الجمهوريةالجزائريةالديمقراطيةالشعبية
République Algérienne démocratique et populaire

وزارةالتعليمالـعـاليوالبحـثالعـلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـامعةسعددحلبالبليدة
Université SAAD DAHLAB de BLIDA

كليةالتكنولوجيا
Faculté de Technologie

قسمالإلكترونيك
Département d'Électronique

Mémoire de Master

Mention Électronique

Réseaux et Télécommunications (RT)

Présenté par

KERMICHE Mohamed Ilyes

Conception et Réalisation d'une plateforme AIoT pour la gestion et la surveillance intelligente du data center du

C.P.I. spa

Proposé par : Dr. ANOU Abderrahmane

Co-encadreur : DAHIA Mohamed Nabil DGA S.I. (CPI spa - filiale Banque d'Algérie -)

Année Universitaire 2022-2023.

ملخص

من أجل ضمان المراقبة والإدارة الذكية ، نقترح على الشركة تصميم وتحقيق منصة باستخدام الذكاء الاصطناعي (الذكاء الاصطناعي) وأدوات إنترنت الأشياء (إنترنت الأشياء ، والمختصرة باسم IoT). لذلك سيكون الهدف من مشروعنا هو تنفيذ منصة AiIoT لمركز البيانات والمناطق الحساسة التي تحمي البنية التحتية لتكنولوجيا المعلومات ، والتي ستوفر لهم إدارة أسهل وأكثر كفاءة للأخيرة ، بالإضافة إلى جعلها أكثر استقلالية واستدامة. سنستخدم أجهزة استشعار مختلفة في عدة مواقع ، بما في ذلك ،(الحرارة والرطوبة والضغط وأجهزة استشعار الحركة,... إلخ) أننا سنتصل بهذه المنصة ، مما سيسمح لنا بالحصول على جميع المعلومات اللازمة في الوقت الفعلي بالإضافة إلى إخطار التنبيهات ، مما يسمح للإدارة باتخاذ قرار سريع وفعال في جميع الأوقات. سيساعد مشروعنا المؤسسة على تنفيذ نظام قادر على اكتشاف الحالات الشاذة للمعدات المرتبطة بمخاطر الحوادث مثل الأعطال والحرائق ، وتنبيه الموظفين إلى مثل هذه المشاكل. . أيضا ، سيقوم هذا النظام بإدارة وصول الموظفين خلال ساعات العمل لتجنب أي تدخل أخرق أو ضار من جانبهم. كما أنها ستجمع بين إنترنت الأشياء (AioT) والذكاء الاصطناعي لتحقيق أهدافها.

الكلمات المفتاحية: الذكاء الاصطناعي - IA إنترنت الأشياء- منصة - AiIoT مركز البيانات

Résumé

Afin d'assurer une surveillance et une gestion intelligente, nous proposons à la société la conception et la réalisation d'une plateforme en utilisant l'intelligence artificiel (IA) et les outils de l'Internet des Objets (Internet Of Things, abrégé en IoT).

Le but de notre projet sera donc de mettre en œuvre une plateforme AiIoT pour leur

Datacenter et zones sensibles qui protège l'infrastructure IT, qui leur offrira une gestion plus facile et efficace de ce dernier, en plus de le rendre plus autonome et durable. Nous utiliserons de différents capteurs à plusieurs endroits, notamment,

(capteurs de chaleur, d'humidité, de pression, de mouvement,...etc) que nous connecterons à cette plateforme, ce qui permettra d'avoir toutes les informations nécessaires en temps réel ainsi que la notification des alertes, permettant ainsi au management une prise de décision rapide et efficace à tout moment.

Notre projet aidera la Société à mettre en place un système capable de détecter les anomalies au niveau des équipements associées aux risques d'incidents telles les pannes et les incendies, alertant le personnel en cas de tels problèmes. Aussi, ce système permettra de gérer l'accès du personnel, durant les heures de travail, pour éviter toute intrusion maladroite ou malveillante de leur part. Aussi, il combinera l'Internet des objets (AioT) et l'intelligence artificielle pour atteindre ses objectifs.

Mots clés : IA- IoT- plateforme AiIoT – Datacenter

Abstract

In order to ensure intelligent monitoring and management, we propose to the company the design and realization of a platform using artificial intelligence (AI) and the tools of the Internet of Things (IoT abbreviated).

The goal of our project will therefore be to implement an AiIoT platform for their Datacenter and sensitive areas that protects the IT infrastructure, which will offer them easier and more efficient management of the latter, in addition to making it more autonomous and sustainable. We'll be using different sensors in several places, including, (heat, humidity, pressure, motion sensors, etc.) that we will connect to this platform, which will allow us to have all the necessary information in real time as well as the notification of alerts, thus allowing management to make a quick and efficient decision at any time.

Our project will help the Corporation put in place a system that can detect equipment anomalies associated with the risks of incidents such as failures and fires, alerting staff to such problems. In addition, this system will allow access to be managed during working hours to avoid awkward or malicious intrusion by staff. It will also combine the Internet of Things (AioT) and artificial intelligence to achieve its objectives.

Keywords: artificial intelligence (AI)- Internet of Things (IoT abbreviated) - AiIoT platform- Datacenter

Dédicace

Je dédie ce mémoire ✍

À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leur prière tout au long mes études,

À mA chère sœur INTISSAR pour ses encouragements permanents, et son soutien moral,

À mon cher poussin frère, Zakaria Abdelwahab, à toute ma famille pour leur soutien tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,

À mes chères amies et amis pour leurs encouragements et accompagniement durant tout mon curssus universitaire.

KERMICHE Mohamed Ilyes

Remerciement

A tous ceux qui ont contribués à la réalisation de cet humble travail,

Au terme de la rédaction de ce projet, je tiens à exprimer ma profonde gratitude à Allah pour sa guidance et sa bénédiction tout au long de ce parcours. Sans son soutien infaillible, rien n'aurait été possible.

Également je tiens à remercier chaleureusement mes encadrants, à savoir Messieurs Abderrahmane ANOU et Mohamed Nabil DAHIA pour leur précieux accompagnement, expertise et disponibilité. Leurs conseils avisés ont été d'une aide précieuse pour moi.

À l'ensemble des Professeurs, Enseignants et étudiants de l'Université Saad Dahlab de Blida,
Je suis reconnaissant de votre environnement de pédagogie stimulant et de votre contribution à mon développement académique.

Enfin, à ma famille et mes amis/ies, je suis profondément reconnaissant pour votre amour, votre soutien inconditionnel et votre présence à mes côtés tout au long de ce parcours.

Merci du fond du cœur à tous ceux qui ont contribué à la réalisation de ce travail.

Remerciement

Je tiens à exprimer ma plus sincère gratitude envers toute l'équipe du CPI Spa pour m'avoir offert l'opportunité de réaliser mon stage au sein de votre entreprise. Ce fut une expérience incroyablement enrichissante qui m'a permis d'acquérir de nouvelles compétences et de découvrir de nombreux aspects passionnants de mon domaine d'études.

Votre soutien, vos conseils et votre accueil chaleureux ont joué un rôle déterminant dans mon développement professionnel. J'ai été impressionné par le professionnalisme et la bienveillance dont vous avez fait preuve tout au long de mon stage.

Je tiens également à remercier spécialement [nom du responsable du stage ou toute personne en particulier] pour son encadrement attentif et ses précieux conseils. Grâce à lui/elle, j'ai pu progresser et me sentir à l'aise dans mon travail quotidien.

Ce stage chez CPI Spa restera sans aucun doute un moment clé de ma carrière et je garderai des souvenirs inoubliables de cette expérience. Je n'aurais pu rêver d'un meilleur endroit pour développer mes compétences professionnelles et personnelles.Encore une fois, merci du fond du cœur pour cette opportunité inestimable. Je serai toujours reconnaissant(e) envers CPI Spa et je serais ravi(e) de rester en contact à l'avenir.

Bien à vous,

[kermiche mohamed ilyes]

Table des matières

Liste des figures

Liste des tableaux

Listes des acronymes et abréviations

API	:	Applications Programming Interface
CPI	:	Centre de Pré Compensation Interbancaire
CU	:	Cas d'Utilisation
DCIM	:	Data Center Infrastructure Management
DET	:	Diagramme d'Etats-Transitions
DSI	:	Direction des Systèmes d'Information
GUI	:	Graphical User Interface
HTTP	:	Hypertext Transfer Protocol
IoT	:	Internet of Things
ISO	:	International Organization for Standardization
IT	:	Information Technology
ITIL	:	Information Technology Infrastructure Library
JavaEE	:	Java Enterprise Edition
JS	:	JavaScript
JSON	:	JavaScript Object Notation
JWT	:	JSON Web Token
MQTT	:	Message Queuing Telemetry Transport
REST	:	Representational State Transfer
RH	:	Ressources Humaines
SGBD	:	Système de Gestion de Base de Données
SI	:	Système(s) d'Information
SMSI	:	Système de Management de la Sécurité de l'Information
SMTP	:	Simple Mail Transfer Protocol
SQL	:	Structured Query Language
TCP/IP	:	Transmission Control Protocol/Internet Protocol
UML	:	Unified Modeling Language
URL	:	Uniform Resource Locator

INTRODUCTION GENERALE

INTRODUCTION GENERALE

D'après une étude réalisée par Synergy Research, les investissements mondiaux dans les centres de données ont connu une croissance significative de dix-sept pour cent (17 %) en 2018, atteignant un montant record de 150 milliards de dollars. Ce boom remarquable est largement attribué à la demande en constante augmentation de trafic, de données et de puissance de calcul dans les centres de données. De nos jours, nous dépendons tous des centres de données qui jouent un rôle essentiel dans notre société numérique. Qu'il s'agisse de nos smartphones, ordinateurs, objets connectés, réfrigérateurs ou même stimulateurs cardiaques, tout est désormais connecté aux centres de données.

Toutefois, l'existence même de ces centres de données engendre un ensemble de défis liés à leur gestion. Parmi ces défis, on trouve les risques de dommages causés par des incidents tels que les incendies, les inondations et les intrusions malveillantes. De plus, les problèmes liés au matériel lui-même, comme les pannes d'équipement, peuvent également se poser. Il est donc impératif de relever ces défis pour assurer un fonctionnement efficace et sécurisé des centres de données.

La Banque d'Algérie a créé le Centre de Pré-Compensation Interbancaire (C.P.I spa) dans le but principal de mettre en œuvre et d'exploiter un système automatisé de compensation des paiements de masse dématérialisés par les banques commerciales. Ce système revêt une importance cruciale, car il est chargé de gérer les fluctuations des comptes des clients et d’arrêter les soldes des banques, mais il est également exposé à divers incidents, ce qui le rend vulnérable, par conséquent, il est essentiel de trouver une solution permettant d'anticiper au mieux de tels problèmes et de les éviter, ou le cas échéant, de les traiter le plus rapidement possible.

Ce document est divisé en trois chapitres : le premier chapitre concerne l’étude de l’existant, le deuxième chapitre sera consacré à l’état de l’Art, où nous traiterons des sujets de l’IoT, des Datacenters et de la sécurité des systèmes d’information, le troisième chapitre traitera la conception et la réalisation, constituant ainsi, la partie contribution de ce document. Ce chapitre comprend 4 volets, le premier traitera l’étude de l’existant au niveau de CPI spa, nous y expliquerons les problèmes constatés dans les solutions existantes. L’étape qui suivra, nous la consacrerons à l’étude du système cible. Et en fin, la conception et à la réalisation du système cible.

CHAPITRE 1

CHAPITRE 1 : Étude de l’existant

1.1 Introduction

Avant d'aborder l'étude de la solution, il est essentiel de procéder à une analyse approfondie de l'état actuel de la supervision et de la sécurisation de l'environnement qui abrite le système de paiement de masse A.T.C.I. Dans cette section, nous présenterons tout d'abord notre organisme d'accueil. Ensuite, nous fournirons des détails organisationnels et techniques sur la supervision et la sécurisation de l'environnement actuel qui abrite le système de paiement de masse A.T.C.I, dans le contexte d'une organisation type qui fait l'objet de notre étude de cas. Enfin, nous conclurons par un diagnostic permettant d'identifier les lacunes ainsi qu'une analyse des risques afin de définir les principaux axes d'amélioration.

1.2 Présentation de l’organisme d’accueil

Le 04 août 2004, la Banque d’Algérie a créé le Centre de Pré-Compensation Interbancaire (C.P.I) dont l’objectif principal est la mise en œuvre et l’exploitation d’un système automatisé de compensation des paiements de masse dématérialisé par les banques commerciales.

Le C.P.I spa est un opérateur technique qui assure la gestion et l’administration du système Télé Compensation Interbancaire (A.T.C.I) par délégation de la Banque d’Algérie. Le système A.T.C.I assure la compensation électronique des chèques, des effets, des transactions par cartes, des virements et des prélèvements échangés entre les participants qui sont la Banque d’Algérie, les banques, le Trésor public et Algérie Poste.

La C.P.I spa a pour mission :

- La gestion du système qui assure la compensation électronique des instruments de paiement de masse (chèques, effets, virements, prélèvements et transactions monétiques).
- L’exécution des diligences nécessaires au bon déroulement des opérations techniques qui conditionnent le fonctionnement du système A.T.C.I.
- Le calcul et le déversement des soldes multilatéraux de télé compensation dans le système de règlements bruts en temps réel.

- L’archivage des données, des images scannées et des valeurs télécom pensées.

1.3 Présentation de l’étude de cas

Le Centre de Pré Compensation Interbancaire (CPI) exerce la fonction d’opérateur du système d’échange et de compensation de paiement de masse. Il assume quatre fonctions essentielles : la gestion des échanges, de la télé compensation, des mouvements nets de règlement et l’archivage des données.

La plate-forme centrale de Télé-compensation, gérée par le CPI, et dont il a la responsabilité, est conçue pour contrôler et assurer un échange interbancaire sécurisé et automatisé des paiements de masse et leur compensation suivant les règles de neutralité et de transparence.

Du fait de l’importance du rôle joué par ce centre dans les transactions monétaires au niveau national, la sécurité de celui-ci est une question cruciale. En particulier, nous nous intéresserons à la sécurité physique du Datacenter du centre. Celui-ci peut être vulnérable à une grande variété de menaces (Accès par les employés à des heures non autorisées, accès hors personnel, incendie).

Dans le cadre de notre travail, nous menons notre étude de l’existant. Dans ce qui suit, nous présenterons l’organisation générale, l’existant métier et technique. Ainsi que les anomalies identifiées et une analyse des risques. Pour finir, nous proposons un ensemble d’axes d’amélioration.

1.4 Organisation générale

CPI spa qui fait sujet de notre étude est structuré selon l’organigramme suivant : une Direction Générale, le département d’audit, la cellule de risque et de contrôle interne sont directement reliés à la Direction Générale. Le reste des fonctions est réparti en directions assurant l’aspect opérationnel et administratif de l’organisation.

Pour nos besoins, nous allons détailler la composition de la Direction Système d’Information où se situe l’unité responsable de la gestion des accès logiques sous forme de département de Sécurité des Systèmes d’Information.

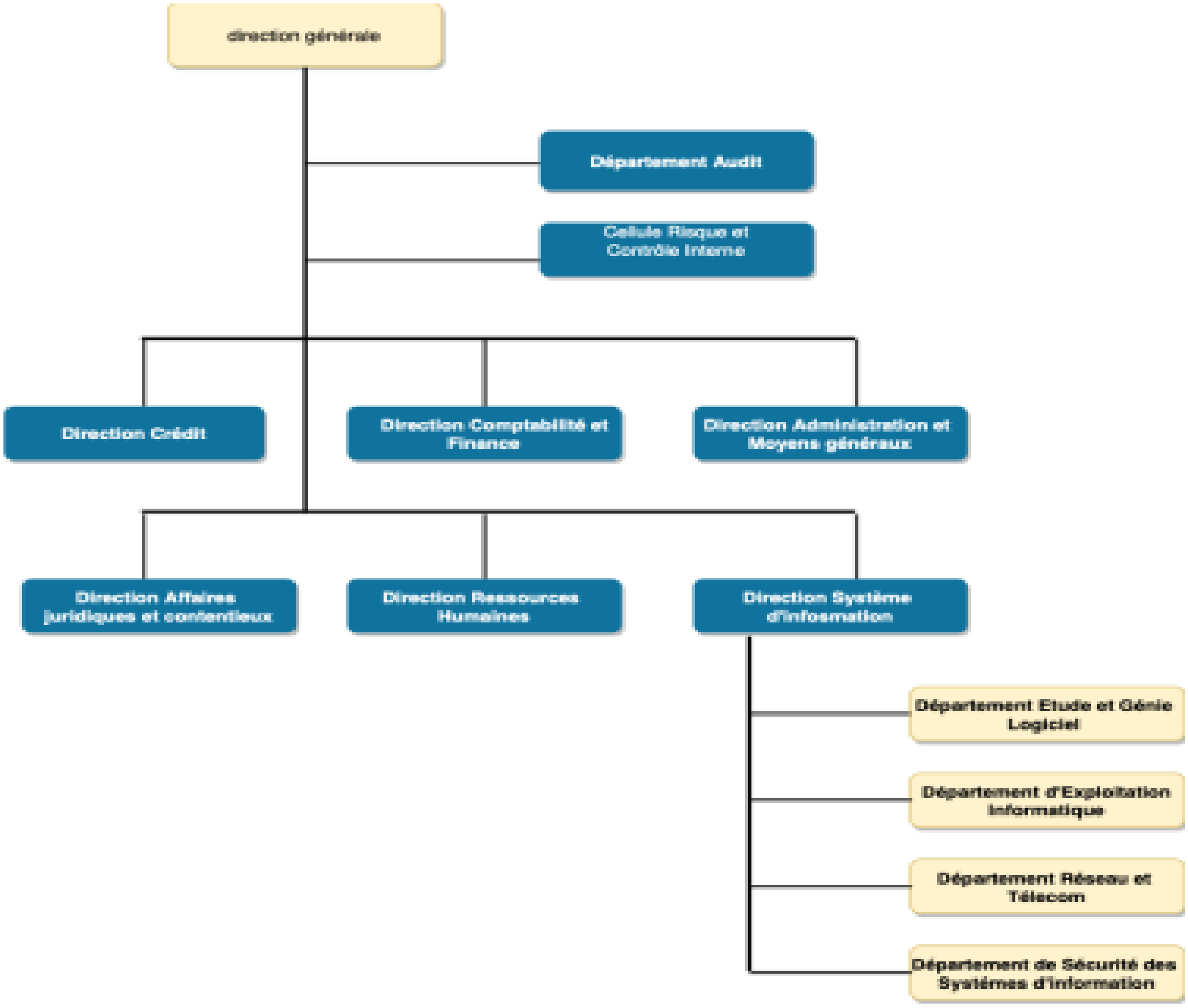

Figure 1. 1: Organigramme du CPI spa.

1.5 Politique de sécurité physique

La sécurité physique a trait à l'application de mesures de protection physiques et techniques pour prévenir l'accès illicite à des informations classifiées.

Des mesures de protection minimales sont déterminées sur la base d'une évaluation du risque et sont obligatoires dans tous les lieux où des informations classifiées sont conservées ou traitées. En fonction de leur utilisation, ces lieux sont départagés en zones administratives et zones sécurisées. Le chargé de la sécurité doit s'assurer que les mesures de protection répondent aux exigences établies.

Les mesures de sécurité physiques d'un Datacenter dépendent de la taille de ce dernier. Les Datacenter contiennent souvent une grande quantité d'équipements informatiques (serveurs, commutateurs et routeurs, infrastructures d'alimentation et refroidissement et équipement de communication). Ces équipements peuvent être contenus dans une armoire, qu'il est facile et simple de protéger par un verrou physique, ou dans un entrepôt, où des mesures de sécurité physique supplémentaires (par exemple, accès par badge, vidéosurveillance, alarmes ou vigiles) peuvent être plus adéquates.

1.5.1 Processus de gestion de sécurité physiques et alertes système de surveillance

La première mesure de protection consiste à installer des caméras et des agents de sécurité autour du périmètre. Les entrées du Datacenter sont surveillées par des caméras. Les Datacenter ne sont pas pourvus de fenêtres en verre, ce qui crée une sécurité supplémentaire. En revanche chaque porte représente un risque pour la sécurité physique : caméras, serrures et gardes de sécurité sont donc une protection contre ce niveau d'attaque.

La vidéosurveillance est toujours très utile pour les Datacenter. Des caméras en circuit fermé dotées de fonctions complètes de vision panoramique, d'inclinaison et de zoom doivent surveiller les points d'accès extérieurs ainsi que toutes les portes intérieures et la salle des serveurs. Les images des caméras doivent être sauvegardées numériquement et archivées hors site pour éviter toute manipulation non autorisée.

1.5.2 Système d'authentification multi facteurs

Chaque Datacenter doit suivre des procédures de sécurité de type “confiance zéro” qui intègrent l'authentification multifactorielle.

Par ailleurs, chaque point d'accès doit nécessiter d'au moins deux formes d'identification ou d'autorisation afin de garantir que personne ne sera autorisé à entrer par la sécurité s'il lui manque une forme d'authentification.

Si un attaquant réussit à franchir une porte, le niveau de sécurité physique suivant est une cage de Faraday. L'attaquant ne peut pas la traverser sans autorisation et sans la clé correspondante. Cette clé peut être une clé traditionnelle, un code à entrer dans un dispositif de sécurité, une carte à scanner ou encore un système biométrique. Les systèmes biométriques sont les plus sûrs, mais ils sont aussi les plus coûteux. Les Datacenter de niveau 4 sont toujours équipés d'un de ces systèmes.

Les visiteurs d'un Datacenter sont étroitement surveillés, car très peu de personnes doivent parcourir les locaux. Les visiteurs doivent avoir un accès limité aux équipements et être accompagné par un employé. Les visiteurs reçoivent un badge lors de leur visite et une signature est requise dans un registre à chaque entrée et à chaque sortie des locaux.

1.5.3 Système d'alarme

En plus du risque de dommages matériels et matériels résultant d'un incendie ou d'un incident de sécurité, il existe également un risque de perte de performance opérationnelle et de réputation.

1.6 Processus de gestion des ressources humaines

L'analyse de la politique de gestion des ressources humaines nous a permis de représenter la procédure de gestion comme suit :

1.6.1 Rôles et responsabilités

La politique définit les responsabilités de chacune des parties prenantes dans la procédure ainsi que les règles d'administration qu'ils se doivent de respecter.

Les responsabilités sont les suivantes :

- Le coordinateur métier : il s'agit de l'initiateur d'une demande de création, d'attribution, de modification, ou de suppression des privilèges.
- L'administrateur système : chargé de l'implémentation des droits d'accès dans le système d'information

1.6.2 Démarche existante de la gestion des ressources humaines

À partir des informations recueillies dans le cadre des entretiens avec les personnes en charge de la gestion de ces ressources humaines en vue de prendre connaissance des pratiques appliquées à date en termes d'octroi, de modification et de révocation des accès, nous avons déterminé que la démarche réelle suivie par les employés de CPI spa pour la gestion des accès diffère de la procédure. Ci-dessous les processus comme rapportés :

Gestion de nouvelles recrues : Lorsqu'un nouveau collaborateur est recruté au sein de l'organisme, un gestionnaire des ressources humaines informe par email les administrateurs des systèmes/réseaux et des plateformes IT au sein de la Direction des Systèmes d'Information.

L'administrateur lui crée les privilèges lui étant nécessaires pour l'exécution des tâches relatives à son poste, en se basant sur les matrices des habilitations formalisées à cet effet.

Gestion des départs : Lorsqu'un employé quitte (définitivement ou temporairement) l'organisme, un gestionnaire des ressources humaines informe par email les administrateurs des systèmes/réseaux et des plateformes IT au sein de la Direction des Systèmes d'Information.

L'administrateur lui désactive l'ensemble des droits d'accès aux ressources informatiques.

Gestion des réactivations : Lorsqu'un employé reprend le service au sein de l'organisme, un gestionnaire des ressources humaines informe par email les administrateurs des systèmes/réseaux et des plateformes IT au sein de la Direction des Systèmes d'Information.

Les administrateurs réactivent l'ensemble des droits d'accès aux ressources informatiques suspendus auparavant. Ainsi, la communication sur les demandes d'accès est effectuée manuellement à travers un échange d'emails ne permettant aucun contrôle sur le contenu de la demande. En outre, l'organisme n'utilise aucun outil informatique dédié à la gestion des droits d'accès et le traitement des demandes d'octroi, modification, suspension, suppression, et réactivation des accès. La démarche suivie est supportée seulement par des outils de bureautique à l'image de :

• La suite Microsoft Office : Excel, Word, etc. qui sont utilisés quotidiennement pour diverses tâches.

