Demande de proposition : Cahier des charges pour une infrastructure réseau et logicielle pour hôpital de campagne

1. Contexte et Objectifs du Projet

Les hôpitaux de campagne jouent un rôle essentiel dans les situations d'urgence, de catastrophe naturelle ou de conflits armés. Ils doivent être déployés rapidement sur le terrain et être prêts à offrir des services médicaux complets pour gérer un flux important de patients dans des environnements souvent peu favorables. La mise en place d'un système d'information performant et d'une infrastructure de communication fiable est cruciale pour assurer la qualité des soins, la coordination des équipes médicales, et la sécurité des informations sensibles.

Ce projet vise donc à développer et implémenter une infrastructure réseau et logicielle complète pour un hôpital de campagne capable de gérer efficacement ses opérations. Le projet inclut la gestion des flux de données médicales et administratives, la communication entre les différents intervenants (médecins, infirmiers, personnel administratif), et la protection de l'ensemble du système contre les menaces de sécurité.

Problématiques:

Les hôpitaux de campagne sont confrontés à plusieurs défis spécifiques, notamment :
- Déploiement rapide dans des environnements inconnus ou peu stables.
- Gestion de la connectivité dans des conditions de communication limitées ou instables.
- Confidentialité et sécurité des données médicales dans des zones à risque élevé d'espionnage ou d'attaque cyber.
- Facilité d'utilisation par un personnel médical potentiellement non formé aux outils numériques complexes.
- Continuité du service en cas de coupure du réseau ou de panne matérielle.

Objectifs du Projet:

Le projet a pour objectif de fournir un système d'information et de communication fiable, sécurisé et adaptable à un hôpital de campagne, avec les caractéristiques et fonctionnalités suivantes :

1. Mise en place d'une infrastructure réseau adaptée :
   - Déploiement d'une architecture réseau comprenant des équipements filaires (switches et routeurs) et un réseau Wi-Fi sécurisé.
   - Capacité à gérer jusqu'à 50 utilisateurs simultanés, comprenant le personnel médical et administratif.

- Isolation des différentes parties du réseau via des VLANs pour segmenter le trafic entre la direction, l'administration, et les services médicaux.

2. Gestion efficace des données médicales :
- Capacité de stockage et de gestion des données pour jusqu'à 300 patients simultanément.
- Implémentation d'un système de gestion de base de données permettant de consigner les informations médicales telles que les diagnostics, les résultats d'analyses, et les traitements en cours.
- Intégration de systèmes de sauvegarde automatisée pour éviter toute perte de données.

3. Sécurité et protection des données :
- Conformité avec les normes de sécurité HDS (Hébergeur de Données de Santé) pour garantir la confidentialité et l'intégrité des données des patients.
- Mise en place de protocoles de sécurité comme le chiffrement TLS/SSL pour la transmission des données et 802.1X pour l'authentification sur le réseau.
- Déploiement de pare-feu et de systèmes de détection d'intrusion (IDS) pour protéger l'infrastructure des attaques externes.

4. Communication interne fluide :
- Mise en place de services de messagerie sécurisée (type WhatsApp sécurisé) pour le personnel médical afin de faciliter la communication et la collaboration.
- Possibilité de visioconférence sécurisée pour la consultation de spécialistes à distance, même dans des conditions de bande passante limitée.

5. Connectivité fiable et stable :
- Déploiement de points d'accès Wi-Fi pour offrir une connectivité sans fil à tout le personnel médical, avec couverture totale de l'hôpital de campagne.
- Réseau Wi-Fi sécurisé avec contrôle d'accès pour limiter l'utilisation aux seuls utilisateurs autorisés et éviter les interférences.
- Configuration d'un réseau VPN pour permettre des échanges sécurisés avec d'autres structures médicales distantes.

6. Déploiement rapide et opérationnalité immédiate :
- Le système doit être déployé et opérationnel en 7 jours maximum, avec une configuration standardisée pour permettre une reproduction facile dans d'autres hôpitaux de campagne.
- Préparation de kits de déploiement contenant tous les équipements préconfigurés pour un montage rapide sur site.

