PROJET CYBER

THEME : SYSTEME BIOMETRIQUE DANS LA ZONE AEROPORTUAIRE

Membres du Groupe :

- Claude Bernard **DJEUMEGNI**
- Arnold Edwin **FOMEDONG**
- Klett Guewen **VOUBOU MOUDODOU**

1 Résumé

Aujourd'hui, nous vivons dans une société où la sécurité des systèmes technologiques jouent un rôle crucial et incontournable. La Cybersécurité occupe une place importante dans le monde d'aujourd'hui et de plus en plus de personnes se font hackés que ce soit des banques, des hôpitaux, des aéroports …

En effet, la sécurité aéroportuaire est devenue un enjeu stratégique majeur dans un contexte où les exigences de sûreté et de conformité aux normes internationales ne cessent de se renforcer. En France comme dans les autres pays du monde, la modernisation des infrastructures aéroportuaires passe nécessairement par l'adoption de technologies innovantes en matière de cybersécurité pour faire face aux enjeux et aux menaces croissantes. En effet, comment garantir la sécurité des aéroports face à la multiplicité des menaces (terrorisme, cyberattaques, trafic illicite, intrusions) tout en assurant un flux de passagers efficace et respectueux des libertés individuelles ? C'est dans cette perspective qu'est née l'idée de notre projet : une solution de contrôle d'accès basée sur la reconnaissance faciale et les empreintes, destinée à sécuriser l'accès aux zones sensibles d'un aéroport telles que les zones 0d'embarquement, les pistes, les salles de contrôle et les locaux techniques.

Ce système biométrique permet une authentification rapide, fiable et non intrusive du personnel et des passagers. Il permettra aussi de réduire les risques d'intrusion en automatisant les contrôles manuels. Face à des menaces en constante évolution et à des exigences croissantes de la part des organismes de régulation internationaux (tels que l'**OACI**), les aéroports doivent moderniser leurs dispositifs de contrôle tout en garantissant fluidité, efficacité et conformité légale. Dans ce contexte, la mise en œuvre de technologies biométriques, notamment la reconnaissance faciale, représente une réponse innovante et pertinente aux besoins actuels de sécurité et d'optimisation opérationnelle.

Ce projet s'inscrit précisément dans cette démarche d'amélioration continue de la sécurité et de la conformité réglementaire au sein des aéroports. Il propose le développement et le déploiement d'une solution de contrôle d'accès basée sur la reconnaissance faciale et les empreintes digitales, destinée à restreindre et sécuriser l'accès aux zones sensibles de l'aéroport

Le besoin métier identifié repose sur deux constats principaux :

1. **La nécessité de limiter les intrusions non autorisées**, qui représentent un risque majeur pour la sécurité des opérations aériennes.

2. **L'automatisation des contrôles manuels** actuellement utilisés, jugés à la fois lents, coûteux en ressources humaines, et vulnérables face aux erreurs humaines ou aux tentatives de fraude. La solution proposée reposera sur l'intégration d'un système biométrique permettant une authentification rapide, fiable et non intrusive des individus (personnel autorisé, agents de sécurité, prestataires et passagers dans certains cas). Ce système permettra également d'assurer une traçabilité complète des accès, grâce à l'enregistrement sécurisé des identifications, des horaires de passage et des zones franchies, renforçant ainsi les capacités de supervision et d'audit.

   Le projet inclura plusieurs volets complémentaires essentiels à sa mise en œuvre :

- **Une analyse approfondie du cadre réglementaire**, notamment les exigences de la **CNIL**, du **RGPD** et des autorités de l'aviation civile, afin d'assurer la conformité de la solution sur le plan juridique et éthique.
- **Une conception d'architecture sécurisée**, garantissant la protection des données biométriques et leur traitement dans un environnement résilient face aux cyberattaques.
- **Une évaluation multidimensionnelle des risques**, couvrant les aspects techniques (cybersécurité), juridiques (protection des données, consentement), mais aussi réputationnels (perception publique, acceptabilité sociale de la biométrie).
- **Un budget prévisionnel détaillé**, tenant compte des coûts d'acquisition, d'intégration, de formation du personnel, de maintenance et des mises à jour réglementaires futures. Enfin, des **mesures techniques** et **organisationnelles** seront définies pour accompagner le déploiement de la solution, incluant la gestion des habilitations, la sensibilisation des utilisateurs, la mise en place de protocoles de secours et de surveillance, ainsi qu'un plan de retour d'expérience pour ajuster le système selon les retours du terrain. Ainsi, ce projet vise à offrir une solution complète et évolutive, en réponse aux impératifs de sûreté, de performance et de conformité des aéroports modernes, en plaçant la technologie biométrique au service d'une sécurité renforcée et intelligente.

2 Description de l'entreprise et du besoin métier

FlySecure Maintenance (FSM) est une entreprise fictive spécialisée dans la maintenance aéronautique et l'exploitation d'infrastructures aéroportuaires. Fondée en 2009, FSM s'est progressivement imposée comme un acteur clé dans le domaine de la sécurité et de la fiabilité des installations aéroportuaires au sol. Son siège est réparti sur trois grands hubs européens, ce qui lui confère une forte proximité avec ses clients et une grande capacité d'intervention sur le territoire.

L'entreprise compte aujourd'hui **350 collaborateurs**, dont **120 techniciens hautement qualifiés**, capables d'intervenir dans des environnements critiques, en horaires décalés, et souvent dans des conditions d'urgence. Cette expertise technique est au cœur de la valeur ajoutée de FSM.

La mission principale de l'entreprise est d'assurer la **maintenance préventive et corrective** des systèmes aéroportuaires au sol, qu'il s'agisse d'équipements embarqués, de systèmes informatiques spécifiques à l'exploitation aéroportuaire, ou de dispositifs de sécurité.
Les prestations de FSM incluent notamment :

- Une maintenance 24h/24 et 7j/7, garantissant la disponibilité des infrastructures critiques,
- La supervision IoT des équipements, permettant une détection anticipée des anomalies,
- Des interventions d'urgence sur site dans des délais très courts,
- L'automatisation des contrôles techniques, visant à optimiser la fiabilité des installations tout en réduisant les temps d'immobilisation.

