arabic

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 : IA_StartUp15/2023

Mémoire

Présenté pour obtenir le diplôme de master académique en

Informatique

Parcours : **Intelligence Artificielle (IA)**

Système de contrôle d'accès par badge virtuel

Par : Sabrina Medjeneh

Soutenu le 02/07/2023 devant le jury composé de :

Abdelli Belkacem	MCB	Président
Belouaar Houcine	MCA	Rapporteur
Zerarka NourElhouda	MCB	Examinateur
	MCB	Examinateur

Année universitaire 2022-2023

Remerciement

Je suis reconnaissante à Allah pour m'avoir accordé la détermination et la force nécessaires pour accomplir ce modeste travail. Je tiens également à exprimer ma profonde gratitude envers mon superviseur, **Dr. Houcine Belouaar**, pour ses efforts, ses conseils et sa patience tout au long de cette période.

Je tiens à remercier toutes les personnes qui m'ont aidé à accomplir ce travail. Je suis reconnaissant envers tous ceux qui m'ont apporté leur aide et leur soutien sous toutes leurs formes. Je sais que cette réalisation n'aurait pas été possible sans votre assistance et votre encouragement.

Dédicaces

Derrière chaque grande femme se trouve un homme, et je suis reconnaissante envers cet homme extraordinaire qui a fait ressortir le meilleur de moi et m'a encouragée constamment, mon époux Meftah.

Je suis reconnaissante pour les plus belles bénédictions d'Allah, ma mère et mon père.

À mes perles précieuses,Anouar,Kamar, Roudina et Saleh.

À mes chers frères et leurs épouses.

À ma deuxième famille, la famille de mon mari.

À mes amies Hakima, Dounia et Safaa.

ملخص

النظام الموصوف هو نظام تحكم في الوصول يعتمد على شارة افتراضية باستخدام رمز الإستجابة السريع (QR code) يوفر طريقة مريحة وآمنة لإدارة الوصول إلى المناطق مراقبة. يتلقى المستخدمون رمز فريدًا على تطبيق الهاتف المحمول الخاص بهم ، والذي يتم التحقق منه بعد ذلك بواسطة مستشعر مزود بماسح ضوئي يتحقق الخادم المركزي من هوية المستخدم ويصرح بالوصول إذا لزم الأمر. يسمح تطبيق الهاتف المحمول للمستخدمين بإدارة وصولهم ، بينما تسمح واجهة المسؤول للمسؤولين بإدارة أذونات الوصول وعرض الإحصائيات.

يوفر التطبيق أيضًا ميزات مثل إنشاء رمز الاستجابة السريعة في الوقت الفعلي ، وأمن البيانات ، وإدارة الأعمال ، وتحديثات النظام المنتظمة ، وجمع ملاحظات العملاء من أجل التحسينات المستقبلية. ينصب التركيز على السلامة وسهولة الاستخدام.

الكلمات المفتاحية : شارة إفتراضية, رمز الإستجابة السريع, مراقبة الوصول.

Abstract

The described system is a virtual badge-based access control system using QR code. It provides a convenient and secure method for managing access to restricted areas. Users receive a unique QR code on their mobile application, which is then scanned by a sensor equipped with a QR scanner. The central server verifies the user's identity and grants access if necessary. The mobile application allows users to manage their access, while the admin interface allows administrators to manage access permissions and view statistics.

The application also offers features such as real-time QR code generation, data security, enterprise management, regular system updates, and collecting customer feedback for future improvements. The focus is on security, user-friendliness.

Keywords : QR code,virtual badge,access control.

Résumé

Le système décrit est un système de contrôle d'accès basé sur un badge virtuel utilisant des codes QR. Il offre une méthode pratique et sécurisée pour gérer l'accès aux zones restreintes. Les utilisateurs reçoivent un code QR unique sur leur application mobile, qui est ensuite vérifié par un capteur équipé d'un scanner QR. Le serveur central vérifie l'identité de l'utilisateur et autorise l'accès si nécessaire. L'application mobile permet aux utilisateurs de gérer leur accès, tandis que l'interface administrateur permet aux administrateurs de gérer les autorisations d'accès et de consulter les statistiques.

L'application offre également des fonctionnalités telles que la génération de codes QR en temps réel, la sécurité des données, la gestion d'entreprise, les mises à jour régulières du système et la collecte des commentaires des clients pour les améliorations futures. L'accent est mis sur la sécurité, la convivialité.

Mots-clés : code QR,badge virtuel,contrôle d'accés.

Table des matières

Table des figures

Introduction Générale

La sécurité organisationnelle est l'une des principales priorités des entreprises modernes, car les dirigeants d'entreprise cherchent à protéger leur siège social, leurs données et leurs actifs numériques contre les menaces internes et externes. Au fur et à mesure que la technologie a évolué, des systèmes de sécurité avancés ont émergé, visant à fournir aux organisations une protection efficace et complète. Historiquement,les systèmes de sécurité reposaient sur une protection physique telle que des serrures, des portails et des gardes. à mesure que la technologie a évolué, de nouvelles technologies sont apparues qui se concentrent sur la sécurité numérique. Ces technologies comprennent des systèmes de sécurité avancés tels que des systèmes de contrôle d'accès, des systèmes de détection d'intrusion, le cryptage, l'authentification à deux et trois facteurs. Ces dernières années, la technologie du badge virtuel s'est imposée comme une solution innovante dans le domaine de la sécurité des entreprises. Les badges virtuels utilisent la technologie du code QR pour fournir un moyen sûr et flexible de vérifier l'identité d'un utilisateur et d'accorder l'accès à des zones spécifiques. Les avantages des badges virtuel sont la facilité d'utilisation et la rapidité de mise en œuvre, ainsi que la possibilité de suivre et d'enregistrer l'accès à des fins de rapport et d'examen. Il offre également un haut niveau de sécurité. En bref, les systèmes et technologies de sécurité ont évolué pour répondre aux défis

actuels de protection des organisations. Des technologies avancées telles que Badge Virtuel permettent aux entreprises d'atteindre des niveaux élevés de sécurité pour leurs installations et de maintenir l'intégrité de leurs données et actifs numériques.

Chapitre I

Généralités sur le contrôle d'accès

I.1 Introduction

La sécurité des bâtiments et des locaux est un enjeu central pour la protection des personnes et des biens. Le contrôle d'accès est l'un des moyens les plus importants pour sécuriser les zones sensibles ou interdites et restreindre l'accès au personnel autorisé. Il existe aujourd'hui de nombreuses techniques de contrôle d'accès, allant des simples clés à celles utilisant des systèmes biométriques sophistiqués. Chaque technique présente des avantages et des inconvénients et doit être choisie en fonction des besoins spécifiques de chaque situation.

Dans ce chapitre, nous allons explorer les différentes techniques de contrôle d'accès, leurs avantages et inconvénients, ainsi que les enjeux liés à leur mise en place et à leur gestion. Nous verrons également comment les évolutions technologiques continuent de transformer le domaine du contrôle d'accès, et quels sont les nouveaux défis que ces technologies soulèvent. En somme, ce chapitre vise à donner un aperçu complet du contrôle d'accès, de ses enjeux et de ses perspectives d'avenir.

I.2 Différentes techniques de contrôle d'accès

Le choix de la technologie de contrôle d'accès dépend des exigences de sécurité de chaque organisation. Différentes méthodes, telles que les systèmes physiques, électroniques et biométriques, ont chacune leurs avantages et leurs inconvénients. Cette section détaille ces différentes techniques de contrôle d'accès.[7]

I.2.1 Contrôle physique

Les contrôles physiques peuvent inclure des barrières, des portes verrouillées, des clôtures et des caméras de surveillance pour surveiller les entrées et sorties. En complément, les entreprises peuvent également mettre en place des procédures d'identification strictes pour s'assurer que seules les personnes autorisées ont accès aux zones restreintes.[9]

I.2.1.1 Différents types de contrôle physique

les capteurs, les actionneurs et les dispositifs de commande. Les capteurs sont des dispositifs qui mesurent une grandeur physique telle que la température, la pression ou la luminosité. Les actionneurs, quant à eux, sont des dispositifs qui produisent un mouvement ou une force en réponse à un signal de commande. Les dispositifs de commande permettent de réguler et d'ajuster le fonctionnement des capte. [2]

I.2.1.1.1 Serrure mécanique Les serrures à clé sont les plus simples et les plus courantes, tandis que les serrures à combinaison et électroniques offrent une sécurité accrue grâce à l'utilisation de codes ou de cartes d'accès. Il est important de choisir la serrure qui convient le mieux à vos besoins en matière de sécurité et de commodité d'utilisation. Figure IV.2

FIGURE I.1 – Serrure mécanique

I.2.1.1.2 Barrières et portails Les barrières peuvent être contrôlées manuellement ou automatiquement à l'aide de systèmes de contrôle d'accès tels que des cartes d'identification ou des codes PIN. Elles offrent une sécurité supplémentaire en empêchant les véhicules non autorisés d'entrer dans les zones restreintes et en limitant l'accès aux personnes autorisées uniquement.

FIGURE I.2 – Barrières et portails

I.2.1.1.3 Portes et fenêtres blindées Les dispositifs de sécurité modernes sont équipés de technologies avancées telles que les capteurs de mouvement, les caméras de surveillance et les alarmes silencieuses pour garantir une protection maximale. De plus, certains dispositifs peuvent être connectés à des systèmes de sécurité centralisés pour une gestion plus efficace et une réponse rapide en cas d'urgence.

FIGURE I.3 – Portes et fenêtres blindées

I.2.1.1.4 Clôtures et murs de sécurité Ils peuvent être composés de barrières physiques, de caméras de surveillance, de détecteurs de mouvement et d'autres technologies avancées. Ces dispositifs sont essentiels pour assurer la sécurité des personnes travaillant dans ces installations ainsi que pour protéger les informations et les équipements sensibles qu'elles contiennent.

FIGURE I.4 – Clôtures et murs de sécurité

I.2.1.1.5 Système de surveillance Les systèmes de sécurité modernes sont équipés de caméras de surveillance et de capteurs sophistiqués pour détecter les

mouvements et les bruits inhabituels, offrant ainsi une protection maximale contre les intrusions et les cambriolages.

FIGURE I.5 – Système de surveillance

I.2.1.2 Avantages et inconvénients du contrôle physique

Ainsi, dans les environnements où la sécurité est une priorité absolue, le contrôle physique peut être une solution efficace. Cependant, pour les entreprises qui ont besoin d'une plus grande flexibilité dans la gestion de l'accès, il peut être préférable d'opter pour des solutions de contrôle d'accès électronique plus avancées.[11]

I.2.2 Systèmes de contrôle électronique

Un système de contrôle d'accès électronique est un dispositif qui utilise la technologie électronique pour contrôler l'accès aux espaces restreints. Ils offrent une alternative aux méthodes de contrôle physiques telles que les serrures mécaniques et les portails.[17]

I.2.2.1 Différents types de Systèmes de contrôle électronique

les cartes magnétiques, les codes PIN, les lecteurs d'empreintes digitales et les scanners rétiniens. Ces systèmes sont utilisés pour restreindre l'accès à des zones sensibles telles que les laboratoires de recherche, les salles de serveurs et les locaux de stockage de données confidentielles. Ils permettent également de suivre l'activité des utilisateurs autorisés et d'assurer la sécurité .[13]

I.2.2.1.1 Carte d'accès en présentant la carte devant un lecteur. Elle est souvent utilisée dans les entreprises, les hôpitaux et les universités pour contrôler l'accès aux zones sécurisées. En plus de faciliter la gestion des accès, elle permet également de suivre les mouvements des personnes autorisées dans les différentes zones.[4]

FIGURE I.6 – Carte d'accès

I.2.2.1.2 Les codes PIN Le code PIN est souvent utilisé pour protéger les informations personnelles et financières des utilisateurs, comme les numéros de carte de crédit ou les données bancaires. Il est important de choisir un code PIN fort et de ne jamais le partager avec quiconque pour garantir la sécurité de ses informations sensibles.

FIGURE I.7 – Les code PIN

I.2.2.1.3 Système de contrôle d'accès à distance Les systèmes de contrôle d'accès peuvent également être utilisés pour surveiller et enregistrer les entrées et sorties des personnes autorisées, ce qui peut être utile pour la sécurité et la gestion des ressources humaines. En outre, certains systèmes de contrôle d'accès peuvent intégrer des technologies telles que la reconnaissance faciale ou les cartes RFID pour une identification plus rapide et plus précise des utilisateurs autorisés.

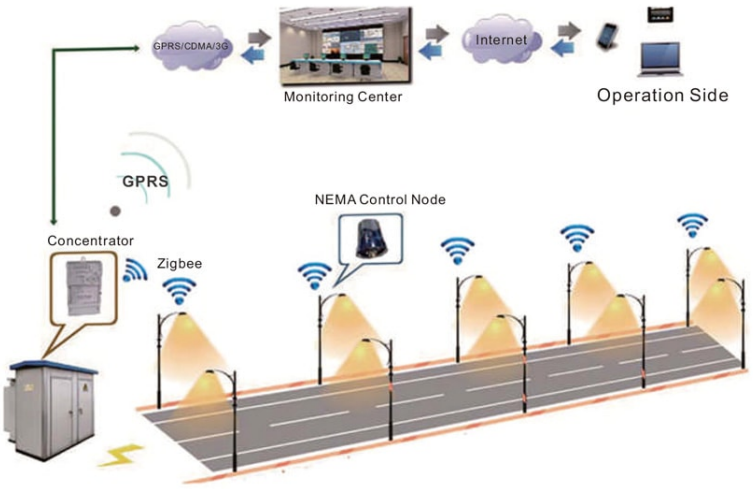

FIGURE I.8 – Système de contrôle d'accès à distance

I.2.2.1.4 Système de contrôle biométrique à des zones sécurisées. Ces technologies de reconnaissance biométrique sont considérées comme plus sûres que les méthodes traditionnelles telles que les mots de passe et les cartes d'identité, car elles sont difficiles à falsifier. Cependant, il est important de garantir la protection des données biométriques collectées pour éviter toute utilisation abusive ou violation de la vie privée.

FIGURE I.9 – Système de contrôle biométrique

I.2.2.2 Avantages et inconvénients des systèmes de contrôle électronique

Les systèmes de contrôle d'accès électroniques présentent plusieurs avantages, notamment en termes de flexibilité, de sécurité et de contrôle centralisé. Cependant, cette méthode présente également des inconvénients tels que le coût élevé, la nécessité d'un réseau informatique et le risque de piratage.

I.2.3 Les systèmes de contrôle biométrique

Un système de contrôle biométrique est une technologie de contrôle d'accès qui reconnaît et identifie les individus en fonction de leurs caractéristiques physiques ou

comportementales uniques telles que les empreintes digitales, les traits du visage, l'iris des yeux, la voix et les signatures. Les systèmes de contrôle biométrique deviennent de plus en plus importants pour la sécurité, en particulier dans les domaines de l'accès aux bâtiments et des données sensibles.[16]

I.2.3.1 Différents types de systèmes de contrôle biométrique

les systèmes de reconnaissance faciale, les systèmes de reconnaissance d'empreintes digitales, les systèmes de reconnaissance vocale et les systèmes de reconnaissance d'iris. Chacun de ces types de système utilise des caractéristiques biométriques uniques pour identifier et authentifier les individus. Les systèmes biométriques sont largement utilisés dans les domaines de la sécurité, de l'accès aux bâtiments et des transactions financières .[16]

I.2.3.1.1 Système de reconnaissance faciale Ces systèmes sont souvent utilisés pour la sécurité et l'identification des personnes dans les espaces publics ou privés. Cependant, ils soulèvent des préoccupations quant à la vie privée et la protection des données personnelles.