• Un outil de mailing pour assurer la communication entre les différents acteurs impliqués.

1.5 Diagnostic et critiques

L'analyse des documents et des informations recueillies dans le cadre de notre .projet nous a permis de définir les problèmes majeurs. Nous avons adopté le modèle causes-effets d'Ishikawa pour présenter les anomalies identifiées :

1.5.1 Anomalie : incendie

Causes

- Les incendies venant de l'extérieur.
- Les files et les câbles.
- Les espaces d'aération.

- La chaleur et la fumée.
- L'équipement de chauffage, de ventilation et de climatisation ou CVC.
- Les matériaux combustibles.

Conséquences

- Au niveau humain : les Datacenter ont des équipes sur site qui sont potentiellement en danger en cas d'incendie, que ce soit à cause des flammes et/ou émanation de la fumée qui peuvent être corrosives et qui diminuent la visibilité en cas d'évacuation et d'intervention des secours. Il faut aussi prendre en compte les personnes vivantes à proximité, dans le cas des Datacenter situés au sein de zones habitées.
- Au niveau économique : Les dégâts sont généralement divisés entre matériels (destruction physique des serveurs et de l'équipement sur place) et immatériels (perte de données professionnelles pour les entreprises hébergées, fermeture de leurs sites et serveurs).
- l'impact environnemental : les Datacenter sont remplis de composants électroniques et de métaux rares, des matériaux polluants pour l'environnement.

1.5.2 Anomalie : températures excessives

Causes

- Les points chauds dans un centre de données sont définis par l'ASHRAE TC 9.9 comme des zones où l'air entrant dans les serveurs, les systèmes de stockage, les routeurs ou tous autres équipements électroniques sera supérieur à 27 °C. La zone arrière des racks et les zones dans les allées chaudes ne sont pas considérées comme des points chauds.

Conséquences

- Les points chauds peuvent réduire la fiabilité et endommager les équipements électroniques en raison de l'incapacité de dissiper la chaleur générée. Les fabricants de serveurs et de matériel informatique peuvent justifier le refus du service de garantie en raison de la violation des termes du contrat de service par la présence de zones chaudes.

1.5.3 Anomalie : fuites et dégâts des eaux

Causes

- les inondations peuvent survenir en dehors d'une zone inondable et lors de précipitations modérées, et que le niveau de la nappe phréatique peut devenir une préoccupation.
- Les fourreaux, les chambres de tirage et les tranchées peuvent se remplir d'eau et devenir une voie pour l'humidité.

Conséquences

- L'eau et l'humidité peuvent provoquer des problèmes instantanés tels que des court-circuit et des décharges partielles.

1.5.4 Anomalie : gaz et fumés

Causes

- En cas de départ de feu, il sera attisé par l'apport d'air frais constant et les fumées risqueront de se répandre par le réseau de gaines.

Conséquences

- Les fumées sont l'un des vecteurs de propagation les plus courants. Elles sont chaudes et combustibles. Par ailleurs, elles causent des dommages irréversibles aux équipements électroniques par la suie qu'elles déposent.

1.5.5 Anomalie : Non-respect de la politique de gestion des accès

Causes

- Demandes des accès transmises directement de l'initiateur vers l'exécution sans passer par la validation. - Absence d'un outil uniforme pour le traitement des demandes.
- Le manque de conscience vis-à-vis la sécurité de l'information de la part des membres de l'organisation. - La négligence et l'abandonnement des meilleures pratiques au sein de l'organisation.

Conséquences

- Non-respect des règles de sécurité pendant l'attribution, la modification, et la désactivation des droits d'accès.
- Accorder des accès sensibles à des personnes non habilitées à exploiter ces derniers. - Aucune traçabilité de la demande d'accès ni de sa validation et donc aucune partie ne peut être tenue responsable dans le cas d'un accès illicite.
- Augmenter le risque d'accès illicite aux SI de l'organisation.

1.6 Analyse des risques

Dans cette partie, nous présentons les résultats de l'analyse des risques que nous avons effectuée en partant des anomalies énumérées précédemment. L'objectif de cette dernière est de corroborer la pertinence de notre diagnostic et pour nous guider dans l'élaboration des lignes directrices de notre système cible.

Il existe de multiples méthodes et normes permettant de couvrir tous les aspects du processus de gestion des risques en entreprise, nous nous sommes basés sur l'étude comparative du PR. R CHALAL sur les méthodes disponibles d'analyse des risques. Ainsi, nous avons décidé de suivre la démarche définie par la méthode EBIOS dans notre étude.

Étude de contexte :

Objectif de l'étude: L'objectif de cette étude est d'analyser ainsi que de gérer les risques liés à l'environnement abritant le système de paiement de masse A.T.C.I. Le besoin exprimé par le CPI spa est le suivant : il souhaite superviser et sécuriser l'environnement abritant le système de télé compensation interbancaire ATCI, vu la sensibilité du système hébergé au niveau des sites, les zones seront supervisées et sécurisées en matière d'environnement (température, mouvement ..), il nous faudra donc étudier toutes les sources des menaces liées à l'environnement abritant le système de paiement de masse A.T.C.I.

Le CPI souhaite aussi assurer une conformité des processus de gestion de sécurité dans le futur vis-à-vis des recommandations et best practices des standards de l'ISO 27001 et 27002, ainsi que l'ITIL et la législation Sarbanes-Oxley « SOX ».

Périmètre de l'étude Processus de supervision et la sécurisation de l'environnement abritant le système de paiement de masse A.T.C.I.

Selon les besoins exprimés par le CPI, et des recherches que nous avons pu mener sur les différentes normes et méthodes permettant la supervision et la sécurisation des Datacenter, il a été convenu que le scope de notre étude portera sur les processus suivants :

- Processus de gestion des risques d'incendie

Le CPI souhaite qu'une alerte soit lancée dès la détection d'un incendie avec des informations précisées sur ce dernier.

- Processus de gestion des risques de températures excessives

Le CPI souhaite qu'une alerte soit lancée s'il y a des changements dans la température de l'environnement avec des informations précisées sur ces changements.

- Processus de gestion des risques de fuites et dégâts des eaux

Le CPI souhaite qu'une alerte soit lancée s'il y a des fuites et dégâts des eaux dans l'environnement avec des informations précisés sur ces changements.

- Processus de gestion des risques de gaz et fumés

Le CPI souhaite qu'une alerte soit lancée s'il y a de gaz ou fumés dans l'environnement avec des informations précisés sur ces derniers.

- Processus de télésurveillance

Le CPI souhaite que le Datacenter soit surveillé 24h/24h.

- Respect de la politique de gestion des Ressources Humaines

Le CPI a formalisé et centralisé de manière claire le processus de gestion des Ressources Humaines, et ce, afin que la politique mise en place par ses soins soit respectée.

- Processus de gestion des demandes d'accès (demandes de création, révocation, et de mobilités internes). Les insuffisances au niveau des processus de gestion des accès seront analysées et couvertes au cours de notre étude.

- Contrôle de l'habilitation des utilisateurs à acquérir les privilèges demandés

Du fait que 90 % de l'ensemble des attaques sont causées par des erreurs humaines (Kaspersky, 2020), nous devons couvrir les risques liés à l'habilitation des utilisateurs et des privilèges dont ils peuvent disposer.

Sources de menaces : Afin d'assurer la sécurité de l'information ainsi que le système d'information, les critères suivants ont été retenus : disponibilité, intégrité, confidentialité et traçabilité.

Types de sources de menaces	Retenue ou non	Exemple
Phénomène naturel	Oui	• Séismes • Inondations…etc.
Catastrophe naturelle ou sanitaire	Oui	• Panne d'électricité • Coupure d'internet • Incendie
Virus non ciblé	Oui	• Cheval de Troie
Source humaine interne, malveillante, avec de faibles capacités	Oui	• Employé malveillant
Source humaine interne, malveillante, avec des capacités importantes	Oui	• Manager ou coordinateur malveillant
Source humaine interne, malveillante, avec des capacités illimitées	Oui	• Employé malveillant ayant accès aux données sensibles de l'organisation
Source humaine externe, malveillante, avec de faibles capacités	Oui	• Prestataire tiers
Source humaine externe, malveillante, avec des capacités importantes	Oui	• Intervenant contractuel ayant accès aux plateformes de l'organisation
Source humaine externe, malveillante, avec des capacités illimitées	Non	
Source humaine interne, sans intention de nuire, avec de faibles capacités	Oui	• Stagiaire • Personnel d'entretien
Source humaine interne, sans intention de nuire, avec des capacités importantes	Oui	• Un manager peu consciencieux ou peu sérieux

Source humaine interne, sans intention de nuire, avec des capacités illimitées	Oui	• Administrateur système peu consciencieux
Source humaine externe, sans intention de nuire, avec de faibles capacités	Oui	• Entourage du personnel
Source humaine externe, sans intention de nuire, avec des capacités importantes	Oui	• Intervenant contractuel
Source humaine externe, sans intention de nuire, avec des capacités illimitées	Non	

Tableau 1. 1: Analyse des risques, sources de menaces.

Métriques d'évaluation :

Les critères de sécurité retenus : Afin d'assurer la sécurité de l'information ainsi que le système d'information, les critères suivants ont été retenus : disponibilité, intégrité, confidentialité et traçabilité.

Critère	Description (Agence nationale de la sécurité des systèmes d'information, 2010a)
Disponibilité	L'accès aux ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues. Les services et ressources sont accessibles rapidement et régulièrement.
Intégrité	Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.
Confidentialité	Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées (notions de droits ou permissions). Tout accès indésirable doit être empêché.

Traçabilité	Garantis que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

Tableau 1. 2 : Analyse des risques, métriques d'évaluation.

Échelle de disponibilité : L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveaux de l'échelle	Description détaillée de l'échelle
Plus de 48h	Le bien essentiel peut être indisponible plus de 48 heures.
Entre 24h et 48h	Le bien essentiel doit être disponible dans les 48 heures.
Entre 4h et 24h	Le bien essentiel doit être disponible dans les 24 heures.
Moins de 4h	Le bien essentiel doit être disponible dans les 4 heures.

Tableau 1. 3: Analyse des risques, échelle de disponibilité.

Échelle d'intégrité : L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes d'intégrité :

Niveaux de l'échelle	Description détaillée de l'échelle
Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée.
Maitrisé	Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée.

Intègre	Le bien essentiel doit être rigoureusement intègre.

Tableau 1. 4: Analyse des risques, échelle d'intégrité.

Échelle de confidentialité : L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveaux de l'échelle	Description détaillée de l'échelle
Public	Le bien essentiel est public.
Limité	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.
Réservé	Le bien essentiel ne doit être accessible qu'au personnel (interne) impliqué.
Privé	Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.

Tableau 1. 5: Analyse des risques, échelle de confidentialité.

Échelle de traçabilité : L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de traçabilité :

Niveaux de l'échelle	Description détaillée de l'échelle
Non traçable	La trace du bien essentiel n'est pas enregistrée.
Traçable	La trace du bien essentiel doit être sauvegardée et exploitable.

Tableau 1. 6: Analyse des risques, échelle de traçabilité.

Échelle de gravité : L'échelle suivante sera utilisée pour estimer la gravité des événements redoutés et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
Négligeable	L'organisation surmontera les impacts sans aucune difficulté.
Significative	L'organisation surmontera les impacts malgré quelques difficultés.
Sévère	L'organisation surmontera les impacts avec de sérieuses difficultés.
Critique	L'organisation ne surmontera pas les impacts (sa survie est menacée).
Catastrophique	L'organisation ne surmontera pas les impacts (sa survie est impossible).

Tableau 1. 7: Analyse des risques, échelle de gravité.

Échelle de vraisemblance : L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
Extrêmement Rare	Cela ne devrait jamais se (re)produire.
Rare	Cela ne devrait pas se (re)produire.
Peu probable	Cela pourrait se (re)produire.
Probable	Cela devrait se (re)produire un jour ou l'autre.

Fréquent	Cela va se (re)produire fréquemment.

Tableau 1. 8: Analyse des risques, échelle de vraisemblance.

Les biens identifiés : Les processus liés à la gestion des accès inclus dans le cas de notre étude permettent de traiter et de couvrir l'ensemble des opérations liées aux accès logiques des utilisateurs au sein de l'organisation, nous allons lister dans ce qui suit les biens essentiels identifiés :

Processus métier	Processus essentiels	Informations essentielles	Dépositaires
Gestion de télésurveillance	Surveillance de télévisions installées au niveau de salle de supervision et maintenance	• Guides d'utilisation • Documentations de matériels • Informations personnelles des utilisateurs • Politique d'accès aux salles de surveillance • Liste des contacts (Fournisseurs, Autorité de maintenance)	Coordinateur métier RH
Gestion des alarmes	Surveillance de matériels d'alarmes et maintenance	• Guide d'utilisation • Documentations de matériels • Liste des contacts (Fournisseurs, Autorité de maintenance)	Coordinateur métier RH
Respect de la politique de gestion des accès	Mise en place de processus respectant les meilleures pratiques régies par les	• Politique gestion des accès communiquée aux utilisateurs • Processus d'attribution et de gestion	Coordinateur métier RH

	normes citées précédemment	des accès formalisés • Meilleures pratiques liées à la gestion des accès	
Processus de gestion des demandes d'accès	• Processus de demande de création d'accès • Processus de révocation d'accès utilisateur (Deprovisionning) • Processus liés aux mobilités internes • Processus liés à la réactivation des utilisateurs	• Informations personnelles de l'utilisateur • Informations organisationnelles de l'utilisateur (service, département …etc.) • Rôles organisationnels de l'utilisateur • Habilitations de l'utilisateur • Accès de l'utilisateur	Coordinateur métier RH
Contrôle de l'habilitation des utilisateurs à acquérir les privilèges demandés	Vérification de l'habilitation de l'utilisateur à recevoir l'accès demandé en amont de sa Création	• Rôle organisationnel de l'utilisateur • Habilitations de l'utilisateur • Matrice des habilitations de l'organisation • Accès demandés par l'utilisateur	Coordinateur métier RH

Tableau 1. 9 : Analyse des risques, biens identifiés.

Études des événements redoutés

Événement redouté	Besoin de sécurité	Source de menaces	Impacts	Gravité
Incendie	Traçable	- Les incendies venant de l’extérieur. - Les fils et les câbles. - Les espaces d’aération. - La chaleur et la fumée. - L’équipement de chauffage, de ventilation et de climatisation ou CVC. - Les matériaux combustibles.	- des équipes sur site qui sont potentiellement en danger - les personnes vivant à proximité, dans le cas de notre Datacenter situé au sein de zones habitées. - destruction physique des serveurs et de l’équipement sur place - perte de données professionnelles pour les entreprises hébergées, fermeture de leurs sites et serveurs - Les composants électroniques et métaux rares, matériaux polluants pour l’environnement	Catastrophique
températures excessives	Traçable	- La zone arrière des racks et les zones dans les allées chaudes	- réduction la fiabilité et endommage des équipements électroniques	Critique
fuites et dégâts des eaux	Limité	- les inondations - Les fourreaux, les chambres de tirage et les tranchées peuvent se remplir d’eau et devenir une voie pour l’humidité	- des court-circuités et des décharges partielles.	Catastrophique

gaz et fumés	Limité	- Employé peu sérieux/malveillant - Intrusion malicieuse dans les systèmes de l'organisation	- Pertes dues à la fraude interne - Sanctions judiciaires, disciplinaires ou administratives liées à une non-conformité dans les résultats financiers - Atteinte à l'image de l'organisation	Critique
Contrefaçon de documents	Intègre	- Employé peu sérieux/ malveillant - Intrusion malicieuse dans les systèmes de l'organisation	- Pertes financières dues à la fraude interne - Atteinte à l'image de l'entreprise	Critique
Erreur de paramétrage	Traçable	Employé peu sérieux	- Accès non autorisé aux données sensibles - Augmentation de privilèges - Oubli de comptes dormants	Sévère
Non-respect des obligations législatives ou réglementaires	Limité	Employé peu sérieux	Sanctions judiciaires, disciplinaires ou administratives liées à une non-conformité dans la gestion des accès des systèmes financiers	Critique

Dysfonctionnement de l'activité des systèmes	Moins de 4h	Intrusion malveillante dans les systèmes de l'organisation	Altération ou suppression de données sensibles	Catastrophique
Tentative d'usurpation d'identité numérique (Augmentation du niveau de privilège)	Traçable	- Employé malveillant - Prestataire externe malveillant	- Accès non autorisé aux données sensibles - Pertes dues à la fraude interne - Altération ou suppression de données sensibles	Critique

Piratage des applications de l'organisation	Moins de 4h	Intrusion malicieuse dans les systèmes de l'organisation	- Accès non autorisé aux données sensibles - Pertes dues à la fraude interne - Altération ou suppression de données sensibles - Atteinte à l'image et à la réputation de l'organisation	Catastrophique
Exploitation malveillante des comptes dormants au sein des systèmes de l'organisation	Limité	- Employé malveillant - Prestataire externe malveillant - Mauvaise gestion des comptes utilisateur (oubli de désactivation)	- Altération ou suppression de données sensibles - Divulgation d'informations sensibles	Sévère
Divulgation de l'information ou vol de données	Limité	- Employé malveillant - Prestataire externe malveillant	- Atteinte à l'image de l'entreprise - Pertes financières dues à une atteinte à la réputation de l'entreprise	Critique
Utilisation malveillante des systèmes par un prestataire tiers	Traçable	- Prestataire malveillant - Oubli de révocation d'un compte pour prestataire	-Altération ou suppression de données sensibles -Divulgation d'informations sensibles	Sévère
Accès à des ressources sensibles par un utilisateur non autorisé	Limité	- Employé malveillant - Prestataire externe malveillant - Erreur dans l'attribution des accès	- Altération ou suppression de données sensibles - Divulgation d'informations sensibles	Catastrophique
Propagation d'un code malicieux entre systèmes informatiques	Limité	- Employé malveillant - Intrusion externe malveillante dans les systèmes de l'entreprise	- Altération ou suppression de données sensibles - Fraude externe - Atteinte à l'image de l'entreprise	Catastrophique

Tableau 1. 10 : Les événements redoutés.

Études des risques

Identification des risques nous avons pu établir une liste des risques possibles à partir des événements redoutés listés ci-dessus.

Risque identifié	Niveau de risque	
	Vraisemblance	Gravité
Risque d'incendie	Catastrophique	Rare
Risque de températures excessives	Critique	Rare
Risques de fuites et dégâts des eaux	Catastrophique	Rare
Risques de gaz et fumés	Critique	Rare
Risque de non-détection des transactions non notifiées (intentionnellement)	Critique	Probable
Risque de non-détection des documents contrefaits	Sévère	Probable
Risque d'erreur dans l'affectation des privilèges aux utilisateurs	Sévère	Peu probable
Risque de non-conformité vis-à-vis des Réglementations	Critique	Rare
Risque d'intrusion pouvant entrainer des dysfonctionnements dans les systèmes au-delà de 4 heures	Catastrophique	Probable
Risque lié à l'usurpation de l'identité numérique d'un employé de l'organisation (Augmentation en privilèges)	Critique	Probable
Risque de piratage des applications de l'organisation pouvant entrainer un arrêt au-delà de 4h	Catastrophique	Probable
Risque lié à l'oubli et à l'exploitation malveillante de comptes dormants au sein des systèmes de l'organisation	Critique	Peu Probable
Risque lié à la divulgation de l'information ou au vol de données	Critique	Probable
Risque lié à la non-détection d'utilisation malveillante des systèmes par un prestataire externe	Sévère	Peu probable

Risque lié à la non-détection d'une intrusion entrainant une propagation de code malicieux au sein des systèmes de l'organisation	Catastrophique	Rare

Tableau 1. 11 : Analyse des risques, échelle de traçabilité.

Ainsi, les risques ont été classés selon leur gravité et leur vraisemblance dans ce qui suit.

Gravité	catastrophique 5		- Risque lié à la non-détection d'une intrusion entrainant une propagation de code malicieux au sein des systèmes de l'organisation - Risque d'incendie - Risques de fuites et dégâts des eaux		- Risque de piratage des applications de l'organisation pouvant entrainer un arrêt au-delà de 4h - Risque d'intrusion pouvant entrainer des dysfonctionnements dans les systèmes au-delà de 4 heures	
	Catastrophique 4		- Risque de non-conformité vis-à-vis des réglementations - Risque de températures excessives - Risques de gaz et fumés	- Risque lié à l'oubli et à l'exploitation malveillante de comptes dormants au sein des systèmes de l'organisation	- Risque de non-détection de transactions non notifiées (intentionnellement) - Risque lié à l'usurpation de l'identité numérique d'un employé de l'organisation (Augmentation en privilèges) - Risque lié à la divulgation de l'information ou au vol de données	
	Sévère 3			- Risque d'erreur dans l'affectation des privilèges aux utilisateurs - Risque lié à la non-détection d'utilisation malveillante	- Risque de non-détection de documents contrefaits	

				des systèmes par un prestataire externe		
	Significative 2					
	Négligeable 1					
		1. Extrême ment Rare	2. Rare	3. Peu probable	4. Probable	5. Fréquen t
		Vraisemblance				

Tableau 1. 12: Analyse des risques, matrice de criticité.

Légende :

Risques négligeables	Risques significatifs	Risques intolérables

Tableau 1. 13 : Analyse des risques, échelle d'intégrité.

Les risques liés à la gestion des accès logiques aux plateformes de l'organisation représentent tous un point de départ critique. Point duquel peut survenir tout type d'attaque ayant des conséquences sévères, voire fatales, sur l'organisation. Ainsi, nous pouvons donc remarquer que tous les risques listés ci-dessus doivent être prévenus ou traités, aucun de ces derniers ne peut être négligé au cours de l'élaboration de la solution permettant de gérer les accès. Dans ce qui suit, nous allons identifier pour chaque risque la mesure la plus adéquate et les besoins en termes de sécurité liés à ceux-ci.

Objectifs de sécurité

Le client souhaite principalement éviter ou réduire les risques s'apparentant à la gestion et au contrôle des accès logiques aux systèmes de l'organisation.

Le tableau suivant présente les objectifs de sécurité identifiés (les croix correspondent aux premiers choix, les plus entre parenthèses correspondent aux autres possibilités acceptées)

Risque	Objectif de sécurité		
	Évitement	Réducti-on	Prise
Risque d'incendie	+	x	+
Risque de non-détection de documents contrefaits	+	x	
Risque d'erreur dans l'affectation des privilèges aux utilisateurs	x	+	+
Risques de fuites et dégâts des eaux	x		
Risque de températures excessives	x		
Risques de gaz et fumés	x		
Risque d'intrusion pouvant entrainer des dysfonctionnements dans les systèmes au-delà de 4 heures		x	+
Risque lié à l'usurpation de l'identité numérique d'un employé de l'organisation (Augmentation en privilèges)	x	+	+
Risque de piratage des applications de l'organisation pouvant entrainer un arrêt au-delà de 4h		x	+
Risque lié à l'oubli et à l'exploitation malveillante de comptes dormants au sein des systèmes de l'organisation	x	+	+
Risque lié à la divulgation de l'information ou au vol de données	+	x	
Risque lié aux non-détections d'utilisation malveillante des systèmes par un prestataire externe	x	+	+
Risque lié aux non-détections d'une intrusion entrainant une propagation de code malicieux au sein des systèmes de l'organisation	+	x	

Tableau 1. 14 : Analyse des risques, échelle d'intégrité.

Nous pouvons donc remarquer que pour la totalité des risques significatifs identifiés, la mesure la plus adéquate à prendre est l'évitement. Ces risques peuvent être évités en prenant les mesures nécessaires en amont, tels qu'un contrôle régulier des documents, ou une validation à plusieurs paliers ainsi qu'un suivi permanent des comptes utilisateurs. Pour ce qui est des risques intolérables identifiés au cours de cette étude, deux d'entre eux peuvent être évités par une solution de gestion des accès, quant aux autres, cette même solution permettra de les réduire considérablement.