FSM opère principalement auprès des grands aéroports européens, des compagnies aériennes low-cost à forte rotation ainsi que des gestionnaires d'infrastructures aéroportuaires. Grâce à sa réactivité, à la technicité de ses équipes et à son engagement en matière d'innovation – notamment dans le domaine de la cybersécurité FSM bénéficie d'une image de partenaire fiable, compétent et tourné vers l'avenir.

Plusieurs éléments différencient FSM de ses concurrents :

- Une **grande réactivité**, essentielle dans un secteur où chaque minute compte,
- Une **maîtrise technique pointue** des systèmes complexes de l'aéroportuaire,

- Une **culture d'innovation**, notamment dans les technologies numériques et les solutions de sécurité intelligente.

2.1 Problématique métier

Dans un contexte où la menace sécuritaire évolue et où les exigences de conformité se renforcent, **FSM** est confrontée à une problématique critique :
la recrudescence des tentatives d'intrusion dans les zones sensibles, notamment par usurpation d'identité lors des interventions techniques de nuit ou en horaires décalés. Ces intrusions représentent un risque majeur pour la sécurité des infrastructures et des personnels.

À cela s'ajoute une autre difficulté : **le renforcement des dispositifs de contrôle des passagers**, qui impose une vigilance accrue et une coordination optimale entre les services de sécurité et les équipes opérationnelles, notamment en période de forte affluence ou de crise.
Ainsi, l'entreprise se pose une question centrale :

***Comment sécuriser efficacement l'accès aux zones sensibles des aéroports tout en maintenant une fluidité opérationnelle et une traçabilité des accès, dans un environnement marqué par des menaces cyber croissantes et des exigences réglementaires strictes (RGPD, CNIL, aviation civile)* ?**

Cette problématique constitue le point de départ du projet de mise en place d'un **système de contrôle d'accès biométrique par reconnaissance faciale** et **empreintes digitale** combinant **sécurité, fiabilité, conformité et efficacité opérationnelle**.

2.2 Objectif métier :

Mettre en place un **système d'authentification biométrique multi-facteur** pour contrôler l'accès :

- **Renforcer la sécurité des zones sensibles** en limitant les risques d'intrusion par usurpation d'identité.

- **Fiabiliser l'identification du personnel intervenant de nuit** grâce à des dispositifs de contrôle renforcés.
- **Optimiser le contrôle des passagers** tout en maintenant un flux fluide aux heures de pointe.

Garantir la conformité réglementaire en matière de sûreté aéroportuaire.

3 Description de la solution

3.1 Description fonctionnelle

La solution que nous proposons repose sur un système de contrôle d'accès biométrique hybride utilisant la **reconnaissance faciale** et la **lecture d'empreintes digitales** pour sécuriser l'accès aux zones sensibles de l'aéroport. Elle est destinée à être utilisée par le **personnel autorisé** (agents de piste, maintenance, sécurité, douanes) et potentiellement les **passagers** pour des accès plus rapides.

Les objectifs sont :

- Renforcer l'authentification du personnel
- Automatiser les points de contrôle d'accès
- Réduire la fraude, la falsification et les erreurs humaines
- Tracer les accès en temps réel
- Fluidité du parcours passagers

3.2 Contexte d'utilisation

La solution sera déployée dans les zones à risque ou réglementées :

- Entrées des **zones de fret**, **pistes**, **salles de contrôle**, **zones douanières**
- Entrées réservées au **personnel technique ou de sécurité**
- Portes d'accès aux **systèmes informatiques critiques**

Chaque employé et passager disposera d'un **profil biométrique stocké de manière chiffrée** et devra s'authentifier via un lecteur biométrique double facteur (caméra faciale + capteur d'empreintes) pour déverrouiller les accès.

3.3 Technologies mobilisées et Fonctionnement global

Pour garantir un niveau de sécurité optimale et un système robuste, nous devons utiliser des technologies de pointe que nous allons énumérer ci-dessous.

- **Caméra reconnaissance faciale HD avec IA embarquée:**
- Les caméras utilisées sont de **haute résolution** permettant de capter **des détails fins du visage**(traits, relief, expressions).
- Elles embarquent des algorithmes de deep learning qui permettent une détection rapide des visages, une comparaison automatique en temps réel avec les profils enregistrés dans la BD et un filtrage intelligent.
- Les données faciales sont traitées localement puis chiffrées avant son envoi.

- **Capteurs d'empreintes digitales capacitives et optiques:**
- **Capteurs capacitifs:** Elles se basent sur la détection des différences de conductivité électrique entre les crêtes et les vallées de l'empreinte. Ces capteurs offrent des avantages de **haute précision et une difficulté de tromperie**.
- **Capteurs optiques:** Elles se basent sur **une capture visuelle** de l'empreinte via une lumière **LED** et capteur optique. Ces capteurs ont pour avantages **une solidité et fiabilité** pour des usages fréquents.

- **Logiciel de traitement biométrique:** Elles jouent un rôle important dans l'analyse, la comparaison, la capture et la gestion des données biométriques. Ayant pour but **d'extraire les caractéristiques biométriques, détecter les fraudes…** Comme exemple nous pouvons citer:
- **IDEMIA**: Fournisseur reconnu dans la biométrie pour la sécurité publique, les aéroports et les gouvernements.
- **Thales Cogent:** Solution biométrique performante utilisée pour l'empreinte digitale.

- **Base de données chiffrée AES-256.**
  - AES(Advanced Encryption Standard) est un algorithme de chiffrement symétrique.
  - Le 256 indique une clé de chiffrement de 256 bits.