FIGURE I.10 – Système de reconnaissance faciale

I.2.3.1.2 Système de reconnaissance d'empreintes digitales Cette technologie est de plus en plus courante dans les systèmes de sécurité, tels que les portes d'entrée des entreprises et les coffres-forts personnels. Elle offre un niveau de sécurité élevé car chaque empreinte digitale est unique et difficile à falsifier.

FIGURE I.11 – Système de reconnaissance d'empreintes digitales

I.2.3.1.3 Système de reconnaissance de l'iris Ces systèmes de reconnaissance de l'iris sont souvent utilisés pour des applications de sécurité, telles que le contrôle d'accès à des zones restreintes ou la vérification d'identité pour les transactions financières. Ils offrent un haut niveau de précision et sont considérés comme l'une des méthodes les plus fiables de reconnaissance biométrique.

FIGURE I.12 – Système de reconnaissance de l'iris

I.2.3.1.4 Système de reconnaissance vocale Cette technologie est largement utilisée dans les domaines de la sécurité et de l'identification personnelle, tels que les contrôles d'accès aux bâtiments ou les transactions bancaires en ligne. En outre, elle peut également être intégrée à des applications de reconnaissance vocale pour améliorer la précision de la transcription.

FIGURE I.13 – Système de reconnaissance vocale

I.2.3.1.5 Système de reconnaissance de signature Cette technologie est couramment utilisée pour sécuriser les accès physiques et numériques, tels que les portes d'entrée des bâtiments ou les comptes en ligne. Les systèmes de reconnaissance de signature peuvent également être utilisés pour détecter la fraude dans les transactions financières en comparant la signature sur un chèque ou une facture à celle de l'utilisateur autorisé.

I.2.3.2 Avantages et inconvénients des systèmes de contrôle biométrique

Les systèmes de contrôle biométrique présentent plusieurs avantages, tels que la sécurité accrue et la réduction des fraudes. Cependant, ils peuvent également être

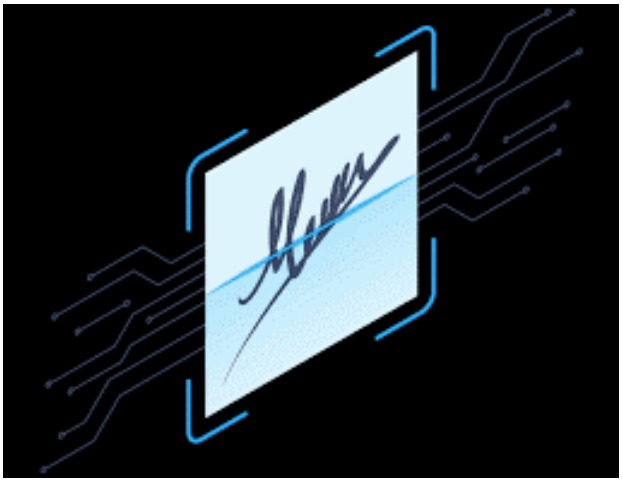

FIGURE I.14 – Système de reconnaissance de signature

coûteux à mettre en place et peuvent présenter des problèmes de confidentialité des données personnelles. En outre, certaines personnes peuvent éprouver des difficultés à utiliser ces systèmes en raison de problèmes physiques ou d'autres limitations. [22]

I.2.3.2.1 Avantages

1. **Sécurité accrue** Les systèmes biométriques sont également plus pratiques que les méthodes traditionnelles de contrôle d'accès, car ils ne nécessitent pas de cartes ou de codes d'identification qui peuvent être perdus ou volés. En outre, les données biométriques sont difficiles à falsifier, ce qui renforce la sécurité globale du système.
2. **Précision** Les technologies biométriques les plus courantes incluent la reconnaissance faciale, la reconnaissance d'empreintes digitales, la reconnaissance de l'iris et la reconnaissance vocale. Cependant, ces technologies ne sont pas infaillibles et peuvent être sujettes à des erreurs ou à des piratages, ce qui soulève des préoccupations en matière de protection de la vie privée et de

sécurité des données.

3. **Vitesse** Cela est dû au fait que les systèmes biométriques ne nécessitent pas de saisie manuelle de données, ce qui réduit considérablement le temps nécessaire pour vérifier l'identité d'une personne. De plus, les systèmes biométriques sont également plus fiables car ils sont basés sur des caractéristiques physiques uniques de chaque individu, telles que les empreintes digitales ou la reconnaissance

I.2.3.2.2 inconvénients

1. **Risque de confidentialité** Les données biométriques peuvent être utilisées pour identifier une personne de manière unique, ce qui peut poser des risques pour la sécurité si elles sont mal utilisées. Par conséquent, il est important de mettre en place des mesures de sécurité appropriées pour protéger ces données sensibles.
2. **Coût** Cependant, ces systèmes offrent un niveau de sécurité élevé en comparaison avec les méthodes traditionnelles de contrôle d'accès. Ils peuvent également être plus pratiques pour les utilisateurs, car ils ne nécessitent pas de porter une carte ou une clé pour accéder à un bâtiment ou à une zone sécurisée.
3. **Fiabilité** Cela peut entraîner des erreurs de reconnaissance, ce qui peut avoir des conséquences graves dans les domaines de la sécurité et de l'identification. Pour améliorer la fiabilité des systèmes biométriques, il est important d'investir dans des capteurs de haute qualité et de développer des algorithmes plus sophistiqués pour l'analyse biométrique.

I.2.4 Badge virtuel

Un badge virtuel est une représentation numérique d'un badge ou d'un identifiant physique. Il est souvent utilisé dans des environnements en ligne ou numériques pour identifier les réalisations, les compétences ou les qualifications d'une personne. Les badges virtuels peuvent prendre de nombreuses formes, telles qu'une image numérique ou une icône, et peuvent être affichés sur des sites Web, des profils de médias sociaux ou des CV numériques. Ils sont souvent utilisés dans les environnements d'apprentissage en ligne pour indiquer l'achèvement d'un cours ou la maîtrise d'une compétence spécifique. Les badges virtuels peuvent également être utilisés par les organisations pour reconnaître les réalisations des employés ou pour suivre les progrès vers des objectifs spécifiques. Ils offrent aux individus un moyen pratique et portable de présenter leurs compétences et leurs réalisations, et peuvent aider à renforcer leur crédibilité et à établir leur réputation professionnelle dans le monde en ligne.[34]

I.2.4.1 Avantages et inconvénients de badge virtuel

Les avantages du badge virtuel sont nombreux, notamment la facilité d'utilisation et la réduction des coûts liés à la production et à la distribution de badges physiques. De plus, les badges virtuels peuvent être facilement mis à jour et personnalisés en fonction des besoins de l'utilisateur. Cependant, certains inconvénients peuvent inclure des problèmes de sécurité potentiels et une dépendance accrue aux technologies numériques.[6]

I.2.4.1.1 Avantages

1. **Sécurité accrue** Les badges peuvent également être programmés pour limiter

l'accès à certaines zones ou à certaines heures, renforçant ainsi la sécurité globale du système. En outre, les données collectées par les badges peuvent être utilisées pour améliorer la gestion des accès et des autorisations au fil du temps.

2. **Vitesse** Les badges virtuels permettent également une traçabilité plus précise des mouvements et des activités des utilisateurs, ce qui peut être utile pour la gestion de la sécurité et la prise de décisions stratégiques. En outre, ils peuvent être facilement intégrés à d'autres systèmes de contrôle d'accès pour renforcer encore plus la sécurité globale.
3. **Coût** Cependant, ces systèmes offrent une sécurité accrue en empêchant l'accès non autorisé et en permettant une surveillance plus précise des activités des employés. Il est donc important pour les entreprises de peser les coûts par rapport aux avantages potentiels avant de décider d'implémenter un système de contrôle biométrique.

I.2.4.1.2 inconvénients

1. **Complexité technique** la mise en œuvre et la gestion des badges virtuels peuvent être complexes d'un point de vue technique, en raison de la nécessité pour les entreprises de fournir une infrastructure complexe et de l'intégrer avec les systèmes existants.
2. **Fiabilité** les badges virtuels peuvent dépendre des technologies de communication et de réseau, ce qui peut entraîner des problèmes de fiabilité et des interruptions de service en cas de problèmes de réseau ou de communication.
3. **Menaces de sécurité** les badges virtuels peuvent être exposés à des menaces de sécurité telles que les cyberattaques et le vol d'informations sensibles.

4. **Problèmes de confidentialité** l'utilisation des badges virtuels peut impliquer la collecte et le stockage de données personnelles des utilisateurs.
5. **Dépendance à la technologie** l'utilisation des badges virtuels dépend de technologies avancées et de dispositifs compatibles. Il peut être difficile pour certaines entreprises d'investir dans cette technologie et de la mettre à disposition de tous les utilisateurs.

I.2.5 Comparaison des différentes techniques de contrôle d'accès

1. **Niveau de sécurité** à accéder à une zone restreinte. Les badges virtuels peuvent également être gérés à distance, ce qui permet aux administrateurs de modifier rapidement les autorisations d'accès en cas de besoin. En outre, les badges virtuels sont souvent plus pratiques pour les utilisateurs car ils peuvent être stockés sur un téléphone portable ou une montre connectée plutôt que d'avoir à porter un badge physique.
2. **Rapidité** De plus, les badges virtuels offrent une plus grande flexibilité en termes de gestion des accès, tandis que les systèmes biométriques offrent une sécurité accrue grâce à l'identification unique de chaque individu. Cependant, il est important de noter que les coûts d'installation et de maintenance des systèmes biométriques peuvent être plus élevés que ceux des badges virtuels ou des méthodes manuelles.
3. **Coût** . En outre, les badges virtuels peuvent être facilement mis à jour et gérés à distance, ce qui en fait une solution pratique pour les entreprises ayant des employés mobiles ou travaillant à distance.
4. **Complexité** à utiliser, les systèmes de contrôle de la biométrie peuvent également être plus coûteux en raison de l'investissement initial dans l'équipement

et la formation du personnel. Cependant, ils offrent une sécurité accrue car les empreintes digitales, les iris ou les traits du visage sont uniques à chaque individu et ne peuvent pas être facilement falsifiés ou volés.

I.3 Thechnique d'implémentation d'un système de contrôle d'accès

L'implémentation d'un système de contrôle d'accès peut être un processus complexe qui nécessite une planification minutieuse et une gestion de projet efficace. Voici quelques étapes clés à suivre lors de l'implémentation d'un système de contrôle d'accès [3] :

1. **Évaluation des besoins :** Il est également important de prendre en compte les différents niveaux d'accès nécessaires pour chaque employé ou utilisateur, ainsi que les éventuelles réglementations en matière de sécurité qui s'appliquent à votre secteur d'activité. En prenant en compte tous ces éléments, vous pourrez choisir le système de contrôle d'accès le plus adapté à vos besoins spécifiques.
2. **Sélection du système :** elle peut varier en fonction de plusieurs facteurs tels que la taille de l'entreprise, le nombre d'employés, le niveau de sécurité requis et les risques potentiels. Il est donc important de bien évaluer ces critères avant de choisir la méthode de contrôle d'accès la plus adaptée.
3. **Planification de l'installation :** est un élément clé à prendre en compte lors de la conception d'un système de sécurité efficace. Il est également important de considérer les besoins spécifiques de chaque site et les risques potentiels pour déterminer les fonctionnalités nécessaires du système.

4. **Installation et configuration :** pour assurer la sécurité de votre entreprise. Ces dispositifs permettent de limiter l'accès aux zones sensibles et de suivre les mouvements des employés dans le bâtiment. En outre, ils peuvent être intégrés à des systèmes de vidéosurveillance pour renforcer encore plus la sécurité.
5. **Formation initiale et continue :** Assurez-vous également que les employés comprennent l'importance de la sécurité des données et de la protection de la vie privée des clients. En outre, organisez régulièrement des séances de formation pour maintenir les connaissances des employés à jour et pour sensibiliser aux nouvelles menaces potentielles en matière de sécurité.
6. **Test et essai :** Les tests fonctionnels permettent de vérifier si toutes les fonctionnalités du système sont opérationnelles, tandis que les tests d'acceptation utilisateur garantissent que le système répond aux exigences spécifiques de l'utilisateur final. En outre, il est important de réaliser des tests de sécurité pour s'assurer que le système est protégé contre les attaques externes et internes.
7. **Entretien et assistance :** et une sécurité maximale. Il est également important de mettre à jour régulièrement les logiciels et les protocoles de sécurité pour rester à jour avec les dernières menaces et vulnérabilités. Enfin, il est recommandé de former régulièrement le personnel chargé de la gestion du système pour s'assurer qu'ils sont bien informés des dernières pratiques de sécurité et des procédures opérationnelles.

Tout d'abord, il est important de définir clairement les rôles et les responsabilités de chaque utilisateur du système. Ensuite, il est recommandé de mettre en place des procédures de surveillance et d'audit régulières pour détecter toute activité suspecte ou non autorisée. Enfin, une formation continue des utilisateurs sur les bonnes

pratiques de sécurité informatique peut contribuer à renforcer la sécurité glob.

I.4 Gestion des accès

La gestion des accès est un élément clé de tout système de contrôle d'accès. Il est utilisé pour assurer la sécurité organisationnelle en contrôlant l'accès aux ressources, aux données et aux installations et en veillant à ce que seules les personnes autorisées aient accès aux informations et équipements sensibles. Voici les éléments clés de la gestion des accès :

1. **Identification et authentification :** Une fois que l'utilisateur est authentifié, il peut être autorisé à accéder à certaines zones ou ressources en fonction de son niveau d'autorisation. Cela permet de garantir la sécurité des données et des biens physiques dans les entreprises et les organisations.
2. **Cession de droits :** Cela garantit que chaque utilisateur a uniquement accès aux informations et aux fonctionnalités qui sont nécessaires pour effectuer ses tâches professionnelles. De plus, la gestion des accès permet de suivre l'activité des utilisateurs et de détecter toute activité suspecte ou non autorisée.
3. **Gestion des autorisations :** Elle est essentielle pour assurer la confidentialité et l'intégrité des informations sensibles, ainsi que pour prévenir les attaques externes et internes. En outre, la gestion des accès permet également de suivre l'utilisation des ressources et de détecter toute activité suspecte ou non autorisée.
4. **Audit et surveillance :** Les outils de surveillance peuvent inclure des journaux d'audit, des alertes de sécurité et des analyses de comportement pour identifier les activités suspectes. En cas de violation de sécurité, une réponse

rapide et appropriée doit être mise en place pour minimiser les dommages potentiels et prévenir toute future violation.

5. **Gestion des incidents :** Les systèmes de contrôle d'accès modernes peuvent également fournir des rapports détaillés sur les activités des utilisateurs, ce qui peut aider à identifier les problèmes potentiels avant qu'ils ne deviennent des incidents de sécurité. En outre, la mise en place de politiques et de procédures claires pour la gestion des accès peut aider à prévenir les erreurs humaines et les violations involontaires de la sécurité.

Cela implique de mettre en place des politiques de sécurité solides et de former les employés à leur application, ainsi que d'utiliser des outils de gestion d'accès tels que l'authentification à deux facteurs et la surveillance des activités utilisateur. En outre, une approche proactive peut aider les entreprises à se conformer aux réglementations en matière de protection des données et à renforcer leur réputation auprès des clients.

I.5 Le code QR

Un code QR (Quick Response) est un type de code-barres en deux dimensions qui peut être scanné rapidement à l'aide d'un smartphone ou d'un lecteur de code QR. capable de stocker des informations plus complexes par rapport aux codes-barres traditionnels. Un code QR est composé de modules noirs et blancs disposés dans un motif carré. Il peut contenir différents types de données, tels que des liens URL, des numéros de téléphone, des adresses e-mail, des textes, des coordonnées géographiques, des événements de calendrier, etc. Lorsqu'un utilisateur scanne un QR code à l'aide d'une application de lecture appropriée, les informations contenues dans le code sont décodées et affichées sur l'appareil [32].