2.3.7 Axes d'amélioration

Afin de remédier aux anomalies identifiées et aux risques analysés, il est nécessaire de définir les grandes lignes directrices de notre projet qui permettront de renforcer la sécurité. Ainsi, partant des recommandations des normes ISO 27001 et 27002, ainsi que les meilleures pratiques de l'ITIL et la législation SOX, nous avons déterminé les principaux axes d'améliorations pour un système d'information de gestion des accès :

Au niveau technique

- Automatiser les communications entre les composants de système d'alerte, de surveillance et de gestion d'accès.
- Renforcement avec les capteurs manquants.
- Implémentation d'une plateforme de gestion et automatisation des alertes.
- Intégration de l'IA dans des composants d'infrastructure.
- Implémentation d'une application, pour contrôler et recevoir des alertes à partir du système à distance et en temps réel.
- Implémentation d'une couche de sécurisation de l'interopérabilité entre composants au niveau des appareils, des logiciels et de la plateforme.
- Outiller les processus de traitement des demandes d'accès.
- Centraliser et structurer l'accès aux informations sur les habilitations et privilèges.
- Informatiser les documents relatifs à la gestion des accès.

Au niveau organisationnel

- Améliorer la traçabilité sur les l'accès et les habilitations.
- Optimiser la répartition des responsabilités.

- Optimiser les processus de traitement des RH.

1.4 Conclusion

L'analyse de l'existant nous a permis de comprendre les processus actuels de gestion des accès, d'identifier les anomalies et de déterminer les axes d'amélioration potentiels. Cette compréhension nous a ensuite aidés à élaborer une solution appropriée pour résoudre la problématique énoncée. De plus, l'analyse des risques réalisée a renforcé notre compréhension des enjeux de la gestion des accès et son impact sur le bon fonctionnement de l’organisation.

Dans le chapitre suivant nous présenterons des généralités sur l’IOT intrnet of things qui nous aidera à réaliser notre travail.

CHAPITRE 2

État de l'art

2. État de l'art

2.1 Introduction

Dans ce chapitre, nous fournissons des informations générales sur l'Internet des objets. Tout d'abord, nous proposons quelques définitions pertinentes au concept. Ensuite, nous allons présenter les deux architectures les plus utilisées dans l'Internet des Objets, ainsi que les protocoles et standards communs de ces derniers. À la fin de ce chapitre, nous déroulerons les différents domaines d'application de l'Internet des objets, les divers avantages qu'il offre ainsi que les défis et les limites auxquels il est confronté.

2.2 Internet des objets

Depuis la fin des années 1980, Internet a connu des changements bouleversants. La dernière étape consiste à utiliser ce réseau mondial pour communiquer avec des objets ou entre objets. Cette évolution s'appelle l'Internet des objets (IoT pour the Internet of Things). L'Internet des objets se développe si rapidement qu'il est prévu que d'ici 2025, il y aura près de 75,44 milliards d'appareils Internet des objets connectés à Internet [(htt)].

2.2.1 Définitions

L'expression de l'Internet des objets a été utilisée pour la première fois par Kevin Ashton en 1999. Il a utilisé la technologie d'identification par radiofréquence (RFID) pour limiter les seuls objets connectés identifiables de l'Internet des objets [1].

Le terme a été officiellement introduit par l'Union internationale des télécommunications (UIT) dans un rapport de 2005. L'Internet des objets (Iots) est l'infrastructure dynamique d'un réseau mondial. Ce réseau mondial possède des capacités d'autoconfiguration basées sur des normes et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et sont intégrés de manière transparente dans le réseau [2].

Selon le IEEE "Special report : Internet of Things" publié en 2014, "l'IoT est un réseau de dispositifs équipés de capteurs qui sont connectés à Internet" [IEEE, 2014]. L'IEEE, en tant qu'une des organisations de normalisation les plus importantes, travaille sur les normes relatives à l'IoT.

L’Oxford Dictionary fournit une définition concise de l’Internet des objets, c’est-à-dire « inter- connectés via Internet d’appareils informatiques intégrés dans des objets du quotidien afin qu’ils puissent envoyer et recevoir des données » [3].

L’UIT définit l’Internet des objets comme ”l’infrastructure mondiale de la société de l’information, qui permet des services avancés grâce au développement continu d’éléments interconnectés (physiques et virtuels) basés sur les technologies de communication et d’information interopérables existantes” [4].

1. Point de vue conceptuel : L’Internet des Objets caractérise les objets physiques connectés comme ayant leur propre identité numérique et pouvant communiquer entre eux. Ce réseau établit un pont entre le monde physique et le monde virtuel.
2. Point de vue technique : L’Internet des Objets consiste en une identification numérique directe et standardisée (adresse IP, smtp, protocole http, etc.) d’objets physiques à l’aide d’un système de communication sans fil (qui peut être une puce, Bluetooth ou Wi-Fi).

2.2.2 Architecture de l’IoT

L'architecture de l'IoT se compose de différentes couches interconnectées. La couche physique comprend les objets connectés, les capteurs et les actuateurs. La couche réseau assure la connectivité et la transmission des données. La couche de gestion des données stocke, gère et analyse les données collectées. Enfin, la couche d'application comprend les applications et les services qui utilisent les données de l'IoT pour fournir des fonctionnalités spécifiques.

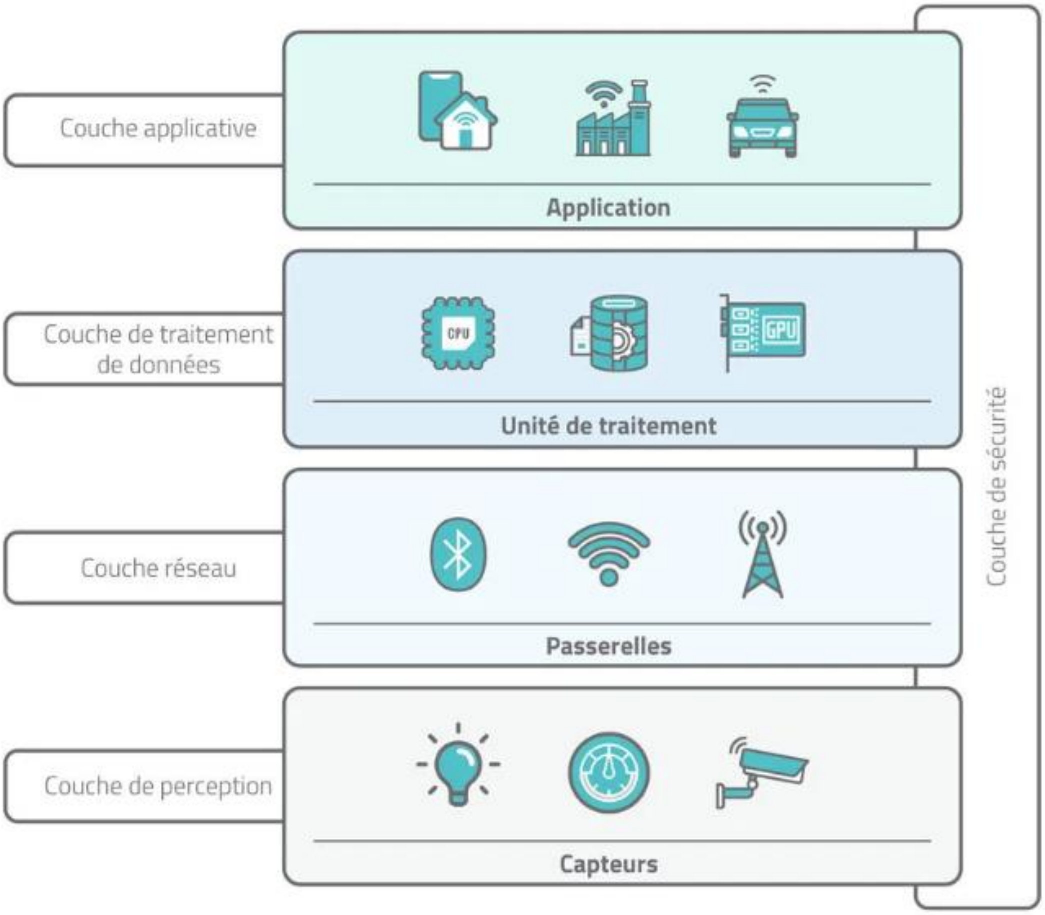

Figure 2. 1 Architecture de l'IoT [5]

2.3 Les objets connectés

2.3.1 Définition

Les objets connectés sont des objets physiques qui intègrent des capteurs, des logiciels et des technologies de communication pour se connecter à Internet et partager des données avec d'autres objets ou systèmes. Ils peuvent être autonomes ou faire partie d'un réseau plus vaste.

2.3.2 Relations entre les objets connectés

Les objets connectés peuvent interagir entre eux de différentes manières. Ils peuvent échanger des données directement ou via des passerelles qui agrègent les informations provenant de plusieurs objets. Les objets connectés peuvent également coopérer pour exécuter des tâches complexes ou se contrôler mutuellement.

2.3.3 Les types des objets connectés

Les objets connectés peuvent appartenir à différentes catégories, notamment les appareils domestiques intelligents (thermostats, éclairages, électroménagers connectés), les dispositifs portables (montres, trackers de fitness), les capteurs environnementaux, les véhicules connectés, les équipements industriels, etc.

2.4 Protocoles et standards de l'IoT

2.4.1 Protocoles et standards de la couche liaison de données IoT

Les protocoles et standards de la couche liaison de données IoT permettent la communication entre les objets connectés et les réseaux. Certains exemples de protocoles couramment utilisés sont Zigbee, Z-Wave, Bluetooth Low Energy (BLE) et Wi-Fi [6].

2.4.2 Les protocoles de la couche réseau

Les protocoles de la couche réseau facilitent l'acheminement des données entre les objets connectés, les passerelles et les serveurs. IPv6 est largement utilisé dans l'IoT pour fournir des adresses uniques à chaque appareil connecté.

2.4.3 Les protocoles de communication

Les protocoles de communication permettent l'échange de données entre les objets connectés et les applications ou systèmes qui les utilisent. Certains exemples populaires de protocoles de communication dans l'IoT incluent MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol) et HTTP (Hypertext Transfer Protocol).

2.5 Les plateformes IoT

Les plateformes IoT sont des infrastructures logicielles qui fournissent des fonctionnalités et des outils pour la gestion, l'analyse et l'exploitation des données générées par les objets connectés. Elles offrent des services tels que la connectivité, le stockage des données, l'analyse des données, la gestion des appareils et des utilisateurs, ainsi que des interfaces de programmation pour le développement d'applications IoT.

2.5.1 Types de plateformes IoT

Il existe différents types de plateformes IoT adaptées à divers besoins et cas d'utilisation. Les plateformes de connectivité IoT se concentrent sur la gestion des connexions et de la communication entre les objets connectés. Les plateformes de gestion des appareils IoT offrent des fonctionnalités avancées pour le suivi, la surveillance et la gestion à distance des appareils connectés. Les plateformes d'analyse IoT permettent d'extraire des informations précieuses à partir des données IoT et de les utiliser pour la prise de décision. Exemples de plateformes IoT : AWS IoT, Microsoft Azure IoT, Google Cloud IoT.

2.5.2 Les avantages de l'IoT

L'IoT offre de nombreux avantages dans divers domaines :

- Amélioration de l'efficacité et de la productivité grâce à l'automatisation des processus et à la collecte de données en temps réel.
- Optimisation des ressources et réduction des coûts grâce à une utilisation plus intelligente des équipements et des infrastructures.
- Amélioration de la qualité de vie grâce à des services et applications intelligentes, telles que la domotique et les systèmes de santé connectés.
- Création de nouvelles opportunités commerciales et de nouveaux modèles économiques basés sur les services et les données.

2.6 Domaines d'application de l'IoT

2.6.1 Smart home

L'IoT trouve des applications dans les maisons intelligentes, où les objets connectés tels que les thermostats intelligents, les systèmes d'éclairage automatisés, les caméras de sécurité et les assistants vocaux permettent aux utilisateurs de contrôler et de gérer leur domicile de manière plus efficace et confortable.

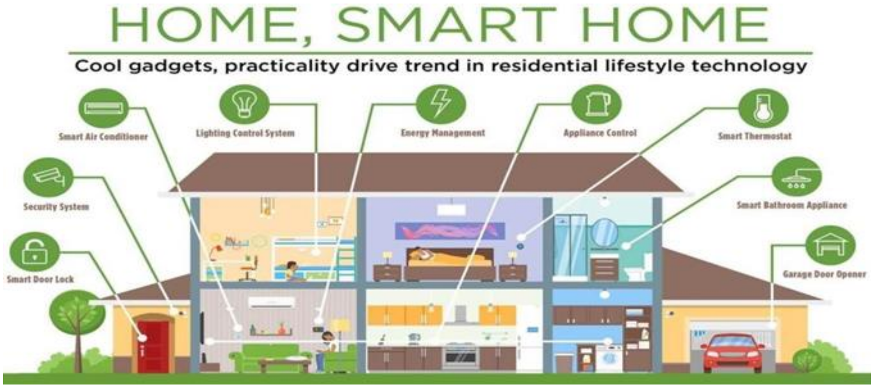

Figure 2. 2: Smart home.

2.6.2 Smart cities

Les villes intelligentes utilisent l'IoT pour améliorer la gestion des ressources, la mobilité urbaine, la sécurité publique, la gestion des déchets, l'éclairage public intelligent et la surveillance environnementale [7].

2.6.3 L'IoT industriel

Dans le secteur industriel, l'IoT est utilisé pour la surveillance et le contrôle des équipements, la maintenance prédictive, l'optimisation des processus de production et la gestion de la chaîne d'approvisionnement.

2.6.4 Voitures connectées

Les voitures connectées intègrent des technologies IoT pour offrir des fonctionnalités telles que la navigation GPS, l'assistance à la conduite, la gestion des flottes de véhicules et la connectivité avec les infrastructures routières.

Figure 2. 3: Voitures connectées.

2.6.5 Healthcare

L'IoT est utilisé dans le domaine de la santé pour créer des systèmes de santé connectés. Cela comprend des dispositifs portables qui surveillent les signes vitaux, des piluliers intelligents pour la gestion des médicaments, des systèmes de suivi à distance pour les patients atteints de maladies chroniques, et des solutions d'analyse des données pour améliorer les soins de santé.

2.6.6 Agriculture

L'IoT joue un rôle important dans l'agriculture de précision, permettant aux agriculteurs d'optimiser l'utilisation des ressources telles que l'eau et les engrais, de surveiller les conditions environnementales, de suivre la santé des cultures et du bétail, et de prendre des décisions basées sur les données pour améliorer les rendements et la productivité [8].

2.7 Les limites et les défis de l'internet des objets

2.7.1 Les limites de l'IoT et les défis de l'IoT

Malgré ses nombreux avantages, l'IoT présente également des limites et des défis. Certains des défis incluent la sécurité et la confidentialité des données, la gestion des énormes quantités de données générées, l'interopérabilité entre les différents systèmes IoT, la durée de vie limitée des batteries des objets connectés et les préoccupations éthiques liées à la collecte et à l'utilisation des données personnelles [9].

2.8 Conclusion

L'Internet des objets (IoT) est une technologie émergente qui transforme la manière dont nous interagissons avec le monde physique[10]. Grâce à la connectivité et à la collecte de données, l'IoT ouvre de nouvelles opportunités dans de nombreux domaines tels que la domotique, les villes intelligentes, l'industrie, les véhicules connectés, la santé et l'agriculture. Dans ce chapitre, nous avons essayé de clarifier certains concepts liés à l'IoT. Nous avons valu également différentes technologies de réseau utilisées dans l'IoT. Nous avons essayé de décrire certaines plateformes IoT existantes et leurs architectures internes. Nous sommes arrivés à la conclusion que chacun a sa propre approche interne et sa propre vision, et malgré les différences, chacun utilise sa propre façon de répondre aux besoins de ses utilisateurs[11]. Cependant, malgré le plus grand succès de cette dernière, elle doit surmonter un certain nombre de défis et de contraintes qui entravent son développement et son déploiement à grande échelle, à savoir l'interopérabilité, et surtout la segmentation verticale de son marché.

CHAPITRE 3

Étude, conception et réalisation

Chapitre 3 : Étude, conception et réalisation

3.1 Introduction

Le présent chapitre se concentre sur l'étude, la conception et la réalisation d'une plateforme IOT dans le cadre de sécurisation du Datacenter. Ce chapitre vise à fournir une vue d'ensemble détaillée du processus suivi par la société pour développer et mettre en place ce système en mettant l'accent sur les aspects clés de l'étude, de la conception et de la réalisation. Dans cette phase d'étude, nous avons examiné attentivement les besoins et les objectifs du système, en tenant compte des exigences fonctionnelles et non fonctionnelles. Nous avons réalisé une analyse approfondie des processus existants, identifié les lacunes et les opportunités d'amélioration, et évalué les différentes options technologiques et architecturales disponibles. Cette étude préliminaire a permis de définir les objectifs et les contraintes du système, en fournissant une base solide pour la phase de conception. La phase de conception a été axée sur la création d'une architecture logicielle solide et extensible pour le système. Nous avons utilisé les principes de conception orientée objet et les meilleures pratiques pour modéliser les différentes composantes du système, définir les interactions entre elles et spécifier les fonctionnalités clés. Nous avons également pris en compte les aspects de sécurité, de performance et de convivialité lors de la conception de l'interface utilisateur. Enfin, la phase de réalisation a impliqué la mise en œuvre concrète du système, en utilisant les outils et les technologies appropriés. Nous avons suivi une approche itérative et incrémentale pour le développement, en réalisant des tests réguliers et des ajustements pour garantir la qualité et la robustesse du système. Nous avons également procédé à une intégration rigoureuse des différents modules et composantes, en veillant à ce que le système fonctionne de manière cohérente et efficace. Ce chapitre détaille donc l'étude préliminaire, la conception architecturale, les choix technologiques, la mise en œuvre et les résultats obtenus lors de la réalisation du système. Il met en évidence les défis rencontrés, les solutions adoptées et les enseignements tirés tout au long du processus. En fin de compte, ce chapitre vise à fournir une compréhension approfondie du système développé et des décisions prises pour atteindre les objectifs du projet.

3.2 Étude analytique du «DATACENTRE » du C.P.I. spa

Les données sont cruciales pour chaque entreprise au 21ème siècle. Toutes les tailles d'entreprises s'appuient sur les données pour effectuer leurs activités quotidiennes. Par conséquent, la disponibilité des données est un défi majeur qui nécessite des emplacements appropriés pour leur stockage. Ces emplacements doivent avoir des propriétés garantissant une disponibilité 24 heures sur 24 et une protection de haut niveau contre les menaces potentielles.
Les industries des centres de données et des télécommunications sont toutes deux essentielles à l'économie mondiale. Ces plateformes fonctionnent en permanence 24 heures sur 24, 7 jours sur 7, 365 jours par an. Tout temps d'arrêt de leurs systèmes peut avoir d'énormes répercussions, voire des catastrophes, qui ne peuvent être ignorées. De plus, ces plateformes sont confrontées à un énorme défi en raison de la demande croissante. En 2025, on estime que 75.44 milliards d'appareils connectés seront utilisés. C'est grâce à de nouvelles applications comme le cloud computing, ainsi qu'à la croissance structurelle des entreprises fournissant ces services.

3.2.1 Les composants d'un Datacenter

Les centres de données peuvent abriter de grands réseaux d'ordinateurs et d'espaces de stockage. Certaines entreprises utilisent ces centres pour stocker de grandes quantités de données, qui peuvent être traitées, organisées et arrangées. En s'appuyant sur un centre de données, de nombreuses entreprises diraient qu'il s'agit d'un élément essentiel de leurs opérations quotidiennes. Un centre de données est composé de nombreux composants différents. Les éléments de base comprennent les routeurs réseau, les pare-feu, les racks physiques, les câbles et les sous-systèmes de stockage. De plus, il existe des ordinateurs appelés serveur qui sont inclus dans chaque centre de données de base. Les centres de données ont besoin d'un emplacement sécurisé suffisamment grand pour accueillir tous leurs équipements. Cela comprend un interrupteur électrique, des réserves d'énergie, des générateurs de secours, un système de ventilation et de refroidissement et un système de distribution d'énergie. De plus, ces centres ont besoin d'une connexion Internet suffisamment puissante pour gérer l'équipement. En utilisant plusieurs centres de données, les grandes entreprises peuvent réduire la latence, augmenter les performances et améliorer la fiabilité des applications[12].

Un centre de données basique regroupe des :

- Des serveurs
- Des sous-systèmes de stockage
- Des commutateurs de réseau
- Des routeurs
- Des firewalls
- Des câbles et des racks physiques permettant d'organiser et d'interconnecter tout cet équipement informa- tique.

3.2.2 Infrastructure adéquate pour un Datacenter

Pour garantir un bon fonctionnement du Datacenter on doit lui assurer une infrastructure adéquate, comme suit :

- Un système distribution d'énergie.
- Un commutateur électrique.
- Des réserves d'énergie.
- Des générateurs dédiés au backup.
- Un système de ventilation et de refroidissement.
- Une puissante connexion Internet.

NB : une telle infrastructure nécessite un espace physique suffisamment grand et sécurisé.

3.2.3 Les différents types de centres de données

Les Datacenters ne sont pas déterminés par leur taille physique. Les petites entreprises peuvent utiliser une petite salle où sont juxtaposés plusieurs serveurs et espaces de stockage interconnectés. Les entreprises informatiques de grande envergure, comme Facebook, Amazon ou Google, peuvent quant à elles remplir un immense entrepôt. Il est également possible de mettre en place des installations mobiles, telles que des containers, aussi appelés « Datacenter in a box », pouvant être déplacés et déployés au besoin.[13]

Il est en revanche possible de définir un Datacenter selon :

- Son niveau de fiabilité.
- Son niveau de résilience.

On classe ainsi les centres de données par tiers. En 2005, l'ANSI et la TIA ont publié le standard ANSI/TIA-942, Télécommunications Infrastructure Standard for Datacenters. Ce standard définit quatre tiers de designs de Datacenter, (voire la figure suivante).

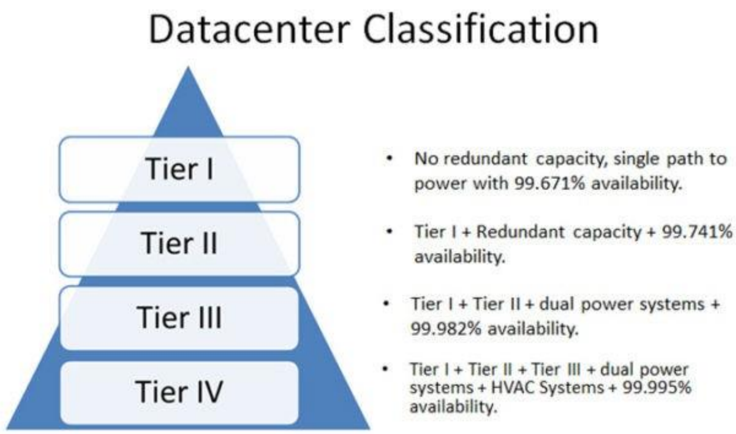

Figure 3. 1: Les différents tiers du Datacenter.

3.3 Architecture et design d'un Datacenter

Théoriquement, n'importe quel espace suffisamment vaste peut servir de Datacenter. Cependant, le design et l'implémentation d'un Datacenter nécessitent de prendre plusieurs précautions. Par-delà les problèmes basiques du coût et des taxes, les sites sont sélectionnés sur de nombreux critères, comme :

- La localisation géographique.
- La stabilité météorologique.
- L'accès aux routes et aux aéroports.
- La disponibilité énergétique.
- Les télécommunications ou encore l'environnement politique.

Une fois qu'un site est sécurisé, l'architecture d'un Datacenter peut être conçue en portant attention à l'infrastructure électrique et mécanique, et aussi à la composition et à disposition de l'équipement informatique.

Tous ces critères dépendent du tiers de Datacenter visé.

3.4 La sécurité et la sureté d'un Datacenter

Les administrateurs de Datacenters font face à d'importants challenges. Ils doivent sécuriser les nouveaux environnements de Datacenter sans en compromettre les performances ni le fonctionnement.

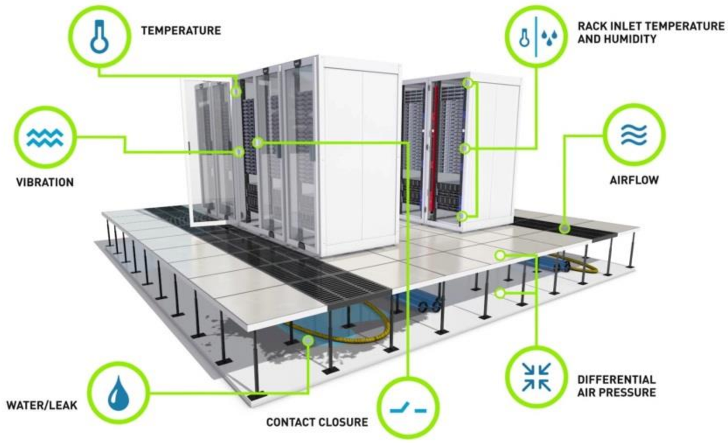

Figure 3. 2: Les paramètres d'environnement du Datacenter.