Ces bases de données empêche toute lecture ou vol de données en cas de piratage ou de fuite et assure **la confidentialité, l'intégrité et la disponibilité.**

- **Serveur d'authentification avec journalisation des accès (SIEM intégré).**

Elle valide, bloque l'identité de l'utilisateur à chaque tentative d'accès tout en comparant les données par les capteurs biométriques. Chaque action est enregistrée tel que: ***les tentatives d'accès, la validité, le refus, type d'authentification, le lieu, l'identité de l'utilisateur.*** Ce serveur va suivre les activités, auditer les accès et détecter les comportements anormaux**.** Grace au **SIEM** intégré la détection d'intrusions, accès inhabituels se fera automatiquement. Comme exemple nous pouvons citer: Splunk, IBM QRADAR,Wazuh.

- **Système de gestion des identités (IAM) interface avec le SIRH**

Ce système est une plateforme logicielle qui s'occupe de la gestion des identifiants, des droits d'accès et d'autorisation. Il est connecté **directement au SIRH** qui contient toutes les informations RH qui va permettre d'automatiser l'attribution ou la suppression des accès.

- **Back-end securisé en réseau local et cloud hybride avec segmentation.**

Le back-end constitue le cœur du système. Il héberge les services critiques d'authentification, de traitement des données biométriques et de gestion d'accès. Pour notre système nous avons utilisée deux type qui sont **le réseau local** et **le cloud hybride**

3.3.1 Avantages et intérêt de la solution

Bien plus qu'une simple innovation technologique, cette solution va transformer profondément les processus de contrôle d'accès et d'identification. En voici les principaux bénéfices.

- **Sécurité renforcée** : double authentification biométrique difficile à falsifier
- **Réduction de la fraude** : plus de badges perdus ou partagés
- **Gain de temps** : identification instantanée sans besoin de manipulation physique
- **Traçabilité accrue** : chaque accès est enregistré et peut être audité
- **Conformité RGPD et standards ISO/IEC 27001** en sécurité de l'information
- **Expérience utilisateur fluide** pour le personnel, sans friction

3.3.2 Retour d'expérience (hypothétique, basé sur cas réels similaires)

Nous avons recueilli des informations comme quoi il existence des systèmes similaires dans les pays tels que :

- **Changi Airport (Singapour)** : déploiement de la reconnaissance faciale pour l'embarquement
- **Aéroport de Dubaï** : couloir intelligent utilisant la biométrie pour l'immigration
- **Aéroport d'Orly** : tests de contrôle d'accès biométrique pour le personnel technique

La mise en place de ce type de système à très vites permis d'observer des résultats importants tant sur le plan de la sécurité que de l'efficacité. Nous avons recueilli comme améliorations de performances globales :

- Une **diminution des intrusions de 70 %**
- Une **amélioration de 40 % des temps de passage**
- Amélioration du moral des équipes techniques (+15 % de satisfaction)
- Une **meilleure acceptation des procédures de sécurité** par les utilisateurs

4 Contexte réglementaire

La mise en place de notre système de contrôle d'accès basé sur des données biométriques dans l'environnement aéroportuaire est soumise à différemment réglementations telles qu'un ***cadre réglementaire strict*** à la fois ***national et international***. Ce cadre vise à protéger les ***données personnelles sensibles***, garantir la ***transparence***, assurer la ***proportionnalité des traitements*** et éviter tout abus.

Réglementation européenne : RGPD (*Règlement Général sur la Protection des Données*)

Le RGPD (UE 2016/679), en vigueur depuis 2018, encadre les traitements de données à caractère personnel dans toute l'Union européenne. Les ***données biométriques*** sont considérées comme **sensibles** (article 9), et leur traitement est ***interdit par principe***, sauf exceptions strictes :

4.1 Conditions autorisant le traitement :

- Consentement explicite et éclairé de la personne concernée
- Nécessité pour des raisons de ***sécurité publique***, de ***sûreté*** ou de ***prévention des fraudes***
- Traitement encadré par une ***loi nationale*** ou des ***intérêts vitaux***

4.2 Obligations RGPD pour l'entreprise :

- **DPIA obligatoire (*analyse d'impact relative à la protection des données*)**

  Le DPIA est un outil exigé par le RGPD (Règlement Général sur la Protection des Données) lorsqu'un traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.
  L'objectif est d' Identifier les risques liés à un traitement de données personnelles,évaluer leur gravité et leur vraisemblance et proposer des mesures pour les réduire ou les éliminer.

- ***Désignation*** d'un **Délégué à la protection des données (DPO)**

La fonction de délégué à la protection des données consacrée par le règlement général sur la protection des données s'inscrit à deux niveaux dans la démarche d'obligation pour les entreprises de mettre en oeuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données :

- La désignation d'un délégué à la protection des données constitue, d'une part, l'une des diligences permettant d'attester des démarches mises en oeuvre en termes de gestion de la conformité, au même titre par exemple que la rédaction d'études d'impact ou la réalisation d'opérations d'audit. Ce faisant, le délégué à la protection des données est vecteur de sécurité juridique et permet au responsable de traitement de ménager sa responsabilité, notamment

pénale, eu égard aux obligations lui incombant au titre de la réglementation informatique et libertés.

- Le délégué à la protection des données apparaît, d'autre part et plus largement, comme le coordonnateur du plan de mise en conformité que chaque responsable de traitement doit mettre en oeuvre sur le plan opérationnel concernant les différents outils de gestion de la conformité définis par le règlement général sur la protection des données : registre des traitements, études d'impact.

- Respect des **droits des personnes** : information, accès, rectification, opposition

Les personnes concernées doivent être **informées de manière claire, concise et accessible,** Les personnes peuvent obtenir confirmation que des données les concernant sont traitées , Les personnes peuvent demander :**La correction** de données inexactes **La mise à jour** de données incomplètes.