Les codes QR sont utilisés dans de nombreux domaines et offrent diverses possibilités d'utilisation. Voici quelques exemples :

1. **Marketing** Les codes QR sont souvent utilisés dans des campagnes publicitaires pour permettre aux utilisateurs d'accéder rapidement à des informations supplémentaires, des offres spéciales, des promotions ou des concours en scannant le code.
2. **Paiement mobile** Certains systèmes de paiement mobile utilisent des codes QR pour permettre aux utilisateurs de régler des achats en scannant le code à partir de leur appareil mobile.
3. **Billetterie électronique** Les codes QR sont couramment utilisés pour les billets d'événements, les cartes d'embarquement, les billets de cinéma, etc. Ils permettent une validation rapide et facile à l'entrée en scannant simplement le code.
4. **Suivi des produits** Les codes QR peuvent être utilisés pour suivre et retracer les produits, en fournissant des informations sur leur origine, leur traçabilité, leur date de fabrication [3].

I.6 Les évolutions technologiques dans le contrôle d'accès

Les systèmes de contrôle d'accès ont évolué au fil du temps et incluent des technologies avancées telles que l'Internet des objets (IoT), l'intelligence artificielle (IA) et la reconnaissance faciale. Ces développements ont rendu les systèmes de contrôle d'accès plus sophistiqués et plus efficaces pour protéger les installations et les données. L'un des développements récents en matière de contrôle d'accès est l'uti-

lisation de la biométrie. Il utilise des caractéristiques physiques uniques telles que les empreintes digitales, la rétine et la voix pour identifier les personnes. Étant donné que les caractéristiques biométriques sont uniques à chaque individu, la biométrie est considérée comme plus sûre que les méthodes traditionnelles telles que les mots de passe et les codes PIN.

Les systèmes de contrôle d'accès sont également de plus en plus connectés aux réseaux informatiques et aux applications cloud, permettant aux administrateurs de gérer à distance les accès et d'accéder aux données en temps réel. Les appareils IoT tels que les caméras et les capteurs peuvent également être intégrés dans les systèmes de contrôle d'accès pour améliorer la sécurité et surveiller l'activité sur site. L'intelligence artificielle est également de plus en plus utilisée dans le contrôle d'accès pour améliorer la précision de la détection et la sécurité globale. Les algorithmes d'IA peuvent être utilisés pour identifier les anomalies et détecter les tentatives d'accès non autorisées en temps réel, permettant aux administrateurs de prendre des mesures pour protéger leurs installations et leurs données [14].

I.7 Conclusion

Le contrôle d'accès est un aspect important de la sécurité physique et informatique. Les systèmes de contrôle d'accès sont utilisés dans diverses installations. Entreprises, organismes de santé, gouvernements, institutions financières. Les méthodes de contrôle d'accès ont évolué au fil du temps, des clés et serrures traditionnelles aux systèmes de contrôle électroniques sophistiqués et aux techniques biométriques avancées. Bien qu'il existe de nombreux avantages à utiliser un système de contrôle d'accès pour protéger vos locaux et vos données, il est également important de comprendre les limites et les vulnérabilités potentielles. Les systèmes de contrôle d'accès

doivent être mis à jour et évalués régulièrement pour rester efficaces contre les menaces actuelles et futures. En fin de compte, le choix d'un système de contrôle d'accès dépend des besoins spécifiques et des objectifs de sécurité de chaque installation. Il est important que les administrateurs de sécurité travaillent en étroite collaboration avec des experts techniques pour évaluer les options disponibles et mettre en œuvre des systèmes de contrôle d'accès efficaces et robustes pour protéger leurs installations et leurs données.

Chapitre II

Internet des objets (IoT)

II.1 Introduction

L'Internet des objets (IoT) est la technologie qui permet de connecter les objets du quotidien à Internet pour collecter et partager des données. Avec la popularité croissante des smartphones et des objets connectés, l'IoT devient une tendance de plus en plus importante dans le monde de la technologie. L'IoT offre de nombreuses opportunités pour améliorer notre quotidien et transformer de nombreux domaines tels que la santé, l'agriculture, la logistique ou encore les villes intelligentes. Cependant, à mesure que les appareils connectés prolifèrent, l'IoT soulève également des inquiétudes concernant la sécurité et la confidentialité des données. Ce chapitre passe en revue les principes fondamentaux de l'IoT, les avantages et les défis associés à cette technologie, les implications commerciales, ainsi que les tendances et perspectives futures de l'IoT.

II.2 Définition internet des objets (IoT)

Internet des objets signifie "IoT" s'agit d'un réseau d'appareils physiques, de véhicules, d'appareils et d'autres éléments qui intègrent des capteurs, des logiciels et une connectivité et permettent l'échange de données avec d'autres appareils et systèmes sur Internet. L'Internet des objets permet à ces appareils de collecter et de partager des données en temps réel, ce qui leur permet d'effectuer diverses tâches et d'automatiser les processus sans intervention humaine. Les données générées par les appareils IoT peuvent être utilisées pour l'analyse, l'analyse et la prise de décision afin d'augmenter l'efficacité, d'améliorer la sécurité et d'améliorer l'expérience dans divers secteurs tels que la maison intelligente, les transports, les soins de santé et l'industrie [29].

II.3 Définition d'un Objet connecté (OC)

Un objet connecté dans l'Internet des objets (IoT) est un appareil physique qui est connecté à Internet et peut échanger des données avec d'autres appareils. Cela inclut les montres intelligentes, les thermostats intelligents, les caméras de sécurité connectées, les réfrigérateurs intelligents, etc. Ces objets sont équipés de capteurs et de connexions réseau qui leur permettent de collecter, envoyer et recevoir des données. Ils peuvent être contrôlés et surveillés à distance et des décisions peuvent être prises sur la base des données collectées [29].

II.3.1 Les éléments clés d'un objet connecté

Les éléments clés d'un objet connecté sont les suivants :

1. **Capteur :** Les capteurs sont un composant important des objets en réseau.

Il peut collecter diverses données telles que la température, l'humidité, la pression, la luminosité et le mouvement. Les capteurs jouent un rôle important dans la collecte d'informations sur l'environnement et les utilisateurs.

2. **Connectivité :** Les objets connectés ont des capacités de communication sans fil telles que le Wi-Fi, le Bluetooth, la technologie cellulaire et d'autres protocoles de communication. Il vous permet de vous connecter à Internet et à d'autres appareils pour échanger des données et recevoir des instructions.
3. **Plateforme de traitement des données :** Les données collectées à partir des objets connectés sont souvent transmises à des plateformes de traitement de données. La plate-forme permet un stockage, une analyse et un traitement efficaces des données. Il peut également fournir des capacités d'intelligence artificielle ou d'apprentissage automatique qui tirent des informations utiles des données collectées.
4. **Interface utilisateur :** Les objets connectés ont généralement une interface utilisateur qui permet aux utilisateurs d'interagir avec l'objet. Cela peut prendre la forme d'applications mobiles, de panneaux de contrôle, d'écrans tactiles ou d'autres moyens permettant aux utilisateurs de configurer, de surveiller ou de contrôler des objets connectés.
5. **Alimentation :** Les objets connectés nécessitent une source d'alimentation telle que des piles, des batteries rechargeables, ou une connexion permanente au réseau électrique. Une source d'alimentation stable et pérenne est indispensable au bon fonctionnement des objets connectés.
6. **Sécurité :** La sécurité est un aspect important des objets connectés. Avec la collecte et l'échange fréquents de données sensibles, il est important de mettre en place des mesures de sécurité solides pour protéger les informations contre

les accès non autorisés, le piratage et les violations de données.

En combinant ces éléments, les objets connectés peuvent créer des solutions innovantes dans divers domaines tels que la domotique, la santé, l'industrie, les transports, etc., en offrant des fonctionnalités avancées, une connectivité intelligente et une interactivité avec les utilisateurs [29].

II.3.2 Les caractéristiques d'un objet connecté

Les caractéristiques d'un objet connecté peuvent varier en fonction de sa fonctionnalité spécifique et du domaine d'application. Cependant, voici quelques caractéristiques courantes des objets connectés :

1. **Connectivité sans fil :** Les objets connectés peuvent se connecter à d'autres appareils et à Internet à l'aide de technologies sans fil telles que le Wi-Fi, le Bluetooth, le NFC (Near Field Communication) et les réseaux cellulaires. Cela leur permet d'échanger des données et de communiquer avec d'autres appareils.
2. **Capteurs et collecte de données :** Les objets connectés disposent de capteurs et peuvent collecter diverses données sur leur environnement et leurs utilisateurs. Ces capteurs peuvent mesurer des paramètres tels que la température, l'humidité, la pression, la luminosité, la géolocalisation et le mouvement.
3. **Interactivité :** Les objets connectés offrent généralement une interface utilisateur à travers laquelle les utilisateurs peuvent interagir avec l'objet. Cela peut se faire via une application mobile dédiée, des écrans tactiles sur site, des commandes vocales ou une interface basée sur les gestes.
4. **Traitement des données et intelligence embarquée :** Les objets connectés peuvent effectuer un certain niveau de calcul directement sur l'appareil lui-

même. Les algorithmes et l'intelligence intégrée peuvent être utilisés pour analyser les données collectées et fournir des informations et des fonctionnalités avancées.

5. **A**utonomie énergétique : Les objets connectés doivent toujours fonctionner sur piles ou sources d'énergie autonomes afin de fonctionner en continu. L'autonomie énergétique est un élément clé pour assurer un fonctionnement ininterrompu des objets connectés.
6. **Sécurité et confidentialité :** La sécurité et la confidentialité des informations sont des caractéristiques importantes car les objets connectés traitent souvent des données sensibles. Les appareils doivent mettre en œuvre des mesures de sécurité telles que le cryptage des données, l'authentification et l'autorisation pour protéger les données contre tout accès non autorisé.
7. **Intégration avec d'autres systèmes :** Les objets connectés sont souvent conçus pour être compatibles avec d'autres systèmes et appareils et facilement intégrés dans un écosystème plus large. Il peut être connecté à des plates-formes cloud, des systèmes domotiques, des applications tierces ou utilisé dans le cadre de l'Internet des objets (IoT).

Ces propriétés permettent aux objets connectés d'être polyvalents et interactifs, en collectant, analysant et partageant des informations pour fournir des fonctionnalités avancées, améliorer l'efficacité et enrichir l'expérience utilisateur [28].

II.4 Communication machine à machine (M2M)

La communication machine à machine (M2M) est un concept de communication dans lequel les appareils électroniques interagissent directement les uns avec les autres

sans intervention humaine. Il s'agit d'une forme de communication automatisée de machine à machine qui permet de transférer des informations, des données et des commandes entre des appareils connectés. La communication M2M est basée sur une technologie sans fil ou filaire qui permet aux appareils de se connecter et d'échanger des données de manière transparente. Les appareils peuvent être équipés de capteurs, d'actionneurs ou d'autres composants pour collecter des données de l'environnement, effectuer des mesures, contrôler l'appareil, etc. Les applications de la communication M2M vont des domaines industriels et médicaux aux applications domestiques et de ville intelligente [30].

II.5 Historique de l'internet des objets

L'internet des objets est apparu dans les années 1990 lorsque les chercheurs ont commencé à chercher des moyens de connecter des appareils à Internet. Les progrès technologiques au fil des ans ont permis des capteurs plus petits et des coûts de connectivité réduits, ouvrant la voie à l'adoption généralisée des appareils connectés. Aujourd'hui, l'IoT est une tendance majeure dans le monde de la technologie et devrait connaître une croissance exponentielle au cours des prochaines années [14].

II.6 Domaines d'applications IoT

Voici quelques exemples d'applications IoT :

1. **Santé :** Ces appareils sont équipés de capteurs qui collectent des données sur la fréquence cardiaque, le nombre de pas et la qualité du sommeil. Les utilisateurs peuvent ensuite accéder à ces informations via une application mobile pour suivre leur progression et atteindre leurs objectifs de santé et de

fitness [26].

2. **Agriculture :** Les capteurs peuvent également aider à détecter les maladies des plantes et à prévenir les pertes de récoltes, en fournissant des données en temps réel pour une prise de décision rapide et efficace. En outre, l'utilisation de capteurs peut contribuer à réduire l'utilisation d'engrais et de pesticides, ce qui peut avoir un impact positif sur l'environnement et la santé humaine [23].
3. **Ville intelligente :** Les technologies de l'information et de la communication peuvent également être utilisées pour améliorer la qualité de vie des citoyens en fournissant des services tels que la santé à distance, l'éducation en ligne et la sécurité publique intelligente. En outre, elles peuvent aider à promouvoir une économie plus durable en permettant une utilisation plus efficace des ressources naturelles et en favorisant le développement de nouvelles industries vertes.
4. **Industrie :** Les données collectées par ces capteurs peuvent être analysées en temps réel pour détecter les problèmes et permettre une intervention rapide, ce qui peut aider à éviter les temps d'arrêt coûteux et à améliorer la productivité globale de l'entreprise. De plus, les capteurs connectés peuvent également être utilisés pour suivre la qualité des produits et garantir leur conformité aux normes réglementaires [27].
5. **Maison connectée :** ce qui permet aux utilisateurs de contrôler leur maison même lorsqu'ils sont loin. Ces appareils peuvent également être programmés pour s'adapter aux habitudes des utilisateurs et pour économiser de l'énergie [18].

II.7 Composants de l'IoT

Voici les principaux composants de l'IoT :

1. **Capteur :** à l'aide de capteurs. Ces données peuvent ensuite être utilisées pour surveiller et contrôler des systèmes tels que les systèmes de sécurité, les systèmes de surveillance environnementale et les systèmes industriels [19].
2. **Réseau :** Les réseaux IoT sont utilisés dans divers domaines tels que la domotique, la santé, l'agriculture et l'industrie pour collecter des données en temps réel et les analyser afin d'améliorer les performances et l'efficacité des systèmes. Ces réseaux peuvent également être utilisés pour contrôler à distance des appareils et automatiser des processus [19].
3. **Plateforme IoT :** Elle offre une solution complète pour la surveillance, la gestion et le contrôle des appareils connectés, ainsi que pour l'analyse des données collectées. De plus, elle permet aux utilisateurs de créer et de déployer facilement des applications IoT personnalisées pour répondre à leurs besoins spécifiques.
4. **Cloud :** Les données peuvent être stockées et traitées à distance, ce qui permet une utilisation plus efficace des ressources informatiques et une réduction des coûts d'infrastructure pour les entreprises. De plus, les services de cloud computing offrent souvent des fonctionnalités de sécurité avancées pour protéger les données sensibles des utilisateurs [5].
5. **Applications :** Les applications IoT peuvent également aider les entreprises à surveiller et à gérer efficacement leurs opérations, en collectant des données en temps réel sur les performances des machines et des équipements. De plus, elles peuvent contribuer à améliorer la sécurité en surveillant les activités suspectes et en déclenchant des alertes en cas d'incidents.

6. **Sécurité :** Cependant, malgré ces mesures de sécurité, il est important de souligner que les vulnérabilités dans les appareils IoT peuvent encore être exploitées par des cybercriminels. Par conséquent, une approche proactive en matière de sécurité et une mise à jour régulière des logiciels sont essentielles pour garantir la protection des données et des appareils connectés [20].

II.8 Avantages et inconvénients de l'IoT

Tout d'abord, l'IoT peut améliorer l'efficacité opérationnelle et réduire les coûts en permettant une surveillance et un contrôle à distance des équipements. Cependant, cela peut également augmenter les risques de sécurité et de confidentialité des données sensibles, ce qui nécessite une attention particulière pour protéger les informations personnelles et professionnelles. En outre, la complexité croissante [33].

