intrusion sont distribués. Cette

architecture est hautement évolutive et sécurisée, mais elle est également coûteuse à entretenir.

- Classification basée sur le style de travail.

Le système de détection d'intrusion peut être divisé en détection en ligne et détection hors ligne à partir du mode de travail. La détection en ligne peut surveiller la génération de données et les analyser en temps réel. Bien que cette méthode puisse protéger le système en temps réel, il n'est pas facile de garantir des performances en temps réel lorsque le système est à grande échelle. D'autre part, la détection ofine analyse le comportement de l'intrusion après qu'elle se soit produite. Cette méthode peut gérer de nombreux événements mais ne peut pas fournir rapidement des mesures de protection au système.

4. Conclusion

Dans ce chapitre, nous avons présenté les différents types d'IDS selon différents critères de classification avec la présentation générale des différentes techniques utilisées pour la détection d'intrusions. Afin d'obtenir un système de détection d'intrusions compétent et efficace

Chapitre III

Modèle de la transmission sécurisée des données sur l'IoT.

Dans le domaine de l'Internet des Objets (IoT), l'évolution rapide de la technologie a conduit à l'émergence de deux concepts révolutionnaires : la blockchain et le cloud computing.

Ces innovations jouent un rôle crucial dans la transformation numérique en permettant une gestion sécurisée et efficace des données à une échelle sans précédent. Alors que la blockchain promet une sécurité renforcée et une traçabilité inégalée des informations, le cloud offre une infrastructure flexible et évolutive pour le traitement et le stockage des données IoT. Cette synergie entre la blockchain et le cloud ouvre de nouvelles perspectives passionnantes pour le déploiement et la gestion des systèmes IoT à l'ère numérique moderne.

1. La Blockchain

La notion de Blockchain a été apparue en 2008 lors de la création du bitcoin, par un inconnu dont le pseudonyme est Satoshi Nakamoto. La technologie Blockchain est une base de données cryptée et décentralisée, et sa force réside dans le fait qu'elle est décentralisée. Elle permet à toute personne impliquée dans une transaction de savoir avec certitude ce qui s'est passé, quand cela s'est produit, et de confirmer que les autres parties voient la même chose sans avoir besoin d'un intermédiaire fournissant une assurance, et sans avoir besoin de réconcilier les données par la suite (Voir ***Figure 3.1***).

Ce pendant, les Blockchains sont des règles sans précédent, car les fichiers de contenu sont divisés, cryptés et stockés différemment sur des milliers de nœuds à travers le monde qui communiquent entreeux pour produire une chaîne entière. Ce qui rend la fraude ou le piratage extrêmement difficile, car les changements de transaction et les enregistrements de propriété doivent être approuvés par la majorité de toutes les pièces (blocs) pour devenir valides. C'est la raison pour laquelle le traitement des transactions héritées prend un certain temps à mettre en œuvre, car toute modification doit être acceptée dans le « registre » qui est distribué publiquement et vérifié partout, et il n'y a pas d'autorité unique ou de serveur central pour la manipulation [29].

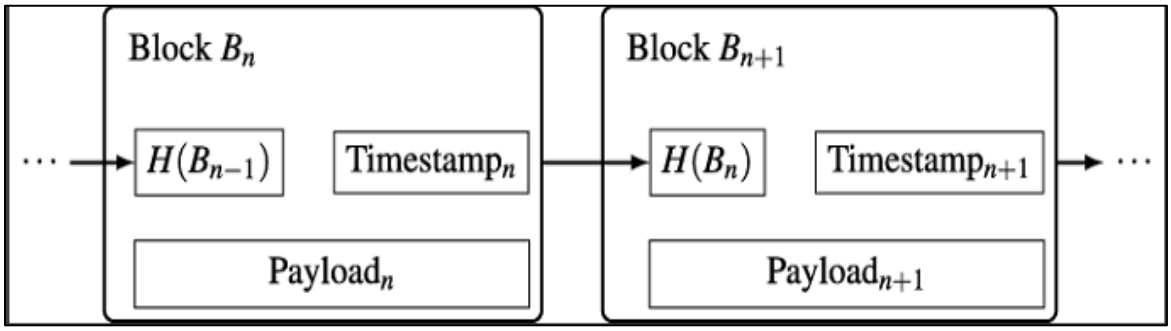

Figure 3.1 Schéma de la Blockchain [29]

- Transaction :

Les transactions sont les choses qui donnent un but à la Blockchain. Ils sont les plus petits blocs de construction d'un système de Blockchain. Les transactions consistent généralement en une addresse de destinataire, une adresse d'expéditeur et une valeur. Les transactions contiennent une ou plusieurs entrées et une ou plusieurs sorties. Une entrée est une référence à une sortie d'une transaction précédente.

- Blocs :

Les blocs sont des structures de données ayant pour but de regrouper des ensembles de transactions et d'être distribués à tous les nœuds du réseau. Chaque bloc contient un en-tête, qui est la métadonnée permettant de vérifier sa validité, tandis que le reste contient des transactions que le mineur a choisi d'inclure dans le bloc qu'il a créé. Le nombre maximum de transactions qu'un bloc peut contenir dépend de la taille du bloc et de la taille de chaque transaction.

- Consensus :

Les mécanismes consensuels sont des protocoles garantissant que tous les nœuds (le périphérique de la chaîne qui gère la chaîne et (parfois) traite les transactions) sont synchronisés les uns avec les autres et conviennent des transactions légitimes à ajouter à la chaîne. Ces mécanismes de consensus sont cruciaux pour une Blockchain afin de fonctionner correctement.

Ils s'assurent que tout le monde utilise la même Blockchain. Tout le monde peut soumettre des éléments à ajouter à la Blockchain. Il est donc nécessaire que toutes les transactions soient constamment vérifiées et que la Blockchain soit constamment auditée par tous les noeuds. Sans un bon mécanisme de consensus, les Blockchains sont exposées à

diverses attaques.

- Smart Contract :

Un « contrat intelligent » est un programme informatique autonome dont le code contrôle et conditionne, sous certaines conditions, le transfert de devises ou d'actifs entre différentes parties.

1.1. Les défis de la blockchain et IoT

L'IoT et la blockchain sont confrontés à de nombreux défis. Certains de ces problèmes sont :

- Transcodage :

Le streaming vidéo activé par la blockchain fait face à un certain nombre de défis. Parmi eux, le transcodage vidéo est une préoccupation majeure. La vidéo originale des contenus sur les plateformes blockchain doivent être transcodés, c'est-à-dire converti en plusieurs représentations dans différents débits, qualités, vidéo codec et résolution, pour les appareils et utilisateurs hétérogènes [30] . Le transcodage vidéo est un processus gourmand en ressources et en temps de calcul. Un autre problème est que les flux binaires du contenu vidéo sont considérablement plus élevés et sont difficiles à incorporer dans des blocs sur une chaîne donnée . Ainsi, il existe de nombreuses possibilités de recherche pour protéger les données vidéo sur les chaînes.

- Sécurité :

Alors que les chercheurs s'efforcent d'améliorer la sécurité offerte par la blockchain, il existe de nombreuses vulnérabilités dans les contrats intelligents et ils sont exposés à des attaques de sécurité et de confidentialité [31]. Par exemple : selfish mining, attaque DNS, mempool attaque, attaque double spending et délai de consensus. Dans l'exploitation selfish mining, les mineurs essaient d'augmenter leur récompense en gardant les blocs privés. Dans Attaque DNS, un attaquant diffuse des informations erronées avec ses pairs alors que, dans une attaque mempool, les nouveaux blocs sont inondés des transactions. Ces blocs sont également soumis à une attaque de double spending dans laquelle deux transactions sont créées à partir des mêmes transactions. De plus, des études récentes ont montré que les blockchain sont soumises à un délai de consensus dans lequel les pairs sont empêchés de lire un consensus. En plus de ces attaques, il y a un certain nombre d'autres attaques face à la blockchain, par exemple DDoS et vol de portefeuilles (theft of wallets). En conséquence, la

sécurité est une préoccupation majeure dans la blockchain qui doit être explorée plus avant.