3.5 La sécurité

Pour protéger le Datacenter des événements non intentionnels, fortuits, accidentels, pouvant affecter sa continuité de service ou son bon fonctionnement il faut mettre en place un système de :

- Détection d'incendie et d'extinction d'incendie
- Détection de températures excessives : urbanisation, confinement, refroidissement.
- Détection de fuites et dégâts des eaux.
- Détection de fuite de gaz.

3.6 La sureté

Pour protéger le Datacenter des actes et des événements intentionnels et malveillants, il faut mettre en œuvre des solutions telles :

- Gestion et contrôle des accès au Datacenter
- Protection périmétrique, passive ou active
- Télésurveillance et vidéo
- Mesures pour assurer la cyber-sécurité des équipements

3.7 DCIM(Data Center Infrastructure Management)

DCIM (Data Center Infrastructure Management) est un logiciel informatique qui aide les opérateurs de centres de données à suivre et à gérer leur infrastructure. Il comprend des outils d'analyse de l'utilisation et de la consommation d'énergie, de surveillance des infrastructures et de gestion du changement. DCIM est récent, mais a déjà intégré de nouvelles fonctionnalités au fil du temps. Les centres de données nécessitent un approvisionnement constant en électricité et un refroidissement suffisant. Cela est dû au fait que de nombreux systèmes informatiques importants reposent sur ces utilitaires. Un DCIM est utilisé pour surveiller l'éfficacitée énergétique et contrôler les coûts énergétiques en collectant des données à partir de toutes les ressources du centre de données. Cela inclut toutes les infrastructures critiques telles que la distribution d'énergie électrique, les alimentations électriques sécurisées, le refroidissement et d'autres équipements sensibles. Les DCIM collectent également des données automatiquement via des capteurs et des logiciels. Ce logiciel combine ensuite des données physiques avec des enregistrements historiques pour créer un tableau de bord central pour la surveillance des données. Les DCIM aident également les gestionnaires de centres de données à planifier les mises à niveau, à modifier les systèmes et à entretenir les systèmes en collectant des données et en les rapportant à un tableau de bord unique. C'est un rôle critique pour les centres comme les hébergeurs, qui doivent constamment s'adapter aux besoins de leurs clients. DCIM permet aux administrateurs de répondre plus rapidement aux problèmes qui entraîneraient des temps d'arrêt ou même des pannes.

3.7.1 Importance du DCMI

À mesure que les infrastructures informatiques deviennent plus complexes, que ce soit sur site ou hors site, l'importance des solutions DCIM augmente. Avant même que les données et les applications ne soient de plus en plus migrées vers des environnements gérés, les entreprises doivent mieux comprendre leurs appareils, les sources d'énergie associées et la connectivité requise. DCIM fournit une fenêtre claire à travers laquelle les voir.

Aujourd'hui, DCIM apporte une plus grande valeur ajoutée dans les environnements distants. Frost & Sullivan montre que 47 % des organisations utilisent aujourd'hui des services gérés, et ce nombre augmentera considérablement. Avec de plus en plus de données et d'applications résidant dans des environnements gérés, DCIM donne aux DSI l'assurance qu'ils ont un contrôle total sur leur infrastructure critique. Alors, que peut faire DCIM pour améliorer la façon dont les organisations utilisent l'hébergement.

3.7.2 Fonctionnement du DCIM

DCIM se compose de capteurs qui collectent automatiquement les données des composants. Ils sont hébergés sur des serveurs ou des serveurs dans un centre de données. Tout est contrôlé par un logiciel de surveillance. Le centre d'exploitation du réseau est chargé d'assurer le fonctionnement optimal du système de surveillance de ce centre de données.

Cela évite les goulots d'étranglement de données. Les experts estiment qu'un tel système de gestion devrait être activé lorsque le centre de données atteint 50 % de sa capacité. Les outils DCIM facilitent l'utilisation maximale d'une infrastructure complexe en stabilisant 85 % des ressources d'énergie et de stockage disponibles.

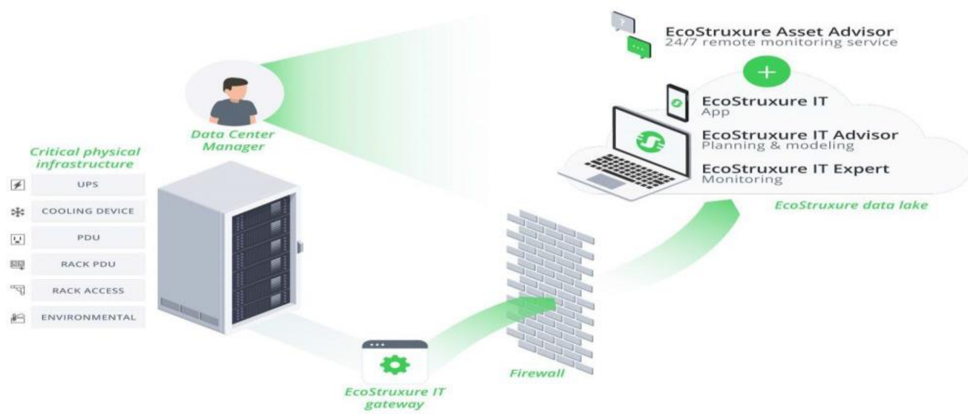

Figure 3. 3: Architecture de la solution DCIM EcoStruxure IT de Schneider Electric.

3.8 Étude du système cible

3.8.1 Objectifs du système cible

L'objectif principal du système projeté est l'amélioration de la supervision et la sécurisation de l'environnement abritant le système de paiement de masse A.T.C.I au sein de CPI SPA. Cet objectif peut être découpé en 3 objectifs secondaires présentés ci-dessous :

- Automatiser les communications entre les composants de système d'alerte, de surveillance et de gestion d'accès.
- Implémenter une plateforme de gestion et automatisation des alertes.
- Implémentation d'une application, pour contrôler et recevoir des alertes à partir du système à distance et en temps réel.
- Implémentation d'une couche de sécurisation de l'interopérabilité entre composants au niveau des appareils, des logiciels et de la plateforme.
- Optimiser les processus de gestion des accès.
- Réduire les risques liés à la sécurité des droits d'accès et des privilèges.

Le tableau ci-dessous représente l'arborescence des objectifs qui sont réalisés à travers des actions décomposées en tâches élémentaires :

3.8.2 Périmètre du système cible

Notre système projeté portera sur la supervision et la sécurisation de l'environnement abritant le système de paiement de masse A.T.C.I qui constitue un processus relevant de la responsabilité de la « Sécurité des Systèmes d'Information ». Ainsi, il sera exploité au niveau de la « Département de Sécurité des Systèmes d'Informations » et regroupe Étude du système cible. Plusieurs processus critiques à la sécurité de l'information. De ce fait, notre système doit assurer une couverture fonctionnelle de dizaines des systèmes informatiques nécessitant une supervision et sécurisation, englobant ainsi les volets suivants :

- La communication entre les composants de système d'alerte, de surveillance et de gestion d'accès
- La gestion et l'automatisation des alertes
- Les traitements des demandes d'accès : attribution, modification, révocation, et réactivation.

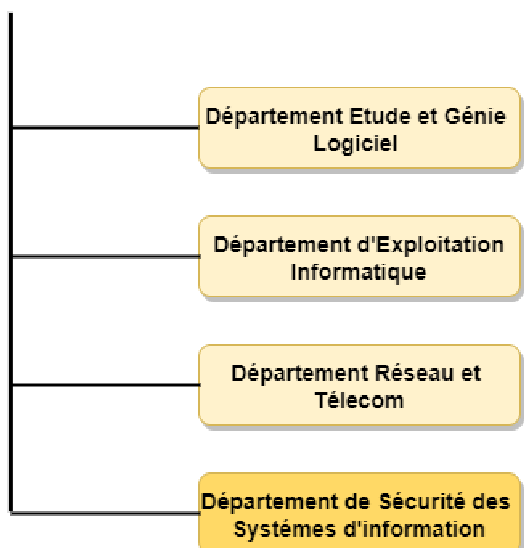

Figure 3. 4: Organigramme DSI.

3.8.3 Acteurs du système cible

Un acteur dans un système d'information représente l'abstraction d'un rôle joué par des entités externes (utilisateur humain, dispositif matériel ou autre système) qui interagissent directement avec le système étudié. L'étude détaillée des processus et des postes de travail dans le chapitre précédent nous a permis de déterminer les différents acteurs intervenant dans notre système. Nous présentons ci-dessous la liste des acteurs du nouveau système :

- **Manager (Responsable Métier)**

C’est le chef d’unité organisationnelle (département, direction, ou autre). Il intervient dans les cas des alertes ou des incidents, il lance la demande de création et intervient dans la revue des accès des membres de son unité organisationnelle.

- **Administrateur système (AppAdmin)**

C’est le responsable de l’administration et de la sécurité de Datacenter au sein de l’organisation. Il est chargé d’exécuter les demandes de création, de modification et de révocation des accès au niveau de Datacenter et de contrôler les différents paramètres de sécurité de l’environnement

- **Ressources Humaines (RH) / Responsable du personnel**

Il représente la structure RH, ou un membre de la structure RH, habilité à initier les demandes de révocation et de réactivation ainsi que le processus de gestion des transferts.

- **Utilisateur / Employé**

Il représente le rôle élémentaire du système. Il s’agit souvent d’un employé au sein de CPI et membre d’une unité organisationnelle. Ses accès et privilèges sont administrés à travers le système sur lequel il a la possibilité de les consulter.

3.8.4 Spécifications fonctionnelles du système cible

Les spécifications fonctionnelles sont réparties selon les actions définies précédemment qui nous permettent d’atteindre les objectifs du système cible. Dans le tableau ci-après, nous avons choisi d’organiser les priorités de notre système futur selon la méthode MSCW :

- Chaque spécification aura une priorité.
- La priorité permet de sélectionner les spécifications les plus importantes.
- Facilite l’ordonnancement.

Priorité	Description

M (Must Have)	Priorité obligatoire et spécification indispensable au système.
S (Should Have)	Spécification importante, mais peut être omise sous conditions.
C (Could Have)	Spécification optionnelle (si le temps le permet).
W (Would Have)	Spécification à prévoir lors des prochaines livraisons du système.

Tableau 3. 1: Méthode MSCW.

3.9 Gestion de paramètres d'environnement

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
1.1	M	Consulter la température moyenne de Datacenter.	1.0
1.2	M	Consulter la température de chaque élément de Datacenter.	1.0
1.3	M	Consulter l'humidité moyenne de Datacenter.	1.0
1.4	M	Consulter l'humidité de chaque élément de Datacenter.	1.0
1.5	M	Détecter s'il y a du mouvement dans le Datacenter.	1.0
1.6	M	Détecter s'il y a du mouvement devant un élément de Datacenter.	1.0
1.7	M	Détecter s'il y a du gaz dans le Datacenter.	1.0
1.8	M	Détecter s'il y a un changement de place d'un élément dans le Datacenter.	1.0
1.9	M	Détecter s'il y a de la poussière sur un élément de Datacenter.	1.0
1.10	M	Lancer des notifications par email, SMS, appel dans le cas d'un incident ou intrusion.	1.0
1.11	M	Sauvegarder l'historique de paramètres de l'environnement.	1.0
1.12	S	Gérer la consommation d'énergie dans le Datacenter.	1.5

Tableau 3. 2: Spécifications - Gestion de paramètres d'environnement.

3.10 Gestion des actifs

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
2.1	M	Consulter la liste des éléments (actifs) dans le Datacenter.	1.0
2.2	M	Introduire un nouveau élément.	1.0
2.3	M	Modifier les informations d'un élément existant.	1.0
2.4	M	Supprimer un élément existant.	1.0
2.5	M	Consulter les informations d'un élément existant.	1.0
2.6	M	Consulter les paramètres d'environnement d'un élément existant.	1.0
2.7	W	Modéliser le Datacenter en 3D	2.0

Tableau 3. 3: Spécifications - Gestion des actifs.

3.11 Gestion des DCIMS

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
3.1	M	Consulter la liste des DCIMS dans le Datacenter.	1.0
3.2	M	Introduire un nouveau DCIM et le lier avec un élément de Datacenter.	1.0
3.3	M	Modifier les informations d'un DCIM existant.	1.0
3.4	M	Supprimer un DCIM existant.	1.0
3.5	M	Consulter les informations d'un DCIM existant.	1.0
3.6	M	Consulter les paramètres d'environnement donnés par un DCIM existant.	1.0
3.7	S	Tester si le DCIM est en bon état	2.0

Tableau 3. 4: Spécifications - Gestion des DCIMS.

3.11 Gestion des composants de DCIMS

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
4.1	M	Consulter la liste des composants d'un DCIM.	1.0
4.2	M	Consulter les informations d'un composant de DCIM existant.	1.0
4.3	M	Consulter les paramètres d'environnement donnés par un composant d'un DCIM existant.	1.0
4.4	M	Tester si le composant de DCIM est en bon état	1.0

Tableau 3. 5: Spécifications - Gestion des composants de DCIMS.

3.12 Gestion des alertes

3.12.1 Gestion des nouvelles alertes

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
5.1	M	Consulter la liste des nouvelles alertes.	1.0
5.2	M	Traiter une alerte.	1.0
5.3	M	Marquer une alerte comme spam.	1.0
5.4	M	Marquer une alerte comme traitée .	1.0

Tableau 3. 6: Spécifications - GGestion des Nouvelles alertes.

3.12.2 Gestion des alertes non traitées

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
6.1	M	Consulter la liste des alertes non traitées .	1.0
6.2	M	Traiter une alerte.	1.0
6.3	M	Marquer une alerte comme spam.	1.0
6.4	M	Marquer une alerte comme traitée .	1.0

Tableau 3. 7: Spécifications - Gestion des alertes non traitées.

3.12.3 Gestion des alertes traitées

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
7.1	M	Consulter la liste des alertes traitées .	1.0
7.2	M	Retraiter une alerte.	1.0

Tableau 3. 8: Spécifications - Gestion des alertes traitées.

3.12.4 Gestion des alertes spam

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
8.1	M	Consulter la liste des alertes spam.	1.0
8.2	M	Traiter une alerte.	1.0
8.3	M	Marquer une alerte comme non-spam.	1.0
8.4	M	Marquer une alerte comme traitée .	1.0

Tab. 3.9: Spécifications - Gestion des alertes spam

3.13 Gestion des ressources humaines

3.13.1 Gestion des demandes de création

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
9.1	M	Initier une demande de création de comptes utilisateur.	1.0
9.2	M	Approuver l’habilitation de l’utilisateur à recevoir les privilèges demandés.	1.0
9.3	M	Rejeter de la demande de création pour un motif à spécifier.	1.0

9.4	M	Dans le cas d'une approbation, exécuter la création.	1.0
9.5	M	Envoyer l'ordre de création à l'administrateur de système concerné.	1.0
9.6	M	Valider la demande de création par l'administrateur	1.0
9.7	M	Signaler une opération de création des privilèges	1.0
9.8	M	Clôturer l'opération.	1.0
9.9	M	Envoyer l'identifiant et du mot de passe du nouveau compte à l'employé	1.0
9.10	M	Indiquer la raison dans le cas d'un échec de création du compte.	1.0
9.11	M	Générer un récapitulatif de la demande de création.	1.0
9.12	C	Annuler une demande de création initiée.	1.1
9.13	M	Spécifier le type de compte à créer (Utilisateur ou Administrateur)	1.0

Tableau 3. 9: Spécifications - Gestion des demandes de création.

3.13.2 Gestion des demandes de révocation

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
10.1	M	Initier une demande de désactivation temporaire/permanente d'un compte utilisateur.	1.0
10.2	M	Dans le cas d'une désactivation temporaire, spécifier la date de retour de	1.0
10.3	M	Demander l'approbation de la date de révocation au manager de l'employé concerné par la demande de révocation.	1.0
10.4	M	Approuver la date de révocation des accès de l'employé.	1.0
10.5	M	Demander un délai supplémentaire avant la révocation par le manager.	1.0
10.6	M	Ouvrir une demande de révocation.	1.0
10.7	M	Envoyer la demande de révocation à l'administrateur de système concerné.	1.0
10.8	M	Notifier le manager de la révocation des comptes de l'utilisateur.	1.0
10.9	M	Suspendre la demande pendant le traitement de la demande du délai	1.0

Tableau 3. 10: Spécifications - Gestion des demandes de révocation.

3.13.3 Gestion des demandes de réactivation

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
12.1	M	Initier une demande de réactivation d'un compte suspendu temporairement.	1.0
12.2	S	Notifier les ressources humaines de la date de réactivation d'un compte	1.1
12.3	M	Ouvrir une demande de réactivation de compte utilisateur.	1.0

12.4	M	Notifier le RH, manager, et l'employé concerné de la réactivation des comptes de ce dernier.	1.0
12.5	S	Prolonger la validité des accès d'un intervenant contractuel.	1.1
12.6	S	Annuler une demande de réactivation.	1.1

Tableau 3. 11: Spécifications - Gestion des demandes de révocation.

3.13.4 Gestion des transferts interdépartementaux

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
13.1	M	Initier la procédure de traitement d'un transfert interdépartemental d'un	1.0
13.2	M	Notifier le manager actuel de l'employé.	1.0
13.3	M	Lancer une demande de révocation des accès actuels de l'employé.	1.0
13.4	M	Notifier le nouveau manager de l'employé du transfert.	1.0
13.5	M	Initier une demande de création des nouveaux comptes de l'employé une fois la désactivation effectuée.	1.0
13.6	M	Notifier les ressources humaines la fin de la procédure du transfert.	1.0
13.7	M	Générer automatiquement d'un récapitulatif du transfert	1.0
13.8	S	Annuler une procédure de transfert.	1.1

Tableau 3. 12: Spécifications - Gestion des transferts interdépartementaux.

3.14 Administration de système

3.14.1 Gestion du dictionnaire de système

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
14.1	M	Configurer la politique de gestion des accès	1.0
14.2	M	Ajouter les applications et systèmes d'information concernés par la gestion des	1.0
14.3	M	Supprimer les applications et systèmes d'information concernés par la gestion des accès.	1.0
14.4	M	Modifier les informations des applications et systèmes d'information concernés par la gestion des accès.	1.0
14.5	M	Configurer la liste des rôles des applications ainsi que leurs privilèges.	1.0
14.6	M	Configurer la liste des droits d'accès compris dans un rôle.	1.0

14.7	M	Ajouter les approbateurs des demandes pour chaque application ou SI.	1.0
14.8	M	Modifier la liste des propriétaires et administrateurs d'une application ou SI	1.0
14.9	S	Configurer les paliers de validation des demandes.	1.1

Tableau 3. 13 : Spécifications - Gestion du dictionnaire de système.

3.14.2 Gestion des comptes utilisateurs

Le tableau suivant regroupe les paramètres et leurs spécifications :

Id	Priorité	Spécification	Cible
15.1	M	Créer un compte utilisateur.	1.0
15.2	M	Supprimer un compte utilisateur.	1.0
15.3	M	Modifier les informations d'un compte utilisateur.	1.0
15.4	M	Configurer les droits d'accès d'un compte utilisateur.	1.0
15.5	M	Visualiser la liste des comptes utilisateurs.	1.0
15.6	M	- Authentifier avec la reconnaissance faciale.	1.0
15.7	S	Réaliser une extraction de la liste des comptes utilisateurs	1.1

Tableau 3. 14 : Spécifications – Gestion des comptes utilisateurs.

3.15 Spécifications techniques du système cible

Une spécification technique ou non fonctionnelle est une exigence qui caractérise une propriété (qualité) désirée du système tel que sa sécurité, sa performance, sa robustesse, sa convivialité, sa maintenabilité, etc. Dans cette partie, nous recensons toutes les contraintes exprimées par le client qui ne traitent pas l'aspect fonctionnel de la solution. Nous avons pu, en collaboration avec notre promoteur et le service IT, définir quelques spécifications techniques que le système doit respecter :

Id	Priorité	Spécification
1	M	Disponibilité 24/7 du système.
2	M	Le système doit être robuste et sécurisé.
3	M	Application du principe du moindre privilège c.-à-d. accorder aux utilisateurs le nombre minimum d'autorisations nécessaires pour compléter leurs travaux.
4	M	Le système doit comporter des règles de sécurité sur les mots de passe (taille minimale, complexité).
5	S	Permission aux utilisateurs de modifier leurs identifiants et mot de passe.
6	M	Le système doit permettre aux utilisateurs de s'authentifier.
7	M	Le système doit être une application web.

8	C	Le système doit permettre l'envoi de notifications par voie d'email, SMS, appel.
9	S	Le système doit permettre d'adapter l'interface aux dimensions de l'écran de l'appareil de l'utilisateur.
10	M	Le système doit être facile à utiliser.
11	M	Le système doit exécuter les travaux dans un temps optimal.
12	M	Le système peut être amélioré par l'ajout d'autres modules pour garantir la souplesse, l'évolutivité et l'ouverture de la solution.
13	M	Le code doit être bien commenté afin de faciliter la maintenance de l'application.

Tableau 3. 15 : Spécifications techniques.

3.15.1 Modèle des cas d'utilisation

Les spécifications recensées dans la partie précédente nous ont permis d'élaborer l'ensemble des cas d'utilisation (CUs) suivants :

Cas d'utilisation	Description
Gestion de paramètres d'environnement	Les activités relatives à la consultation de paramètres d'environnement.
Gestion des actifs	Les activités relatives à l'ajout, suppression, modification des informations d'un élément dans le Datacenter.
Gestion des DCIMS	Les activités relatives à l'ajout, suppression, modification des informations, consultation de retour d'un DCIM liée élément dans le Datacenter.
Gestion des composants de DCIMS	Les activités relatives à l'ajout, suppression, modification des informations d'un DCIM liée à un élément dans le Datacenter.
Gestion des nouvelles alertes	Les activités relatives à la consultation, traitement, classification des nouvelles alertes.
Gestion des alertes non traitées	Les activités relatives à la consultation, traitement, classification des alertes non traitées .
Gestion des alertes traitées	Les activités relatives à la consultation, retraitement, classification des alertes traitées .
Gestion des alertes spam	Les activités relatives à la consultation, traitement, classification des alertes spam.
Gestion des demandes de création	Les activités relatives au traitement des demandes de création d'un nouveau compte utilisateur sur un système donné.
Gestion des demandes de révocation	Les activités réalisées afin de désactiver les droits d'accès d'un utilisateur.
Gestion des demandes de modification	Les activités effectuées pour modifier les privilèges déjà accordés à un utilisateur.
Gestion des demandes de réactivation	Activités réalisées dans le cadre de réactivation d'un compte utilisateur désactivé temporairement.
Gestion des transferts interdépartementaux	Activités relatives à la mise à jour des comptes d'un employé effectuant un transfert entre départements.
Visualisation des informations des accès	Les activités relatives à visualiser l'état des accès d'un objet (département, utilisateur, système) donné.
Administration de la plateforme	Activités relatives à la gestion des comptes utilisateurs et le dictionnaire des habilitations des systèmes.

Tableau 3. 16 : Tableau des cas d'utilisation.

3.16 Présentation du système cible

Pour répondre aux besoins identifiés, nous proposons la mise en place d'une plateforme web support de la gestion des accès logiques et destinée aux différents acteurs impliqués dans la gestion des droits d'accès et habilitations. Cette solution a pour objectif d'optimiser les processus de traitement des demandes d'accès et d'automatiser la validation des habilitations et de la séparation des tâches. Ceci contribuera à réduire les délais et les risques liés aux accès logiques. De plus, notre système centralise les informations relatives aux droits d'accès et fournit des récapitulatifs des demandes, favorisant ainsi la traçabilité et la conformité aux normes de sécurité. À travers le schéma général ci-dessous, nous présentons les différents volets de notre système. Pour une bonne organisation de la solution, nous l'avons découpée en 3 modules dont chacun assure plusieurs fonctionnalités. Ce découpage favorise aussi l'évolutivité de la solution et facilite l'intégration des futurs modules.