Contraintes
- Budget maximal : 200 000 €. Le budget doit couvrir l'achat des équipements, les logiciels nécessaires, la mise en place de la sécurité, et les coûts de formation du personnel.
- Environnement : Les équipements doivent être robustes et capables de fonctionner dans des environnements potentiellement hostiles (températures extrêmes, humidité élevée, absence de connectivité Internet stable).
- Mobilité : L'infrastructure doit être facilement transportable et démontable, permettant à l'hôpital de se déplacer en fonction des besoins sur le terrain.

Risques Potentiels
- Risque de sécurité : Les hôpitaux sont des cibles fréquentes pour les cyberattaques. Une faille dans le système pourrait exposer les données médicales ou causer des interruptions de service.
- Risque de déploiement : Les délais serrés et les environnements instables peuvent entraîner des retards ou des erreurs de configuration.
- Risque de panne : Le matériel utilisé doit être de haute qualité pour éviter les pannes pendant les opérations médicales critiques.

Conclusion
Le succès du projet repose sur la capacité à déployer rapidement une infrastructure robuste et sécurisée, capable de gérer à la fois le flux de données médicales, la communication du personnel, et la continuité des soins pour les patients, tout en assurant une sécurité maximale des informations échangées.

2. Spécifications techniques requises

2.1. Infrastructure réseau

- Réseau local (LAN) : Installation de 4 switches pour connecter 10 ordinateurs, équipements médicaux essentiels et 6 points d'accès Wi-Fi.
- Wi-Fi : Installation de 6 points d'accès Wi-Fi (avec une portée d'environ 100 mètres), garantissant la connectivité des appareils mobiles du personnel médical.
- Sécurité réseau : Mise en place d’un pare-feu d’entreprise et d’un VPN pour sécuriser les connexions et protéger les données.
- Connexion Internet : Utilisation d'une connexion Internet par 4G/5G avec redondance satellite pour garantir une disponibilité continue.

2.2. Infrastructure logicielle

- Système de gestion des patients (DMP) : Logiciel de gestion des Dossiers Médicaux Partagés , permettant de suivre les données cliniques de 300 patients, incluant les traitements et diagnostics.
- Base de données : Serveur de base de données avec une capacité de stockage de 500 Go, permettant de gérer les informations des patients ainsi que les stocks de médicaments et de fournitures médicales.
- Logiciels complémentaires :
  - Gestion des stocks : Suivi en temps réel des médicaments et fournitures avec alertes automatiques en cas de faible stock ou d’utilisation anormale des fournitures.
  - Outils de communication interne : Installation d’une messagerie instantanée sécurisée et d’un système de visioconférence pour le personnel (pour des réunions et communications rapides).

- Application de gestion des lits et salle : Outil pour gérer l'occupation des lits et l'utilisation des salles, avec une vue en temps réel.

2.3. Sécurité des données

1) Sauvegarde des données :

Sauvegarde quotidienne automatique des données sur disques durs externes et dans le cloud sécurisé avec une capacité de rétention de 30 jours.

2) Gestion des accès :

Gestion des rôles avec un contrôle strict des autorisations d'accès(badges) , portail captif mis en place pour les utilisateurs(wifi). Sécurité 802.1x sur le switch avec certificat par utilisateurs pour s'authentifier Réseau segmenté en plusieurs VLAN avec du routage inter-vlan sur le switch.

3) Les Caméras dans l'Internet des Objets (IoT)

Les caméras IoT sont des dispositifs connectés qui captent des flux vidéo et les transmettent via des réseaux pour les analyser, les stocker ou les traiter en temps réel. Voici les caractéristiques qui les rendent essentielles dans l'IoT :

- **Connectivité** : Les caméras IoT se connectent au réseau (filaire ou sans fil) pour envoyer des flux vidéo en direct ou enregistrés vers des serveurs de stockage ou des systèmes de gestion vidéo (VMS).
- **Communication bidirectionnelle** : Les caméras IoT peuvent interagir avec d'autres dispositifs, comme des alarmes, capteurs de mouvement, systèmes de contrôle d'accès, etc.
- **Capacité de traitement embarquée** : Beaucoup de caméras IoT modernes disposent de capacités de traitement intégrées (edge computing), leur permettant de détecter automatiquement les mouvements, reconnaître des formes (visages, objets) ou déclencher des actions automatisées.