- Opération de lecture /écriture :

Sécuriser les liens entre l'infrastructure blockchain et le Les applications IoT lisant et écrivant depuis/vers la blockchain sont cruciales. Protéger une solution basée sur la blockchain ne se limite pas seulement à l'architecture de la blockchain, mais toute la chaîne des requêtes/réponses doit être protégée. La protection de l'ensemble de la chaîne permettra d'éviter l'attaque l'homme de milieu (mainin the middle attack).

- Évolutivité :

La plupart des plates-formes blockchain existantes ne sont pas réalisables pour la grande quantité de données produites par les objets intelligents (IoT). Cet énorme volume de données augmentera considérablement car le nombre d'objets connectés à Internet atteindront 41,6 milliards d'ici 2025. L'état actuel des plateformes blockchain existantes ne leur permet pas de gérer la quantité de données produites par les appareils IoT, sans ralentissement [32]. En cas d'évolutivité, il existe de nombreux d'autres défis. Ceux-ci inclus :

- a majorité des architectures « blockchain en tant que service » sont basé cloud.
- La bande passante disponible est limitée pour prendre en charge le processus des transactions enTemps réel.
- Les techniques traditionnelles de stockage des données des capteurs intelligents embarqués sont fragiles lorsqu'ils traitent et utilisent le DLT, la principale force motrice derrière la blockchain.
- Le gaspillage d'énergie reste un obstacle majeur avec des coûts environnementaux

- Interopérabilité :

Tous les appareils IoT sont connectés par Internet, mais les choses deviennent plus compliquées quand on ajoute blockchain. Diverses plateformes de blockchain sont isolés les uns des autres, et si le défi de l'interopérabilité n'est pas abordé, on se retrouvera avec des objets intelligents connectés à plusieurs réseaux décentralisés isolés . Ça fonctionnait bien à des fins particulières, mais cela ne deviendraitpas Internet de Everything, où tous les appareils sont interconnectés et peuvent interagir l'un avec l'autre. La convergence de la blockchain et de l'IoT fait face à un nombre de problèmes d'interopérabilité [33].

- Régulation :

La conception des réglementations et de la conformité dans l'exécution des transactions n'est pas une tache simple. Les déploiements de la blockchain au niveau des entreprises seront confrontés à de nombreuses questions politiques et juridiques [34]. Parmi eux, la principale question est l'absence d'une réglementation et d'une politique monétaire claires associés aux crypto monnaies. Bien que certains pays se penchant vers le marché de la blockchain, l'IoT a des incertitudes juridiques sur la propriété des données, l'accès, la confidentialité et bien au-delà. Le DLT ne remplace pas le gouvernement, mais il introduit simplement de nouvelles façons de coder les règles et les processus de consensus.

1.2. Avantages blockchain avec IoT

Dans cette section, nous discutons des avantages de l'intégration blockchain avec IoT. Ces avantages comprennent :

- La cyber-sécurité :

L'intégration de la blockchain avec l'IoT offre des avantages contre les cyber attaques [35] . La blockchain traite les messages échangés entre les objets intelligents en tant que transactions. Ces transactions sont validées par des contrats intelligents. Les transactions sont enregistrées en blocs et sont disposés dans le bon ordre et horodaté, lorsqu'ils sont ajoutés. Les plateformes blockchain utilisent des algorithmes cryptographiques qui sécurisent davantage les données et empêche que les enregistrements précédents ne soient modifiés. La conception architecturale d'une plateforme blockchain fournit une sécurité de haut niveau. Si certains objets sont piratés, cela n'affectera pas l'intégralité de système et ses performances. De plus, l'utilisation de l'apprentissage automatique permet l'automatisation de la détection des menaces en temps réel [36].

- Les contrats intelligents :

Blockchain est conçu pour servir de couche de base pour les applications IoT qui impliquent des transactions et des interactions, et les contrats intelligents jouent un rôle important dans celui-ci [37]. Ces contrats sont exécutés automatiquement sans exiger d'intermédiaires pour approuver ou authentifier une transaction lorsque des conditions spécifiques sont remplies. Ces contrats apportent un fonctionnement sécurisé et autonome,

des transferts moins chers et plus rapides, et une diminution de la vulnérabilité de la sécurité des données pour les objets intelligents. Les contrats intelligents rendent les processus de facturation faciles et confortables. Ainsi, les systèmes de paiement spécifiques ne sont plus nécessaires. Une transaction est exécutée, les jetons sont transférés, et ces processus sont clairs et transparents sur la blockchain. Les contrats intelligents gagnent en popularité dans diverses applications. Comme le commerce intelligent, la santé, la ville intelligente, etc[38, 39,40].

- Décentralisation :

Contrairement à l'architecture centralisée traditionnelle, l'utilisation de blockchain améliorent la tolérance aux pannes. [41] une seule blockchain s'exécute sur des milliers d'objets intelligents connectés. Un point de défaillance unique ne désactive pas l'ensemble du réseau. De plus, dans un système décentralisé, les données stockées et traitées ne sont pas contrôlées par un seul appareil.

- La Confiance :

La blockchain permet un facteur de confiance entre les transactions [42]. Les utilisateurs ne sont plus obligés de faire confiance aux entités centralisées pour gérer leurs données. La blockchain permet des règlements plus rapides pour les contrats sans le besoin d'intermédiaires de confiance.

- Réduction des couts :

La blockchain réduit considérablement les coûts de connectivité entre les dispositifs en éliminant la nécessité de l'infrastructure [41]. Par conséquent, pas d'administration, pas de maintenance et de configuration et les frais sont réduits.

- Transparence :

Blockchain est un registre distribué et chaque appareil de l'IoT peut partager une copie de la transaction [43]. En conséquence, chaque appareil peut accéder à la documentation d'une transaction et des modifications qui y sont apportées.

- Cohérence :

IoT et blockchain ont transformé la manière dont les données sont échangées et

conservées [41] . Ces deux technologies assurent une cohérence dans le traitement des données. Blockchain fournit des méthodes sécurisées pour transférer des informations entre les objets intelligents et leurs participants.

1.3. Les types de Blockchain

Les systèmes de Blockchain actuels peuvent être grossièrement classés en troistypes:

- Les Blockchains publiques :

Sont des grands réseaux distribués accessibles, ouvert à tous et à tous les niveaux, et ont un code source ouvert que leur communauté maintien à jour comme Bitcoin.

- Les Blockchains consortium :

Sont des réseaux distribués qui contrôlent les rôles de chaque nœud dans les réseaux tels que Ripple , le code source peut-être ouvert ou non.

- Les Blockchains privées :

Sont plus petites que les autres types, leur accès est complétement contrôlé. Les trois types utilisent la cryptographie pour permettre à chaque nœud de participer à la gestion du grand registre de manière sécurisée sans autorité centrale [44].

1.4. Utilisations de Blockchain

Ces dernières années, la Blockchain a commencé à être reconnue par un public plus large, ce qui a entraîné une augmentation significative du nombre de services proposés et d'applications logicielles, qui seraient basés sur la Blockchain.

- La Blockchain dans la gestion d'actifs:

Il s'agit de transférer en toute sécurité des actifs au sein d'un réseau professionnel. Un actif peut être physique, par exemple un serveur, un ordinateur, ou un actif immatériel tel qu'un logiciel ou un service. La Blockchain offre une fonctionnalité de grand livre partagé, ce qui signifie unevisibilité complète d'un bout à l'autre du réseau de l'entreprise. Elle se concentre uniquement sur cinq événements clés, à savoir la fabrication en série d'actifs pour initier la Blockchain, la réception et la validation d'actifs, la capitalisation d'actifs, l'activation de la garantie et l'installation de l'actif [45].

- La Blockchain dans le Finance:

Les paiements transfrontaliers constituent un processus très important, qui devient assez coûteux et fastidieux en raison de la présence d'intermédiaires inutiles .Il faut plusieurs banques avant que l'argent puis se être collecté .Des services tels que Western Union peuvent être utilisés, ce qui est plus rapide mais aussi coûteux. La Blockchain peut accélérer et simplifier ce processus en éliminant les intermédiaires inutiles. Dans le même temps, cela rend les envois de fonds plus abordables. Jusqu'à présent, les coûts d'envoi de fonds étaient de 5 à 20%. La Blockchain réduit les coûts à 2-3% du montant total et permet des transactions transfrontalières garanties en temps réel [45].