- Mise en œuvre du **Privacy by design & by default**
  L'intégration des principes de "Privacy by design" (protection de la vie privée dès la conception) et de "Privacy by default" (protection par défaut) constitue une exigence essentielle du Règlement Général sur la Protection des Données (RGPD – article 25). Ces principes doivent guider l'ensemble du cycle de vie du projet, depuis la phase de conception jusqu'à l'exploitation du système biométrique, afin de garantir que la protection des données personnelles est intégrée de manière structurelle et proactive, et non comme une mesure corrective a posteriori.
- Mise en place de **mesures techniques et organisationnelles** robustes (chiffrement, accès restreint, logs)
  Le traitement de données biométriques, du fait de leur sensibilité, exige la mise en œuvre de **mesures de sécurité renforcées**, tant sur le plan technique

Qu'organisationnel. Le RGPD (article 32) impose aux responsables de traitement et sous-traitants de garantir un niveau de sécurité **approprié au risque**, en prenant en compte l'état de l'art, les coûts de mise en œuvre, la nature des données traitées et les finalités du traitement.

Dans le cadre d'un système de contrôle d'accès biométrique dans une zone aéroportuaire, cela implique la mise en place d'un ensemble de **dispositifs cohérents et complémentaires**,

destinés à assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données personnelles.

- **Minimisation** : ne collecter que les données strictement nécessaires

Le **principe de minimisation des données** est un pilier fondamental du Règlement Général sur la Protection des Données (RGPD – article 5.1.c). Il impose que les données à caractère personnel collectées soient "adéquates, pertinentes et limitées à ce qui est nécessaire" au regard des finalités pour lesquelles elles sont traitées.

Réglementation française **: CNIL (*Commission nationale de l'informatique et des libertés*)**En France, la CNIL encadre strictement l'utilisation des données biométriques.

4.2.1 Points clés :

- La **reconnaissance faciale et les empreintes** sont soumises à **autorisation préalable** de la CNIL (article 31 de la loi Informatique et Libertés)

  En France, la mise en œuvre de dispositifs de reconnaissance faciale, de lecture d'empreintes digitales ou tout autre traitement biométrique visant à identifier des individus de manière unique est encadrée de manière stricte par la loi Informatique et Libertés. L'article 31 de cette loi, en cohérence avec l'article 9 du RGPD, prévoit un régime d'autorisation préalable délivrée par la Commission nationale de l'informatique et des libertés (CNIL).
  L'usage dans un cadre professionnel ou de sécurité doit être ***justifié, proportionné*** *et* ***documenté***

L'utilisation de données biométriques dans un cadre professionnel (ex. : contrôle d'accès pour les employés, agents ou sous-traitants) ou de sécurité (ex. : filtrage en zone aéroportuaire, prévention des intrusions) est exceptionnelle et encadrée très strictement par la CNIL et le RGPD. En effet, la biométrie est considérée comme un traitement particulièrement intrusif car elle repose sur des caractéristiques uniques et immuables des individus (visage, empreintes, iris, etc.). Ainsi, pour être légitime, un tel usage doit impérativement répondre à trois exigences fondamentales et cumulatives : justification, proportionnalité et documentation.

- Une **analyse d'impact (AIPD)** doit être menée **avant** la mise en œuvre

L'Analyse d'impact relative à la protection des données souvent abrégée AIPD ou DPIA (Data Protection Impact Assessment) est une obligation réglementaire prévue à l'article 35 du RGPD. Elle constitue un outil clé pour évaluer, documenter et maîtriser les risques que fait peser un traitement de données personnelles sur les droits et libertés des personnes concernées.

Dans le cadre de la mise en œuvre d'un dispositif biométrique, en particulier dans un environnement à haut niveau de sécurité comme un aéroport, l'AIPD est obligatoire avant tout déploiement du système.

Transfert de données hors UE interdit sans garanties suffisantes (ex : clause contractuelle type) Le transfert de données personnelles, en particulier de données biométriques sensibles, vers des pays situés en dehors de l'Union Européenne (UE) est strictement encadré par le **RGPD** afin de protéger les droits fondamentaux des personnes concernées.

*4.2.2 **Cas d'exception autorisé : usage de la biométrie dans la sûreté aéroportuaire***

En principe, le ***traitement de données biométriques*** (empreintes digitales, reconnaissance faciale, iris, etc.) est **interdit** par le **RGPD**, sauf dans des cas bien spécifiques, car il s'agit de **données sensibles**. Toutefois, ***des exceptions sont prévues par la loi***, notamment dans le cadre de ***la sécurité publique*** et ***de la sûreté aéroportuaire***.

4.2.2.1 Fondement légal :

Dans le domaine aéroportuaire, l'utilisation de technologies biométriques peut être ***expressément autorisée par des textes réglementaires ou législatifs***, tels que

- Le **Code de l'aviation civile**.
- La **réglementation est émise par la DGAC** (*Direction Générale de l'Aviation Civile*).
- Le **Code des transports** ou d'autres textes relatifs à la **protection des frontières et à la sécurité nationale**.

4.2.2.2 Finalité :

Ces traitements sont autorisés ***dans le but de renforcer la sûreté des installations aéroportuaires***, notamment :

- Le ***contrôle d'accès aux zones sensibles*** (zones réservées aux personnels autorisés)
- La ***vérification d'identité des passagers*** dans les processus d'enregistrement ou d'embarquement.
- La ***prévention d'actes de malveillance ou de terrorisme***.

4.2.2.3 Conditions strictes :

Même lorsqu'un traitement biométrique est autorisé par la loi, il doit respecter **des garanties strictes**, notamment :

1. ***Proportionnalité et nécessité*** du traitement.
2. ***Base légale claire*** (loi, décret ou règlement autorisant explicitement le traitement).
3. ***Durée de conservation limitée*** des données.
4. ***Sécurité renforcée*** (chiffrement, contrôle d'accès).
5. ***Information des personnes concernées*** (panneaux d'affichage, mentions d'information).
6. ***DPIA* (analyse d'impact)** obligatoire avant la mise en œuvre.
7. ***Pas de traitement biométrique sans encadrement clair*** par une autorité publique ou une disposition légale.