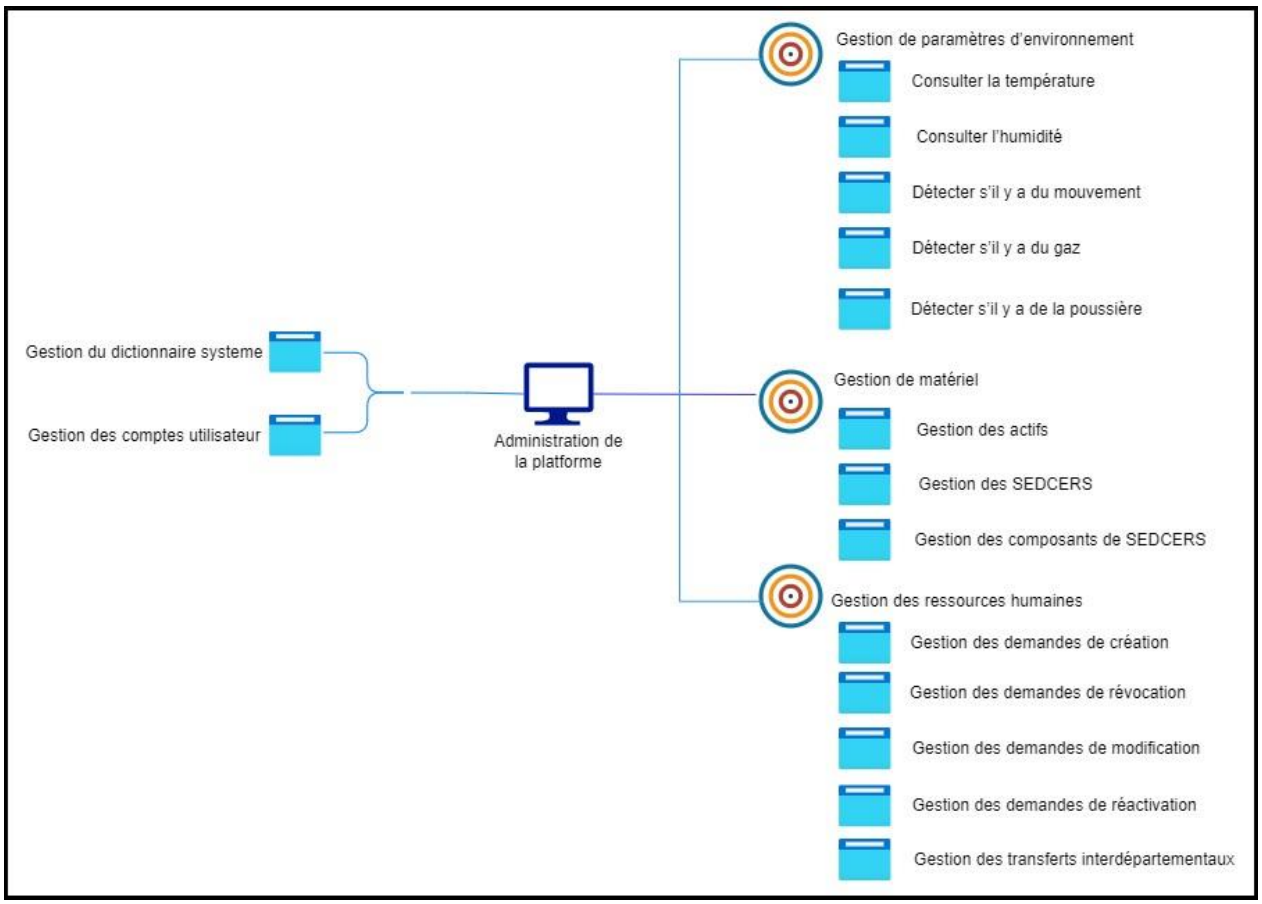

Figure 3. 5: Architecture générale du système cible.

Les volets compris dans notre système sont les suivants :

3.16.1 Gestion de paramètres d'environnement

Il s'agit du module principal de notre système. Il permet de consulter les paramètres d'environnement (température, humidité, mouvement, gaz, poussière), et de lancer des notifications par email, SMS, appel dans le cas d'un incident ou intrusion.

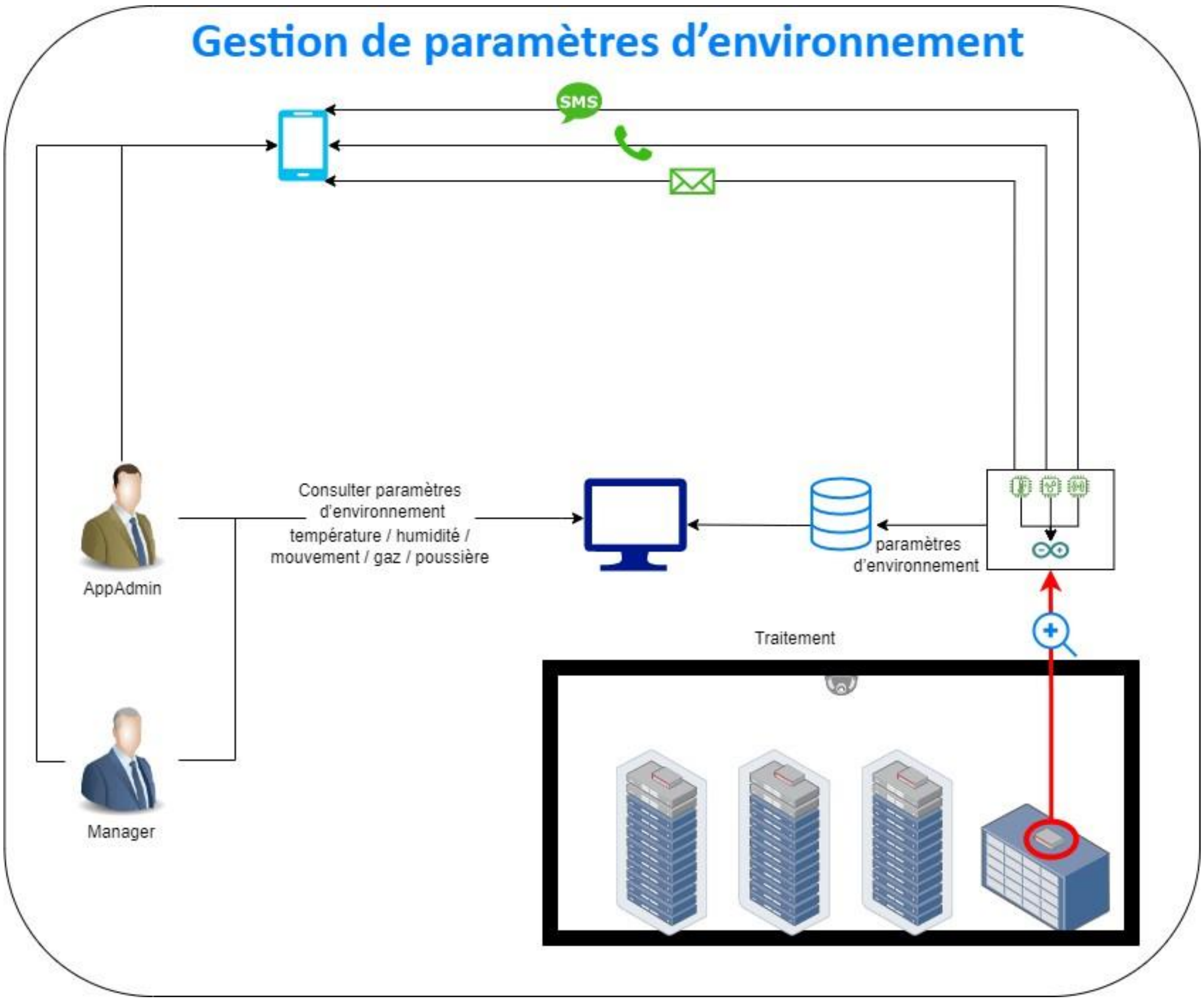

Figure 3. 6 : Système cible – Gestion de paramètres d'environnement.

3.16.2 Gestion de matériel

Le module de gestion des actifs permet d'ajouter, supprimer un élément(actif) ,modifier les informations d'un élément existant, et consulter les paramètres d'environnement d'un élément existant. Ainsi, il permet d'ajouter, supprimer un DCIM, modifier les informations d'un DCIM existant, et consulter les paramètres d'environnement donnés par DCIM existant. Aussi, il permet de consulter la liste des composants d'un DCIM, les informations d'un composant de DCIM existant, et consulter les paramètres d'environnement donnés par un composant d'un DCIM existant et tester si le composant de DCIM est en bon état.

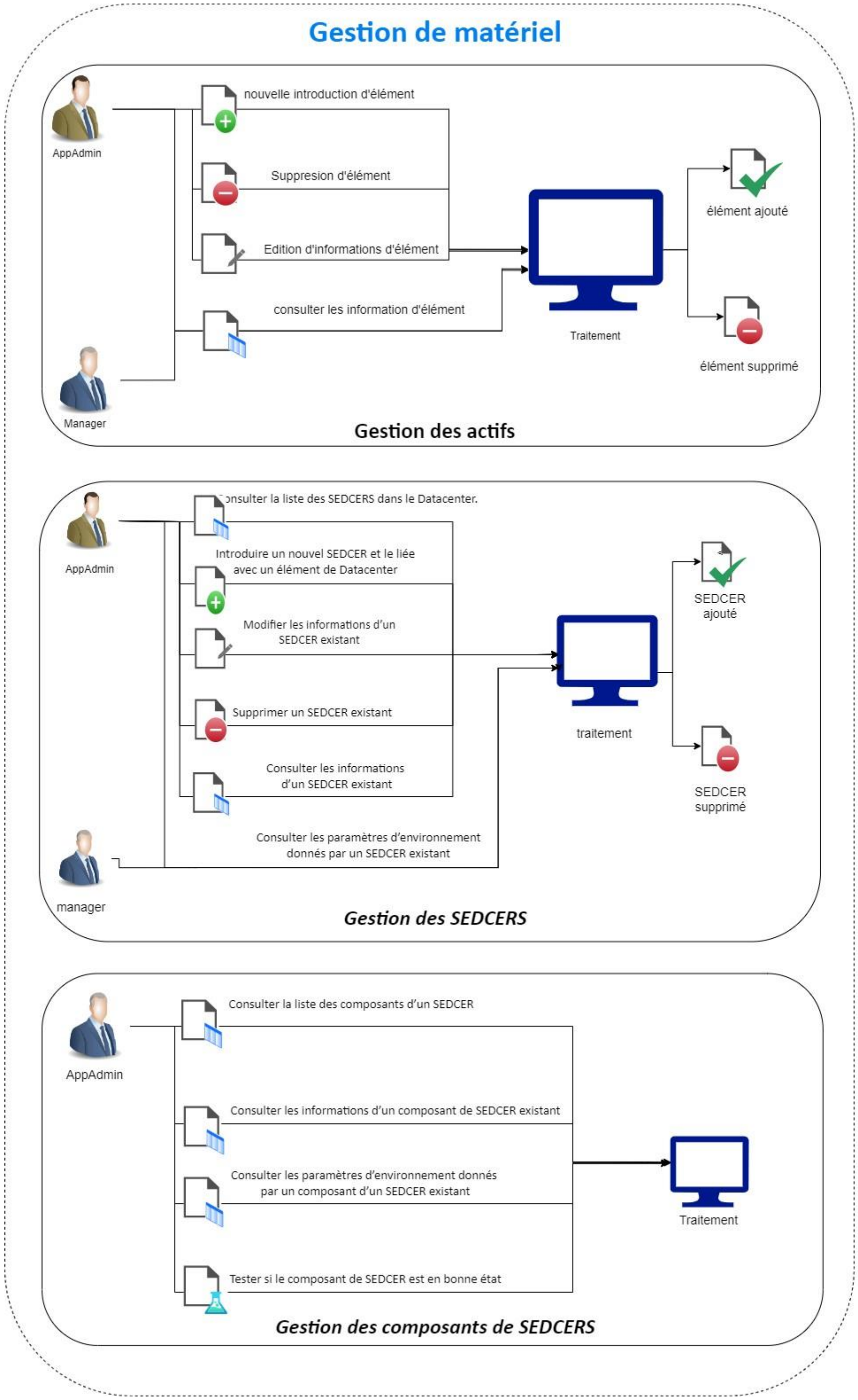

Figure 3. 7 : Système cible – Module de gestion de matériel.

3.16.3 Gestion des alertes

Le module de gestion des alertes permet de gérer les nouvelles alertes, les alertes non traitées, les alertes traitées, les alertes spam.

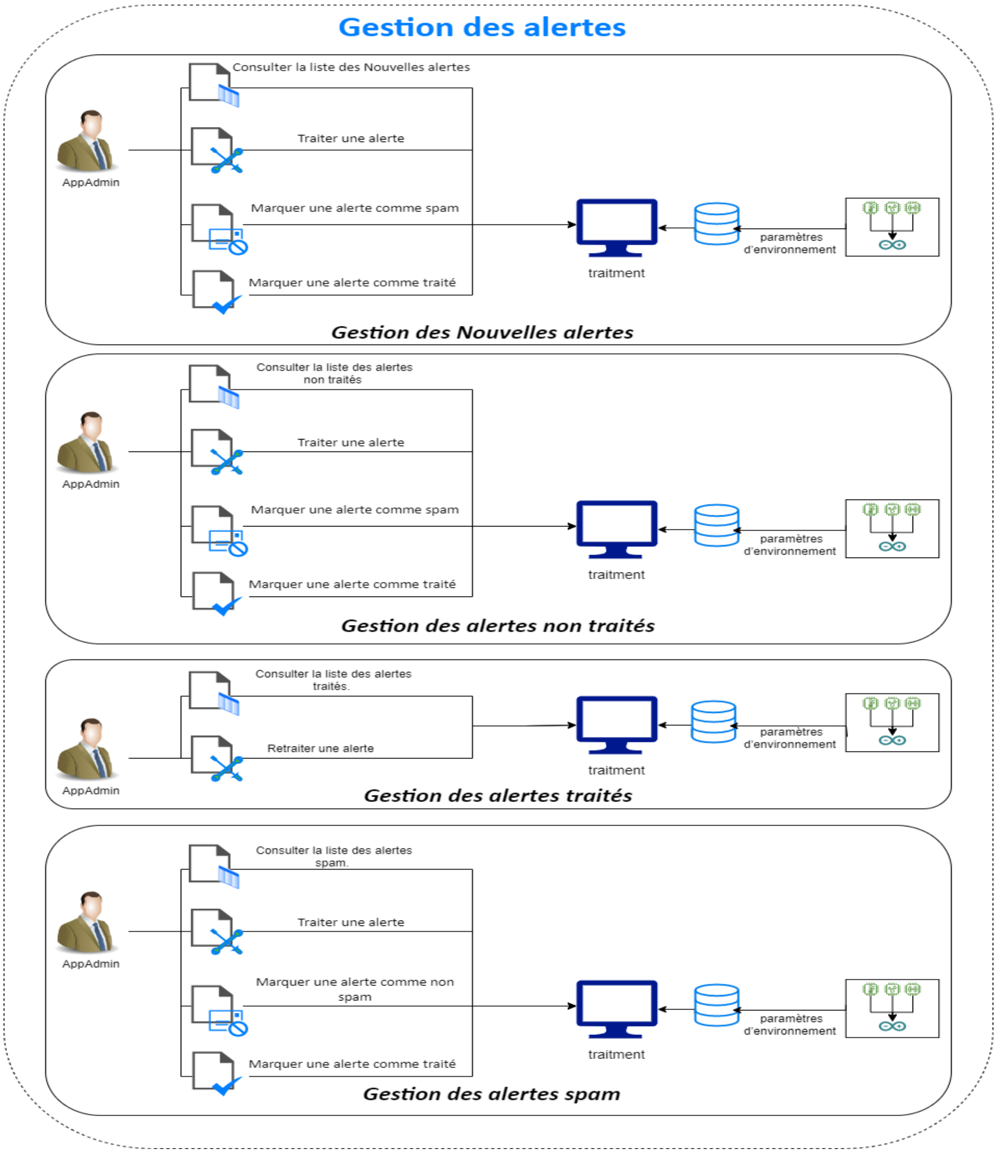

Figure 3. 8 : Système cible – Module de gestion des alertes.

3.16.4 Gestion des ressources humaines

Le module Gestion des ressources humaines permet d'effectuer des demandes d'accès selon un workflow de validation automatisé, et fournit à chaque acteur impliqué dans le processus de traitement d'une demande une interface dédiée à l'accomplissement de ses tâches.

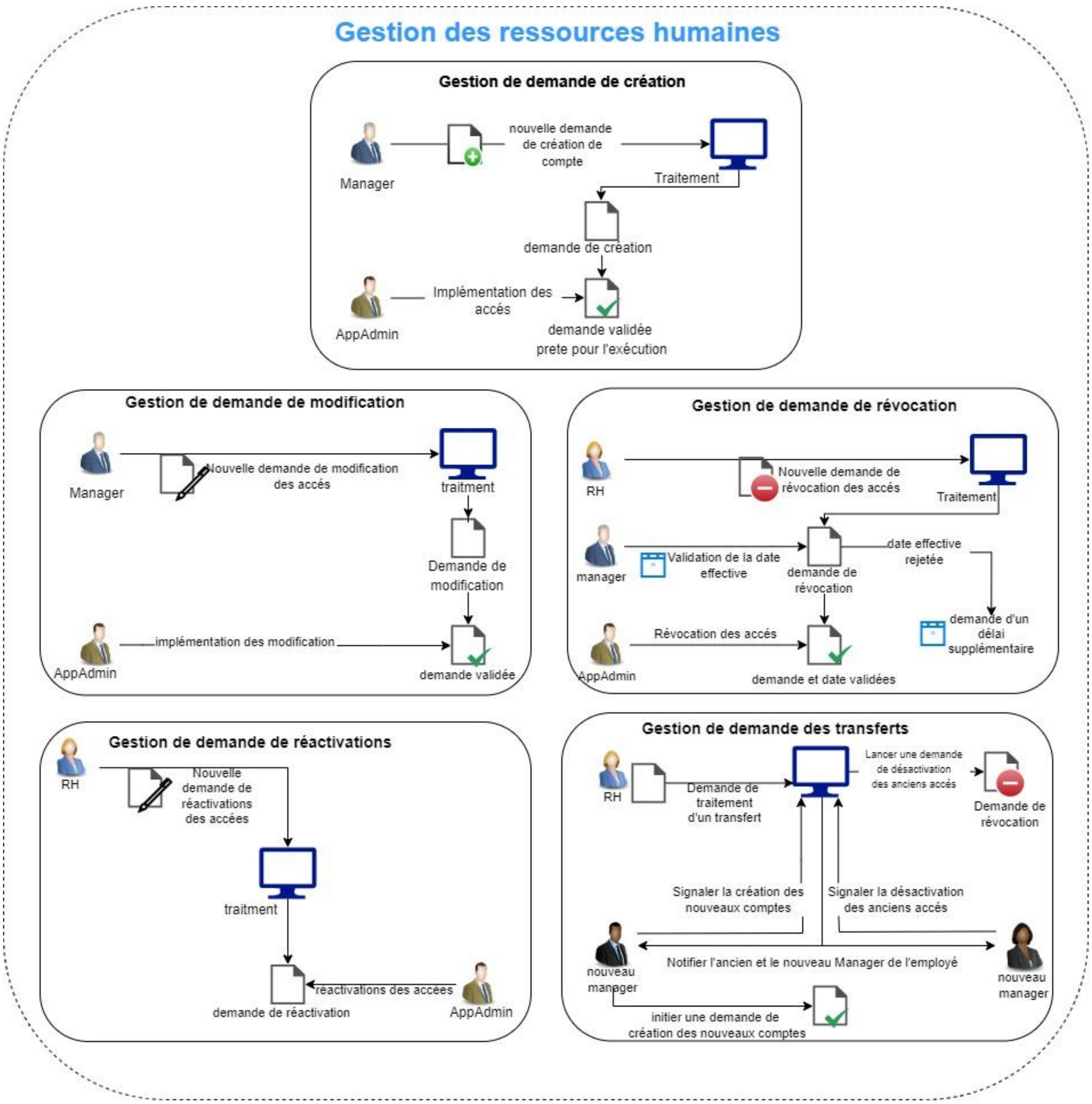

Figure 3. 9 : Système cible – Module de gestion des ressources humaines.

3.16.5 Administration de la plateforme

Le module Gestion des ressources humaines permet d'effectuer des demandes d'accès selon un workflow de validation automatisé, et fournit à chaque acteur impliqué dans le processus de traitement d'une demande une interface dédiée à l'accomplissement de ses tâches.

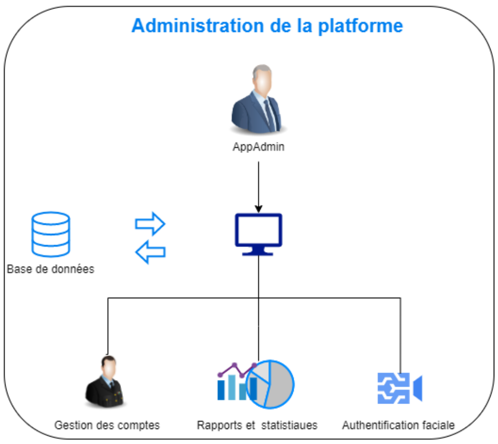

Figure 3. 10 : Système cible – Module d'administration de la plateforme.

3.17 Normes et standards mis en œuvre

La conformité aux normes et standards de la sécurité des systèmes d'information est primordiale pour une gestion des accès logiques réussite. Étant un objectif principal de notre projet, le système cible que nous proposons assure la mise en œuvre les recommandations de la norme ISO 27002, qui constitue la référence en termes de SMSI. Ainsi que les meilleures pratiques du standard NIST SP 800-53 qui fournit une liste de contrôle à respecter pour garantir la résilience des systèmes d'information. De plus, notre système de gestion des accès logiques prend en charge une partie des activités du « Access Management » définie dans ITILv4. La figure suivante présente la projection de ces normes et standards par rapport à notre système :

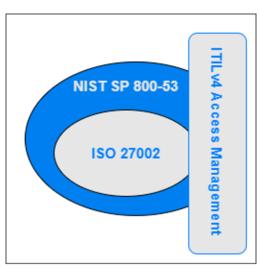

Figure 3. 11 : Normes et standards mis en œuvre.

3.18 Développement d'un nouveau système de supervision et la sécurisation de Datacenters

Concevoir et réaliser un système d'information dédié à supervision et la sécurisation de l'environnement abritant le système de paiement de masse A.T.C.I. dans le cadre d'un projet plus large consistant en la mise en place d'une plateforme AioT (Artificial Intelligence of Things), ciblant ainsi le besoin spécifique de l'organisation. Dans ce cas nous serons amenés à assurer la gestion du projet de la phase d'analyse de besoin jusqu'à son implémentation ainsi que la conduite de changement pour la prise en main.

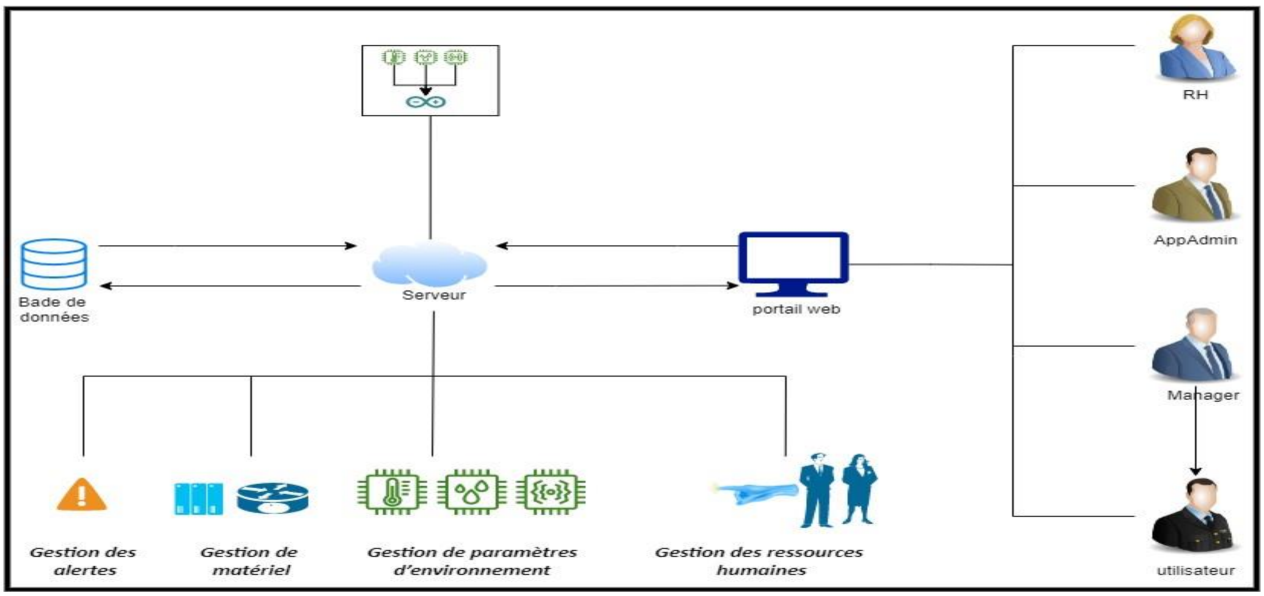

Figure 3. 12 : Schéma de la solution de mise en œuvre 2.