- La Blockchain dans l'IOT:

Les solutions IOT (Internet of things) utilisant les Blockchain peuvent être construites pour maintenir une liste d'enregistrement de données croissante sans cesse et sécurisée par la cryptographie, protégée contre toute modification ou altération. Par exemple, lorsqu'un actif connecté à l'IOT (RFID, par exemple) avec des informations de localisation et de température sensible se déplace le long de divers points d'un entrepôt ou d'une maison intelligente, ces informations pourraient être mises à jour sur une Blockchain. Cela permet à toutes les parties concernées de partager des données et le statut du paquet lors de son déplacement entre différents rassemblements afin de garantir le respect des termes d'un accord [45].

- La Blockchain dans la santé:

Les antécédents médicaux du patient sont stockés dans un système décentralisé, accessible aux médecins traitants et aux prestataires d'assurance médicale [45].

2. Le Cloud

Le Cloud est un immense réseau interconnecté de serveurs puissants qui fournit des services aux entreprises et aux particuliers. L'internet des objets (IoT) est un système de dispositifs informatiques, de machines mécaniques et numériques dotés d'identifiants uniques et capables de transférer des données sur le réseau sans nécessiter d'interaction.

L'IoT génère de nombreuses données et les services en Cloud ouvrent la voie à la circulation de ces données. De plus, l'hébergement en Cloud en tant que service ajoute de la

valeur aux entreprises utilisant l'IoT en leur permettant de réaliser des économies d'échelle pour réduire leur structure de coûts globale.

Le Cloud Computing est un mode de fourniture à la demande de puissance de calcul, de stockage de bases de données, d'applications et de ressources informatiques. Il permet aux organisations de consommer une ressource informatique, comme une machine virtuelle (VM), au lieu de construire une infrastructure informatique sur place [46].

2.1. L'intérêt du Cloud

L'utilisation du Cloud est importante pour agréger les données et en tirer des enseignements, Sans le Cloud, il est beaucoup plus difficile de comparer des données sur des zones étendues. L'utilisation du Cloud permet également d'assurer l'évolutivité. Lorsque vous disposez de centaines, de milliers, voire de millions de capteurs, il serait extrêmement coûteux et énergivore d'affecter de grandes quantités de puissance de calcul à chaque capteur. Au lieu de cela, les données de tous ces capteurs peuvent être transmises au Cloud et y être traitées de manière agrégée [47].

3. Modèle de la transmission sécurisée des données sur l'IoT.

Modèle de système pour assurer la transmission sécurisée des données sur l'Internet des objets (IoT) :

Le modèle de système pour l'analyse collaborative des données , est illustré dans les **figures 3.2** et **3.3** et comprend deux phases : le nettoyage des données et la classification des données. Dans la phase de nettoyage des données, le meilleur effet de nettoyage fourni par le cloud privé est obtenu à partir de la blockchain consortium pour le nettoyage des données (CBD). Les paramètres du modèle (chaque cloud privé partage son modèle via la blockchain consortium) sont utilisés pour identifier les données de mauvaise qualité qui ne seront pas transmises à la phase de classification. Dans la phase de classification, les données de haute qualité obtenues après le nettoyage des données sont principalement utilisées pour l'entraînement et la classification. Les paramètres du modèle sont transmis en toute sécurité via la passerelle de l'interface de programmation d'application (API) au cloud public. Le cloud public collecte les paramètres du modèle de chaque cloud privé, obtient le modèle global en utilisant une moyenne pondérée, puis partage le modèle global avec chaque cloud privé. Lorsque le cloud personnel demande des services au cloud public, la passerelle API

utilise la blockchain consortium pour la classification (CBC) pour effectuer l'authentification et le contrôle d'accès sur le cloud privé afin d'empêcher les utilisateurs non autorisés d'accéder au cloud public, comme illustré dans la **figure 3.2** [47]

Les données entre les clouds privés et publics ne peuvent être échangées qu'après une authentification réussie pour garantir la sécurité des données. Par conséquent, cet article conçoit deux schémas de contrôle d'accès, à savoir un schéma de contrôle d'accès basé sur les rôles amélioré (RAC) et un schéma de contrôle d'accès basé sur la blockchain consortium (BAC). Dans le schéma de contrôle d'accès basé sur les rôles (RAC), nous considérons les droits fonctionnels et les droits des données. Le RAC garantit que seuls les utilisateurs légitimes peuvent utiliser les fonctionnalités logicielles autorisées et accéder aux ensembles de données approuvés dans le système IoT de chaque cloud privé, permettant ainsi le nettoyage et la classification des données. Dans le BAC, le cloud public fournit des services sous forme d'API. [47]

Chaque cloud privé échange des données avec le cloud public via une passerelle API. La passerelle API est un cloud privé et un routeur de tunnel entre les clouds publics. De plus, elle est un équilibreur de charge et même un gestionnaire d'autorisation et de contrôle d'accès. Les clients peuvent accéder aux données avec l'autorisation d'une autorité tierce dans les systèmes d'information traditionnels. Dans cette solution, le cloud privé peut être accédé via l'API. [47]

Le BAC dans la passerelle demande des données directement au cloud public tout en vérifiant l'identité et les autorisations du cloud privé. Le RAC et le BAC protègent la sécurité et la confidentialité des données tout en réduisant la complexité de la configuration des autorisations d'accès et de l'authentification des utilisateurs valides. De plus, deux blockchains consortium sont déployées sur le nœud de la passerelle dans les nœuds du cloud privé et les API pour protéger la sécurité et la confidentialité des données. La première est la blockchain consortium (CBD), qui stocke les modèles d'apprentissage profond pendant la phase de nettoyage des données. La deuxième est la blockchain consortium (CBC), qui conserve les journaux, l'identité du cloud privé et les autorisations pendant la phase de classification. [47]