II.8.1 Avantages

1. **Automatisation :** Cela peut être particulièrement utile dans les industries manufacturières où des tâches répétitives et monotones peuvent être effectuées par des machines, libérant ainsi les travailleurs pour des tâches plus complexes et créatives. De plus, l'automatisation peut également améliorer la précision et la qualité des produits finis [12].
2. **Optimisation :** Les entreprises peuvent également utiliser la technologie pour améliorer leur communication interne et externe, ainsi que pour mieux comprendre les besoins de leurs clients et leur offrir des solutions plus personnalisées. En somme, l'utilisation de la technologie peut avoir un impact positif sur tous les aspects d'une entreprise, de la gestion des opérations à la satis-

faction des clients.

3. **La prévention :** De plus, l'IoT permet également de surveiller en temps réel les équipements et d'anticiper les besoins en maintenance, ce qui peut réduire considérablement les coûts et améliorer la productivité. En somme, l'utilisation de l'IoT dans le domaine industriel peut apporter de nombreux avantages en termes de sécurité, d'efficacité et de rentabilité.
4. **Personnalisation :** Cette personnalisation peut conduire à une meilleure satisfaction client et à une fidélisation accrue, ce qui peut avoir un impact positif sur les résultats financiers de l'entreprise. Cependant, il est important de respecter la vie privée des clients et de s'assurer que les données sont collectées et utilisées de manière éthique et transparente [9].
5. **Innovation :** qui répondent aux besoins des consommateurs. De plus, la concurrence peut également encourager les entreprises à améliorer leur efficacité opérationnelle et à réduire leurs coûts, ce qui peut se traduire par des économies pour les clients.

II.8.2 Inconvénients

1. **Sécurité :** connectés. Il est donc important de mettre en place des mesures de sécurité efficaces telles que l'utilisation de mots de passe forts, la mise à jour régulière des logiciels et la sensibilisation des utilisateurs aux risques potentiels. En outre, il est recommandé d'avoir recours à des solutions de sécurité informatique avancées pour une protection optimale contre les menaces en ligne [12].
2. **Confidentialité :** Les entreprises doivent être transparentes sur la manière dont elles collectent et utilisent ces données, ainsi que sur les mesures qu'elles

prennent pour les protéger contre les violations de sécurité et les abus. Il est également important que les utilisateurs soient conscients de leurs droits en matière de protection des données et qu'ils aient la possibilité de contrôler l'utilisation de leurs informations personnelles.

3. **Coût :** Cependant, les avantages qu'il offre peuvent être considérables en termes de productivité, d'efficacité et de rentabilité pour une entreprise. Il est donc important de peser le coût initial par rapport aux bénéfices à long terme avant de prendre une décision d'investissement dans un tel système.
4. **Complexité :** dans les environnements informatiques modernes. Cela peut entraîner des problèmes de compatibilité et de sécurité, nécessitant une gestion efficace des ressources et une expertise technique spécialisée pour maintenir un réseau stable et sécurisé. De plus, les mises à jour fréquentes des logiciels et des équipements peuvent également ajouter une complexité supplémentaire à la gestion du réseau.
5. **Dépendance :** De plus, une utilisation excessive de la technologie peut avoir des effets négatifs sur la santé mentale et physique des individus, tels que la fatigue oculaire, l'isolement social et le stress. Il est donc important de trouver un équilibre entre l'utilisation de la technologie et les activités hors ligne pour maintenir une vie saine et équilibrée.

II.9 Conclusion

Dans ce chapitre, nous avons abordé les concepts principaux de l'Internet des Objets qui sont les capteurs, le réseau, la plate forme IoT, le cloud et les applications de l'IoT. Ce chapitre est clôturé avec les avantages et les inconvénients de l'IoT.

Chapitre III

Conception du système

III.1 Introduction

Dans ce chapitre nous allons décrire notre solution qui consiste en une architecture permettant la représentation du système de contrôle d'accès par badge virtuel. L'objectif principal de ce système est d'améliorer la sécurité, de simplifier la gestion des autorisations d'accès et d'optimiser l'efficacité opérationnelle au sein des entreprises.

III.2 L'architecture générale de notre système

L'architecture générale de notre système de contrôle d'accès par badge virtuel basé sur un code QR est décrite comme suit :

— **Application mobile :** L'application mobile demande à l'utilisateur de s'authentifier en utilisant une adresse e-mail et un mot de passe fourni par l'administrateur (**étape 1**). Une fois l'utilisateur est authentifié, le système génère

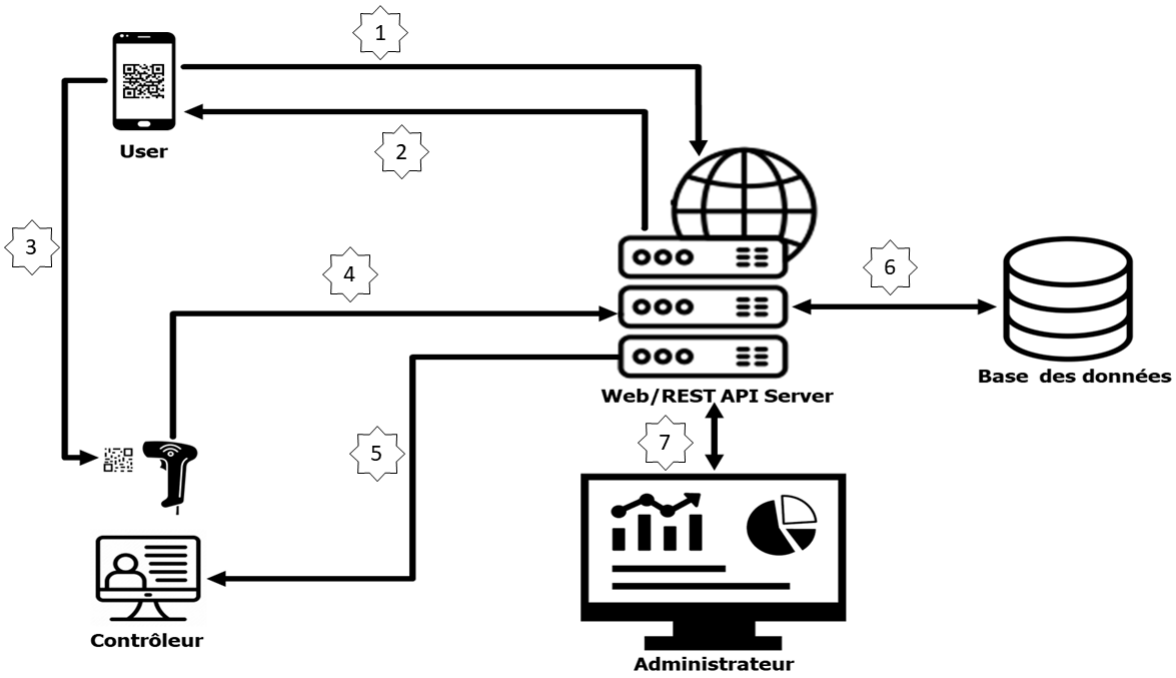

FIGURE III.1 – Architecture générale du notre système

un code QR unique en temps réel qui sera envoyé à l'application mobile représentant le badge d'accès (**étape 2**), pour éviter l'usurpation d'identité ou la falsification de badges, le QR code généré doit être valide uniquement pendant un laps de temps défini par l'administrateur. Cet intervalle de temps est par défaut égal à 5 minutes.

— **Vérification d'identité :** Pour accéder à la zone restreinte, l'utilisateur doit présenter (**étape 3**) le code QR à un contrôleur (lecteur de QR codes). Le lecteur lit le contenu du code QR, et le système vérifie la validité du code auprès d'un serveur central (**étape 4**).

Le serveur web est responsable de la gestion des codes QR et de la vérification d'identité et d'autorisation des utilisateurs. Si l'utilisateur est autorisé à accéder

à la zone restreinte, le serveur central envoie un signal au capteur pour déverrouiller la porte ou la barrière ou afficher les informations à l'agent qui contrôle l'accès (**étape 5**).

— **Interface administrateur :** L'interface administrateur offre aux administrateurs la possibilité de gérer les utilisateurs, leurs droits d'accès et les zones. De plus, les administrateurs peuvent consulter les statistiques d'accès afin d'améliorer leur compréhension des comportements qui contribuent au développement de l'organisation (**étape 7**).

— **Base de données :** La base de données stocke les informations essentielles liées aux utilisateurs, aux badges, aux autorisations d'accès et aux zones. Elle est conçue pour gérer efficacement les données nécessaires au fonctionnement du système (**étape 6**).

III.3 Architecture détaillée du système

Notre système basé sur l'architecture MVC (Model-View-Controller), MVC [8] est un modèle architectural logiciel largement utilisé dans le développement d'applications, en particulier celles basées sur le Web. Il sépare l'application en trois composants interconnectés :le modèle, la vue et le contrôleur.

1. **Modèle :** Le modèle représente les données et la logique métier de l'application. Il encapsule les données et définit comment elles peuvent être manipulées et accessibles. Il contient les règles et le comportement de l'application et les comportements tels que la validation des données, les calculs et les opérations de base de données.

2. **Vue :** La vue représente l'interface utilisateur de l'application el les données

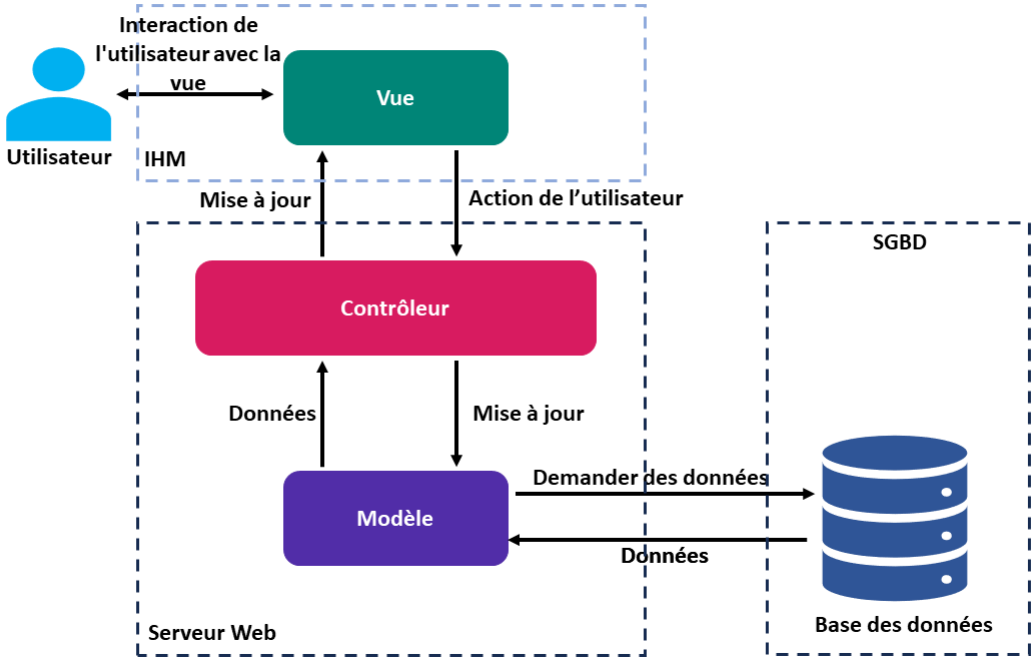

FIGURE III.2 – Architecture détaillée du système

relatives à son accès et la capture des interactions de l'utilisateur.

Les vues présentent les informations de notre modèle d'une manière visuellement attrayante et facile à utiliser. Il peut s'agir d'une page Web, d'un formulaire ou d'un autre composant de l'interface utilisateur.

3. **Contrôleur :** Un contrôleur agit comme un intermédiaire entre le modèle et la vue. Il reçoit les entrées de l'utilisateur à partir de la vue, les traite et met à jour le modèle en conséquence. Il gère les requêtes des utilisateurs, déclenche les actions appropriées dans les modèles et met à jour les vues avec des données mises à jour. Les contrôleurs contrôlent le flux et l'interaction des données au sein d'une application.

Le modèle MVC favorise une séparation des préoccupations, ce qui facilite le développement,

le test et la maintenance de l'application [15]. Il permet un développement modulaire, car chaque composant peut être développé indépendamment. Les modifications apportées à un composant n'affectent pas les autres tant que les interfaces entre eux restent inchangées.

III.3.1 l'interaction entre les composants de notre système

Dans cette section, nous allons expliquer en détails l'architecture de notre système.

III.3.1.1 Interface homme-machine (IHM)

Nous présenter deux interfaces principales : interface d'administration et interface utilisateur.

III.3.1.1.1 Interface d'administration : Elle est utilisée par les administrateurs et accessible via une plate-forme en ligne. Elle offre à l'administrateur la capacité de gérer les informations de l'organisation. Cela inclut les informations de l'utilisateur, En utilisant ce module, l'administrateur peut effectuer diverses tâches telles que Ajouter, mettre à jour et supprimer des enregistrements liés aux utilisateurs de l'organisation.

Ils peuvent également suivre les transactions et gérer des diverses activités. En général, le module vise à rationaliser les processus administratifs et à fournir une plate-forme centralisée pour la gestion de l'entreprise. Voici une explication de certaines des tâches du client dans ce contexte :

1. **Modifier les informations utilisateur** L'administrateur est chargé de mettre à jour les informations des utilisateurs. Il a la capacité de modifier les données personnelles telles que le nom, l'adresse, les coordonnées de contact, et autres.

2. **Définir les autorisations** L'administrateur donne aux utilisateurs la possibilité de définir et de gérer les privilèges au sein de l'organisation. Des accès et des autorisations différents sont attribués à chaque utilisateur en fonction de son rôle au sein de l'organisation. Les autorisations peuvent être configurées avec des paramètres tels que la lecture seule, l'écriture, l'accès à un ensemble spécifique d'informations.
3. **Surveiller les informations et les rapports** Les administrateurs peuvent utiliser pour surveiller les informations sur les utilisateurs et l'organisation et générer des rapports analytiques sur les performances et l'activité.

III.3.1.1.2 Interface d'utilisateur Cette Interface est conçue pour les personnes en relation avec cette Entreprise ou institution accessible via l'application mobile ou la plate-forme en ligne. Le module permet de vérifier l'identité de l'utilisateur et vérifier la validité des autorisations et les pouvoirs qui lui sont accordés.

Le processus de lecture du jeton d'accès via le badge virtuel, de vérification des informations et d'octroi de l'autorisation d'accès se déroulent généralement selon les étapes suivantes :

1. **Génération du code d'autorisation** Lorsqu'un utilisateur peut gagner le badge virtuel, son jeton d'autorisation est généré par l'application. Ce code est un code QR.
2. **Lecture du code d'autorisation** Lorsque l'utilisateur est prêt à accéder à une zone spécifique, un dispositif de lecture compatible (QR code) est utilisé pour lire le code d'autorisation du badge virtuel. Le dispositif de lecture est pointé sur le code et des informations en sont extraites.
3. **Vérification des informations** Une fois qu'un jeton d'autorisation est lu,

les informations cryptées contenues dans le jeton sont envoyées à un serveur ou système central pour vérification. L'information est analysée et décodée pour vérifier son authenticité et sa validité.

4. **Vérification d'identité et des autorisations** Les informations extraites du jeton d'autorisation sont comparées à la base de données associée au système. L'identité de l'utilisateur est vérifiée et les autorisations et pouvoirs qui lui sont accordés sont validés. Cela peut inclure la vérification d'informations telles que le nom de l'utilisateur, son rôle, son niveau d'autorisation et toute autre information pertinente supplémentaire.
5. **Autorisation d'entrée** Si les informations sont vérifiées et que l'identité et les autorisations sont vérifiées, l'autorisation d'accès est accordée à l'utilisateur.

III.3.1.2 Modèle & Base de données

III.3.1.2.1 Modèles Les modèles sont des classes qui sont liées à chaque table de la base de données et sont responsables de la manipulation des données de cette table. Chaque classe modèle est associée à une table spécifique dans la base de données et permet d'effectuer des opérations telles que l'ajout, la suppression, la mise à jour et l'interrogation des données de la table correspondante.

