Ananlysis of security risks

Objectifs de la sécurité

Objectif	Description
Confidentialité	- Protection des données personnelles des utilisateurs, y compris les informations d'identification, les données de localisation, les données de santé, etc.
	- Chiffrement des données sensibles lors de leur transmission sur le réseau.
	- Contrôle d'accès strict pour garantir que seuls les utilisateurs autorisés peuvent accéder aux données confidentielles.
	- Gestion sécurisée des identités et des informations d'authentification.
Intégrité	- Vérification de l'exactitude et de la cohérence des données à chaque étape du processus, y compris la collecte, le stockage et l'analyse. - Utilisation de mécanismes de hachage pour garantir l'intégrité des données stockées.
	- Mise en œuvre de contrôles d'intégrité pour détecter les erreurs de transmission ou les corruptions de données.
	- Sauvegarde régulière des données pour prévenir la perte de données.
Disponibilité	- Mise en place d'une architecture robuste et redondante pour garantir une disponibilité élevée de l'application.
	- Surveillance proactive des performances et des temps de réponse.
	- Répartition de charge pour équilibrer la charge sur les serveurs et éviter les surcharges.
	- Planification régulière de la maintenance et des mises à jour.

Analyse de l'application

Système	Atout	Vulnérabilité	Attaque	Risque	Niveau d'impact	Contre-mesure
Collecte de données	Large couverture des capteurs sur une grande zone	Manque de chiffrement pendant la transmission des données	Attaque de l'homme du milieu	Accès non autorisé aux données des capteurs	Élevé	Implémenter des protocoles de chiffrement pour la transmission des données
	Collecte régulière de données à intervalles fixes	Format de fichier CSV vulnérable	Attaques par injection (par exemple, injection SQL)	Corruption ou manipulation des données	Élevé	Implémenter des mécanismes de validation des entrées pour prévenir les attaques par injection

Système	Atout	Vulnérabilité	Attaque	Risque	Niveau d'impact	Contre-mesure
	Stockage centralisé simplifie la gestion	Accès non autorisé au serveur central	Intrusion sur le serveur	Modification ou vol non autorisé de données	Élevé	Renforcer les mesures de sécurité du serveur, telles que le contrôle d'accès et les systèmes de détection des intrusions
	Utilisation de capteurs basse consommation pour une empreinte écologique réduite	Manque de protection physique des capteurs contre la manipulation ou le vol	Altération physique des capteurs	Perte ou vol de capteurs	Faible	Installer des capteurs dans des boîtiers sécurisés et surveiller les sites de déploiement pour prévenir la manipulation ou le vol
	Utilisation de capteurs alimentés par énergie solaire pour une autonomie prolongée	Manque de redondance dans la collecte des données pour éviter les pertes	Panne temporaire ou définitive des capteurs	Perte de données en cas de panne	Faible	Mettre en place des mécanismes de redondance pour assurer la disponibilité continue des données collectées
Analyse des capteurs	Identifier et maintenir les capteurs défaillants	Manque d'authentification pour les données des capteurs	Attaques de spoofing (par exemple, spoofing IP)	Données de capteur fausses entraînant une analyse incorrecte	Élevé	Implémenter des mécanismes d'authentification pour les données des capteurs afin d'assurer l'intégrité et l'authenticité
	Agréger des données pour l'analyse statistique	Manque de vérifications d'intégrité des données	Manipulation des données	Résultats statistiques trompeurs	Moyen	Implémenter des vérifications d'intégrité des données pour détecter et prévenir la manipulation des données
	Noter et classer les capteurs pour leur similitude	Manque de contrôles d'accès sur le processus de comparaison des capteurs	Accès non autorisé aux données de comparaison	Accès non autorisé à des informations sensibles	Moyen	Implémenter des mécanismes de contrôle d'accès pour restreindre l'accès à la fonctionnalité de comparaison des capteurs
Requête géographique	Positionnement géographique précis	Manque de vérifications d'autorisation pour les requêtes géographiques	Accès non autorisé aux résultats de la requête	Exposition d'informations de localisation sensibles	Moyen	Implémenter des vérifications d'autorisation pour restreindre l'accès à la fonctionnalité de requête géographique