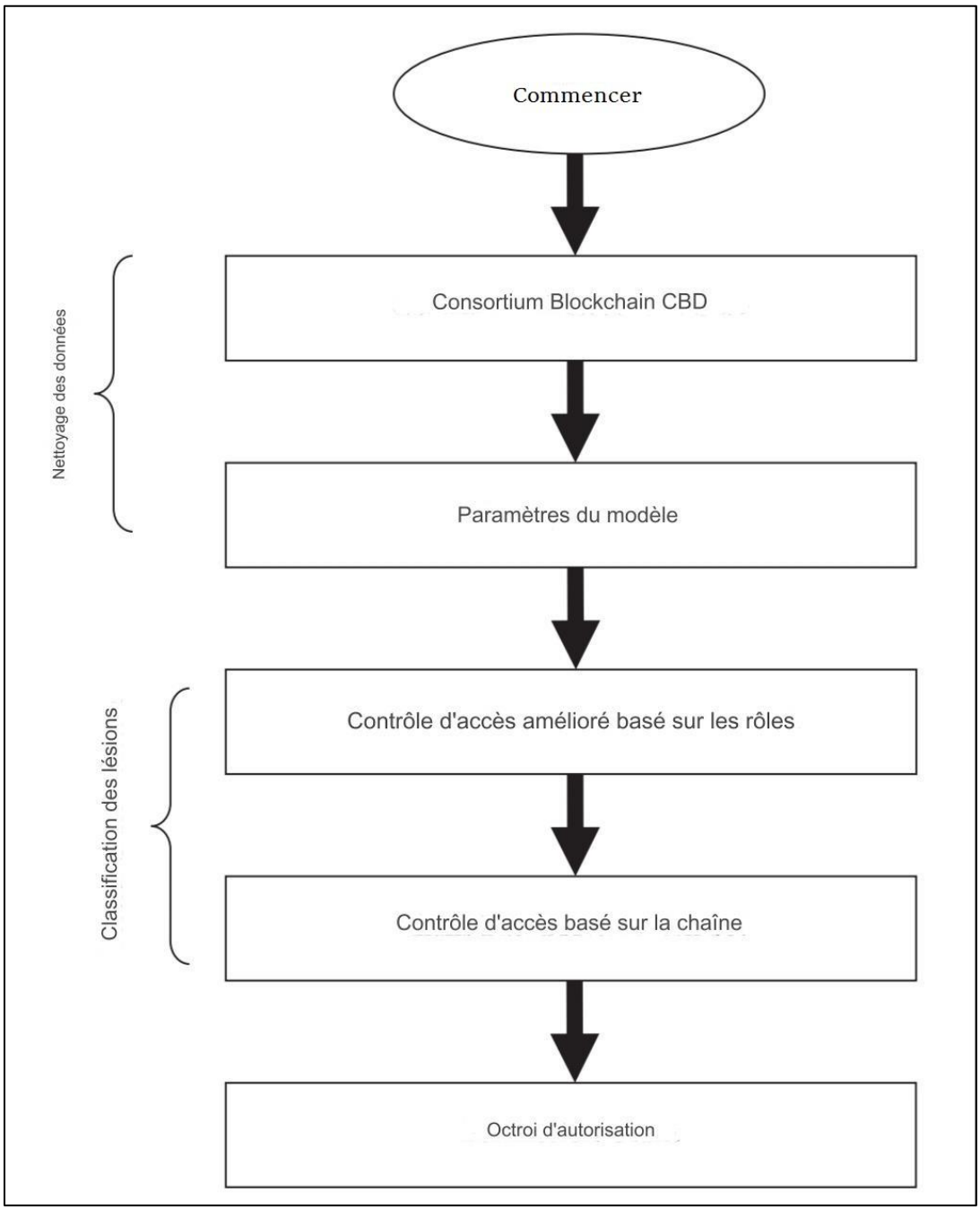

Figure 3.2 : Organigramme proposé [47].

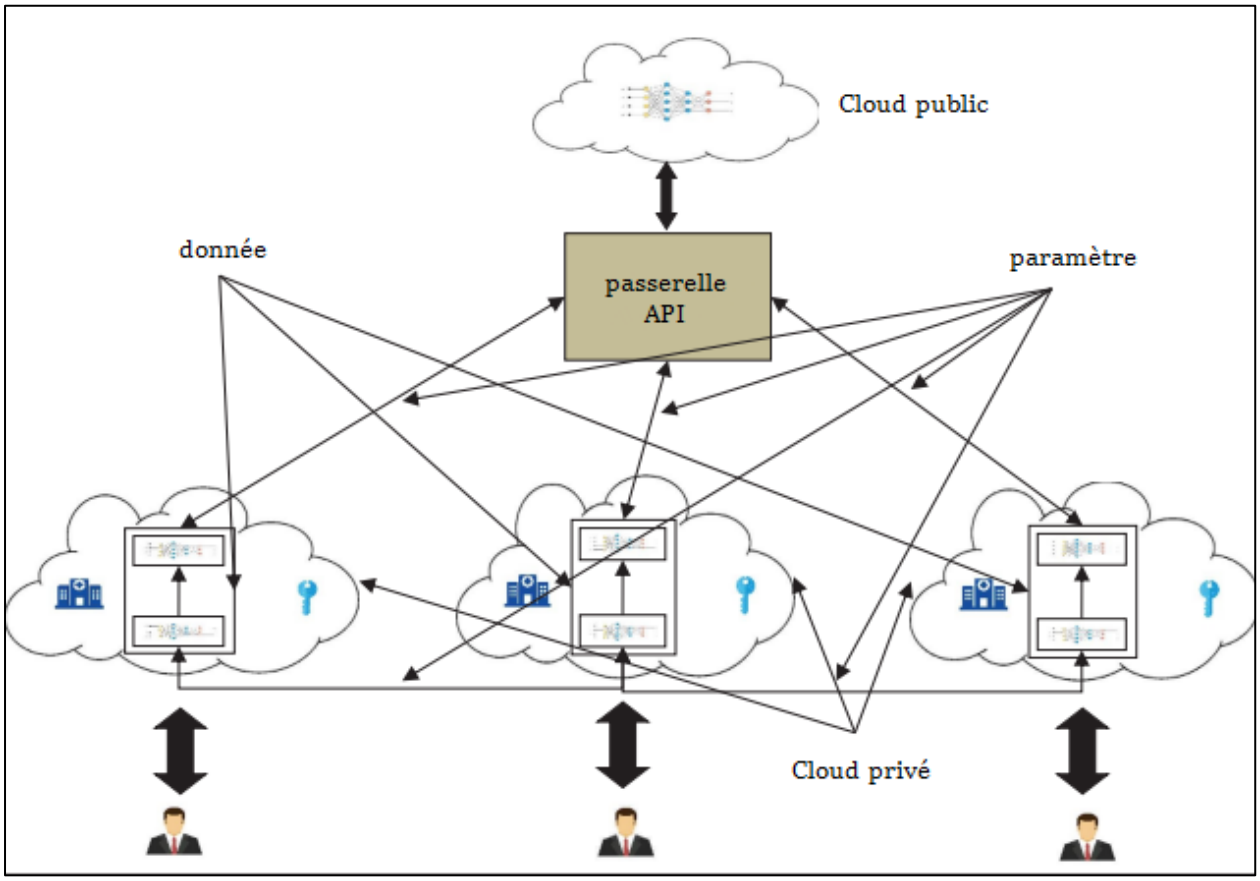

Figure 3.3 : Modèle du système d'analyse collaborative de données sécurisées [47].

4. Conclusion

Dans ce chapitre, nous avons d'abord défini la blockchain et mentionné ses avantages et ses utilisations, en plus des défis. Nous avons également abordé le cloud, et finalement nous avons fait une explication du Modèle de système pour assurer la transmission sécurisée des données sur l'Internet des objets (IoT) .

Chapitre IV

Réalisation

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

1. L'environnement de d´eveloppement

1.1. Langages de programmation

1.1.1. Le langage JAVA

Le langage java a été créé en 1991 par des ingénieurs chez SUN Microsystems qui ont cherché à concevoir un langage applicable à de petits appareils électriques. Pour ce faire, ils ont utilisé une syntaxe très proche de celle du C++, en reprenant le concept de machine virtuelle déjà exploité auparavant par le Pascal UCSD. L'idée consistait à traduire d'abord un programme source, non pas directement en langage machine, mais dans un pseudo langage universel, disposant des fonctionnalités communes à toutes les machines. Ce code intermédiaire, dont on dit qu'il est formé de byte codes, se trouve ainsi compact et portable sur n'importe quelle machine ; il suffit simplement que cette dernière dispose d'un programme approprié (on parle alors de la machine virtuelle) permettant de l'interpréter dans le langage de la machine concernée.

Java est un langage basé sur la programmation orientée objets dont l'objectif est que les logiciels écrits dans ce langage doivent être facilement portables sur plusieurs systèmes d'exploitation tels qu'UNIX, Windows, Mac OS ou GNU/Linux. [48]

1.1.2. Le langage SQL

Pour communiquer avec une base de données, on a besoin de lui envoyer des commandes ou instructions appelées requêtes. Que ce soit pour la création, la suppression d'une table, la modification, l'insertion ou la sélection de données, le langage standard de requêtes est SQL. SQL ou (Standard Query Language) est un langage permettant d'interroger les bases de données de manière simple. Il est doté d'une syntaxe particulière que l'on doit respecter pour que la communication avec la base se passe au mieux.son succès est dû essentiellement à sa simplicité et au fait qu'il énonce des requêtes en laissant le SGBD responsable de la stratégie d'exécution.

SQL couvre les trois fonctions indispensables à la mise en oeuvre et à l'exploitation de bases de données relationnelles :

- la création des données .
- la manipulation des données .
- le contrôle des données.

A part le fait d'envoyer directement les requêtes SQL telles quelles au SGBD, le but ultime de l'utilisation de SQL sera aussi d'inclure ces requêtes SQL dans un programme écrit dans un autre langage. Ceci permet de coupler le SGBD à un langage informatique, donc à un programme. Tel est le cas de MySQL avec PHP.