3.19 Conception du système cible

3.19.1 Diagrammes de classes de conception

Les diagrammes de classes de conception permettent de représenter les entités manipulées par les utilisateurs. Dans notre démarche, ils modélisent la structure de ces entités dans le cadre de développement orienté objet. Nous avons réparti notre diagramme en 4 packages, chacun représentant un volet principal de notre solution. Nous avons aussi adopté le modèle MVC (Model, View, Controller) de sorte que chaque volet contient 3 types de classes :

- **Modèle :** Il s'agit ici des données manipulées à travers le système. Elles seront sauvegardées dans une base de données relationnelle et représentées dans le diagramme par des classes.

- **Contrôleur :** Il lie le modèle à la vue et gère les interactions avec l'utilisateur. Le contrôleur regroupe les différentes fonctions de traitement et agit sur les données (Modèle).
- **Vue :** La vue permet de donner une présentation des données issues du modèle. Dans notre diagramme de classes, la vue n'est pas explicitée directement, mais à travers les interfaces qui permettent à l'utilisateur de visualiser les données.

3.19.2 Gestion de paramètres d'environnement

La figure ci-après regroupe toutes les classes utilisées dans le cadre de la gestion de paramètres d'environnement.

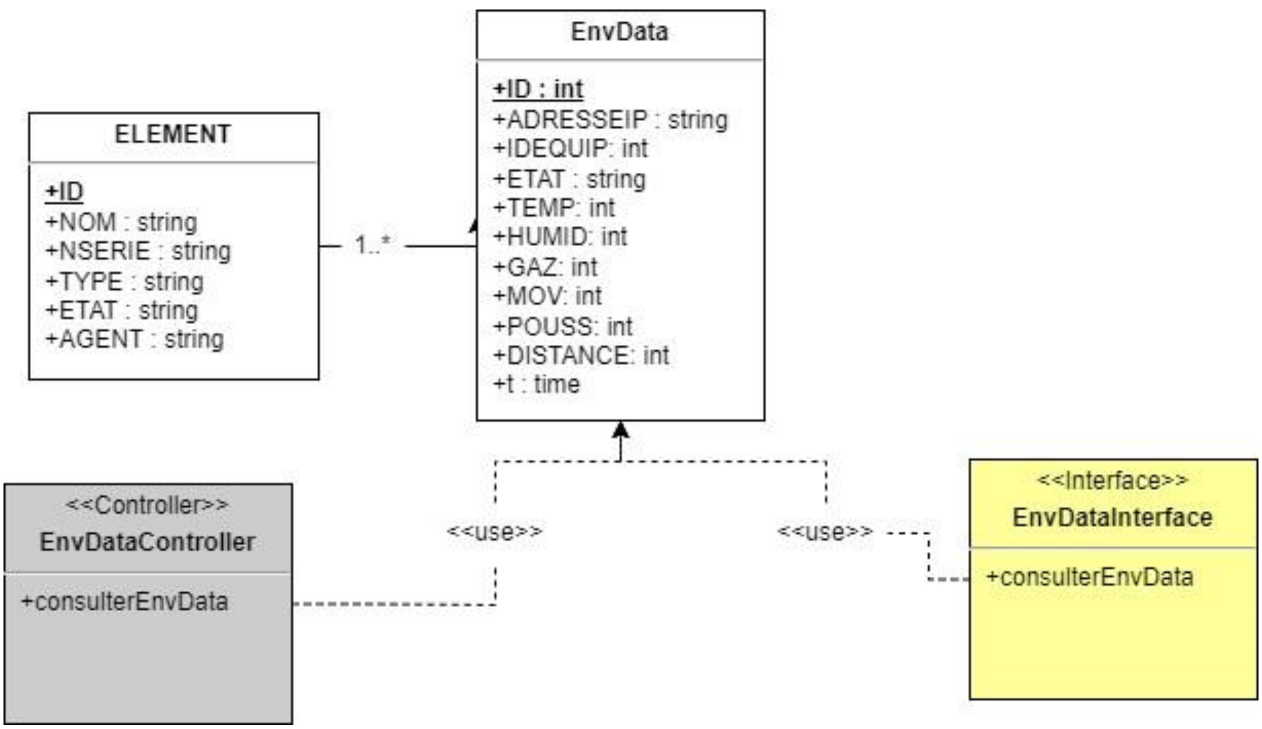

Figure 3. 13 : Diagramme de classes - Gestion de paramètres d'environnement.

3.19.3 Gestion de matériel

La figure ci-après regroupe toutes les classes utilisées dans le cadre de la gestion de matériel(Gestion des actifs, Gestion des DCIMS, Gestion des composants de DCIMS).

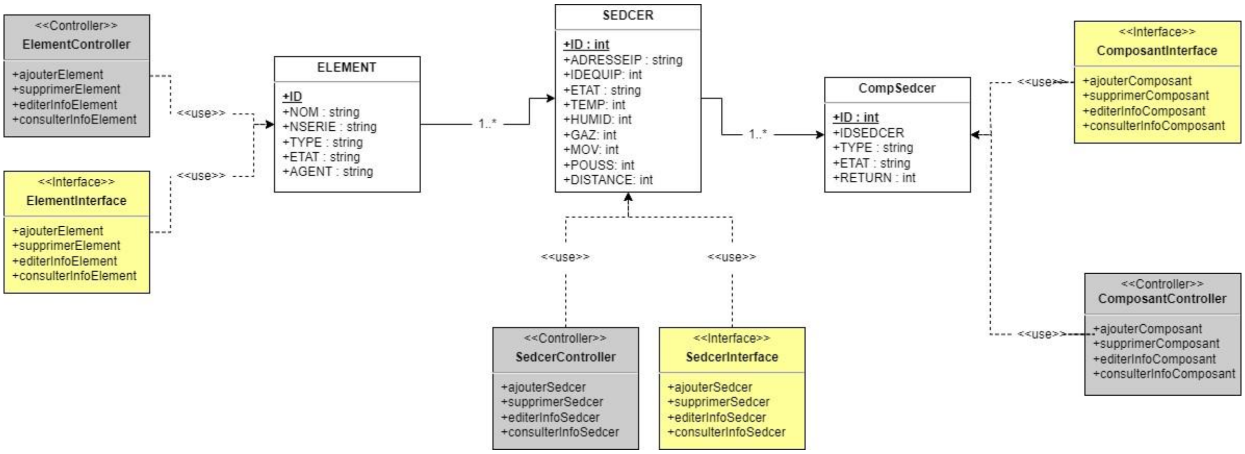

Figure 3. 14 : Diagramme de classes - Gestion de matériel.

3.19.4 Gestion des alertes

La figure ci-après regroupe toutes les classes utilisées dans le cadre de la gestion des alertes(nouvelles alertes , alertes non traitées , alertes traitées , alertes spam).

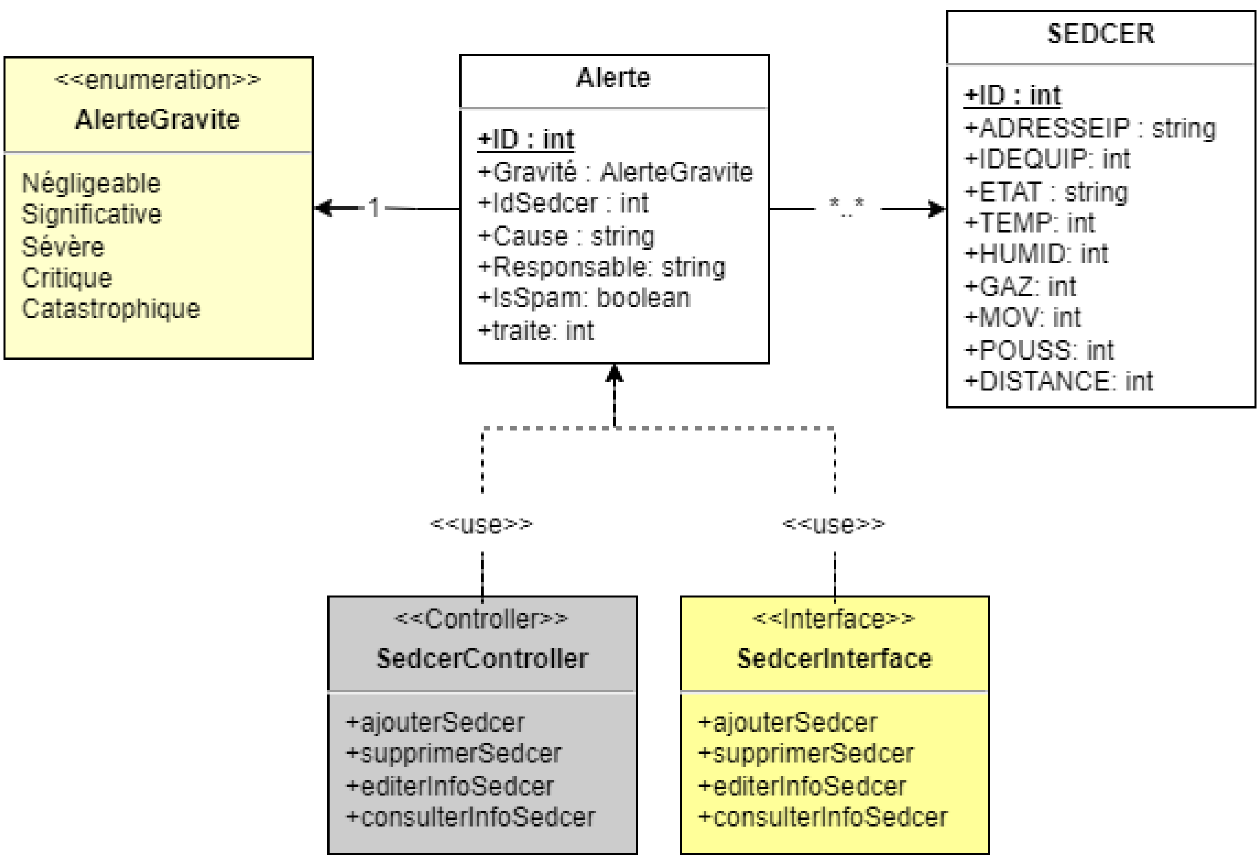

Figure 3. 15 : Diagramme de classes - Gestion des alertes.

3.19.5 Gestion des ressources humaines

La figure ci-après regroupe toutes les classes utilisées dans le cadre de la gestion de création, modification, révocation, et de réactivation. Ainsi que celles nécessaires pour la gestion des transferts interdépartementaux.

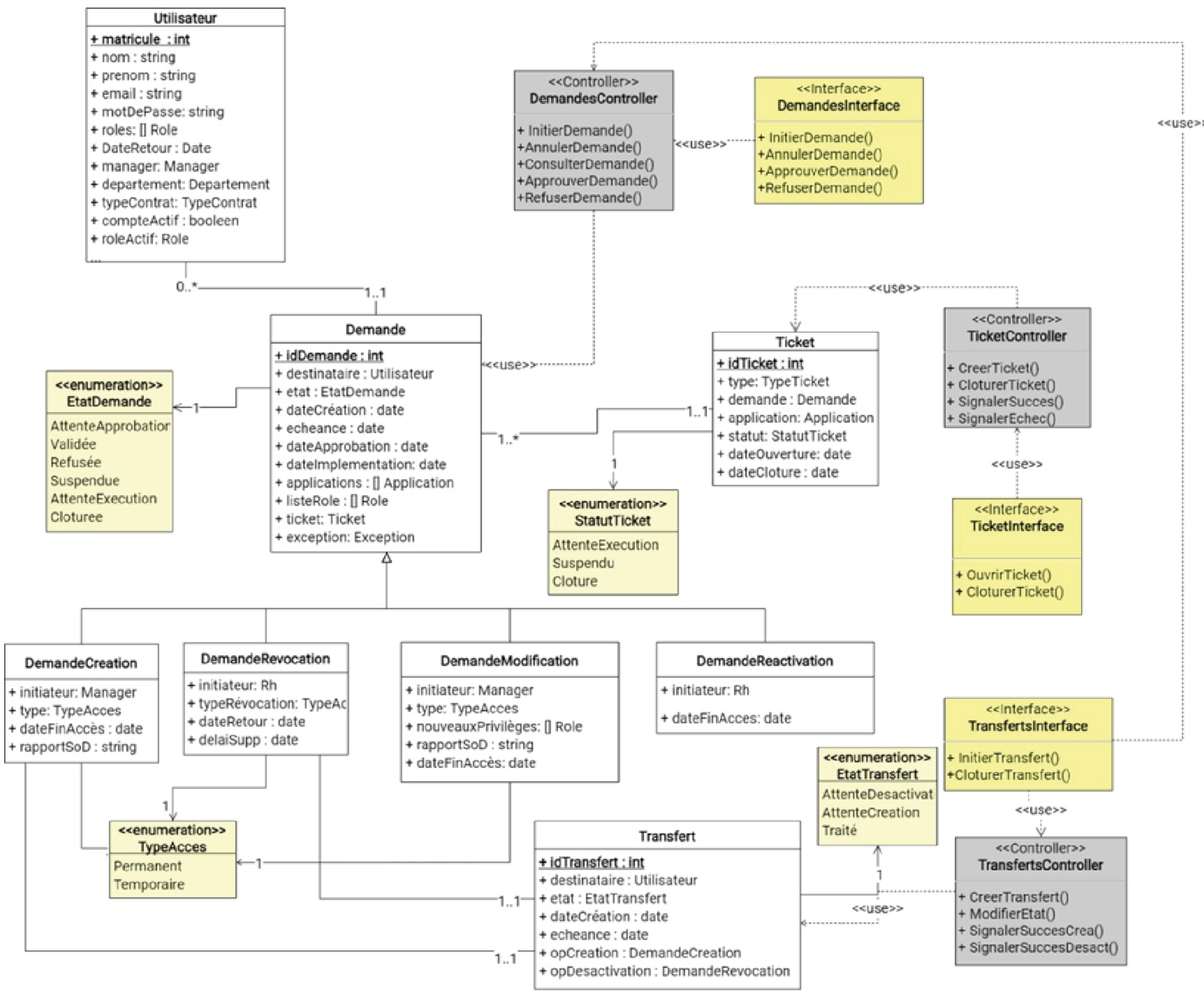

Figure 3. 16 : Diagramme de classes - Gestion des ressources humaines.

3.19.6 Administration de la plateforme

Les classes présentes dans la figure ci-dessous représentent les classes nécessaires pour la gestion des comptes utilisateurs sur notre système. Les fonctions exposées permettent la création, modification et la suppression des différents types de comptes utilisateurs.

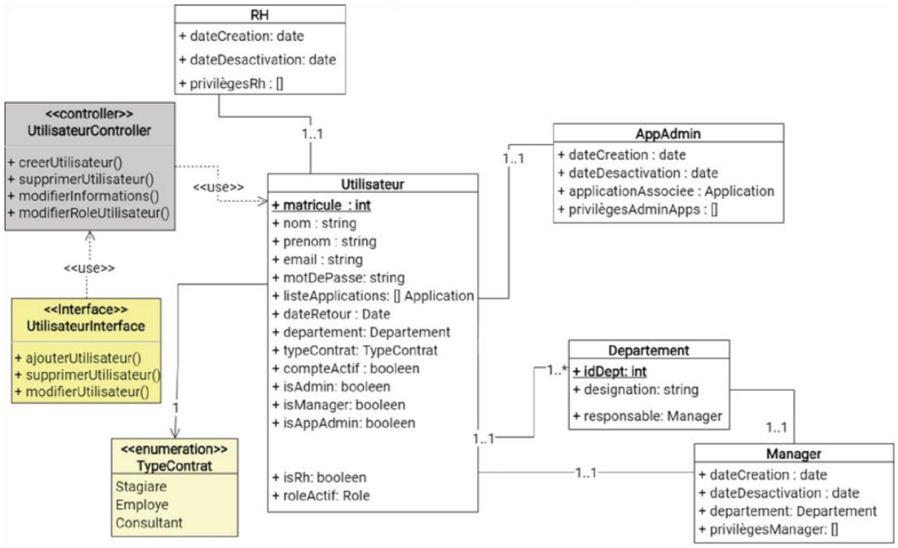

Figure 3. 17 : Diagramme de classes - Administration de la plateforme.

3.20 Architecture logicielle

Pour la réalisation du système cible, nous avons opté pour une architecture client-serveur 3-tier. Un tiers présentation, ou client, qui permet à l'utilisateur d'interagir et d'envoyer des requêtes au tiers métier qui comprend la logique métier et regroupe les différents traitements à effectuer sur la donnée. Ce dernier est chargé de recevoir les requêtes de l'utilisateur et de lui transmettre les données en réponse. Et le tiers d'accès aux données qui permet de communiquer avec la base de données par le biais d'un ORM (Object-Relational Mapping).

Les principaux avantages de cette architecture sont :

- La facilité de déploiement : L'application en elle-même n'est déployée que sur la partie serveur (serveur applicatif et serveur de base de données). Cette facilité de déploiement aura pour conséquence non seulement de réduire le coût de déploiement, mais aussi de permettre une évolution régulière du système.
- Le client ne nécessite qu'une installation et une configuration minime : En effet il suffit d'installer un navigateur web compatible avec l'application pour que le client puisse accéder à l'application, ce navigateur étant par ailleurs souvent installé par défaut sur toutes les machines.
- L'amélioration de la sécurité : Dans un système client-serveur, tous les clients

accédaient à la base de données ce qui la rendait vulnérable. Avec une architecture multitierce l'accès à la base n'est effectué que par le serveur applicatif. Ce serveur est le seul à connaitre la façon de se connecter à cette base. Il ne partage aucune des informations permettant l'accès aux données. Il est alors possible de gérer la sécurité au niveau de ce serveur applicatif.

La communication client-serveur est assurée par des API (Applications Programming Interface), qui désignent une interface normalisée par laquelle un logiciel offre des services à un autre logiciel.[14] Cela permet de créer des écosystèmes d'applications qui sont modulaires et réutilisables et favorisent :

- La séparation entre le backend et frontend.
- L'évolutivité et la scalabilité du système.
- La logique métier sans se préoccuper de la structuration de l'application.

3.21 Réalisation du Système cible

3.21.1 Présentation des outils technologique utilisés

3.21.1.1 Les composants d'un Datacenter

Les principaux composants d'un Datacenter comprennent les serveurs, les systèmes de stockage, les équipements réseau, les systèmes de refroidissement, les groupes électrogènes de secours, les systèmes de gestion de l'alimentation, les systèmes de sécurité et de surveillance, les câblages structurés, ainsi que les logiciels de gestion et de surveillance.

Figure 3. 18 : caméra SAMSUNG SNB-6003P.

Figure 3. 19: Router Cisco.

Figure 3. 20 : Climatiseur de précision (Emerson).

Figure 3. 21: Onduleur chloride APC.

3.21.2 Editeur de code

3.21.2.1 Visual Studio Code

Visual studio code est un éditeur de code open source et gratuit développé par Microsoft, et disponible pour tout type d'OS. Vs code est développé avec le framework Electron et conçu principalement pour développer des projets avec JavaScript, Node.js ou encore TypeScript, l'avantage principal de cet outil réside dans la présence d'un nombre considérable d'extensions permettant de faciliter le développement sous plusieurs langages, l'intégration par défaut d'un terminal permettant le développement et le test sur une seule fenêtre ainsi que l'intégration de l'outil de versionning Git directement au sein de l'éditeur permettant de faciliter le travail en collaboration.

Figure 3. 22 : Logo Visual Studio Code.

3.21.2.2 Arduino IDE

L'IDE Arduino est un éditeur de code et un compilateur qui peut être exécuté sur plusieurs plates-formes. Il est également lié au traitement, un langage de programmation, grâce à son utilisation d'une interface Java. Ce logiciel permet aux programmeurs de compiler et de télécharger leurs programmes via une liaison série, Bluetooth ou USB selon le module. Il est possible d'exécuter le logiciel sans interface, car certains programmeurs ont pu télécharger des programmes via la ligne de commande.[15]

C++, un langage de programmation utilisé pour créer des programmes pour l'Arduino, est compilé avec avr-g++8 et lié à la bibliothèque de développement Arduino.

Figure 3. 23: Logo Arduino IDE.

3.21.3 Gestion de versionning du développement de la plateforme

3.21.3.1 Github

Github est un service web de gestion du développement et des versions des logiciels, il utilise le logiciel de gestion de versions Git, ce site développé en Ruby, est la plus grande application de gestion de versions au monde, ayant atteint plus de 15 millions d'utilisateurs et plus de 40 millions de projets déposés, sera utilisé au cours du développement du projet pour gérer les synchronisations du développement de la plateforme.

Figure 3. 24 : Logo GitHub.

3.21.4 Technologiques de développement

3.21.4.1 Vue JS

Vue est un framework JavaScript qui se concentre sur la composition des composants et le rendu déclaratif. Il a officiellement maintenu des packages et des bibliothèques pour le routage, la gestion d'état et les outils de construction, tels que Nuxt.js, qui sont couramment utilisés pour créer des applications plus complexes.

Des extensions HTML appelées directives5 sont ajoutées au-dessus du HTML normal. Ceux-ci sont intégrés ou personnalisables par l'utilisateur final. Ils peuvent servir de cadre pour créer des applications Web.

Avant d'utiliser Vue.js, il doit être installé sur un environnement Node.js

Figure 3. 25: Logo Vue JS.

3.21.4.2 LARAVEL

Laravel est un framework créé en PHP1 qui utilise le principe modèle-vue-contrôleur dans son développement. Ses sources sont hébergées sur GitHub et sont sous licence MIT. Laravel est une application web open source écrite en POO. Le référentiel Laravel/laravel GitHub contient les premières versions du framework Laravel. À partir de la cinquième version, le code est contenu dans le référentiel GitHub Laravel/framework. En 2016, le référentiel GitHub du framework PHP a obtenu le score global le plus élevé de tous les projets. Peu de temps après, une communauté liée au framework s'est développée. Laravel comprend environ 30 pour cent de ses lignes contenant des composants Symfony. Son grand frère Symfony est toujours utilisé.

Figure 3. 26 : Logo Laravel.

3.21.4.3 C ++

C++ est un langage de programmation compilé permettant la programmation sous de multiples paradigmes, dont la programmation procédurale, la programmation orientée objet et la programmation générique. Ses bonnes performances, et sa compatibilité avec le C en font un des langages de programmation les plus utilisés dans les applications où la performance est critique.

Figure 3. 27: Logo C ++.

3.21.5 Système de gestion de base de données

3.21.5.1 MySQL

MySQL est un système de gestion de bases de données relationnelles (SGBDR). Il est distribué sous une double licence GPL et propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web principalement) que par des professionnels, en concurrence avec Oracle, PostgreSQL et Microsoft SQL Server.

Figure 3. 28 : Logo MySQL.

3.21.6 Outils de test

3.21.6.1 Postman

Postman est une plateforme collaborative permettant notamment le développement d'APIs et d'automatiser les tests, il permet le lancement de requêtes de type REST, GraphQL ou SOAP directement à partir de la plateforme et de consulter les réponses de ces dernières, la création de collections de test d'intégration, le stockage d'informations pour l'exécution de tests dans différents environnements.

Figure 3. 29 : Logo Postman.

Les parties front-end et back-end communiqueront à travers des requêtes http (GET, POST…etc), cela étant assuré du coté client par vue js, ce dernier étant un framework permettant de faciliter les requêtes et au code du coté client de communiquer avec le web, et du coté server, ceci est assuré par Laravel REST framework qui est une bibliothèque fonctionnant avec les modèles standards de PHP pour construire des API de manière flexible.

3.21.7 Présentation de matériel utilisé

3.21.7.1 ARDUINO UNO

L'Arduino UNO est une carte de développement électronique très populaire et largement utilisée. Elle est basée sur un microcontrôleur Atmega328P et est principalement utilisée pour créer des projets électroniques interactifs et des prototypes.