A) . Rôle des Caméras IoT dans les Hôpitaux

Dans le contexte hospitalier, les caméras IoT jouent un rôle essentiel dans plusieurs aspects de la sécurité et de la gestion opérationnelle :

a. Surveillance des Zones Critiques

- **Salles de soins intensifs** : Surveiller l'état des patients et permettre aux médecins de suivre à distance les activités à l'intérieur de ces salles.
- **Salles d'opération** : Suivi en temps réel des interventions chirurgicales et enregistrement des vidéos pour des examens médicaux ultérieurs ou des raisons légales.

- **Pharmacie et zones de stockage** : Prévention du vol ou de l'accès non autorisé aux médicaments et équipements sensibles.

b. Sécurisation des Accès

- Les caméras peuvent être associées aux systèmes de contrôle d'accès (par exemple, des serrures connectées) pour vérifier l'identité des personnes accédant aux zones sensibles comme :
    - Les laboratoires de recherche.
    - Les salles de serveurs ou d'administration.
    - Les zones de stockage de données sensibles.
- Elles peuvent fonctionner en combinaison avec d'autres dispositifs IoT, tels que les **capteurs de mouvement** ou les **détecteurs de présence**, pour renforcer la sécurité et alerter en cas de tentative d'accès non autorisé.

c. Surveillance de la Sécurité Physique

- Les hôpitaux sont des environnements complexes où il est essentiel de s'assurer que seuls les personnels autorisés accèdent aux différentes zones. Les caméras connectées permettent de détecter en temps réel les **comportements anormaux**, comme :
    - Des individus essayant d'entrer dans des zones restreintes.
    - Des objets abandonnés (détection de colis suspects).
    - Des foules ou des attroupements inhabituels pouvant signaler des incidents de sécurité.
- En outre, les caméras connectées peuvent envoyer des alertes automatiques en cas de détection d'activité suspecte, permettant une **réaction rapide** de l'équipe de sécurité.

d. Protection des Patients et du Personnel

- **Surveillance des chambres des patients** : Permettre aux soignants de surveiller les patients sans intrusion directe, en particulier pour les patients en réanimation ou ceux nécessitant une attention constante.
- **Contrôle des accès en cas d'urgence** : Les caméras peuvent être couplées à des dispositifs IoT pour verrouiller ou déverrouiller automatiquement les portes en fonction de la situation (par exemple, en cas d'évacuation ou d'incendie).

e. Supervision des Processus et Conformité

- Suivi des protocoles de sécurité et de conformité (comme les normes d'hygiène et de sécurité).
- Contrôle de la traçabilité des actions (par exemple, surveiller qui a accédé à la salle des médicaments).

B. Fonctionnement Intégré avec le Réseau IoT de l'Hôpital

Les caméras IoT, lorsqu'elles sont intégrées dans un environnement hospitalier, font partie d'un **écosystème global** où elles interagissent avec d'autres dispositifs connectés pour renforcer la sécurité et l'efficacité opérationnelle :

- **Plateformes de Gestion Vidéo** : Les flux vidéo des caméras sont envoyés à des serveurs dédiés ou à des **clouds sécurisés** pour le traitement et le stockage.
- **Détection d'intrusion** : Les caméras peuvent être reliées à un **système de détection d'intrusion** qui analyse les mouvements et déclenche des alarmes.
- **Automatisation des Réactions** : En cas d'alerte (mouvement suspect détecté par une caméra), des actions automatiques peuvent être prises : verrouillage de portes, notification aux responsables, activation de l'enregistrement vidéo.

C. Enjeux de Sécurité des Caméras IoT dans les Hôpitaux

Les caméras connectées dans un hôpital doivent être **particulièrement sécurisées**, car elles peuvent être une cible pour les cyberattaques :

- **Chiffrement des flux vidéo** (par exemple, HTTPS ou TLS) pour éviter l'interception des images.
- **Authentification forte** des utilisateurs (Multi-Factor Authentication, MFA) pour éviter les accès non autorisés aux vidéos.
- **Segmentation réseau** pour isoler les caméras IoT des autres segments du réseau hospitalier.