1.2. Outils de design

1.2.1. Figma

Figma est un éditeur de graphiques vectoriels et un outil de prototypage. Il est principalement basé sur le web, avec des fonctionnalités hors ligne supplémentaires activées par des applications de bureau pour macOS et Windows (par exemple : vous pouvez utiliser des polices locales sur la version desktop). Les Figma Mirror companion apps pour Android et iOS permettent de visualiser des prototypes Figma sur des appareils mobiles. L'ensemble des fonctionnalités de Figma est axé sur l'utilisation dans la conception de l'interface utilisateur et de l'expérience utilisateur, en mettant l'accent sur la collaboration en temps réel [49]

1.2.2. Adobe Illustrator

Adobe Illustrator est un logiciel de création graphique vectorielle. Il fait partie de la gamme Adobe, peut être utilisé indépendamment ou en complément de Photoshop, et offre des outils de dessin vectoriel puissants. Les images vectorielles sont constituées de courbes générées par des formules mathématiques. L'un des outils principaux d'Illustrator étant « la plume » qui permet de tracer des courbes à l'aspect parfait grâce au placement de points d'ancrage et de tangentes qui vont en modifier la courbure. Un des avantages des images vectorielles est qu'elles sont indépendantes de la résolution, c'est-à-dire qu'elles ne perdent pas en qualité lorsqu'on les agrandit. Adapté aussi bien à la création de document papier qu'à celle d'illustrations pour Internet (logos, affiches, etc.) ce logiciel est orienté vers le marché professionnel, il intègre de nombreuses options propres à améliorer la productivité. [50]

1.3. Outils de programmation et d´eveloppement

1.3.1. Eclipse IDE

Eclipse est un environnement de développement intégré, une plateforme de programmation développé par IBM, dont le but est de fournir un environnement robuste et convivial pour les développeurs des logiciels, outils, et systèmes informatiques. Eclipse utilise énormément le concept de modules nommes "plugins" dans son architecture. D'ailleurs, hormis le noyau de la plateforme, nomme "Runtime", tout le reste de la plateforme est développé sous la forme de plugins. Ce concept permet de fournir un mécanisme pour son extension, et ainsi, fournir des 70 opportunités a des tiers de développer des fonctionnalités qui ne sont pas fournies en standard par Eclipse. Les principaux modules de base d'Eclipse fournis concernent le langage de programmation Java. Les modules agissent sur des fichiers qui sont inclus dans le l'espace de travail (appelé workspace). L'espace de travail regroupe les projets qui contiennent une ou plusieurs arborescences de fichiers.[51]

1.3.2. XAMPP

XAMPP est un ensemble de logiciels permettant de mettre en place un serveur web, un serveur FTP et un serveur de messagerie électronique. Il s'agit d'une distribution de logiciels libres (X Apache MySQL Perl PHP) offrant une bonne souplesse d'utilisation, réputée pour son installation simple et rapide. XAMPP est une compilation de logiciels libres et gratuits et la copie en est autorisée sous les termes de la "GNU General Public License". Mais seule la compilation que constitue XAMPP est couverte par la GPL. Du point de vue de XAMPP, l'utilisation commerciale est également gratuite. Plusieurs personnes savent par expérience qu'il n'est pas facile d'installer un serveur web Apache et que ça se complique si on veut y ajouter MySQL, PHP etc. XAMPP est un kit d'installation d'Apache qui contient MySQL, PHP et Perl. Il est réellement très facile à installer et à utiliser. On n'a qu'à le télécharger, le décompresser et l'installer.

Quatre kits XAMPP (XAMPP pour linux, XAMPP pour Windows, XAMPP pour Mac OS X et XAMPP pour Solaris) sont disponibles à l'adresse www.apachefriends.org:

Après l'installation de XAMPP pour Windows voici son panneau de contrôle qui permet de démarrer ou arrêter différents serveurs et/ou configurer ceux-ci à sa guise.

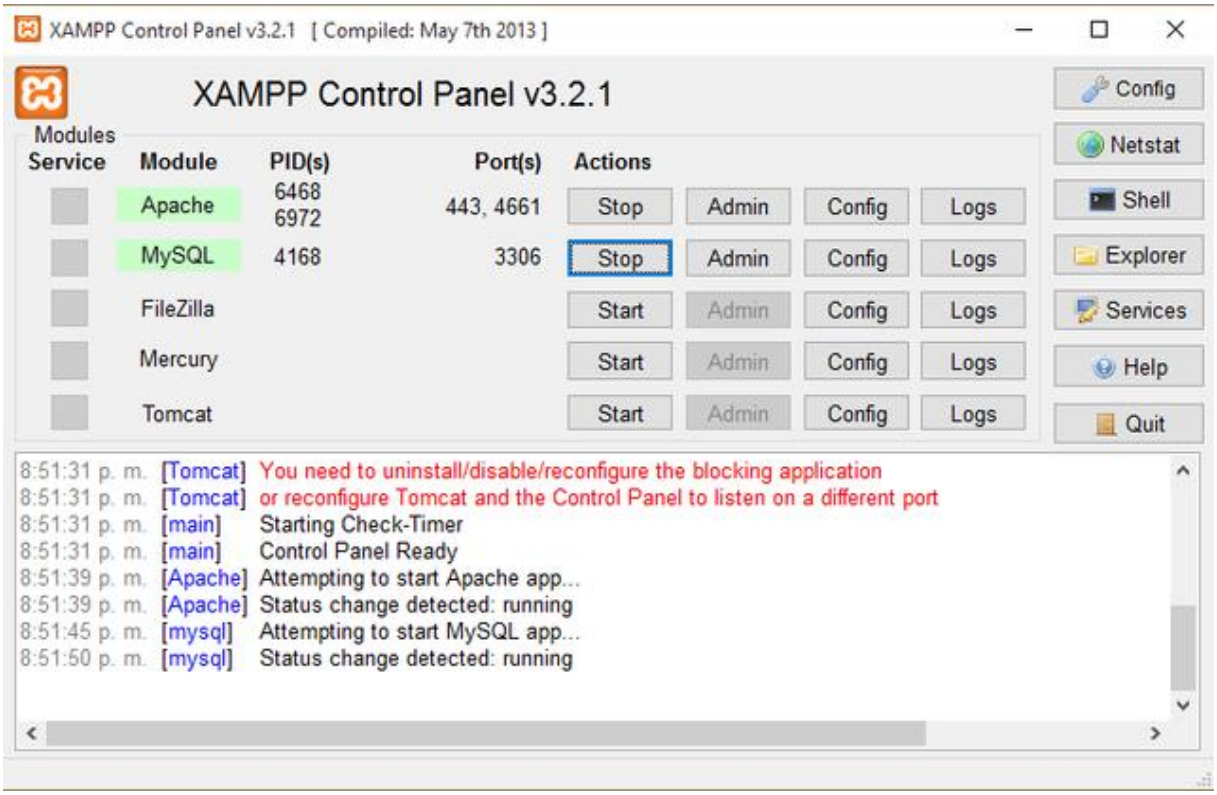

Figure 4.1: Panneau de Contrôle de XAMPP.

1.3.3. PhpMyAdmin

PhpMyAdmin (PMA) est une application Web de gestion pour les systèmes de gestion de base de données MySQL réalisée en PHP et distribuée sous licence GNU GPL. Il s'agit de l'une des plus célèbres interfaces pour gérer une base de données MySQL sur un serveur PHP. De nombreux hébergeurs, qu'ils soient gratuits ou payants, le proposent, ce qui permet à l'utilisateur de ne pas avoir à l'installer.

Cette interface pratique permet d'exécuter, très facilement et sans grandes connaissances dans le domaine des bases de données, de nombreuses requêtes comme les créations de table de données, les insertions, les mises à jour, les suppressions, les modifications de structure de la base de données. Ce système est très pratique pour sauvegarder une base de données sous forme de fichier .sql et ainsi transférer facilement ses données. De plus celui-ci accepte la formulation de requêtes SQL directement en langage SQL, cela permet de tester ses requêtes par exemple lors de la création d'un site et ainsi de gagner un temps précieux.[52]

1.3.4. Google Cloud SQL

- Qu'est-ce que Cloud SQL ?

Cloud SQL est un service qui fournit des bases de données relationnelles entièrement gérées dans le cloud. Ce service propose des moteurs de base de données MySQL, PostgreSQL et SQL Server.

- Comment démarrer avec Cloud SQL ?