III.3.1.2.2 Schéma de base de données Le schéma de base de données fourni comprend plusieurs tables conçues pour stocker des informations liées à un système de gestion d'espace de travail. Les tables sont décrites ci-dessous :

1. **Categories** Cette table stocke les catégories de personnel liées à notre système. Chaque catégorie a un identifiant unique, des noms de catégorie en arabe et

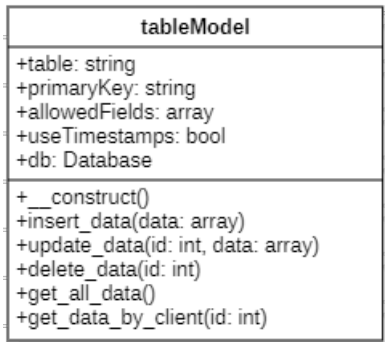

FIGURE III.3 – Classe modèle

en français, un ID du client associé, des horodatages de création et de mise à jour, ainsi qu'un indicateur indiquant si elle dispose de la fonctionnalité de pointage (suivi du temps).

2. **Clients** Cette table stocke des informations sur les clients ou les entreprises utilisant notre système de gestion. Elle comprend des champs tels que l'identifiant du client, les noms en français, en arabe et en anglais, le site web, les coordonnées de contact, la taille de l'entreprise, le statut premium, le jeton d'authentification, les horodatages de création et de modification, les informations de connexion, le navigateur utilisé, la plateforme, les indicateurs mobile et robot, l'adresse IP, la préférence linguistique et l'identifiant du pays associé.
3. **Countries** Cette table stocke des informations sur les pays. Chaque pays a un identifiant unique, des codes ISO à 2 et 3 caractères, des noms en arabe, en anglais, en espagnol et en français.
4. **entrance** Cette table contient des données relatives à les entrée (portes) des l'espace de travail. Elle stocke des informations telles que l'identifiant d'entrée, le nom d'utilisateur, le mot de passe hashé, l'ID du site associé, le numéro d'entrée et l'identifiant du client.

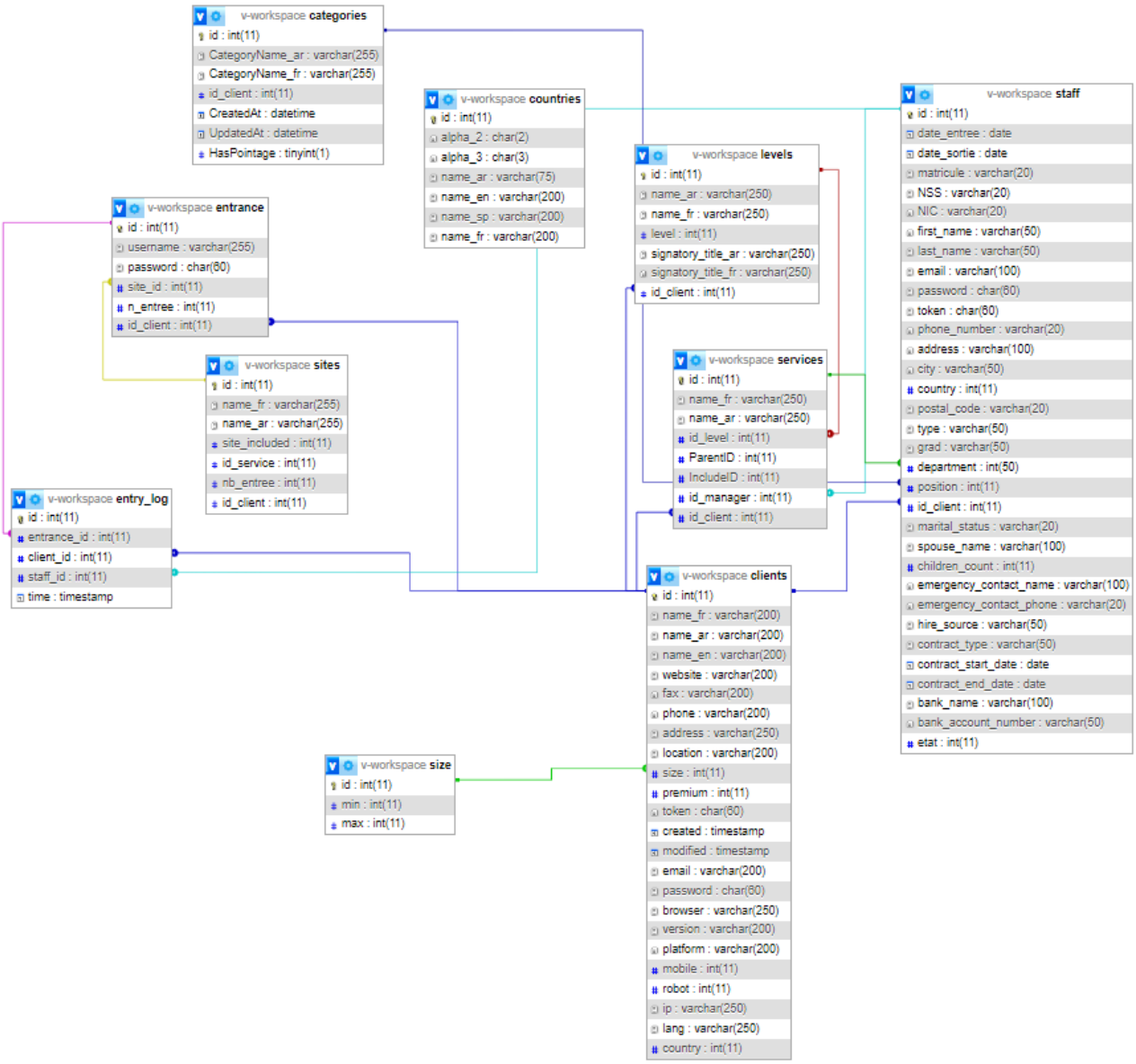

FIGURE III.4 – Le schéma de base de données

5. **Entry_log** Cette table enregistre le journal d'entrée des personnes dans l'espace de travail. Elle enregistre des informations telles que l'identifiant du jour-

nal d'entrée, l'ID de l'entrée, l'ID du client, l'ID du personnel et l'horodatage de l'entrée.

6. **Levels** Cette table représente différents niveaux organisationnels au sein de l'entreprise. Elle stocke l'identifiant du niveau, les noms en arabe et en français, la valeur du niveau, les titres des signataires en arabe et en français, ainsi que l'identifiant du client associé.
7. **Services** Cette table contient des informations sur les services offerts dans l'espace de travail. Elle comprend des champs tels que l'identifiant du service, les noms en français et en arabe, ainsi que l'identifiant du client associé.
8. **Sites** Cette table stocke des informations sur les sites physiques de l'espace de travail. Elle comprend des champs tels que l'identifiant du site, les noms en français et en arabe, l'adresse, la ville, le code postal, l'identifiant du pays associé, l'identifiant du client associé, les coordonnées de latitude et de longitude, ainsi que les horodatages de création et de mise à jour.
9. **Size** Cette table stocke des informations sur la taille des entreprises. Chaque taille a un identifiant unique, ainsi que des valeurs minimale (min) et maximale (max). Ces valeurs peuvent être utilisées pour représenter la taille des entreprises associées dans le système de gestion d'espace de travail.
10. **Staff** Cette table stocke des informations sur le personnel ou les employés travaillant dans l'espace de travail. Elle inclut l'identifiant du personnel, les dates d'entrée et de sortie, des identifiants uniques tels que le matricule, le NSS et le NIC, des détails personnels tels que le prénom, le nom, l'email, le mot de passe hashé, le jeton d'authentification, les informations de contact, l'adresse, la ville, le pays, le code postal, le type de personnel, la formation, le département, le poste, l'identifiant du client associé, le statut marital, le nom

du conjoint, le nombre d'enfants, les coordonnées du contact d'urgence, la source d'embauche, le type de contrat, les dates de début et de fin du contrat, le nom de la banque, le numéro de compte bancaire et l'état.

III.3.2 Fonctionnalité du système

Pour mieux comprendre la fonctionnalité du système, il serait préférable de le représenter sous forme de schéma, dans cette section nous donnerons une représentation de notre système sous forme d'un diagramme de séquence(figure III.5). et le schéma de base de données (figure III.4). Affiche toutes les actions que l'administrateur et l'utilisateur peuvent effectuer

1. **Étape 1**
   - L'administrateur se connecte au système.
   - L'administrateur ajoute toutes sortes d'utilisateurs différents.
   - L'administrateur gère les utilisateurs, donne les permission.
   - confirmation des message par le système.
2. **Étape 2**
   - Responsable se connecte au système.
   - Responsable gère les utilisateurs, modeler les permissions.
   - Responsable peut accéder aux informations des utilisateurs et donner les autorisations et les pouvoirs accordés à chaque utilisateur.
   - Responsable peut sortir des papiers appartenant à l'utilisateur.
   - confirmation des messages par le système.
3. **Étape 3**
   - L'utilisateur se connecte au système.
   - l'utilisateur reçoit un QR code.

— Communication entre l'utilisateur et le responsable.

— confirmation des message par le système.

4. **Étape 4**

— L'administrateur peut consulter les statistiques et les rapports.

— Afficher les statistiques et les rapports par le système.

— envoyer des alertes si des événements critiques se produisent par le système.

III.4 conclusion

Dans ce chapitre, nous avons présenté et décrit en détail la solution pour notre système de gestion d'accès via QR code. Nous avons présenté la structure générale du système, en plus, nous avons présenté une structure détaillée qui présente des fonctions de chaque composant utilisés dans le système.

En outre, nous avons discuté la fonctionnalité du système et représenté l'architecture du système à travers un diagramme de séquence.

Dans la section suivante, nous discuterons de la mise en œuvre de notre système. Nous fournirons des détails sur la façon dont le système est mis en œuvre et les technologies utilisées.

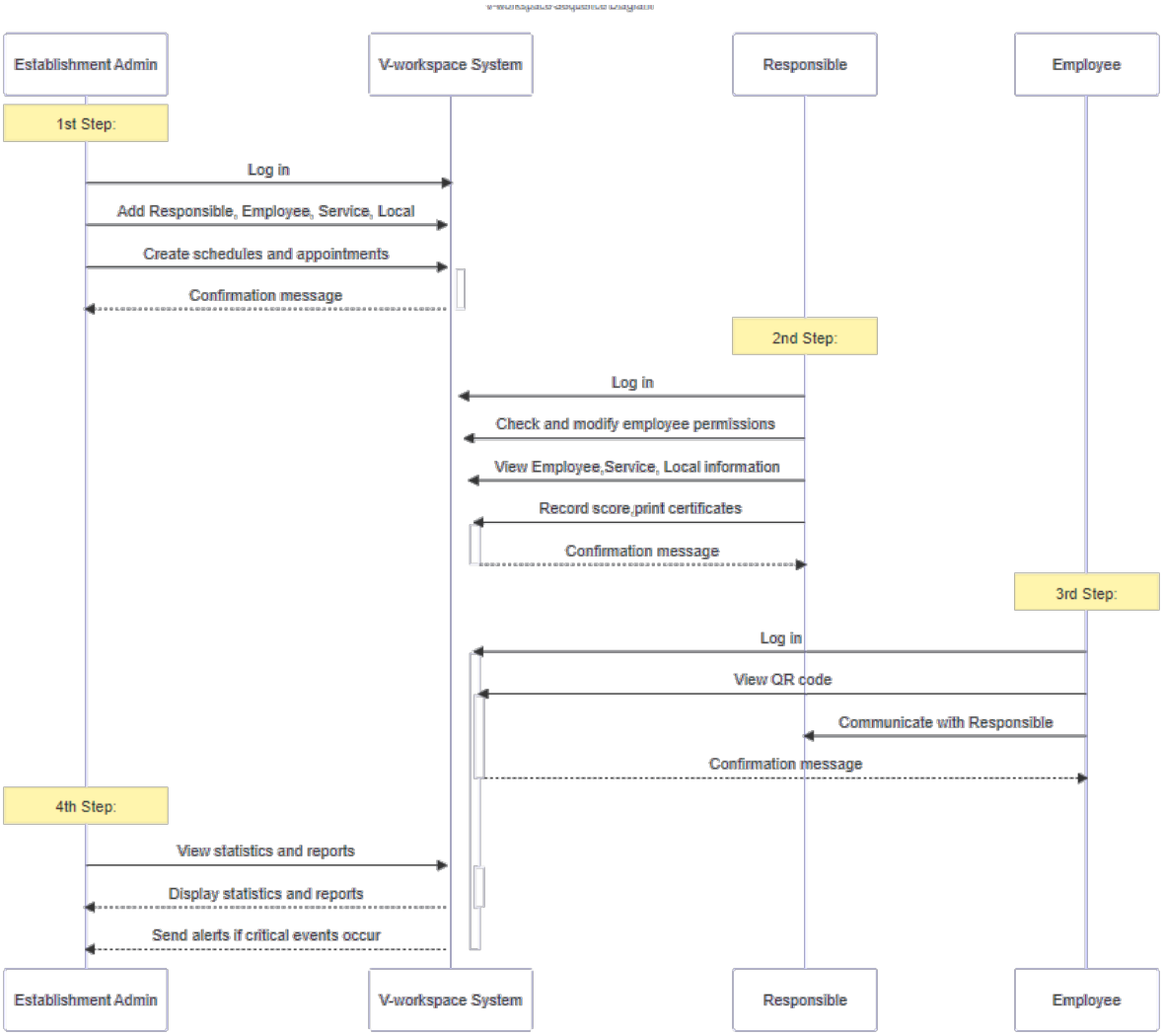

FIGURE III.5 – Diagramme de séquence de notre système

Chapitre IV

Implémentation du Systéme

IV.1 Introduction

Après avoir détaillé l'architecture du système de gestion d'entreprise et décrit le concept principal de notre solution dans le dernier chapitre, nous nous concentrerons dans ce chapitre sur la mise en œuvre et le côté pratique du projet.

Nous commencerons le chapitre en présentant les logiciels et les outils utilisés dans le projet. Ensuite, nous présenterons les résultats obtenus sous forme de captures d'écran et d'images.

IV.2 Outils logiciels

Nous avons utilisé JavaScript, HTML et CSS pour le tableau de bord Web V-workspace, ainsi que les frameworks Laravel et Bootstrap pour l'efficacité du développement. Laravel a fourni des fonctionnalités utiles telles que les migrations de bases de données, l'authentification des utilisateurs et le routage, tandis que Boots-

trap a proposé des composants et des styles d'interface utilisateur préconçus pour un tableau de bord d'aspect professionnel.

Cette combinaison d'outils nous a aidés à créer facilement un V-workspace convivial et fonctionnel.

IV.2.1 JavaScript

JavaScript est un langage de programmation de haut niveau, polyvalent et interprété. Il est largement utilisé pour le développement web côté client, ce qui signifie qu'il est exécuté dans le navigateur des utilisateurs. JavaScript permet d'ajouter des fonctionnalités interactives, de manipuler le contenu des pages web, de réagir aux actions de l'utilisateur et de communiquer avec les serveurs.JavaScript est un élément essentiel du développement Web moderne, aidant à améliorer l'expérience utilisateur, à ajouter de l'interactivité aux pages Web et à créer des applications Web dynamiques.[21]

IV.2.2 Laravel

Laravel est un framework PHP open source robuste et facile à comprendre. Il suit un modèle de conception modèle-vue-contrôleur. Laravel réutilise les composants existants de différents frameworks qui aide à créer une application web. L'application web ainsi conçue est plus structurée et pragmatique. Laravel offre un riche ensemble de fonctionnalités qui intègre les fonctionnalités de base des frameworks PHP comme CodeIgniter, Yii et d'autres langages de programmation comme Ruby on Rails. Laravel est très riche ensemble de fonctionnalités qui augmenteront la vitesse de développement Web [31].