-Déploiement de **capteurs IoT** pour surveiller les environnements critiques (par exemple, capteurs de température et d'humidité dans les salles de stockage médicales).Cela servira à surveiller ert prévenir un éventuel feu dans une batiement et ainsi deployer rapidement des solutions avant que la situation soit hors de contrôle

4) **Implémentation d'un protocole sécurisé pour les appareils IoT** :

   Utilisation de standards comme **MQTT avec TLS** pour assurer une communication sécurisée entre les dispositifs IoT (moniteurs médicaux, dispositifs de diagnostic).

Pour renforcer la sécurité du déploiement MQTT/TLS dans l'hôpital, il est conseillé :

- D'utiliser **TLS v1.2 ou supérieur** pour bénéficier des dernières améliorations en matière de sécurité.
- Mettre en place un **système de gestion des certificats** (PKI) pour gérer facilement les renouvellements et révocations de certificats.
- Activer le **contrôle d'accès basé sur les rôles (RBAC)** pour restreindre les permissions des dispositifs IoT selon leur fonction (par exemple, les moniteurs

cardiaques ne doivent pas avoir accès aux topics réservés aux capteurs de température).

2.4. Maintenance et support

- Documentation complète : Nous souhaitons recevoir une documentation détaillée de l'infrastructure installée (schémas réseau, configurations, etc.).
- Support technique à distance : Un service de support 24/7 doit être disponible pour résoudre tout problème lié au système.
- Maintenance préventive : Prévoir des vérifications régulières (mensuelles) du système, mises à jour des logiciels et ajustement des dispositifs de sécurité.

3. Plan de déploiement souhaité

Jour 1 : Préparation du site et des équipements
- Repérage du site pour l'installation des équipements (routeurs, switches, points d'accès Wi-Fi).
- Vérification de la disponibilité de l'alimentation électrique et des infrastructures physiques nécessaires pour l'installation du matériel.
- Inventaire du matériel et des logiciels nécessaires, déballage et test initial des composants.

Jour 2 : Installation de l'infrastructure réseau
- Installation des routeurs, switches et points d'accès Wi-Fi.
- Configuration des connexions Internet (4G/5G et satellite pour la redondance).
- Mise en place du réseau LAN et initialisation de la connectivité interne.
- Déploiement du pare-feu et du VPN pour sécuriser le réseau.

Jour 3 : Tests de réseau et ajustements
- Tests de la couverture Wi-Fi et ajustements des points d'accès si nécessaire pour garantir une connexion stable et sécurisée.
- Vérification des performances du réseau local et des connexions Internet (4G/5G et satellite).
- Validation de la sécurité des connexions via VPN et pare-feu.

Jour 4 : Installation de l'infrastructure logicielle
- Installation des serveurs et configuration de la base de données.
- Installation et configuration du logiciel de gestion des patients (DMP) et des outils de gestion des stocks, de la communication et de l'occupation des lits.
- Déploiement des outils de communication interne (messagerie, visioconférence).

Jour 5 : Sécurisation des données et sauvegardes
- Mise en place du chiffrement AES-256 pour les données en transit et au repos.
- Configuration des sauvegardes automatiques (sur disque dur et cloud sécurisé).

- Paramétrage de la gestion des accès utilisateurs (authentification à deux facteurs, gestion des rôles).

Jour 6 : Tests fonctionnels et de sécurité
- Tests approfondis du système (connectivité, performances des logiciels, sécurité des données).
- Simulations de cas d'usage pour valider le bon fonctionnement des logiciels (gestion des patients, communication interne, gestion des stocks, etc.).
- Vérification des sauvegardes et des processus de restauration des données.

Jour 7 : Formation et validation finale
- Formation complète du personnel médical et administratif sur l'utilisation des logiciels et de l'infrastructure réseau (session de 4 heures).
- Validation finale de l'ensemble du système avec tous les utilisateurs clés.
- Documentation des configurations réseau et des logiciels, transmission au client.
- Réunion de clôture pour le transfert de responsabilité et signature des documents de fin de projet.