Accédez à la console Cloud SQL, puis créez une instance de base de données. Devenez rapidement opérationnel en vous appuyant sur le guide de démarrage rapide pour MySQL, PostgreSQL ou SQL Server.

Les nouveaux clients bénéficient de 300 $ de crédits à dépenser sur Cloud SQL. Des frais ne vous seront facturés que si vous choisissez de passer à une version payante. (***Lorsque nous avons atteint ce etape, nous avons découvert que nous devions payer pour achever la création d'un serveur de stockage cloud afin de l'exploiter au niveau phpMyAdmin, et de transférer la base de donner de localhost vers ce serveur via l'adresse IP publique***).

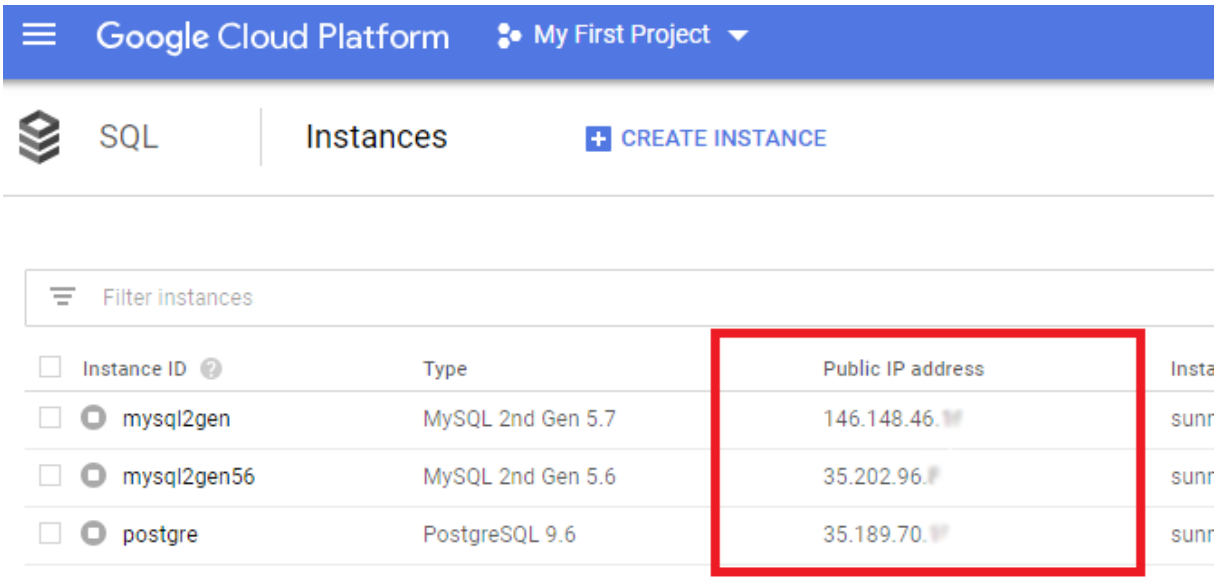

Figure 4.2: SQL Instances (l'adresse IP publique)

En remplaçant le serveur localhost (127.0.0.1) par l'adresse IP publique au niveau de phpMyAdmin, les données peuvent être stockées dans Google Cloud.

2. Principales interfaces

2.1. Interfaces de bienvenue

Lorsqu'une personne arrive à la porte du parking, elle se retrouve devant un écran devant la fenêtre du conducteur avec une interface d'accueil et un bouton pour accéder à la liste de réservation.

Figure 4.3: interfaces de bienvenue

2.2. Interfaces de réservation de stationnement

Quand tu appuie sur le bouton "Parking Reservation " Vous pouvez accéder à l'interface de réservation, qui affiche tous les parkings, les verts ne sont pas réservés, tandis que les rouges indiquent qu'ils sont réservés.

Figure 4.4: Interfaces de réservation de stationnement

2.3. Interface de saisie des informations pour les réservations

Lorsque vous cliquez sur le numéro de parking, une fenêtre apparaît indiquant où saisir le nom, le type de voiture et le numéro de plaque pour réserver et ouvrir la porte du parking.

Figure 4.5: Interface de saisie des informations pour les réservations

2.4. Interfaces d'annulation de réservation

À la sortie, lorsque la personne arrive à la porte du parking en sortant, elle se retrouve devant un écran devant la fenêtre du conducteur qui dispose d'une interface d'annulation de réservation où il faut saisir le numéro de plaque pour annuler et ouvrir la porte.

Figure 4.6: Interfaces d'annulation de réservation

2.5. Interfaces d'informations de réservation

Lorsqu'une réservation est effectuée, les informations de réservation apparaissent dans une interface sur un écran dans la salle de contrôle.

Figure 4.7: Interfaces d'informations de réservation

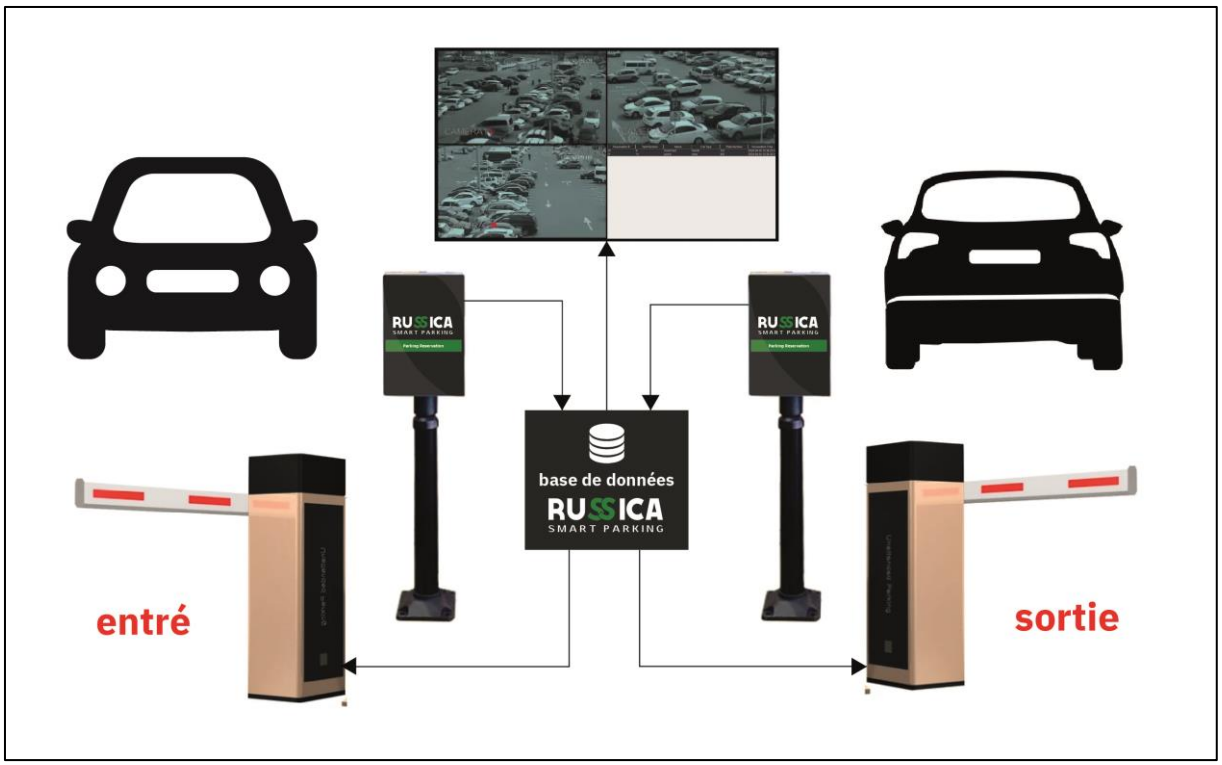

Figure 4.8: schéma de fonctionnement du système " rissica smart parking "

3. La table de la base de données

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra
1	reservation_id	int(11)			No	*None*		AUTO_INCREMENT
2	spot_number	int(11)			No	*None*		
3	name	varchar(100)	utf8mb4_general_ci		No	*None*		
4	car_type	varchar(50)	utf8mb4_general_ci		No	*None*		
5	plate_number	varchar(20)	utf8mb4_general_ci		No	*None*		
6	reservation_time	timestamp			No	current_timestamp()		

Figure 4.9: La table de la base de données au niveau de phpMyAdmin

4. Implémentation d'un système de détection d'intrusion

Pour cette raison, nous avons écrit un code spécial en langage Java dans la class «*IntrusionDetection*» qui détecte l'état de la base de données et affiche les résultats, ainsi qu'en cas d'intrusion indésirable.