4.3 Exemple concret :

Dans certains aéroports français, des **portes automatiques de contrôle aux frontières** utilisent la reconnaissance faciale pour **comparer le visage du passager à la photo de son passeport biométrique**, dans le cadre d'un programme encadré par la loi et contrôlé par la CNIL.

- **Règlementations internationales pertinentes**

ICAO (Organisation de l'Aviation Civile Internationale)

L'ICAO, agence spécialisée de l'ONU, fixe les normes techniques et de sécurité internationales pour les États membres dans le domaine de l'aviation civile, notamment **:**

Normes biométriques :

- L'Annexe 9 à la Convention de Chicago recommande l'usage de passeports biométriques **(MRP - Machine Readable Passports).**
- **L'ICAO** établit les spécifications des éléments biométriques (photo, empreintes, iris) intégrés aux documents de voyage et leur usage lors du passage aux frontières.
- Elle promeut l'usage de SBD (Self-Boarding Devices) et e-gates permettant une vérification d'identité automatisée et sécurisée.

Objectif :

Améliorer :

- La fluidité des flux de passagers.
- La sécurité des installations aéroportuaires.
- L'interopérabilité internationale des systèmes de contrôle aux frontières.

4.3.1 Intégration biométrique dans les e-gates et SBD

Les **e-gates** (portiques automatiques de contrôle) et les **SBD** (Self-Boarding Devices) utilisent la biométrie (généralement la reconnaissance faciale) pour :

- Comparer en temps réel ***le visage du passager*** à la ***photo stockée dans son passeport biométrique.***

- ***Automatiser le contrôle d'identité***, en lien avec les bases de données sécurisées (comme VIS ou SIS en Europe).
- ***Réduire les files d'attente*** tout en maintenant un ***haut niveau de sécurité***.

4.3.2 Recommandations sur la protection des données des passagers et du personnel

Les déploiements biométriques doivent **respecter les principes fondamentaux du RGPD**, même s'ils s'intègrent dans un cadre international :

- ***Information claire et transparente*** des personnes concernées.
- ***Limitation des finalités*** : uniquement pour la vérification d'identité, la sécurité et la sûreté.
- ***Minimisation des données*** collectées.
- ***Sécurité renforcée*** : chiffrement, pseudonymisation, journalisation.
- ***Droit d'accès, de rectification et, dans certains cas, d'opposition*.**
- ***Réalisation d'une analyse d'impact (DPIA*)** obligatoire.

4.3.2.1 Cas particulier : hébergement hors Europe

Privacy Shield / Cloud Act

Problème :

Si tout ou partie du système biométrique (base de données, moteur de reconnaissance, hébergement) est confiée à un prestataire américain (comme AWS, Microsoft Azure, Google Cloud), des risques juridiques existent :

- Le **Privacy Shield**, ancien accord entre l'UE et les États-Unis encadrant les transferts de données, a été **invalidé en 2020** par la Cour de justice de l'UE (arrêt Schrems II).
- Le **Cloud Act** (2018) autorise les autorités américaines à accéder aux données stockées à l'étranger par des entreprises américaines, même sans mandat européen.

Solution RGPD :

Pour **respecter le RGPD**, l'entreprise doit :

1. **Éviter l'hébergement aux États-Unis ou avec des prestataires soumis au Cloud Act**, sauf garanties supplémentaires solides.
2. Utiliser :

    - Un hébergeur cloud souverain européen (ex. : OVHcloud, Outscale, Scaleway) non soumis à la juridiction américaine.
    - Des clauses contractuelles types (SCCs) renforcées.
    - Des mesures techniques supplémentaires : chiffrement fort, cloisonnement, anonymisation.

3. Vérifier que le sous-traitant respecte les principes du RGPD : sécurité, confidentialité, encadrement strict des transferts de données hors UE.

Risques en cas de non-respect

Risque	**Conséquence potentielle**
Traitement non conforme au RGPD	Amende jusqu'à **20 millions d'euros** ou 4 % du CA
Absence d'AIPD validée	Blocage du projet par la CNIL
Violation de données	poursuites judiciaires
Usage disproportionné	Interdiction de traitement, poursuites judiciaires

Transfert illégal hors UE	Suspension immédiate du traitement, sanctions

5 Architecture et règles de sécurité

La solution biométrique de cybersécurité que nous proposons impose une **architecture technique robuste, résiliente et conforme au RGPD**. Cette architecture doit garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données biométriques de toutes personnes durant le cycle de vie de notre système faisant la collecte, le traitement, le stockage, la transmission et la suppression.

5.1 Architecture technique sécuris

5.1.1 Points de collecte

Afin de garantir un haut niveau de fiabilité et de sécurité dans notre processus d'authentification nous nous sommes attardées précisément sur:

- **Capteurs biométriques** (lecteurs d'empreinte, caméras).

- **Sécurisation physique** : matériel certifié (ISO/IEC 30107), protection contre les attaques de type *spoofing*.

5.1.2 Traitement local et périphérique

- Utilisation d'un **moteur de reconnaissance biométrique** (embarqué ou déporté).
- Prétraitement des données (extraction de caractéristiques biométriques).

5.1.3 Serveur d'authentification ou de correspondance

- Comparaison des données biométriques captées avec celles stockées.
- Si déporté sur le cloud, le serveur doit être **hébergé en Europe ou sur un cloud souverain** (OVHcloud, Outscale, etc.).

5.1.4 Stockage des données

- **Chiffrement AES-256** ou supérieur pour les données au repos.
- **Séparation des données identifiantes** (nom, prénom) et des **données biométriques** (template).
- Option : **stockage distribué et pseudonymisation** pour limiter l'impact d'une fuite.