IV.2.3 Bootstrap

Bootstrap est un framework de développement Web gratuit et open-source. Il est conçu pour faciliter le web processus de développement de sites Web réactifs et mobiles en fournissant une collection de syntaxe pour les conceptions de modèles.

En d'autres termes, Bootstrap aide les développeurs Web à créer des sites Web plus rapidement car ils n'ont pas à s'inquiéter sur les commandes et fonctions de base. Il se compose de scripts HTML, CSS et JS pour diverses fonctions et composants liés à la conception Web. L'objectif principal de Bootstrap est de créer des sites Web réactifs et mobiles. Il assure toutes les interfaces les éléments d'un site Web fonctionnent de manière optimale sur toutes les tailles d'écran. Bootstrap est disponible en deux variantes - précompilé et basé sur une version de code source.

Les développeurs expérimentés préfèrent ce dernier car il leur permet de personnaliser les styles en fonction de leurs projets.[25]

IV.2.4 Flutter

Flutter est un framework d'interface utilisateur mobile gratuit et open-source créé par Google et sorti en mai 2017. En quelques mots, il permet de créer une application mobile native avec une seule base de code. Cela signifie que le développeur peut utiliser un langage de programmation et une base de code pour créer deux applications différentes (pour iOS et Android). Flutter se compose de deux parties importantes :

Un SDK (Software Development Kit) : Une collection d'outils qui sont utiles pour développer applications. Cela inclut des outils pour compiler un code en code machine natif (code pour iOS et Androïd).

Un framework (bibliothèque d'interface utilisateur basée sur des widgets) : une

collection d'éléments d'interface utilisateur réutilisables (boutons, entrées de texte, curseurs, etc.) que chacun peut personnaliser selon ses propres besoins.[10]

IV.2.5 XAMPP

XAMPP est une abréviation où X signifie Cross-Platform, A signifie Apache, M signifie MYSQL et Ps signifie PHP et Perl, respectivement.

Il s'agit d'un package Web open source solutions qui incluent la distribution Apache pour de nombreux serveurs et exécutables de ligne de commande ainsi que des modules tels que le serveur Apache, MariaDB, PHP et Perl.

XAMPP aide un hôte ou un serveur local à tester son site Web et ses clients via des ordinateurs et des ordinateurs portables avant de le diffuser sur le serveur principal. C'est une plate-forme qui fournit un environnement approprié pour tester et vérifier le fonctionnement de projets basés sur Apache, Perl, la base de données MySQL et PHP via le système de l'hôte lui-même Parmi ces technologies.

L'architecture du système V- workspace a été conçue dans un souci d'évolutivité, de sécurité et de facilité de maintenance.il donne au admin une vision globale du travail de l'institution et de son évolution, et l'aide à étudier Comportements des travailleurs, c'est-à-dire il facilite la gestion des utilisateurs.[1]

IV.2.6 AJAX

AJAX est une approche du développement d'applications Web utilisant une combinaison de technologies Web établies.

XMLHttpRequest est une API implémentée par la plupart des moteurs de script de navigateur Web modernes pour transférer des données vers et depuis un serveur Web à l'aide de HTTP, en établissant un canal de communication indépendant en

arrière-plan entre un client Web et un serveur.

L'adoption d'AJAX est devenue une option sérieuse non seulement pour les applications nouvellement développées, mais également pour la migration de sites Web existants afin d'augmenter la réactivité.

Le style REST rend impossible une requête HTTP initiée par le serveur, empêchant les serveurs d'envoyer des notifications asynchrones sans une demande du client. Il existe plusieurs solutions utilisées dans la pratique qui permettent toujours au client de recevoir des mises à jour (presque) en temps réel du serveur.[24]

IV.3 Fenêtres principales de l'application

On va présenter les fenêtres principales de notre application et les taches importantes pour l'utilisateur.

IV.3.1 Page Login

Lors de l'accès à notre site Web, la page de connexion (Figure IV.1) s'affiche. Il se compose des éléments suivants :

1. **E**mail Input : Un champ de saisie est fourni pour saisir l'adresse e-mail de l'utilisateur. Cela permet aux utilisateurs de fournir leurs identifiants de connexion.
2. **P**assword Input : Un champ de saisie de mot de passe est disponible pour que les utilisateurs saisissent leurs mots de passe respectifs en toute sécurité.
3. **M**ot de passe oublié ? :Si les utilisateurs oublient leur mot de passe, un lien est fourni pour les aider à récupérer leur compte. Cliquer sur ce lien redirige

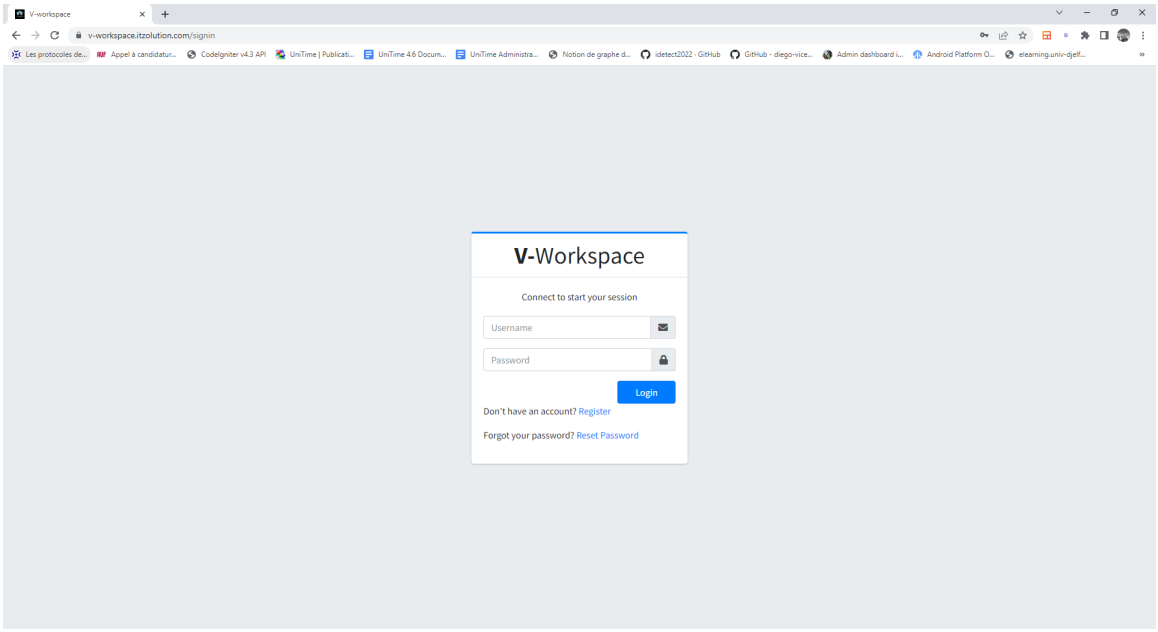

FIGURE IV.1 – Page login

les utilisateurs vers le processus de récupération du mot de passe (figure IV.2).

4. **B**outon login : Un bouton proéminent est placé sur la page, permettant aux utilisateurs d'initier le processus de connexion et d'accéder à leurs comptes en toute sécurité

Si l'utilisateur n'a pas été inscrée auparavant, il doit d'abord inscrée (Figure IV.3).

IV.3.2 Page d'inscription

La page d'inscription permet aux invités de créer un compte et d'accéder à toutes les fonctionnalités du système (Figure IV.3).

1. **Saisie du nom** : un champ de saisie de texte est fourni pour que les utilisateurs saisissent leur nom lors du processus d'inscription.

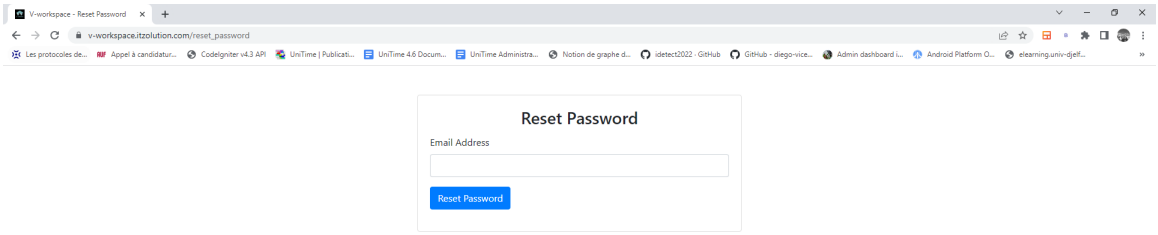

FIGURE IV.2 – Réinitialiser le mot de passe

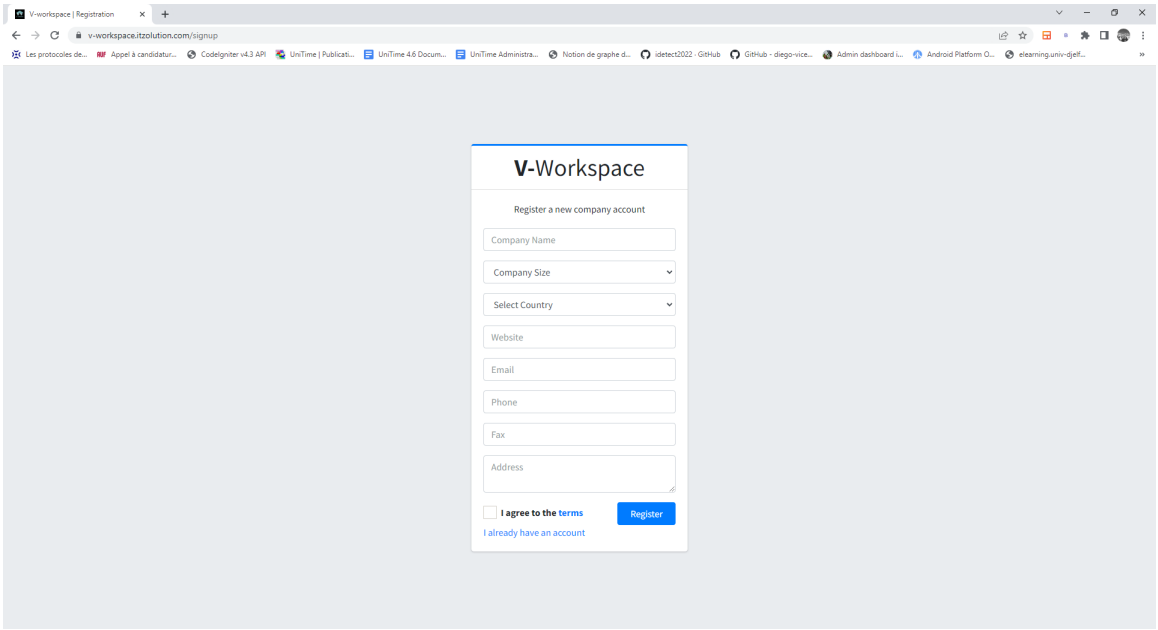

FIGURE IV.3 – Page d'inscription

2. **Email Input** : un champ de saisie est disponible pour que les utilisateurs saisissent leur adresse e-mail, qui sera utilisée comme identifiant de connexion.
3. **Captcha** : un composant captcha est inclus pour assurer la sécurité du processus d'inscription et empêcher les soumissions automatisées. Les utilisateurs peuvent être tenus de relever un défi visuel ou interactif pour vérifier leur authenticité.
4. **Bouton d'inscription** : un bouton visible est placé sur la page pour lancer le processus d'inscription et créer un nouveau compte.
5. **Modal Enregistrement réussi** : une fenêtre modale apparaît, demandant à l'utilisateur de vérifier son adresse email pour continuer le processus d'enregistrement. L'utilisateur doit cliquer sur le lien de vérification envoyé à son e-mail pour entrer le mot de passe.

IV.3.2.1 Page de mot de passe

Après avoir cliqué sur le lien de définition du mot de passe reçu dans l'email, les utilisateurs sont redirigés vers la page "Définir le mot de passe". Cette page permet aux utilisateurs de définir en toute sécurité un nouveau mot de passe pour leur compte. Les étapes suivantes sont impliquées dans le processus :

1. **Suivre le lien du mot de passe** L'utilisateur clique sur le lien de réinitialisation du mot de passe fourni dans l'émail.
2. **Le lien du mot de passe** Le lien contient un jeton unique qui est associé au compte de l'utilisateur et garantit l'authenticité de la demande.
3. **Formulaire de définition du mot de passe** Lorsque l'utilisateur arrive sur la page "Définir le mot de passe", un formulaire lui est présenté pour saisir le mot de passe.

— Mot de passe : les utilisateurs peuvent saisir le mot de passe souhaité dans ce champ. Il est recommandé de définir des mots de passe forts qui incluent une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux pour une sécurité renforcée.

— Confirmer le mot de passe : les utilisateurs doivent ressaisir leur nouveau mot de passe dans ce champ pour garantir l'exactitude.

Si l'enregistrement est terminé avec succès, l'utilisateur est redirigé vers la page de connexion.

IV.3.3 Administrateur

Les utilisateurs disposant de privilèges administratifs ont un accès complet à toutes les fonctions et fonctionnalités de la plateforme. Ils peuvent gérer les comptes d'utilisateurs, les rôles et les autorisations, configurer les paramètres et les préférences du système, générer des rapports et effectuer des tâches administratives.

-Tableau de bord Une fois connectés, les administrateurs sont dirigés vers leur tableau de bord personnalisé, qui fournit un aperçu des informations pertinentes et un accès rapide aux fonctionnalités correspondant au rôle qui leur est attribu (Figure IV.4).

IV.3.3.1 Structures

Cette interface structures pour ajouter tout les structures de l'entreprise.

IV.3.3.2 Staff

Cette interface staff c'est une liste des utilisateurs et tout les informations leur propre au sein d'entrpris. Où l'administrateur peut ajouter et supprimer des infor-

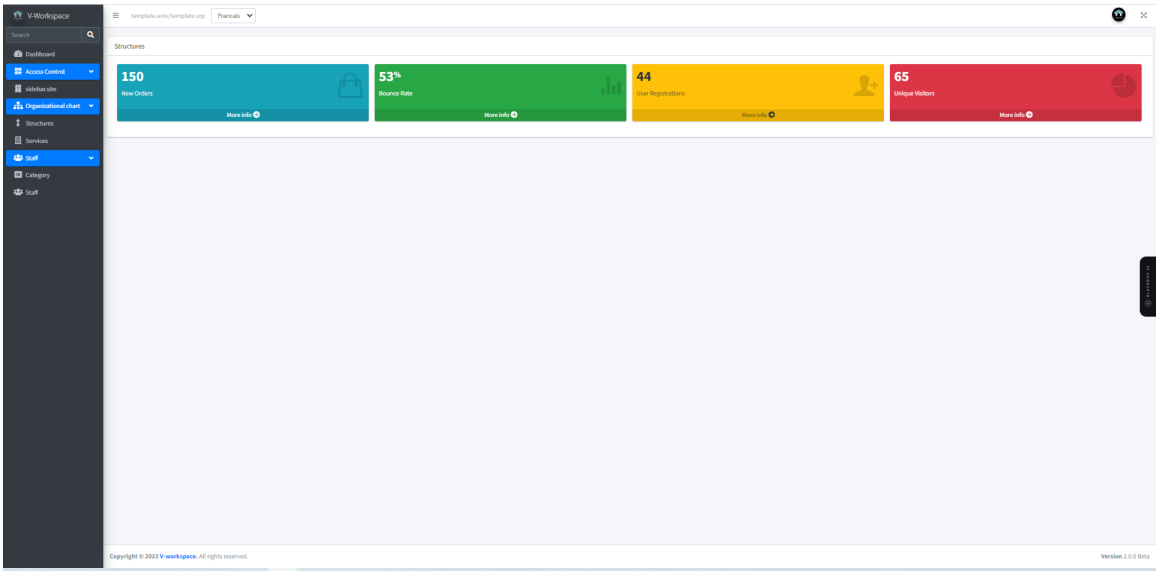

FIGURE IV.4 – Interface d'administrateur

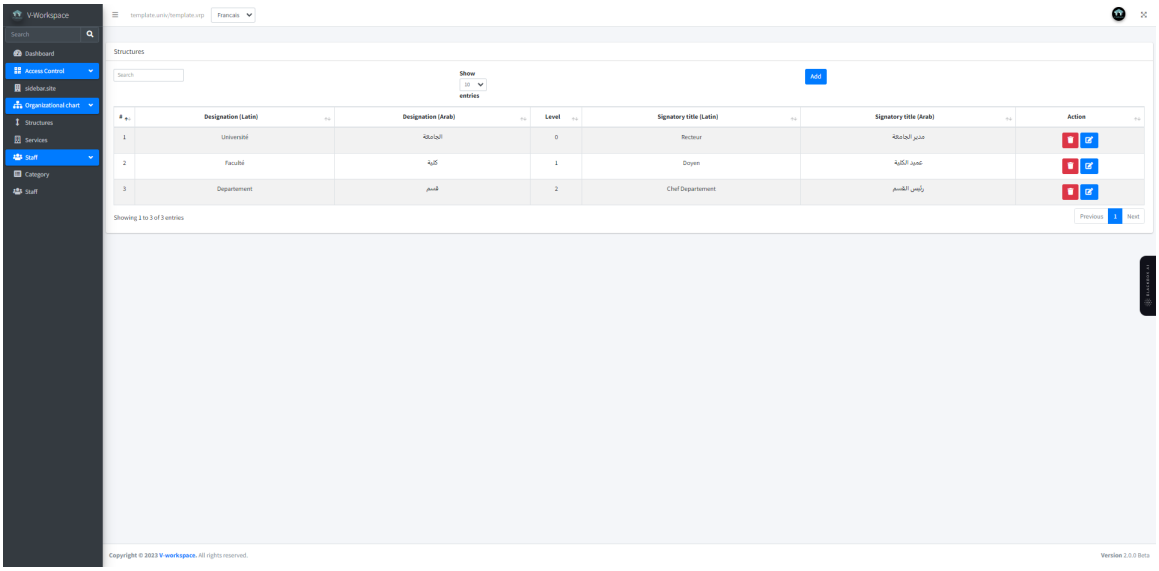

FIGURE IV.5 – Structure

mations(Figure IV.7).