Une autre class «*SQLMonitor*» peuvent être utilisées pour afficher des données sans avoir besoin d'entrer dans la base de données.

```java
import java.util.ArrayList;

public class IntrusionDetection {

    private List<String> maliciousPatterns;

    public IntrusionDetection() {

        maliciousPatterns = new ArrayList<>();
        maliciousPatterns.add("SELECT * FROM parking_reservations WHERE spot_number = ?");
        maliciousPatterns.add("SELECT * FROM parking_reservations WHERE name = ?");
        maliciousPatterns.add("SELECT * FROM parking_reservations WHERE car_type = ?");
        maliciousPatterns.add("SELECT * FROM parking_reservations WHERE plate_number = ?");
    }

    public boolean isSuspicious(String query) {
        for (String pattern : maliciousPatterns) {
            if (query.contains(pattern)) {
                return true;
            }
        }
        return false;
    }

    public void detect(String query) {
        if (isSuspicious(query)) {

            System.out.println("Query is normal   ");

        } else {

            System.out.println("Vrai positif   ");
        }
    }
}
```

Figure 4.10: la class «*IntrusionDetection*»

```java
import java.sql.ResultSetMetaData;

public class SQLMonitor {

    public void logQuery(String query) {
        System.out.println("Executing query: " + query);
    }

    public boolean validateParameters(String query, Object... parameters) {
        int parameterCount = query.length() - query.replace("?", "").length();

        if (parameterCount != parameters.length) {
            System.out.println("Error: Number of parameters provided does not match number of parameters required.");
            return false;
        }
        return true;
    }

    public ResultSet executeQuery(String query, Object... parameters) throws SQLException {
        if (!validateParameters(query, parameters)) {
            throw new SQLException("Invalid number of parameters.");
        }

        Connection connection = DatabaseConnection.getConnection();
        logQuery(query);
        PreparedStatement statement = connection.prepareStatement(query);

        for (int i = 0; i < parameters.length; i++) {
            statement.setObject(i + 1, parameters[i]);
        }

        return statement.executeQuery();
    }

    public void displayResults(ResultSet resultSet) throws SQLException {
        ResultSetMetaData metaData = resultSet.getMetaData();
        int columnCount = metaData.getColumnCount();

        StringBuilder header = new StringBuilder();
        for (int i = 1; i <= columnCount; i++) {
            header.append(String.format("%-20s", metaData.getColumnName(i)));
        }
        System.out.println(header);
        System.out.println("------------------------------------------------------------");


        while (resultSet.next()) {
            StringBuilder row = new StringBuilder();
            for (int i = 1; i <= columnCount; i++) {
                row.append(String.format("%-20s", resultSet.getString(i)));
            }
            System.out.println(row);
        }
```

Figure 4.11: la class «*SQLMonitor*»

```java
    SQLMonitor sqlMonitor = new SQLMonitor();
    IntrusionDetection intrusionDetection = new IntrusionDetection();

    String query = "SELECT * FROM parking_reservations WHERE spot_number = ?";
    String username = "SELECT * FROM parking_reservations WHERE name = ?";

    try {
        intrusionDetection.detect(query);
        ResultSet resultSet = sqlMonitor.executeQuery(query, username);
        sqlMonitor.displayResults(resultSet);
    } catch (SQLException e) {
        e.printStackTrace();
    }
}
```

Figure 4.12: Integration de «*SQLMonitor*» et «*IntrusionDetection*»

```
Query is normal
Executing query: SELECT * FROM parking_reservations WHERE spot_number = ?
reservation_id      spot_number         name                car_type
------------------------------------------------------------
```

Figure 4.13: Le résultat si aucune intrusion n'est appliquée

```
True positive
Executing query: SELECT * FROM parking_reservations WHERE spot_number = ?
reservation_id      spot_number         name                car_type
------------------------------------------------------------
```

Figure 4.12: Le résultat si une intrusion est appliquée

5. Le but de ce projet

Nous avons travaillé sur plusieurs objectifs, que nous mentionnons comme suit :

- Réduire les embouteillages à l'intérieur des parkings en voyant les places de stationnement vides et en les réservant avant d'entrer dans le parking
- Collecter les informations des utilisateurs pour en bénéficier lors de la réservation
- Connaître le propriétaire de chaque voiture dans le parking en envoyant des données à l'écran d'affichage
- Protéger les données des utilisateurs grâce à la technologie blockchain et les systèmes de détection d'intrusion

6. Conclusion

Nous avons abordé dans ce chapitre les différents outils de développement et les langages de programmations utilisés pour le développement dans notre application ainsi que quelques fonctionnalités qu'effectue cette dernière.

Conclusion générale

Dans le cadre de notre projet, nous avons développé un système de stationnement visant à organiser le parking, à stocker et à collecter des informations et à assurer la sécurité. Nous avons tiré parti de la technologie de l'Internet des objets pour pouvoir contrôler l'entrée du parking grâce à ce système. La personne pourra contrôler l'entrée et l'ouvrir en saisissant les informations nécessaires à cet effet, ainsi qu'à la sortie du parking.

Lors de la préparation de notre projet de fin d'études, nous avons essayé de mettre en pratique les connaissances que nous avons acquises pendant cinq années d'études universitaires dans le but de créer un système de stationnement intelligent et de le développer en utilisant de nouvelles méthodes, telles que le système de détection d'intrusion, dans le cadre de l'amélioration de la sécurité, de l'organisation et de la réduction du chaos.

Nous avons profit de l'utilisation de la blockchain dans cette application, en découvrant les contrats intelligents et leur fonctionnement dans la blockchain. Nous considérons cela comme un gain de nouvelles connaissances et une expérience précieuse pour nos études.

Nous avons pris plaisir à travailler sur ce sujet car il représente l'avenir de l'Algérie. Cette idée est un système qui peut aider à améliorer le stationnement des voitures dans les rues de manière plus organisée et sécurisée. Notre projet était lié à plusieurs technologies utilisées, ce qui nous a permis d'acquérir beaucoup d'informations en le réalisant.

Ce projet était vivant, stimulant et motivant pour nous pousser à poursuivre nos études. Nous pensons avoir entrevu une partie de notre future vie professionnelle.

Bibliographie

[01] Benghozi, P.-J., Bureau, S., & Massit-Folea, F. (2008). L'Internet des objets. Quels enjeux pour les Européens

[02] Taleb Omar, Mankouri Abdelkrim. « Programmation de la sécurité Internet des Objet, Etude de cas module WIFI Electric imp », Mémoire de master, Université de Tlemcen, Algérie, 2016.

[03] Evans, D., 2011. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. [Ebook] Etats-Unis : Cisco internet business solutions group (IBSG), pp.2-5. Disponible à : IoT_IBSG_0411FINAL.pdf (cisco.com) [Consulté le 4 février 2022].

[04] L'Internet des Objets : Publié par Sameh Ben Fredj http://blog.xebia.fr/2015/12/02/linternet-des-objets-101/

[05] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE.

[06] S. Dawson-Haggerty, A. Tavakoli and D. Culler, "Hydro: A Hybrid Routing Protocol for LowPower and Lossy Networks," 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, 2010, pp. 268-273.

[07] Évolution du nombre d'objets connectés de l'IoT , Patrick Olivier Kamgueu , dec 2017 https://www.researchgate.net/profile/Patrick-Kamgueu/publication/322724961/figure/fig1/AS:631610282082352@1527599034678/Evolution-du-nombre-dobjets-connectes-de-lIoT-Eva11.png

[08] Sika Technologie , https://x.com/SikaTechnologie/status/870234087386214400

[09] Avnet's Smart City Solutions , iot connect , https://www.iotconnect.io/smart-city-solutions.html

[10] «Insécurité des objets connectés : comment conjuguer l'IoT et la sécurité »,sur Journal du net , 2 mai 2016 (consulté le 16 novembre 2016).