5.1.5 Réseau et transmission

- Utilisation de protocoles sécurisés (**TLS 1.3**, VPN d'entreprise).
- Authentification mutuelle des équipements (*mutual TLS*).
- Journalisation des accès au système.

5.2 Règles de sécurité d'utilisation

Pour protéger les données biométriques, l'entreprise doit appliquer des **politiques de sécurité strictes** :

5.2.1 Authentification forte

- Accès au système par **MFA (authentification multifactorielle)**.

  L'accès à un système traitant des **données sensibles**, comme des données biométriques, doit être strictement contrôlé afin de prévenir tout accès non autorisé, piratage ou fuite de données. Dans ce cadre, l'utilisation d'une authentification multifactorielle (MFA) constitue une mesure de sécurité essentielle, conforme aux exigences du RGPD et aux bonnes pratiques de cybersécurité.

- Limitation des privilèges (principe du **moindre privilège**).

  Dans tout système manipulant des données sensibles notamment des données biométriques , il est essentiel d'encadrer strictement les accès aux ressources,

fonctionnalités et données. À ce titre, le principe du moindre privilège (ou Least Privilege Principle) est une bonne pratique fondamentale en matière de cybersécurité et de conformité au RGPD.

5.2.2 Gouvernance des accès

- Gestion centralisée des identités (**IAM**) et des rôles.

  Dans un système impliquant la gestion de données sensibles telles que les données biométriques, il est indispensable de mettre en place une infrastructure de gestion des identités et des accès (IAM - Identity and Access Management). Cette approche garantit que chaque utilisateur dispose d'un niveau d'accès strictement adapté à ses responsabilités, tout en assurant la traçabilité, la conformité réglementaire et la sécurité des opérations

- Journalisation et **audit régulier** des accès aux composants sensibles.

  Dans tout système manipulant des données sensibles, en particulier des données biométriques, la traçabilité des accès est une mesure de sécurité incontournable. La journalisation des événements (ou logging) et leur audit régulier permettent de garantir la transparence, d'assurer la détection rapide d'anomalies, et de démontrer la conformité du système aux exigences du RGPD et des recommandations de la CNIL.

5.2.3 Cycle de vie des données

- Suppression automatique des données selon les délais légaux (principe de **durée de conservation limitée**).

  L'un des principes fondamentaux du RGPD (article 5, paragraphe 1-e) est celui de la limitation de la durée de conservation des données personnelles. Cela signifie que les données, en particulier les données sensibles comme les informations biométriques, ne peuvent être conservées que le temps strictement nécessaire à la finalité du traitement. Au-delà de cette durée, elles doivent être effacées ou rendues anonymes de manière irréversible.

- **Procédures de purge sécurisée** en cas de changement d'usage ou de sortie du système.
  Le traitement de données biométriques, par nature sensible, impose une gestion

rigoureuse de leur cycle de vie, y compris lors de la fin d'utilisation, d'un changement de finalité, ou de la sortie d'un système ou d'un sous-traitant. Dans ce contexte, il est impératif de mettre en place des procédures de purge sécurisée, garantissant la suppression complète, traçable et irréversible des données concernées.

5.2.4 Détection et réponse aux incidents

- Mise en place d'un **SIEM** (Security Information and Event Management).

Dans un environnement traitant des données biométriques, la surveillance en temps réel, la corrélation des événements de sécurité et la détection précoce des incidents sont essentielles pour garantir l'intégrité du système et la conformité aux exigences du RGPD et des autorités de régulation (comme la CNIL). Pour cela, l'intégration d'un SIEM s'impose comme une brique centrale de la stratégie de cybersécurité.

- Plan de réponse à incident (PRI), y compris **procédure de notification à la CNIL** en cas de fuite.

Dans tout système traitant des **données sensibles**, notamment **biométriques**, la survenue d'un incident de sécurité comme un accès non autorisé, une perte de données ou une attaque informatique peut avoir des conséquences majeures sur les droits et libertés des personnes concernées. Pour s'en prémunir et y réagir efficacement, il est essentiel de disposer d'un **Plan de Réponse à Incident (PRI)** structuré, documenté et testé.

5.2.5 Conformité et vérification

- Réalisation d'une **analyse d'impact (DPIA)** avant mise en œuvre.
- **Audit annuel** de la conformité (interne ou externe).
- Formation des utilisateurs et sensibilisation à la sécurité des données biométriques.

Bonnes pratiques à intégrer

- Utiliser des **templates biométriques non réversibles** (ne permettent pas de reconstituer le visage ou l'empreinte).
- Mettre à jour régulièrement les composants logiciels (patching).
- Prévoir des **mécanismes de consentement** et une interface pour exercer les **droits RGPD** (accès, effacement, opposition).

- Prévoir un **mode de repli non biométrique** en cas d'échec ou d'indisponibilité du système (accès d'urgence).

6 Risques et coûts d'implémentation

L'implémentation d'une solution biométrique dans un environnement sensible comme un aéroport présente des **risques multidimensionnels** : techniques, organisationnels, réglementaires et financiers. Une évaluation rigoureuse de ces risques est nécessaire pour anticiper les défaillances, garantir la conformité et assurer la continuité d'activité.