Figure 3. 30 : ARDUINO UNO.

3.21.7.2 Capteur PIR

Il s’agit d’un capteur de mouvement Arduino simple à utiliser. On allumez-le et attends 1 à 2 secondes que le capteur obtienne un instantané de la pièce immobile. Si quelque chose bouge après cette période, la goupille « alarme » s’abaissera. Ce capteur vérifie la chaleur infrarouge dans son angle de détection. Le corps humain, les animaux domestiques et plusieurs autres choses émettent de l’énergie que le capteur recherche, il se compare à l’instantané et s’il y a un changement récent, il se déclenche.

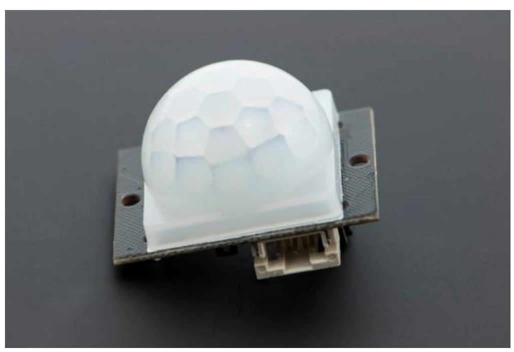

Figure 3. 31: Le capteur PIR.

Spécifications techniques

- Genre : numérique
- Tension d’alimentation : 5 V
- Courant : 50 A
- Température de fonctionnement : 0℃ 70℃
- Niveau de sortie (ÉLEVÉ) : 4V

- Niveau de sortie (BAS) : 0,4 V

- Détecter l'angle : 110 degrés

- Distance de détection : 7 mètres

- Taille : 28 mm × 36 mm (1,1 po x 1,4 po)

- Poids : 25 g

Câblage avec Arduino

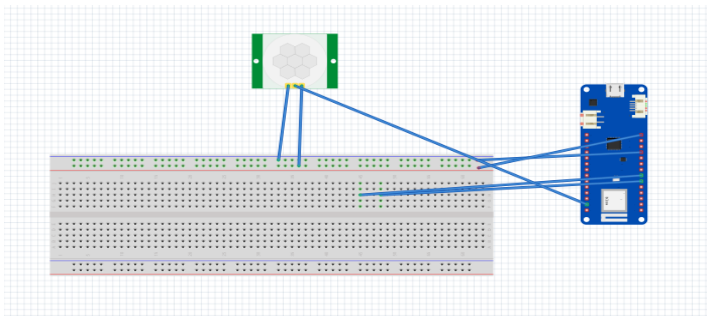

Figure 3. 32 : Câblage de capteur PIR avec Arduino.

3.21.7.3 Grove - Capteur de gaz multicanaux

Trois canaux de gaz indépendants dans un seul boîtier construit avec ATmega168PA les gaz détectables incluent : le monoxyde de carbone (CO), le dioxyde d'azote (NO_2), l'hydrogène (H_2), l'ammoniac (NH_3), le méthane (CH_4), etc.

Figure 3. 33 : Grove - Capteur de gaz multicanaux.

Caractéristiques principales	**Spécifications techniques**
• Trois éléments de détection entièrement indépendants sur un seul boîtier • Construit avec ATmega168PA • Interface I2C avec adresse	• Dimensions : 89 mm x 140 mm x 6,8 mm • Poids : G.W 10g • Batterie : Exclude

programmable • La puissance de chauffage peut être arrêtée pour une faible puissance • Gaz détectables : Monoxyde de carbone (CO), Dioxyde d’azote (NO2), Hydrogène (H2), Ammoniac • (NH3), Méthane (CH4), etc.	• Tension : 3.1 5.25V • Ondulation(@Max Power) : 80 100mV • Puissance de chauffage maximale : 88 mW • Puissance maximale : 150 mW • ADC Précision : 10Bits • Taux : I2C 100kHz • VIL(@I2C) : -0.5 0.99V • VIH(@I2C) : 2.31 5.2V

Tableau 3. 17: Spécifications et Caractéristiques du Grove.

Câblage avec Arduino

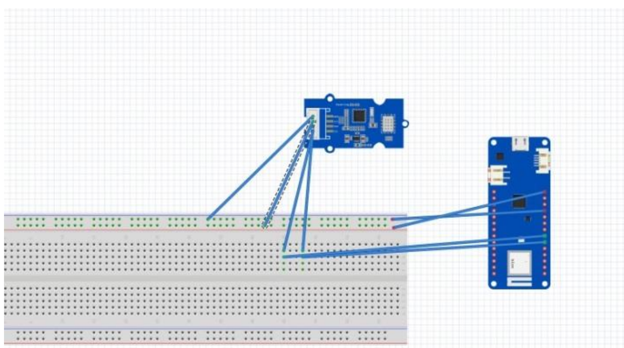

Figure 3. 34 : Câblage de Grove - Capteur de gaz multicanaux avec Arduino uno.

3.21.7.4 Capteur de distance à ultrasons

Un capteur à ultrasons est un appareil électronique qui mesure la distance d’un objet cible en émettant des ondes sonores ultrasonores et convertit le son réfléchi en un signal électrique. Les ondes ultrasonores voyagent plus vite que la vitesse du son audible (c’est-à-dire le son que les humains peuvent entendre). Les capteurs à ultrasons ont deux composants principaux : l’émetteur (qui émet le son à l’aide de cristaux piézoélectriques) et le récepteur (qui rencontre le son après qu’il a voyagé vers et depuis la cible).

Figure 3. 35 : Capteur de distance à ultrasons.

Caractéristiques principales

Ce capteur économique offre une fonctionnalité de mesure sans contact de 2 cm à 400 cm avec une précision de plage pouvant atteindre 3 mm. Chaque module HC-SR04 comprend un émetteur à ultrasons, un récepteur et un circuit de contrôle. Il n'y a que quatre broches dont vous devez vous soucier sur le HC-SR04 : VCC (alimentation), Trig (déclencheur), Echo (réception) et GND (masse). Ce capteur possède des circuits de contrôle supplémentaires qui peuvent empêcher des données "rebondissantes" incohérentes en fonction de l'application.

Spécifications techniques

- Tension de fonctionnement : 5 V CC
- Courant de fonctionnement : 15 mA
- Angle de mesure : 15°
- Distance de portée : 2 cm - 4 m

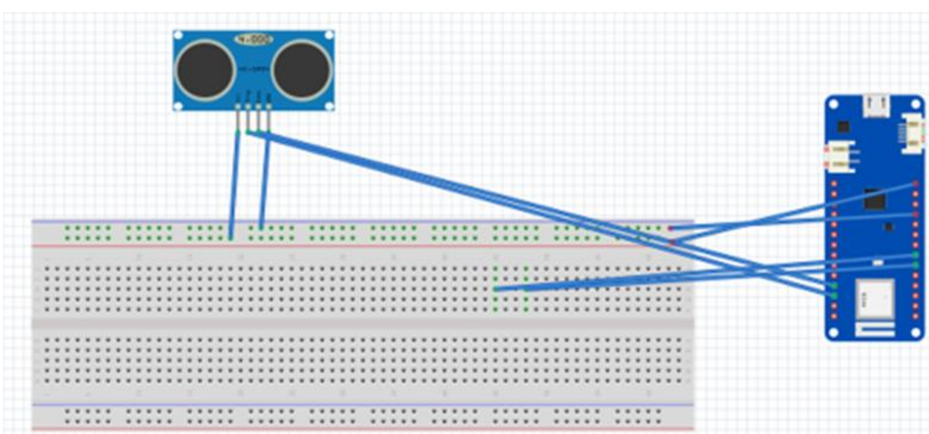

Figure 3. 36: Câblage de Capteur de distance à ultrasons avec Arduino.

3.21.7.5 Capteur DHT 11

Un capteur DHT11 est un capteur d'humidité et de température numérique. Il est couramment utilisé dans les projets électroniques et les systèmes de surveillance où la mesure de l'humidité et de la température est nécessaire.

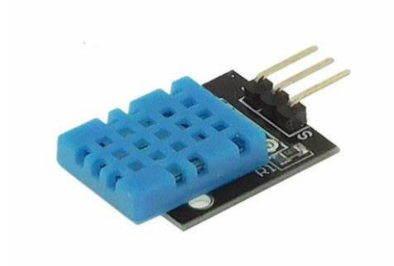

Figure 3. 37 : capteur dht11.

Caractéristiques principales	Spécifications techniques
Comparé au DHT11, ce capteur est plus précis, plus précis et fonctionne dans une plus grande plage de température/humidité, mais il est plus grand et plus cher. Livré avec une résistance 4.7K - 10K, que vous voudrez utiliser comme pullup de la broche de données à VCC.	- Faible coût - Alimentation : 3 à 5V et E/S - 2,5 mA maximum d'utilisation de courant pendant la conversion (lors de la demande de données) - Bon pour des lectures d'humidité de 0 à 100 pour cent avec une précision de 2 à 5 pour cent - Bon pour les lectures de température de -40 à 80°C Précision de ±0,5°C - Pas plus de 0,5 Hz de taux d'échantillonnage (une fois toutes les 2 secondes) - Taille du corps : 27 mm x 59 mm x 13,5 mm (1,05" x 2,32" x 0,53") - 4 broches, espacement de 0,1" - Poids (juste le DHT11) : 2,4 g

Tableau 3. 18 : Spécifications et Caractéristiques du DHT11.

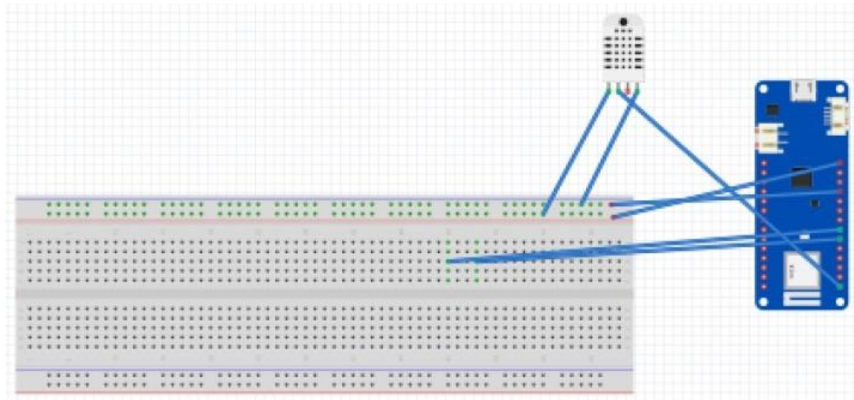

Figure 3. 38 : Câblage de Capteur de température et d'humidité DHT11 avec Arduino.

3.21.7.6 CAPTEUR MQ-135

Le capteur MQ-135 est un capteur de qualité de l'air utilisé pour détecter certains gaz présents dans l'environnement. Il est couramment utilisé pour mesurer la concentration de gaz nocifs tels que l'ammoniac (NH_3), le monoxyde de carbone (CO), le monoxyde d'azote (NO_x) et les composés organiques volatils (COV) dans l'air.

Figure 3. 39 : capteur gaz MQ-135.

Câblage

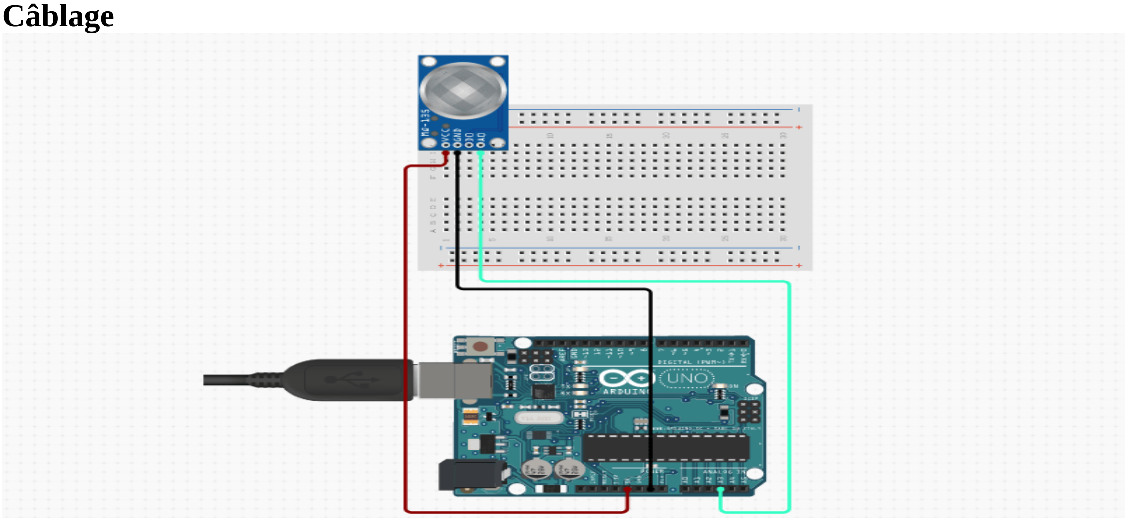

Figure 3. 40: schéma câblage MQ-135.

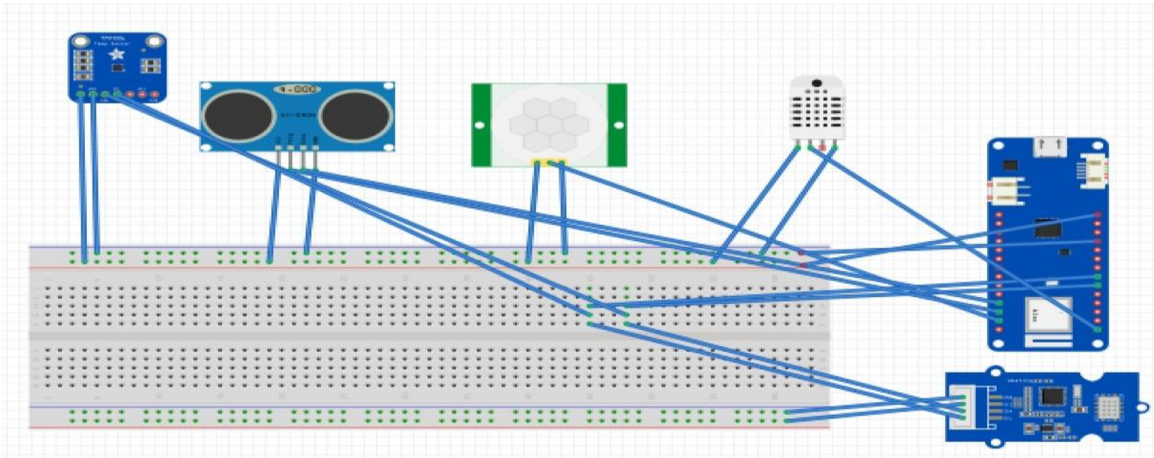

Figure 3. 41: Schéma général de câblage.

Présentation de la partie matérielle

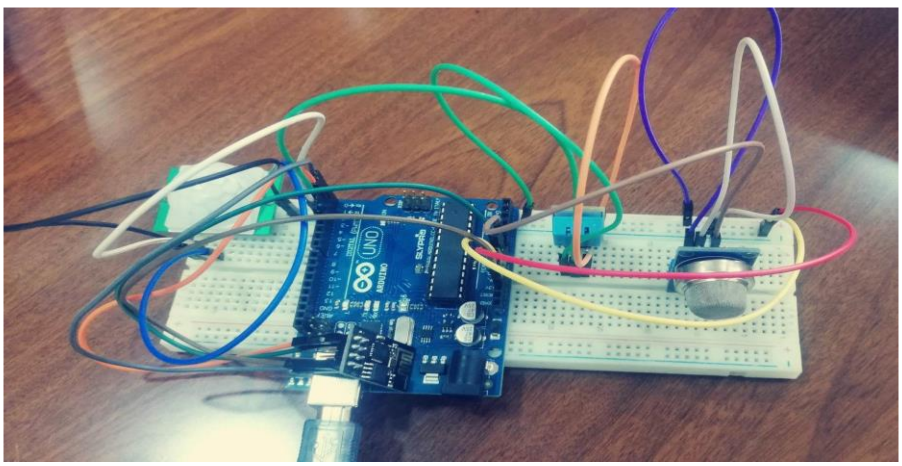

Figure 3. 42 : Présentation de la partie matérielle.

3.21.8 Présentation du système réalisé

3.21.8.1 Présentation de la plateforme

Dans ce qui suit, nous présentons les différentes interfaces du système réalisé :

I. Écran Login de l'application

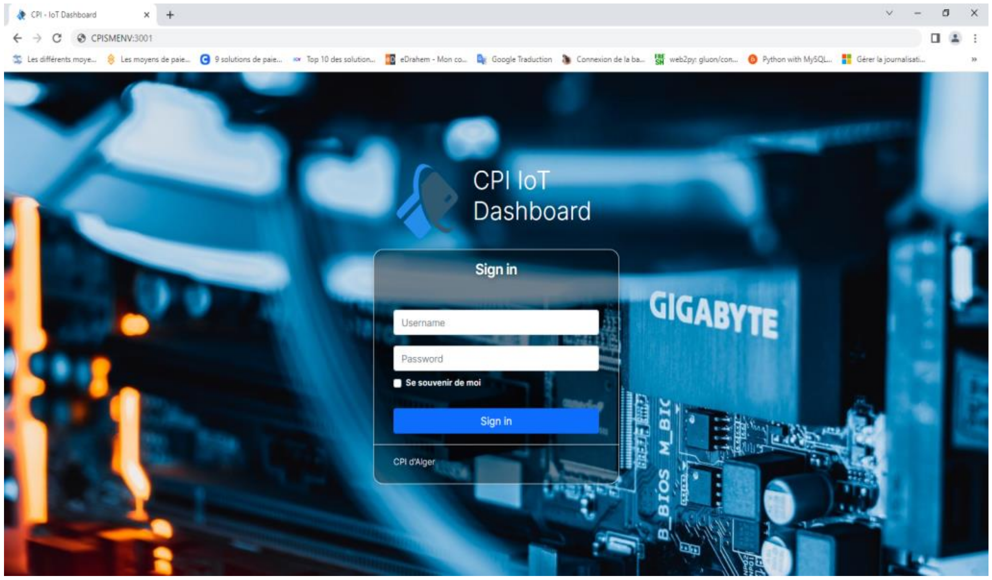

Figure 3. 43 : Écran Login de l'application.

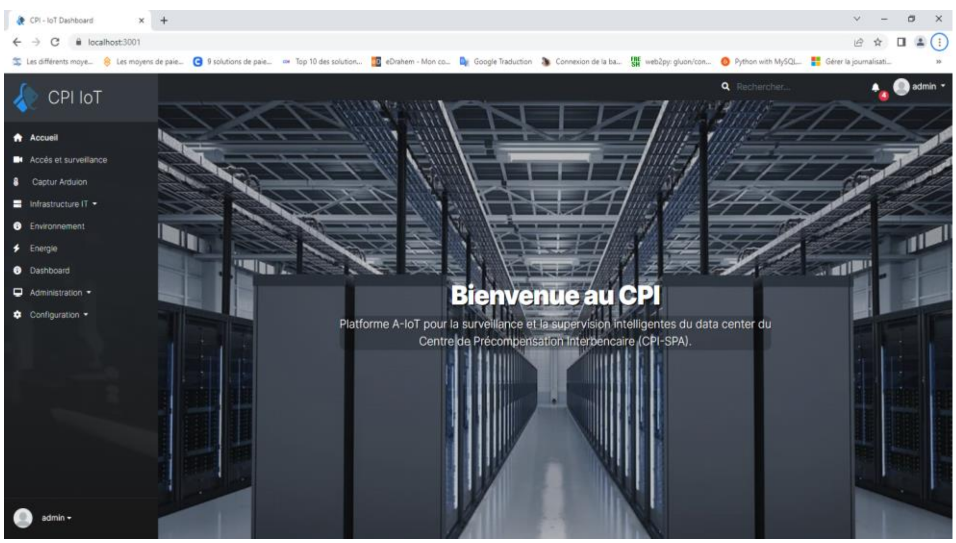

Figure 3. 44: Ecran d'accueil.

II. Écran de Tableau de bord de matériel

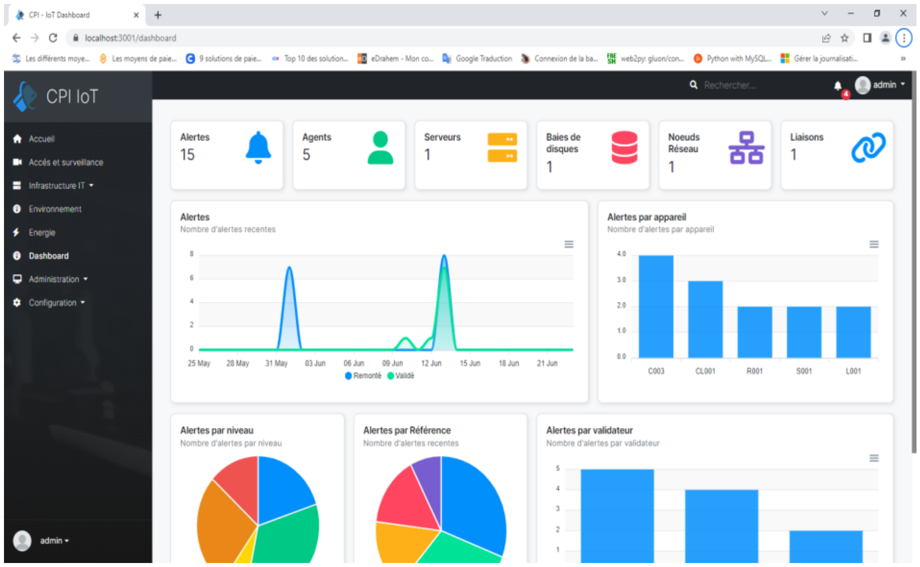

Figure 3. 45 : Écran de Tableau de bord de matériel.

3.21.8.2 Paramètres d'environnement

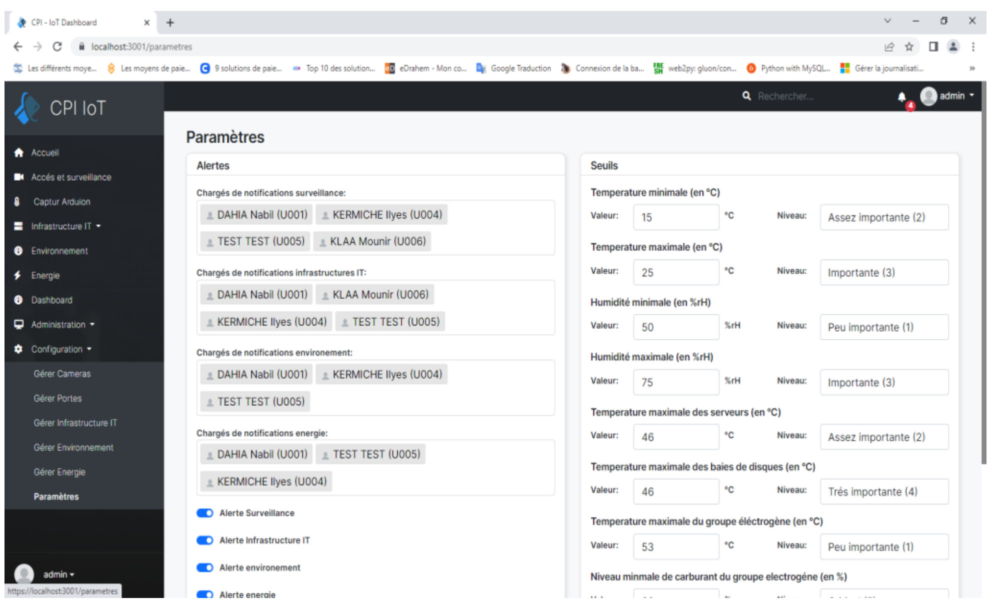

Figure 3. 46 : Écran de Paramètres d'environnement.