[11] A technical review of wireless security for the internet of things : Software defined radio perspective, José de Jesús Rugeles Uribe, Edward Paul Guillen, Leonardo S. Cardoso https://doi.org/10.1016/j.jksuci.2021.04.003

[12] Perry Lea, Internet of Things for Architects : Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security

[13] «Focus sur le chiffrement homomorphe [archive] », sur Le Monde Informatique, 2 septembre 2020

[14] « Qu’est-ce que la blockchain ? [archive] », sur blockchainfrance.net (consulté le 23 juillet 2016)

[15] [Groth et Sahai 2008] (en) Jens Groth et Amit Sahai, « Efficient Non-interactive Proof Systems for Bilinear Groups », Eurocrypt,? 2008 (DOI 10.1007/978-3-540-78967-3_24, lire en ligne [archive])

[16] David J. Brooks and Michael Coole, Security Science, School of Science, Edith Cowan, University, Perth, WA, Australia : Intrusion Detection Systems. DOI : https://doi.org/10.1007/978-3319-69891-5_161-1

[17] Hung-Jen Liao Chun-HungRichardLin Ying-ChihLin Kuang-YuanTung Intrusion detection system : A comprehensive review http://dx.doi.org/10.1016/j.jnca.2012.09.004

[18] X. Zhan, H. Yuan et X. Wang, « Recherche sur le système de détectiond'intrusion dans les réseaux à chaînes de blocs », dans Actes de la Conférence internationale 2019 sur les réseaux informatiques, l'électronique et l'automatisation (ICCNEA), pp. 191-196, Xi'an,Chine, septembre 2019.

[19] CM Ou, « Systèmes de détection d'intrusion basés sur l'hôte inspirés par l'apprentissage automatique des systèmes immunitaires artificiels basés sur des agents », dansActes du Symposium international IEEE 2019 sur les innovations dans les systèmes et applications intelligents (INISTA), pp. 1–5, Sofa, Bulgarie, juillet 2019.

[20] L. Hong, « Systèmes de détection d'intrusion basés sur un mécanisme immunitaire », dansActes de la Conférence internationale 2009 sur la sécurité des réseaux, les communications sans fil et l'informatique de confiance, pp. 568-571, Wuhan, Chine, avril 2009.

[21] DS Bauer et ME Koblentz, « NIDX-an expert system for real-time network intrusion détection », dansActes des actes de 1988. Symposium sur les réseaux informatiques, pp. 98-106, Washington, DC, États-Unis, août 1988.

[22] Y. Shen, Y. Fei, LF Zhang, A. Ji-yao et ML Zhu, « Un système de détection d'intrusion basé sur un appel système », dansActes de la 1ère conférence internationale IEEE et IFIP 2005 en Asie centrale sur Internet, p. 4, Bichkek, septembre 2005.

[23] A. Garg et P. Maheshwari, « Un système hybride de détection d'intrusion : une revue », dansActes de la 10e Conférence internationale sur les systèmes et le contrôle intelligents (ISCO) 2016, pp. 1–5, Coimbatore, Inde, janvier 2016.

[24] EM Campos, PF Saura, A. González-Vidal et al., « Évaluation de l'apprentissage fédéré pour la détection d'intrusion dans l'Internet des objets : examen et défis »,Réseaux informatiques, vol. 203, numéro d’article 108661, 2022.

[25] A. Mihoub, OB Fredj, O. Cheikhrouhou, A. Derhab, et M. Krichen, « Détection et atténuation des attaques par déni de service pour l'Internet des objets à l'aide de techniques

d'apprentissage automatique rétroactives »,Informatique et génie électrique, vol. 98, numéro d'article 107716, 2022.

[26] Détection d'intrusions paramétrée par la politique de sécurité grâce au contrôle collaboratif des flux d'informations au sein du système d'exploitation et des applications : mise en œuvre sous Linux pour les programmes Java. Decembre 2008 Auteur : Guillaume Hiet Adresse : https://www.researchgate.net/publication/30514332_Detection_d%27intrusions_parametree_par_la_politique_de_securite_grace_au_controle_collaboratif_des_flux_d%27informations_au_sein_du_systeme_d%27exploitation_et_des_applications_mise_en_oeuvre_sous_Linux_po Consulté le 24 mai 2021

[27] «These Devices May Be Spying On You (Even In Your Own Home) »,surForbes (consulté le 16 novembre 2016)

[28] «Piratage massif de sites Internet : quand les objets connectés attaquent [archive] », surLeParisien (consulté le 16 novembre 2016)

[29] Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). « When Intrusion Detection MeetsBlockchain Technology » : A Review. IEEE Access, 6, 10179 - 10188. https://doi.org/10.1109/ACCESS.2018.2799854

[30] He, Q., Zhang, C., Ma, X., Liu, J., 2017. Fog-based transcoding for crowdsourced video livecast. IEEE Commun. Mag. 55, 28–33.

[31] Chen, H., Pendleton, M., Njilla, L., Xu, S., 2020. A survey on ethereum systems security : vulnerabilities, attacks, and defenses. ACM Comput. Surv. 53, 1–43.

[32] Novo, O., 2018. Blockchain meets iot : an architecture for scalable access management in iot. IEEE Internet Things J. 5, 1184–1195

[33] Yuan, R., Xia, Y.-B., Chen, H.-B., Zang, B.-Y., Xie, J., 2018. Shadoweth : private smart contract on public blockchain. J. Comput. Sci. Technol. 33, 542–556.

[34] Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al. 2016. Blockchain technology : beyond bitcoin. Appl. Innovat. 2, 71.

[35] Kshetri, N., 2017. Can blockchain strengthen the internet of things ? IT Professional 19, 68–72.

[36] Salah, K., Rehman, M.H.U., Nizamuddin, N., Al-Fuqaha, A., 2019. Blockchain for ai : review and open research challenges. IEEE Access 7, 10127–10149.

[37] Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., 2018. On blockchain and its integration with iot. Challenges and opportunities. Future Generat. Comput. Syst. 88, 173–190.

[38] Kuo, T.-T., Kim, H.-E., Ohno-Machado, L., 2017. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inf. Assoc. 24, 1211–1220.

[39] Hackius, N., Petersen, M., 2017. Blockchain in logistics and supply chain : trick or treat ? In : Proceedings of the Hamburg International Conference of Logistics (HICL). Epubli, pp. 3–18.

[40] Lee, J., Mtibaa, A., Mastorakis, S., 2019. A case for compute reuse in future edge systems : an empirical study. In : 2019 IEEE Globecom Workshops (GC Wkshps). IEEE, pp. 1–6.

[41] Swan, M., 2015. Blockchain : Blueprint for a New Economy. O'Reilly Media, Inc. Taivalsaari, A., Mikkonen, T., 2017. A roadmap to the programmable world : software challenges in the iot era. IEEE Software 34, 72–80.

[42] Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A., 2018. Bubbles of trust : a decentralized blockchain-based authentication system for iot. Comput. Secur. 78, 126–142.

[43] Dorri, A., Steger, M., Kanhere, S.S., Jurdak, R., 2017. Blockchain : a distributed solution to automotive security and privacy. IEEE Commun. Mag. 55, 119–125.

[44] T.Laurence. La Blockchain pour les nulls,2018.

[45] D. Puthal, N. Malik, P. Saraju Mohanty, E. Kougianos, and G. Gautam Das. Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems, 2018.

[46] https://iotindustriel.com/iot-iiot/cloud-computing-iot-le-duo-incontournable/

[47] Security and Communication Networks Volume 2023, Article ID 3171334, 10 pages https://doi.org/10.1155/2023/3171334

[48] Programmer en java, claudedelannoy ,5eme Edition ,733 pages.

[49] Gonzalez, « Figma Wants Designers to Collaborate Google-Docs Style [archive] », WIRED, WIRED (consulté le 1er juin 2020)

[50] Nicolas Six, « Charles Geschke, pionnier de l'informatique et cofondateur d'Adobe, est mort », Le Monde, 19 avril 2021

[51] Eclipse IDE for Java Developers, http://www.eclipse.org.

[52] http://www.phpmyadmin.net, consulté le 21/05/2014