6.1 Typologie des risques

6.1.1 . Risques cybersécurité

Risque	**Description**	**Niveau d'exposition**	**Impact potentiel**
Vol de données biométriques	Piratage de la base de données biométrique ou interception en transit	Élevé si chiffrement mal configuré	Atteinte à la vie privée, sanctions RGPD
Falsification / spoofing	Utilisation de masques 3D ou d'empreintes falsifiées	Moyen à élevé selon le capteur	Accès non autorisé à des zones sensibles
Ransomware ou DDoS	Attaque sur les serveurs d'authentification	Moyen	Interruption de service, perte d'accès

6.1.2 Risques organisationnels

Risque	**Description**	**Niveau d'exposition**	**Impact potentiel**
Manque de formation	Utilisation incorrecte du système, erreurs humaines	Élevé	Fausse authentification, blocage d'accès
Réorganisation non anticipée	Mauvaise intégration dans les processus métiers existants	Moyen	Résistance au changement, surcoût

6.1.3 Risques juridiques et réglementaires

Risque	**Description**	**Niveau d'exposition**	**Impact potentiel**
Non-conformité RGPD	Absence de DPIA, consentement non recueilli, durée de conservation excessive	Élevé	Amendes pouvant aller jusqu'à 4 % du CA annuel mondial
Transfert illégal de données	Hébergement dans un pays non adéquat (Cloud Act, absence de SCC)	Élevé	Procédures CNIL, perte de réputation

6.1.4 Risques réputationnels

- Perte de confiance des utilisateurs (clients ou salariés).
- Médiatisation d'une faille de sécurité ou d'un traitement abusif.
- Dégradation de l'image de marque et impact commercial

6.2 Estimation des coûts d'implémentation

Les coûts peuvent varier selon la **taille de l'organisation**, le **nombre de points d'accès**, le **type de technologie biométrique**, et le **niveau de sécurité souhaité**. Voici une estimation basée sur une hypothèse pour une **entreprise de 500 salariés avec 5 points d'accès sécurisés** :

6.2.1 Coûts techniques

Poste budgétaire	**Détail**	**Coût estimé**
Capteurs biométriques (caméras + scanners)	5 points d'accès x 2 capteurs x 800 €	8 000 €
Serveur de traitement biométrique	Matériel et logiciel sous licence	5 000 €
Hébergement sécurisé (cloud souverain)	12 mois de service	4 000 €
Développement logiciel / API / intégration SI	Connexion avec annuaire LDAP, système d'accès, etc.	12 000 €
Chiffrement, VPN, TLS, journalisation	Achat et configuration de sécurité réseau	3 000 €
Maintenance (1 an)	Support technique, mises à jour	3 500 €

Sous-total technique : 35 500 €

6.2.2 Coûts humains et organisationnels

Poste budgétaire	**Détail**	**Coût estimé**
Formation des utilisateurs	10 sessions pour le personnel	2 000 €
Sensibilisation RGPD et sécurité	Ateliers ou e-learning	1 500 €

Gestion de projet (Chef de projet + RSI)	20 jours homme à 600 €/j	12 000 €

Sous-total organisationnel : 15 500 €

6.2.3 Coûts juridiques et réglementaires

Poste budgétaire	**Détail**	**Coût estimé**
Réalisation d'une DPIA	Par un expert DPO / consultant RGPD	2 500 €
Consultation CNIL (si projet à risque élevé)	Optionnel mais recommandé	1 000 €
Rédaction de politique de confidentialité / charte interne	Juriste RGPD	2 000 €

Sous-total juridique : 5 500 €

Total estimé du projet :

56 500 € TTC, hors évolution/montée en charge ou internationalisation du dispositif.

6.3 Hypothèses utilisées

- 500 utilisateurs.
- 5 points d'accès.
- Solution déployée sur site unique.
- Recours à des prestataires européens conformes RGPD.
- Projet sur 12 mois.

En résumé : tableau synthétique

Type de risque	**Niveau de gravité**	**Solutions préventives**

Cyber (fuite, spoofing)	Élevé	Chiffrement, anti-spoofing, journalisation
Juridique (RGPD)	Élevé	DPIA, consentement, hébergement UE
Organisationnel	Moyen à élevé	Formation, conduite du changement
Financier	Moyen	Budget maîtrisé via appels d'offres
Réputationnel	Élevé (si incident)	Communication transparente, plans de remédiation

7 Mesures correctives

Les mesures correctives sont les actions concrètes à mettre en œuvre pour traiter les risques identifiés (voir point 6) dans le cadre du déploiement d'une solution biométrique. Contrairement aux mesures préventives (comme la sécurisation initiale ou la formation), les mesures correctives interviennent en réponse à un incident, à une faille ou à un audit non satisfaisant, pour rétablir un niveau de sécurité adéquat et corriger les vulnérabilités détectées.

Objectif des mesures correctives

- Réduire l'exposition aux risques résiduels.
- Corriger des défaillances identifiées (techniques, humaines ou organisationnelles).
- Mettre en conformité la solution avec les exigences légales, normatives ou internes.
- Limiter les conséquences d'un incident (ex. : fuite de données, accès frauduleux).
- Améliorer en continu la sécurité globale de la solution.

7.1 Typologie des mesures correctives à appliquer

*7.1.1 **Mesures correctives techniques***

Situation	Mesure corrective	Détail
Fuite de données biométriques (accès non autorisé)	Révocation immédiate des accès compromis et mise à jour des clés de chiffrement	Génération de nouvelles clés, surveillance renforcée via SIEM
Vulnérabilité logicielle découverte	Application immédiate du correctif de sécurité (patch)	Suivi actif des CVE et de l'éditeur logiciel
Spoofing ou contournement d'un capteur biométrique	Remplacement du capteur par un modèle certifié ISO/IEC 30107-3	Déploiement de capteurs anti-contrefaçon (détection de chaleur, profondeur, texture)
Non-journalisation des accès sensibles	Ajout d'un module de journalisation centralisée	Intégration à un SIEM pour corrélation des événements et alertes temps réel
Défaut de suppression des données expirées	Mise en œuvre d'un processus de purge automatisé	Tâche planifiée selon politique de conservation définie

7.1.2 Mesures correctives organisationnelles

Situation	Mesure corrective	Détail
Manque de sensibilisation du personnel	Organisation de sessions de formation ou e-learning ciblé	Obligatoire pour les administrateurs et utilisateurs
Politique de sécurité inadaptée ou obsolète	Révision de la politique interne de sécurité et des procédures	Mise à jour annuelle ou après tout incident