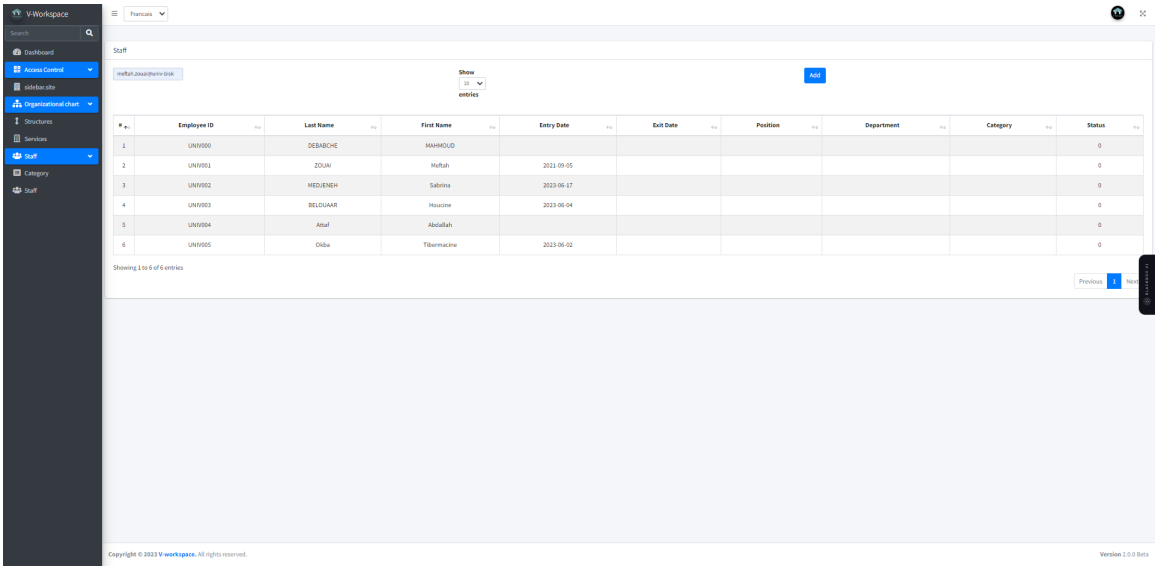

FIGURE IV.6 – Staff

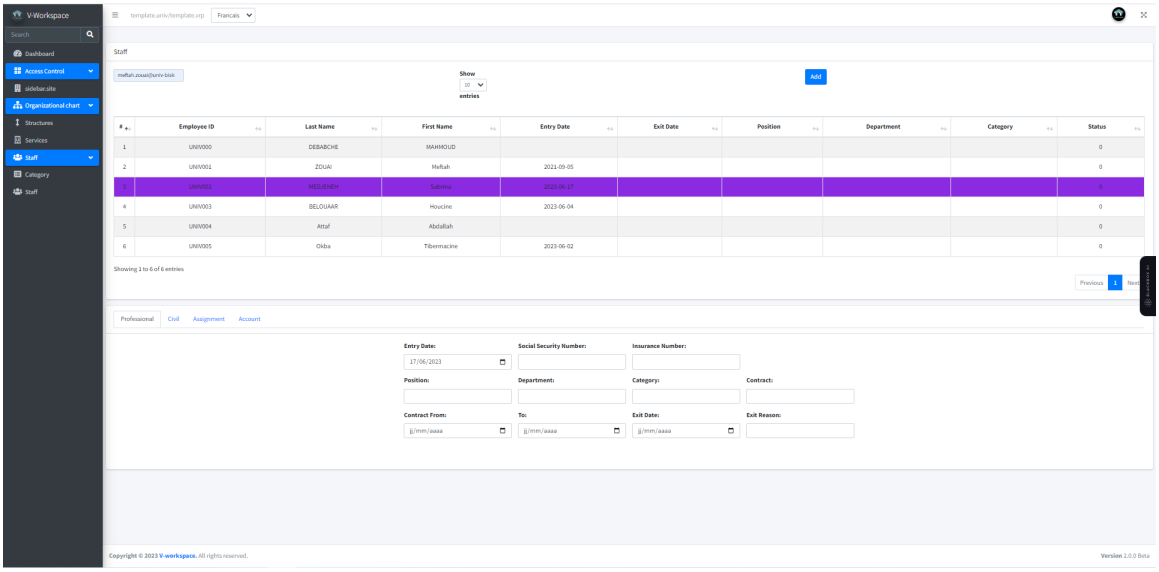

FIGURE IV.7 – Staff mod

IV.3.3.3 Service

Cette page défini les service existant dans l'entreprise.

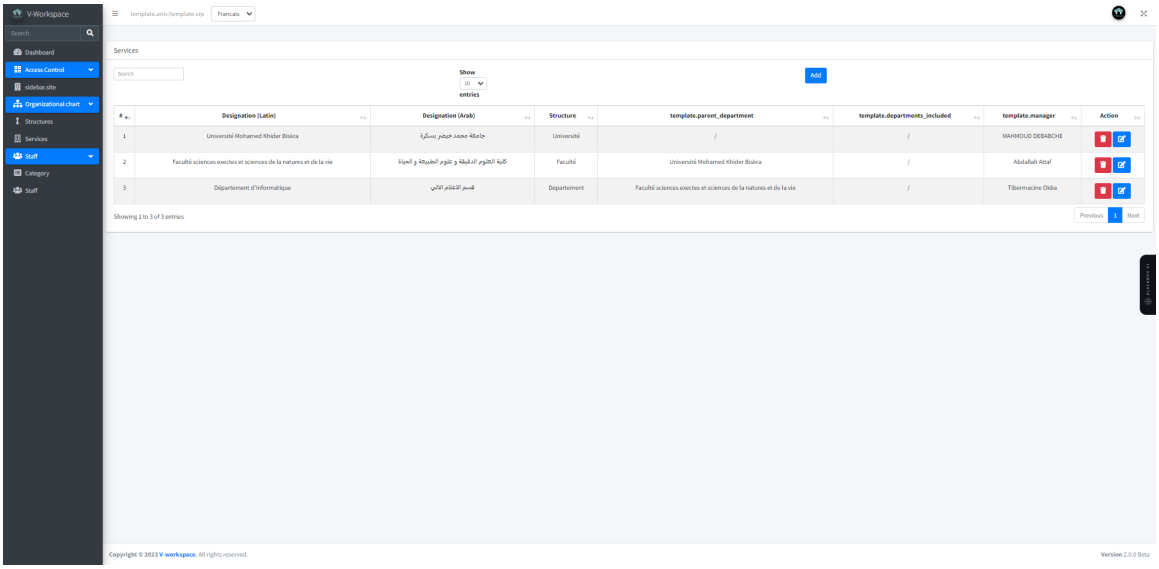

FIGURE IV.8 – Service

Cette fenêtre pour ajout un nouvelle service(Figure IV.9).

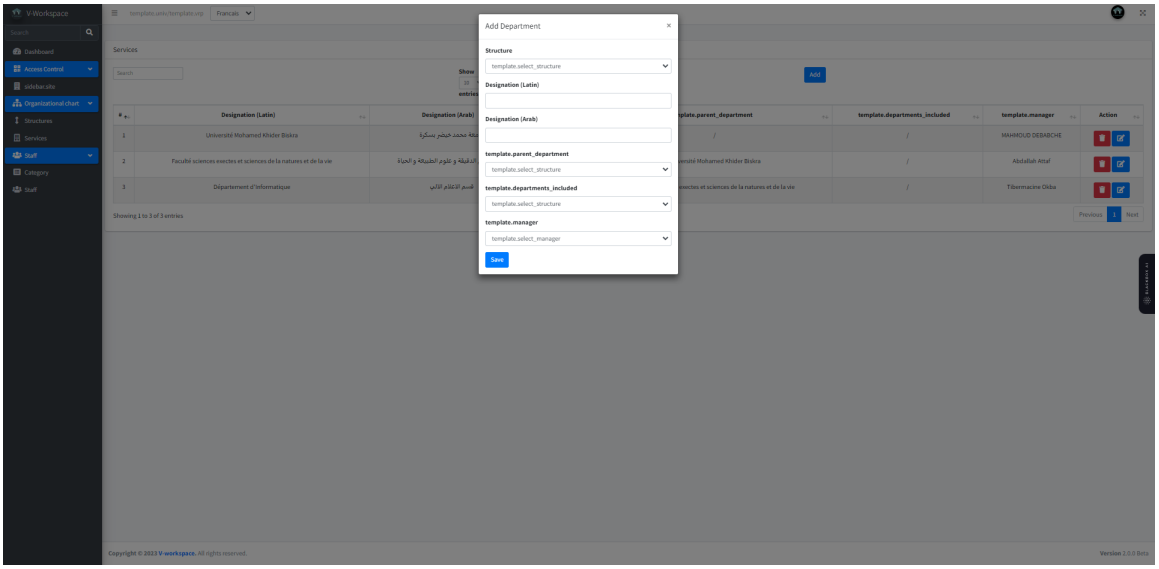

FIGURE IV.9 – Ajout service

IV.3.3.4 Chef service

Les utilisateurs disposant de privilèges de services de chef ont un accès presque complet aux fonctionnalités de la plate-forme, mais cela ne peut être appliqué que pour gérer leur service.

- Tableau de bord : Après la connexion, les services du chef sont dirigés vers leur tableau de bord personnalisé et ont une vue sur leur service, qui fournit un aperçu des informations pertinentes et un accès rapide aux fonctionnalités correspondant au rôle qui leur est attribué.

IV.3.4 Application mobile

Le badge représente les utilisateurs au sein de l'organisation.

Une fois que l'utilisateur s'est connecté à l'aide du nom d'utilisateur et du mot de passe, il obtient un code QR, qui représente le badge virtuel (Figure IV.10) .

IV.3.5 Contrôleur

IV.3.5.1 Contrôleur login

Cette page de connexion est destinée au controleur, et se compose des éléments suivants : saisie du nom d'utilisateur et du mot de passe, qui sont déterminés par l'entreprise

IV.3.5.2 Interface contrôler

interface de contrôleur pour vérifie les autorisation d'accès.ET la vérification se fait en lisant le code QR (Figure IV.12). Après avoir scanner le code QR, et si

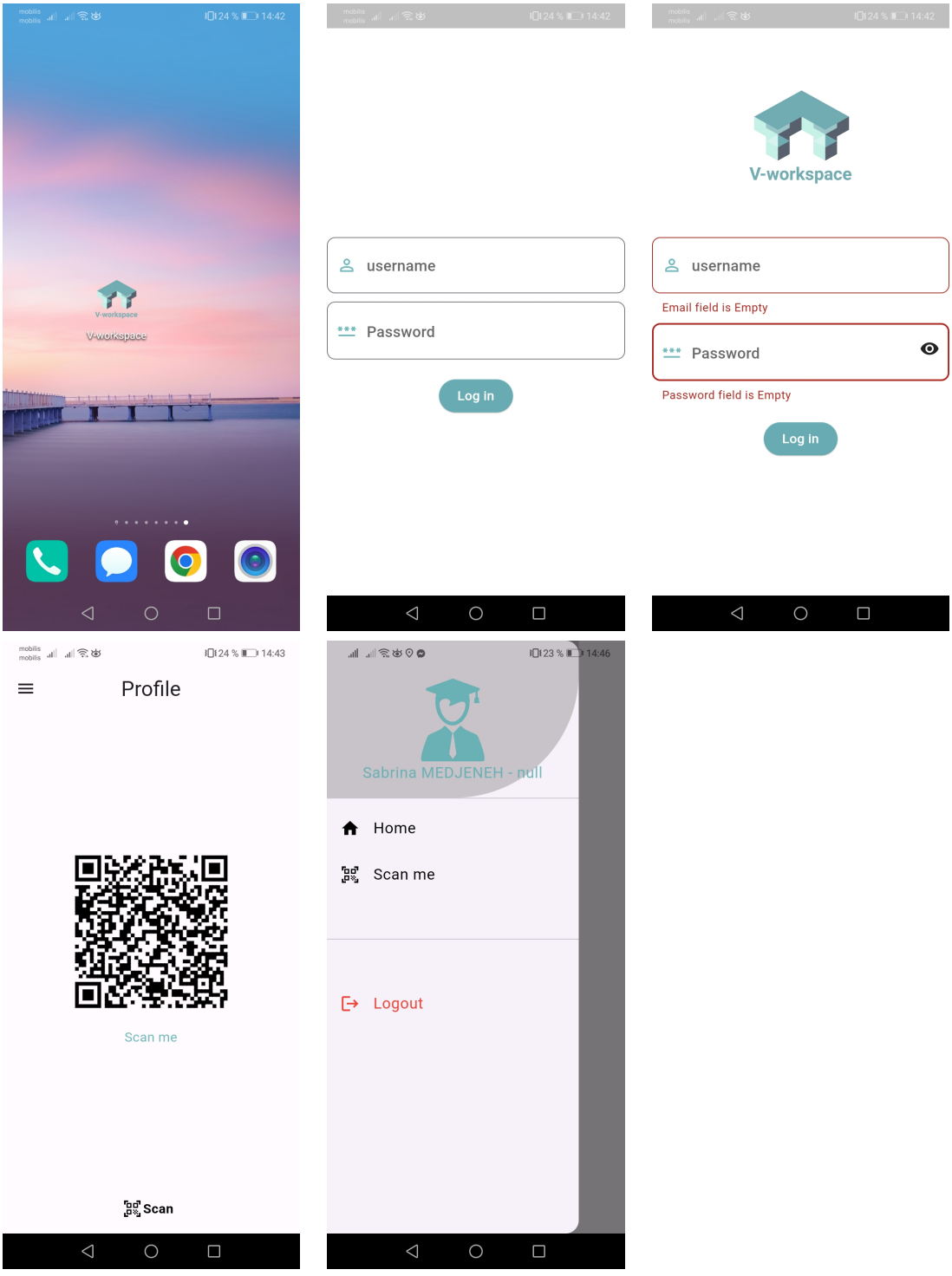

FIGURE IV.10 – Application mobile.