Système	Atout	Vulnérabilité	Attaque	Risque	Niveau d'impact	Contre-mesure
	Capacités de requête en temps réel	Manque de validation des entrées pour les coordonnées géographiques	Manipulation des entrées	Résultats de requête invalides ou trompeurs	Moyen	Implémenter des mécanismes de validation des entrées pour garantir la validité des coordonnées géographiques
Performance	Algorithmes efficaces pour l'analyse des données	Manque de surveillance de l'utilisation des ressources	Attaques par déni de service	Performance de l'application dégradée	Élevé	Implémenter des mécanismes de surveillance des ressources et de limitation de débit pour atténuer les attaques par déni de service
	Temps d'exécution minimal pour les algorithmes	Manque de mesures d'optimisation	Exploitation des faiblesses algorithmiques	Exécution inefficace des algorithmes	Élevé	Optimiser les algorithmes pour améliorer les performances et l'utilisation des ressources
Interface Utilisateur	Interface utilisateur sur mesure en fonction des rôles	Manque d'authentification pour les rôles utilisateur	Accès non autorisé aux données sensibles	Exposition d'informations sensibles à des utilisateurs incorrects	Moyen	Implémenter des mécanismes d'authentification pour les rôles utilisateur afin d'assurer le contrôle d'accès
	Accès restreint aux données	Manque de communication sécurisée entre l'interface utilisateur et les données	Interception ou manipulation des données	Accès ou modification non autorisés des données	Élevé	Implémenter des protocoles de communication sécurisée entre l'interface utilisateur et le stockage des données
	Interface utilisateur conviviale avec une courbe d'apprentissage réduite	Manque de gestion des sessions utilisateur pour prévenir les accès non autorisés	Session volée ou usurpée	Accès non autorisé à l'interface utilisateur	Faible	Mettre en œuvre des mécanismes de gestion de session robustes pour empêcher les accès non autorisés
	Accès restreint aux fonctionnalités de l'interface utilisateur basé sur les privilèges	Manque de journalisation des activités utilisateur pour l'audit et la surveillance	Activité malveillante ou suspecte	Incapacité à suivre ou à détecter les activités malveillantes	Faible	Mettre en œuvre une journalisation efficace des activités utilisateur pour la détection et la réponse aux incidents
Surveillance des performances	Capacité à surveiller les performances des systèmes pour détecter les anomalies	Manque de sécurité dans les mécanismes de surveillance des performances	Attaques visant à altérer les données de surveillance	Détection inexacte ou altération des performances du système	Élevé	Implémenter des mécanismes de surveillance sécurisés et des contrôles d'intégrité pour les données de performance

Système	Atout	Vulnérabilité	Attaque	Risque	Niveau d'impact	Contre-mesure
	Temps de réponse rapide aux événements critiques	Manque de tolérance aux pannes	Panne ou indisponibilité du système	Temps de réponse retardé ou défaillance du système	Élevé	Concevoir une architecture résiliente avec des mécanismes de redondance et de récupération en cas de panne
Gestion des autorisations	Attribution de droits d'accès en fonction des rôles et des responsabilités	Manque de vérifications d'autorisation lors de l'attribution des droits d'accès	Attribution de droits d'accès inappropriés ou excessifs	Accès non autorisé à des données sensibles ou à des fonctionnalités critiques	Moyen	Implémenter des mécanismes de contrôle d'accès basés sur des règles et des politiques de sécurité
	Gestion sécurisée des identités et des informations d'authentification	Manque de sécurité dans le stockage et la transmission des informations d'identification	Vol ou compromission des informations d'identification	Utilisation frauduleuse des identités ou accès non autorisé	Élevé	Implémenter des protocoles et des techniques de cryptage sécurisés pour protéger les informations d'identification
Intégrité des données	Maintien de l'intégrité des données pour garantir leur fiabilité et leur précision	Manque de mécanismes de vérification de l'intégrité des données	Altération ou corruption des données	Perte de fiabilité ou d'exactitude des données	Moyen	Implémenter des mécanismes de vérification d'intégrité pour détecter et prévenir la corruption des données