Incapacité à répondre aux demandes RGPD (droits des personnes)	Mise en place d'un guichet unique RGPD interne ou DPO externalisé	Interface d'exercice des droits avec accusé de réception sous 1 mois
Défaillance dans la gestion des habilitations	Audit des droits d'accès et réattribution basée sur les rôles	Implémentation d'un processus de recertification périodique des accès
Absence de plan de continuité (PCA) ou de reprise (PRA)	Création et test d'un PCA/PRA dédié au système biométrique	Sauvegardes hors ligne, procédures de bascule, délais de rétablissement (RTO/RPO) définis

7.1.3 Mesures correctives réglementaires et juridiques

Situation	**Mesure corrective**	**Détail**
Absence ou insuffisance de DPIA	Réalisation ou mise à jour de l'analyse d'impact	Collaboration avec le DPO, documentation complète, validation interne
Hébergement non conforme au RGPD	Migration vers un cloud souverain ou mise en place de SCC renforcées	OVHcloud, Outscale, ou hébergement sur site
Absence de consentement ou transparence floue	Refonte de la politique de confidentialité et des interfaces utilisateurs	Ajout d'un module de consentement explicite, facilement réversible
Notification de la CNIL obligatoire non effectuée	Création d'un protocole de notification RGPD post-incident	Déclaration dans les 72 heures, fiches types prêtes, cellule d'alerte activable

7.1.3.1 Exemple de plan d'action correctif

N°	Risque constaté	Mesure corrective
1	Capteur contournable (spoofing)	Remplacement par capteur certifié
2	Absence de journalisation	Intégration au SIEM
3	DPIA absent	Réalisation avec le DPO
4	Données conservées au-delà du délai légal	Implémentation de politique de purge automatique

Clés de succès d'une démarche corrective efficace

- **Réactivité :** identifier et corriger rapidement les failles détectées.
- **Traçabilité :** documenter chaque mesure corrective dans un registre**.**
- **Pilotage :** assigner un responsable par action et suivre les délais d'exécution**.**
- **Communication :** informer les parties prenantes concernées**.**
- **Amélioration continue :** alimenter le retour d'expérience dans la gestion de projet.

8 Conclusion

Ce projet de cybersécurité appliqué au secteur de l'aéronautique illustre l'importance croissante des technologies biométriques dans la sécurisation des accès à des infrastructures critiques. En choisissant de travailler sur un système de contrôle d'accès biométrique combinant la reconnaissance faciale et les empreintes digitales, nous avons confronté des problématiques à la fois **technologiques, humaines, juridiques et stratégiques**.

À travers l'analyse du **besoin métier**, nous avons identifié les faiblesses des systèmes traditionnels de contrôle d'accès (badges, mots de passe) et démontré l'intérêt d'une solution basée sur l'**identité biologique unique des utilisateurs** pour renforcer la sûreté des zones sensibles d'un aéroport. Cette solution cyber, bien qu'efficace, implique de respecter un cadre réglementaire rigoureux, notamment le **RGPD** et les exigences de la **CNIL**, tout en assurant la **conformité technique**, la **résilience**, et l'**acceptabilité par les utilisateurs**.

Comme un véritable **chef de projet**, cette démarche a permis de :

- Structurer un plan d'implémentation clair,
- Identifier les **coûts associés** et les **risques opérationnels**,
- Proposer des **mesures correctives** pour garantir la sécurité et la pérennité de la solution.

En somme, cette réflexion nous a permis de simuler la mise en œuvre d'un projet à fort enjeu dans un environnement réel, avec toutes les **contraintes et exigences d'une entreprise moderne**. Ce type de projet prépare les futurs professionnels à concilier **innovation technologique**, **cybersécurité**, **réglementation**, et **réalité terrain**, dans une logique de **gestion globale des risques**.

Glossaire des acronymes

RGPD – *Règlement Général sur la Protection des Données*

Règlement européen (UE 2016/679) en vigueur depuis 2018, visant à encadrer le traitement des données personnelles et à garantir les droits fondamentaux des citoyens de l'UE en matière de vie privée.

CNIL – *Commission Nationale de l'Informatique et des Libertés*

Autorité administrative indépendante française chargée de veiller à la protection des données personnelles et au respect des droits numériques.

OACI – *Organisation de l'Aviation Civile Internationale* (en anglais ICAO)

Agence spécialisée des Nations Unies chargée de fixer les normes et réglementations mondiales pour la sécurité, l'efficacité et la régularité de l'aviation civile.

SIRH – *Système d'Information des Ressources Humaines*

Ensemble de logiciels et outils numériques permettant de gérer de façon centralisée les processus RH (paie, recrutement, formation, absences, etc.).

IAM – *Identity and Access Management*

Gestion des identités et des accès. Système permettant de créer, gérer et contrôler l'accès des utilisateurs aux ressources numériques d'une organisation, tout en assurant la sécurité et la traçabilité.

SCC – *Standard Contractual Clauses* (*Clauses Contractuelles Types*)

Clauses juridiques définies par la Commission européenne pour encadrer les transferts de données personnelles vers des pays tiers non reconnus comme offrant un niveau de protection adéquat.

AIPD – *Analyse d'Impact relative à la Protection des Données* (en anglais DPIA – Data Protection Impact Assessment)

Étude obligatoire dans certains cas pour évaluer les risques liés au traitement de données sensibles et définir les mesures de protection appropriées.

PRI – *Plan de Réponse à Incident*

Ensemble des procédures prévues pour réagir rapidement et efficacement à un incident de sécurité informatique (fuite de données, attaque, etc.), incluant la notification à la CNIL si nécessaire.

SIEM – *Security Information and Event Management*

Outil de supervision et d'analyse centralisée des événements de sécurité du système d'information (logs, alertes, anomalies), utilisé pour détecter et répondre aux menaces en temps réel.

MFA – *Multi-Factor Authentication* (*Authentification multifacteur*)

Méthode de vérification de l'identité d'un utilisateur via au moins **deux facteurs distincts** : un mot de passe + un code SMS, une empreinte digitale, ou une carte physique, etc.