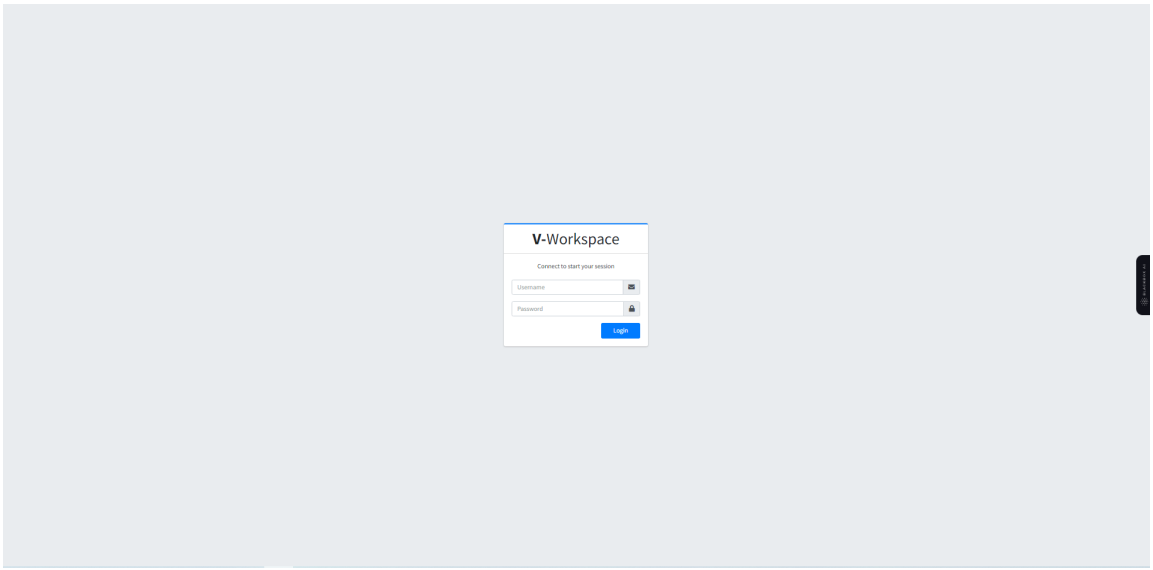

FIGURE IV.11 – Contrôler login

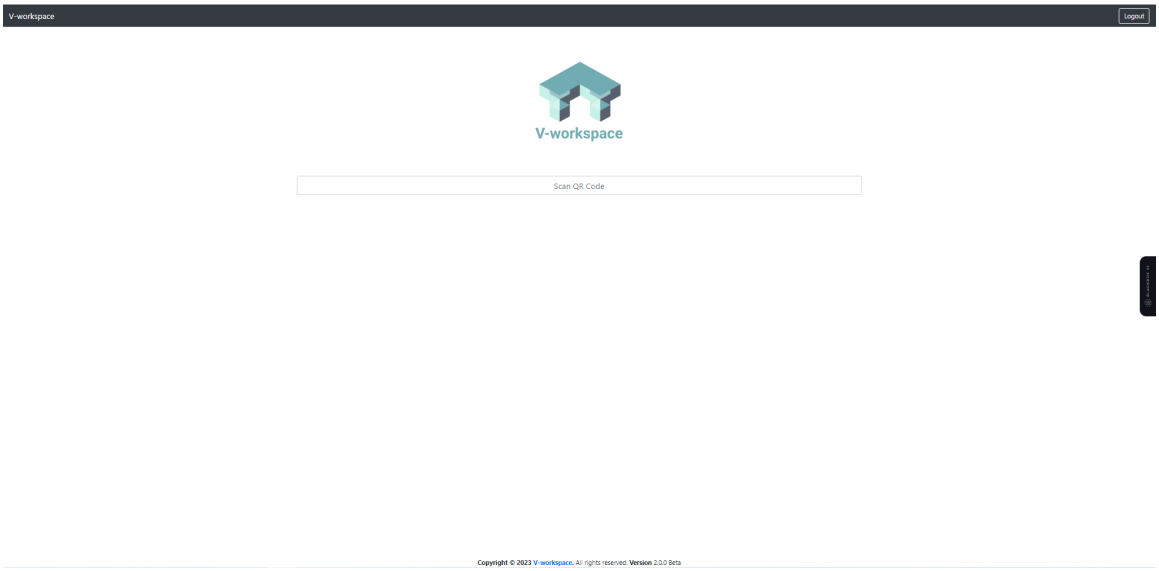

FIGURE IV.12 – Interface contrôler

l'utilisateur est enregistré auprès de l'entreprise, ses informations apparaîtront dans l'interface du contrôleur(Figure IV.13)

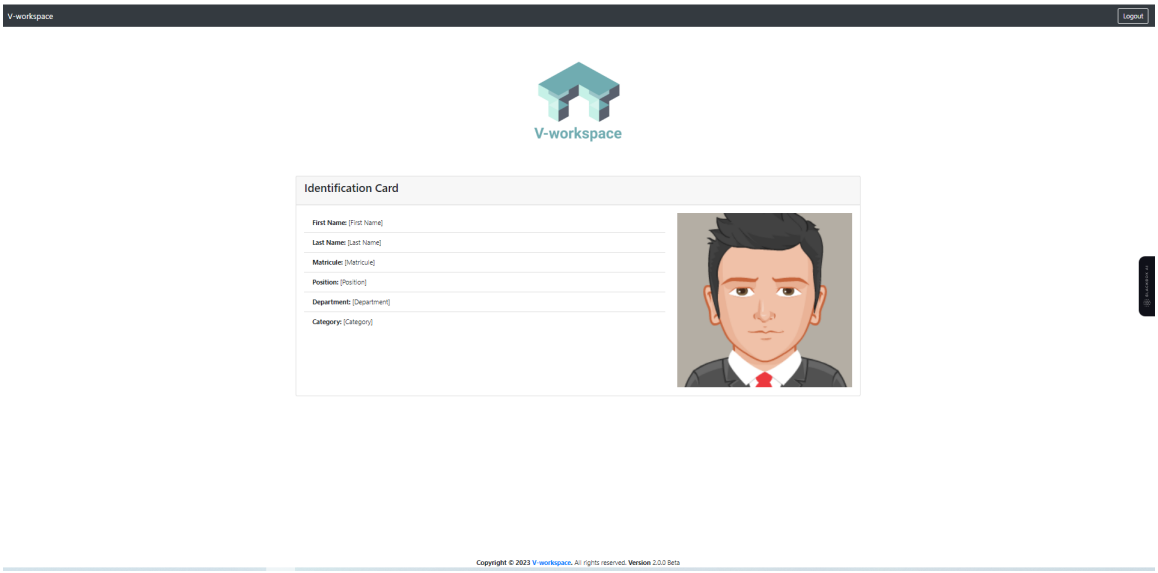

FIGURE IV.13 – Validation du QR code.

IV.4 Conclusion

En conclusion, ce chapitre a approfondi la mise en œuvre de notre solution de badge virtuel (V-workspace). Nous avons montré les outils logiciels utilisés dans le processus de développement, en soulignant leur importance. De plus, nous avons introduit un tableau de bord Web complet, soigneusement conçu avec des pages séparées conçues pour les entreprises, qui favorise une interaction fluide et une gestion globale de l'entreprise.

Une application mobile développée pour les utilisateurs est également mise en avant comme badge virtuel, démontrant la facilité d'accès et la commodité offerte par notre système.

Conclusion Générale

Dans ce mémoire, nous avons présenté notre système de contrôle d'accès par badge virtuel. Le premier chapitre portait sur les techniques de contrôle d'accès, les types et les avantages et inconvénients de chaque type et la différence entre eux.

Tandis que le deuxième chapitre portait sur l'internet des objets et certains concepts qui s'y rapportent, son fonctionnement, son architecture ses structures et ses domaines.

Dans le troisième chapitre nous avons présenté la structure générale et détaillée de notre système et explique son fonctionnement. Comme continuité de ce travail, nous envisagerons d'étendre à un ERP.

Enfin, nous avons affiché l'exécution de notre système et les interfaces principales avec une explication sur leurs fonctionnalités.

Bibliographie

[1] Zaenal Abidin and Alwi Mahatir. Alat monitoring kehadiran karyawan wpk dengan smartcard rfid berbasis iot via web xampp. *SinarFe7*, 5(1) :28–32, 2022.

[2] Elke Altenburger. Alarm will sound : Student perceptions of risk-free space at school. *Children, Youth and Environments*, 33(1) :50–75, 2023.

[3] MWEPU MWANSA Andy. Implémentation d'un système de contrôle d'accès à une maison et à son éclairage (domotique).

[4] Julian Ashbourn. *Biometrics : advanced identity verification : the complete guide*. Springer, 2014.

[5] José A Barriga, Pedro J Clemente, Miguel A Pérez-Toledano, Elena Jurado-Málaga, and Juan Hernández. Design, code generation and simulation of iot environments with mobility devices by using model-driven development : Simulateiot-mobile. *Pervasive and Mobile Computing*, page 101751, 2023.

[6] Huseyin Cavusoglu, Zhuolun Li, and Seung Hyun Kim. How do virtual badges incentivize voluntary contributions to online communities ? *Information & Management*, 58(5) :103483, 2021.

[7] Steven Commander et al. Le moment est-il venu de mettre à niveau votre système de contrôle d'accès ?–global security mag online. 2023.

[8] Yuvi Darmayunata, Mariza Devega, and Yuhelmi Yuhelmi. Development of web-based single channel multi steps online queuing system with model view controller. *Sinkron : jurnal dan penelitian teknik informatika*, 8(1) :390–397, 2023.

[9] Sophie Dramé-Maigné. Blockchain et contrôle d'accès : Vers un internet des objets plus sécurisé.

[10] Muhammad Akbar Faiz, Dana Sulistiyo Kusumo, and Muhammad Johan Alibasa. Flutter framework code portability measurement on multiplatform applications with iso 9126. In *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*, pages 36–40. IEEE, 2022.

[11] Nurul Farida and Muhamad Syauqillah. Ring of security review on the vital objects of the electricity subfield. *Jurnal Ekonomi*, 12(02) :1248–1258, 2023.

[12] Apostolos Gerodimos, Leandros Maglaras, Mohamed Amine Ferrag, Nick Ayres, and Ioanna Kantzavelou. Iot : Communication protocols and security threats. *Internet of Things and Cyber-Physical Systems*, 2023.

[13] Nana Kwame Gyamfi, Mustapha Adamu Mohammed, Kwaku Nuamah-Gyambra, Ferdinand Katsriku, and Jamal-Deen Abdulah. Enhancing the security features of automated teller machines (atms) : A ghanaian perspective. *International Journal of Applied Science and Technology*, 6(1), 2016.

[14] Ahmad Khalil, Nader Mbarek, and Olivier Togni. Adaptation du contrôle d'accès pour la sécurité de l'iot, 2022.

[15] Jyoti Khandelwal. Model view controller frameworks for mobile view website. In *Designing and Developing Innovative Mobile Applications*, pages 250–266. IGI Global, 2023.

[16] Ali Khider. *Un système biométrique multimodal basé sur la fusion visage-iris*. PhD thesis, 2023.

[17] Elam Kyungu Lukomba, Bertin Umba Nkulu, Grace Mwangal Kapend, Placide Mwepu Malango, Vivien Mumba Kyankasu, and Penouël Hemedykahola. Système de pointage des agents par badge électronique rfid à la direction des recettes du lualaba. *International Journal of Innovation and Applied Studies*, 39(2) :631–642, 2023.

[18] Manon Maricq and Nadia Steils. Smart homes technologies : do they really help households to reduce their energy consumption ?

[19] P Navya and D Sudha. Artificial intelligence-based robot for harvesting, pesticide spraying and maintaining water management system in agriculture using iot. In *AIP Conference Proceedings*, volume 2523. AIP Publishing, 2023.

[20] Guadalupe Ortiz, Meftah Zouai, Okba Kazar, Alfonso Garcia-de Prado, and Juan Boubeta-Puig. Atmosphere : Context and situational-aware collaborative iot architecture for edge-fog-cloud computing. *Computer Standards & Interfaces*, 79 :103550, 2022.

[21] Addy Osmani. *Learning JavaScript design patterns*. " O'Reilly Media, Inc.", 2023.

[22] P Jonathon Phillips, Alvin Martin, Charles L Wilson, and Mark Przybocki. An introduction evaluating biometric systems. *Computer*, 33(2) :56–63, 2000.

[23] Vu Khanh Quy, Nguyen Van Hau, Dang Van Anh, Nguyen Minh Quy, Nguyen Tien Ban, Stefania Lanza, Giovanni Randazzo, and Anselme Muzirafuti. Iot-enabled smart agriculture : architecture, applications, and challenges. *Applied Sciences*, 12(7) :3396, 2022.

[24] Hendi Rahmat. Penerapan asynchronous javascript and xml pada form desain kaos drag and drop website start-up kaosyay. *Jurnal Teknologi Pintar*, 3(5), 2023.

[25] NV Ravindhar, Sai Sonica CH, M Kiruthiga, et al. Product rental web application using html, css, bootstrap, php, and sql. In *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*, pages 1368–1371. IEEE, 2023.

[26] Soroor Rezaei. *Utilisation de la blockchain pour les données médicales et le contrôle d'accès en e-Santé*. PhD thesis, Université Laval, 2022.

[27] Yousaf Murtaza Rind, Muhammad Haseeb Raza, Muhammad Zubair, Muhammad Qasim Mehmood, and Yehia Massoud. Smart energy meters for smart grids, an internet of things perspective. *Energies*, 16(4) :1974, 2023.

[28] Adel ROZTANE and Weam ALI MERINA. *Utilisation des objets connectés dans la gestion efficace des poteaux incendie.* PhD thesis, Directeur : Mr MEGNAFI Hicham/Co-Directeur : Mr BENNACER Djamel, 2022.

[29] Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, and Burkhard Stiller. Landscape of iot security. *Computer Science Review*, 44 :100467, 2022.

[30] Rajagopal Sudarmani, Kanagaraj Venusamy, Sathish Sivaraman, Poongodi Jayaraman, Kannadhasan Suriyan, and Manjunathan Alagarsamy. Machine to machine communication enabled internet of things : a review. *Int J Reconfigurable & Embedded Syst ISSN*, 2089(4864) :4864, 2022.

[31] Andri Sunardi et al. Mvc architecture : A comparative study between laravel framework and slim framework in freelancer project monitoring system web based. *Procedia Computer Science*, 157 :134–141, 2019.

[32] Ramesh Velumani, Hariharasitaraman Sudalaimuthu, Gaurav Choudhary, Srinivasan Bama, Maranthiran Victor Jose, and Nicola Dragoni. Secured secret sharing of qr codes based on nonnegative matrix factorization and regularized super resolution convolutional neural network. *Sensors*, 22(8) :2959, 2022.

[33] Meftah Zouai, Abdelhak Merizig, Ichrak Boudjelkha, Houcine Belouaar, Okba Kazar, Guadalupe Ortiz, Abderrahmane Lakas, and Zina Houhamdi. Design and development of an iot-based solar powered camouflaged robot for military applications. In *2022 International Arab Conference on Information Technology (ACIT)*, pages 1–6. IEEE, 2022.

[34] M Willy Zwaenepoel, M Marc Shapiro, M Renaud Lachaize, and M Noël DE PALMA. Résilience et dimensionnement dans des environnements virtualisés.