3.21.8.3 Gestion de matériel

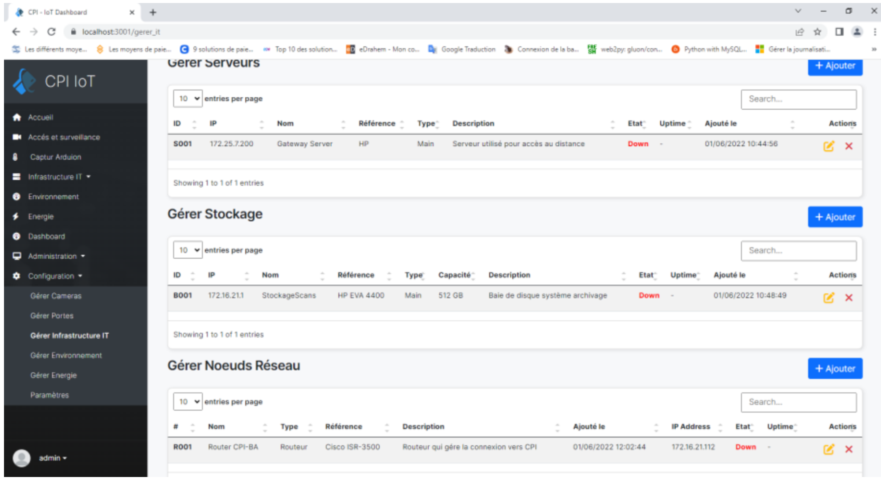

Figure 3. 47 : Écran Gestion de matériel- plateforme IT.

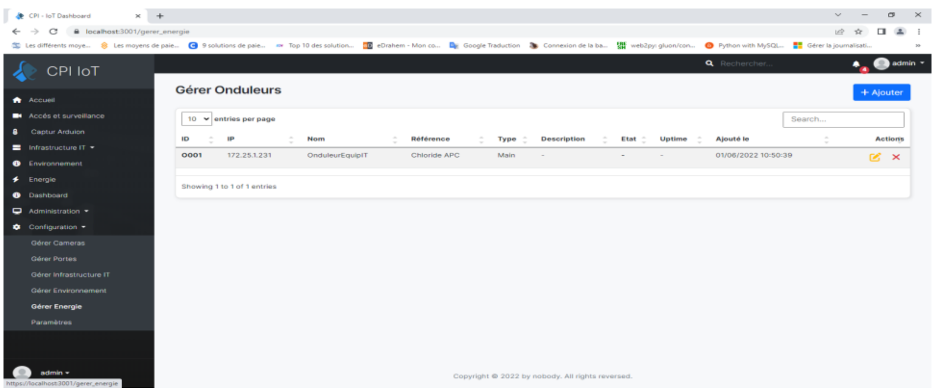

Figure 3. 48 : Écran Gestion de matériel- Onduleurs.

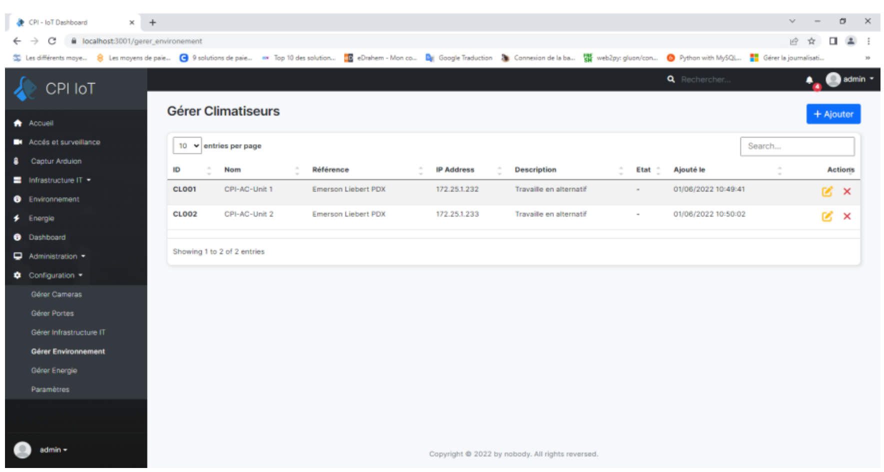

Figure 3. 49 : Écran Gestion de matériel- Climatiseurs.

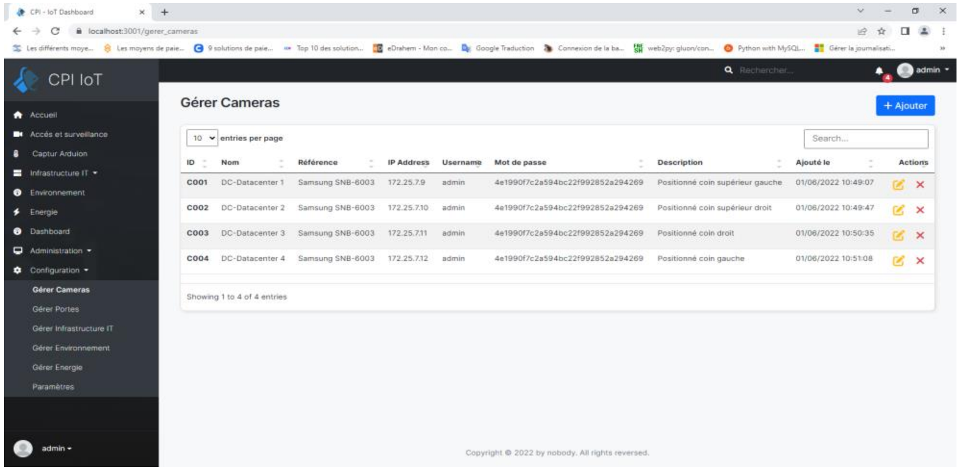

Figure 3. 50 : Écran Gestion de matériel- Caméras.

3.21.8.4 Gestion des alertes

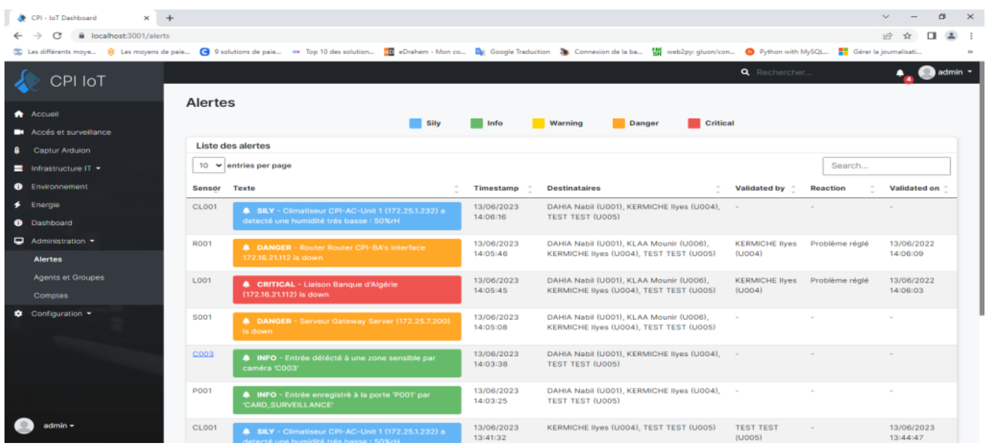

Figure 3. 51 : Écran Gestion des alertes.

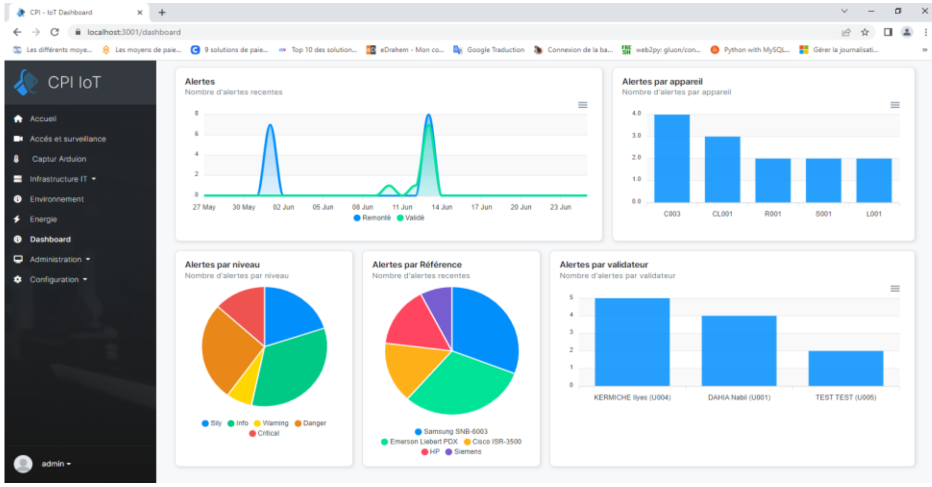

Figure 3. 52 : Écran Gestion des alertes-tableau de bord.

3.21.8.5 Gestion des ressources humaines

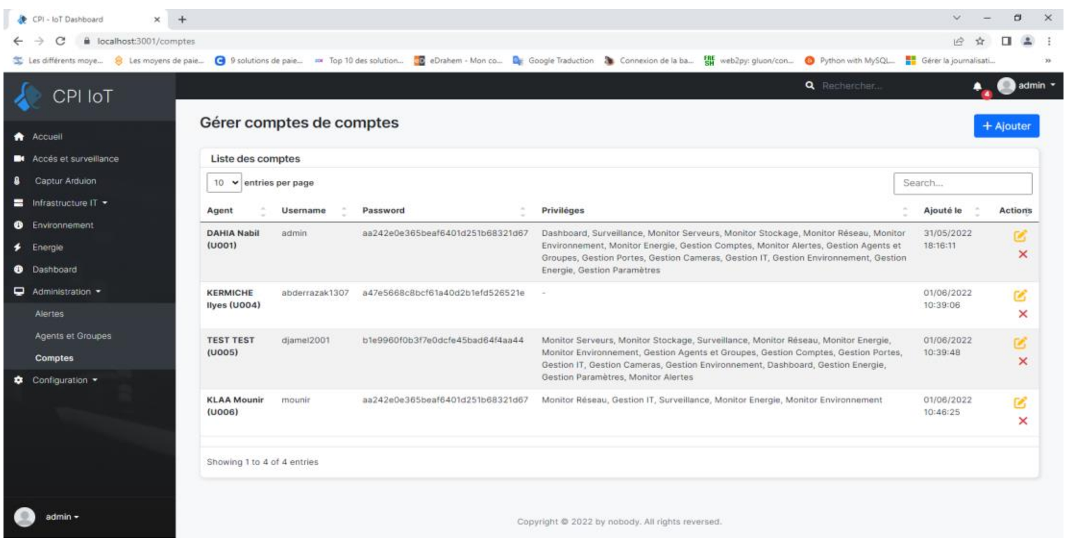

Figure 3. 53 : Écran Gestion des ressources humaines- création des comptes.

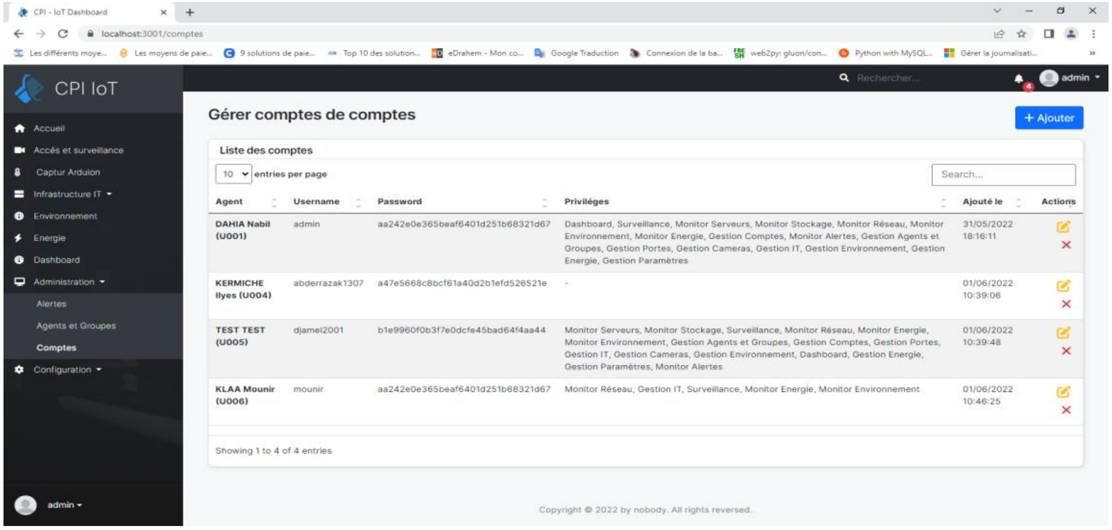

Figure 3. 54 : Écran Gestion des ressources humaines- gestion des comptes.

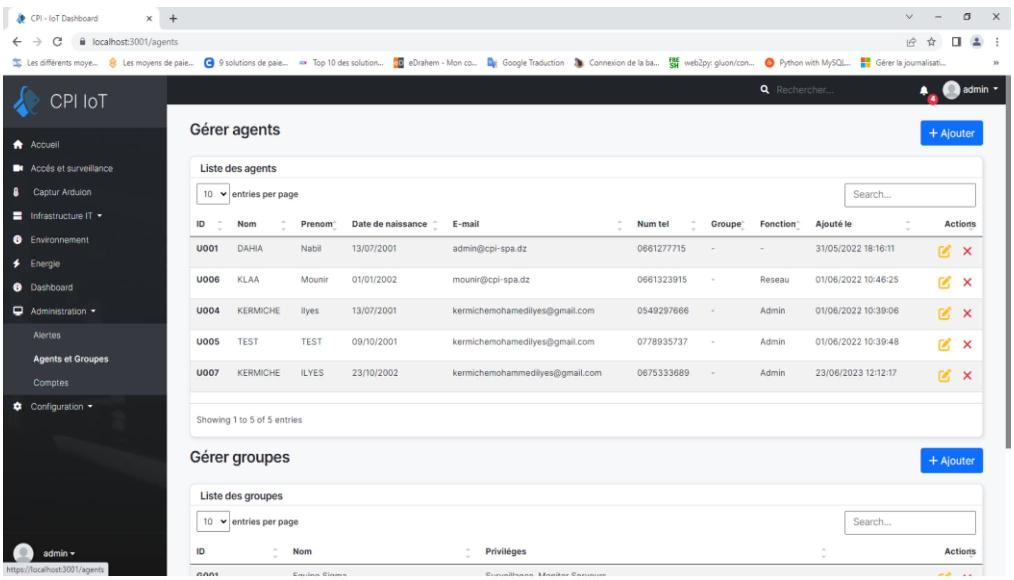

Figure 3. 55 : Écran Gestion des ressources humaines- gestion des privilèges.

3.21.8.6 Capteurs Arduino

Figure 3. 56 : connexion Arduino-application.

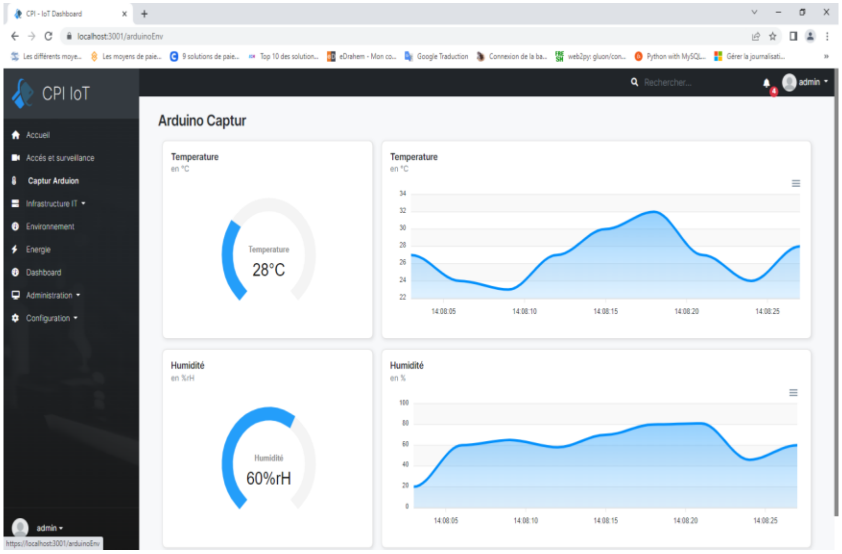

Figure 3. 57 : Écran Gestion de l'environnement Arduino.

3.21.9 Sécurité du système réalisé

3.21.9.1 Contrôle d'accès défaillant

Les restrictions sur ce que les utilisateurs authentifiés peuvent avoir accès ou sont autorisés à faire ne sont souvent pas correctement appliquées. Les attaquants peuvent exploiter ces failles pour accéder à des fonctionnalités ou des données non autorisées, telles que l'accès aux comptes d'autres utilisateurs, la visualisation de fichiers sensibles, la modification des données d'autres utilisateurs, la modification des droits d'accès, etc.

3.21.9.2 Cross-Site Scripting XSS

Les failles XSS se produisent chaque fois qu'une application inclut des données non fiables dans une nouvelle page Web sans validation ou échappement approprié, les attaques de type XSS se produisent lorsqu'un attaquant introduit un script dans le navigateur de la victime qui finit par s'exécuter, ce qui peut détourner les sessions des utilisateurs ou rediriger l'utilisateur vers des sites malveillants.

3.21.9.2 Mesures de sécurité appliquées

Dans le but de sécuriser notre système, nous avons mis en place les mesures de sécurité suivantes assurant l'authentification, la confidentialité, l'intégrité, et la non-répudiation de l'origine :

- **Authentification :** L'authentification au niveau de notre système est réalisée avec la technologie du JWT (JSON Web Token). Nous donnons la description détaillée de cette dernière en Annexe.

- **Confidentialité :** Les mesures prises pour garantir la confidentialité des données de notre système sont :
    - Protection de l'accès à la base de données par un mot de passe et la limitation de la connaissance de celui-ci à l'administrateur de la plateforme uniquement.
    - Hachage des données d'authentification (mot de passe).
    - Séparation le serveur d'application du serveur de base donnée.

- Intégrité : Pour garantir cela, nous avons réalisé ce qui suit :
    - L'assurance d'une séparation des tâches dynamique (2 rôles conflictuels ne peuvent être activés en même temps).
    - Protection des données contre toute altération en exigeant un token valide lors de l'appel des API.

- **Non-répudiation :** Pet aspect est assuré par le JWT.

3.21.10 Impacts estimés du système

Au cours du développement de notre système, nous avons consulté avec les employés du CPI SPA à la fin de chaque sprint à travers une série de tests sur les fonctionnalités de système afin de juger de la pertinence de ces dernières et de pouvoir analyser l'utilisation de ce système en situation réelle par les acteurs auxquels il est destiné (Managers, Responsables RH…Etc.). Nous avons pu au cours de cette étude quantifier les résultats de ces tests auprès des responsables du CPI SPA. Les résultats ont été synthétisés dans ce qui suit :

- Le système a permis d'augmenter le nombre d'alertes traitées par le Manager de 60%. Ces nouvelles alertes constituent des problèmes potentiels étant ainsi évités.
- Le système a facilité grandement la veille sur l'état des différents équipements selon l'équipe chargée de cette tâche, ce qui a pour bienfait secondaire de réduire les erreurs éventuelles.
- Le système permet de garder une traçabilité sur tout changement dans les paramètres d'environnement.
- Le système a permis de réduire les accès non autorisés aux équipements de 90%.
- Le système a permis de définir clairement les droits d'accès de chaque employé du Datacenter, garantissant une forte traçabilité en cas d'erreur humaine maladroite ou mal intentionnée.

3.22 Conclusion

Nous avons présenté à travers ce dernier chapitre un aperçu sur la phase de développement de notre système, commençant par les choix technologiques et les critères d'évaluation qui nous ont permis de faire ces derniers ainsi que le prototype réalisé.

Vu la nature sensible des données manipulées par le système, nous avons accordé une grande importance à l'aspect de sécurité. Nous avons également veillé à ce que notre système soit évolutif qui permet la prise en charge des exigences des standards ISO 27000 et les recommandations d'ITIL sur la gestion des habilitations.

Bien que notre mission s'achève avec l'implémentation du système, cette étape n'est pas la dernière dans le processus de développement des SI. En fait, elle est suivie d'une phase de déploiement et de tests permettant de vérifier que le produit répond aux exigences du C.P.I spa et d'identifier d'éventuelles corrections à apporter.

Conclusion générale

Conclusion générale

Ce travail présente la réalisation d'une plateforme IoT pour le Datacenter du CPI Spa. À travers trois chapitres distincts, nous avons exploré l'existant de l'endroit d'étude, examiné l'état de l'art de l'IoT et détaillé le processus de conception et de réalisation du système.

Dans le premier chapitre, nous avons effectué une étude approfondie de l'endroit d'étude, le Datacenter du CPI spa. Nous avons analysé son infrastructure, ses processus et ses besoins spécifiques en matière de gestion des équipements et de surveillance. Cette étude a permis de mettre en évidence les lacunes et les défis auxquels le Datacenter était confronté, ouvrant ainsi la voie à la conception d'une solution innovante. Le deuxième chapitre était consacré à l'état de l'art de l'IoT. Nous avons examiné les avancées technologiques, les standards et les meilleures pratiques dans le domaine de l'IoT, en mettant l'accent sur leur pertinence pour notre projet. Cette revue de la littérature nous a permis de comprendre les tendances actuelles, les applications pratiques de l'IoT et les possibilités offertes par cette technologie pour optimiser la gestion des centres de données. Dans le troisième chapitre, nous avons abordé la conception et la réalisation du système IoT pour le Datacenter du CPI spa. Nous avons élaboré une architecture logicielle solide en utilisant les principes de l'IoT et de la conception orientée objet. Nous avons développé des capteurs intelligents, des protocoles de communication sécurisés et une interface conviviale pour surveiller les équipements et collecter les données pertinentes. La réalisation du système s'est déroulée en suivant une approche itérative et incrémentale, en procédant à des tests rigoureux et à des ajustements pour garantir la qualité et la fiabilité du système. En conclusion, la plateforme IoT réalisée pour le Datacenter du CPI spa représente une avancée significative dans l'amélioration de la gestion des équipements et de la surveillance des données. Elle permet de collecter des informations précieuses en temps réel, d'optimiser les processus opérationnels et de prendre des décisions éclairées pour assurer un fonctionnement optimal du Datacenter. Cette réalisation ouvre également la voie à de nouvelles possibilités d'innovation et de développement dans le domaine de l'IoT pour les centres de données. Ce rapport met en évidence l'importance de l'IoT dans l'optimisation des infrastructures informatiques et souligne les avantages tangibles qu'il peut apporter. Cependant, il convient de souligner que le domaine de l'IoT est en constante évolution, et de nouvelles opportunités et défis continueront d'émerger. Il est donc essentiel de rester à l'affût des développements technologiques et de continuer à innover pour rester compétitif dans un environnement en perpétuelle transformation.

Bibliographie

[1] : (F. A. Alhaidari and E. J Alqahtani. Securing communication between fog computing and iot using)

[2] (K. et al Ashton. That 'internet of things' thing. rfid journal. RFID journal, 22(7) :97–114, 2009.)

[3] : (Special report : The internet of things. IEEE, 2014.)

[4] : (The internet of things -executive summary. challenges to the network. ITU, 2005.)

[5] : ("Internet of Things (IoT): A Literature Review," by S. Al-Fedaghi, S. A. Al-Sharhan, and M. A. Al-Shayeji.)

[6]: ("Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," by A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi.)

[7]: ("A Review of Internet of Things (IoT) Technologies in Smart Cities," by N. A. Suryadevara, S. C. Mukhopadhyay, and A. H. Lim.)

[8]: ("Internet of Things (IoT) in Agriculture: A Comprehensive Review," by M. H. R. Siddique, A. K. Paul, and A. A. R. Mamun.)

[9]: ("Challenges and Opportunities of Internet of Things (IoT): A Review," by A. Rayes, N. A. B. Abu, and N. E. A. Basaruddin)

[10]: Yu W.-Zhang N. Yang X. Zhang H. Lin, J. and W Zhao. A survey on internet of things : Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5) :1125–1142, 2017.

[11]: Igor Brandao Machado Matsuo S K Korkua Long Zhao, Yuhao Zhou. Design of an industrial iot-based monitoring system for power substations. In 2019 IEEE/IAS 55th Industrial and Commercial Power Systems Technical Conference (I CPS), page 1–6, 2019.

[12]: Axel Moinet. Définition d'une architecture iot sécurisée et adaptative basée sur la blockchain.

PhD thesis, ESIREM, 2019.

[13]: N Naik. Choice of effective messaging protocols for iot systems : Mqtt, coap, amqp and http. IEEE international systems engineering symposium (ISSE), page 1–7, 2017.

[14]: Dmitrii Dobriborsci Igor Pantiukhin Piotr Czekalski, Aleksandr Kapitonov. Introduction to the iot. 2019.

[15]: Soma Barman Samik Basu, Mahasweta Ghosh. Raspberry pi 3b+ based smart remote health monitoring system using iot platform. Proceedings of the 2nd International Conference on Com-munication, Devices and Computing, pages 473–484, 2020.