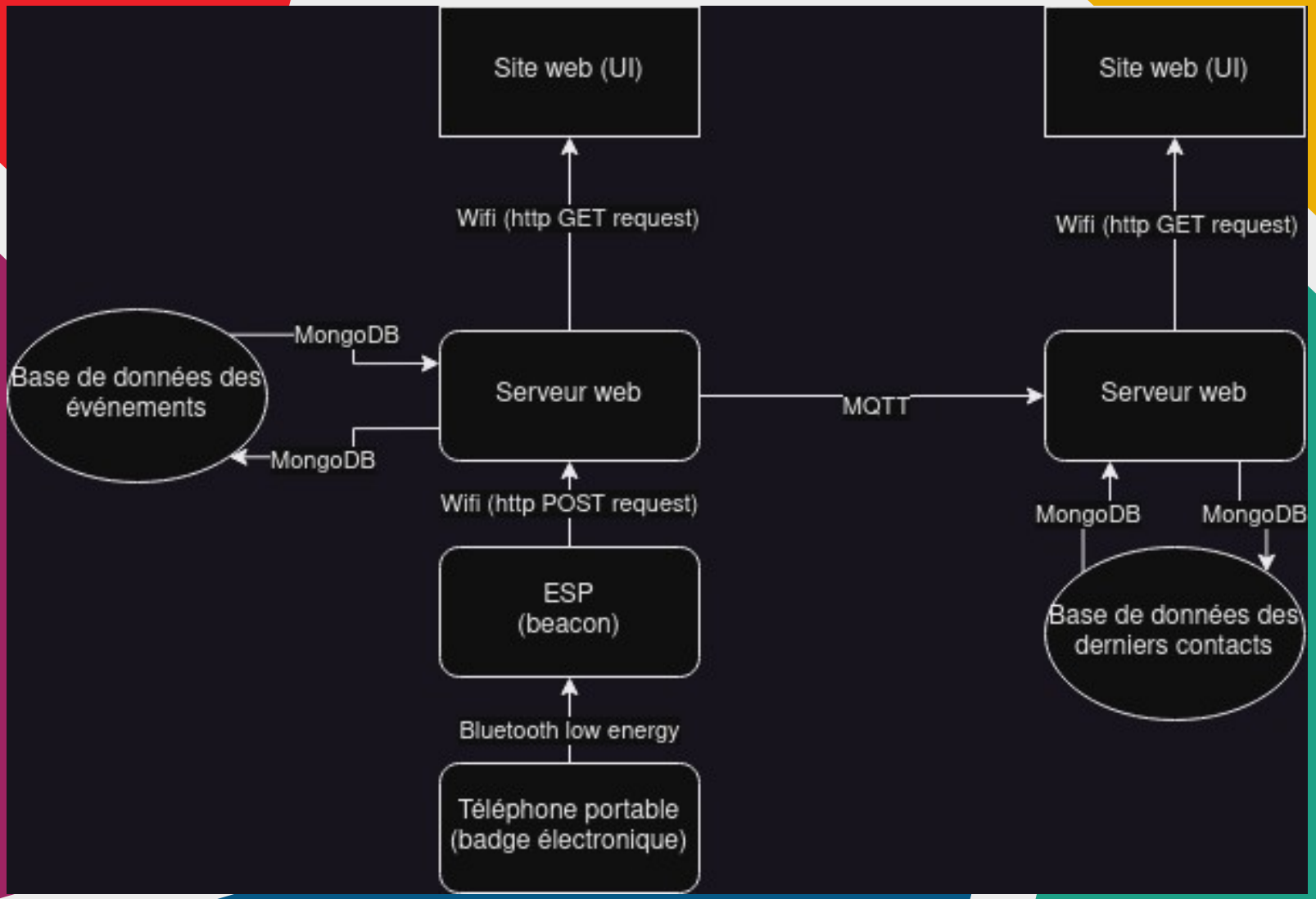
Rapport APP5
Session 6

Pascal-Emmanuel Lachance,
lacp3102
Philippe Gauthier,
gaup1302

Structure


Site web (UI)
Site web (UI)
Wifi (http GET request)
Wifi (http GET request)
MongoDB
Base de données des événements
Serveur web
MQTT
Serveur web
MongoDB
Wifi (http POST request)
MongoDB
MongoDB
ESP (beacon)
Base de données des derniers contacts
Bluetooth low energy
Téléphone portable (badge électronique)

Alternatives sans nuages

- On pourrait garder les heures d'entrées et de départ des locaux sur le téléphone portable des employés. Au lieu de programmer un serveur web, il faudrait programmer une application pour cellulaire. Lorsqu'un utilisateur a la COVID, il suffirait d'envoyer un message à toutes les applications et l'application pourrait faire la comparaison avec ses données locales et déterminer s'il y a une collision. Pour déterminer depuis quand la pièce est vide, les beacons pourraient garder le timestamp de la dernière connexion pour pouvoir l'indiquer au consierge par exemple.

- Avantages:
  - Les données personnelles sont stockés localement
  - Pas de serveurs externes
  - Il est possible de complètement anonimiser les données personnelles lors des envois.

- Désavantages:
  - Les employés doivent télécharger une application
  - Il n'y a pas de bases de données centralisées

Relai exposé à internet

Si le relai était exposé à internet, Il faudrait absolument encrypter les données, ce que MQTT ne fait pas. Deux possibilités faciles s’offrent à nous: changer de protocole de communication, par exemple pour du https qui serait encrypté. On peut aussi ajouter une couche d’encryption au MQTT.

Localisation sans beacon

On pourrait installer des routeurs dans chaque pièce, vu le protocole WiFi se connectant à la borne réseau ayant le plus fort signal, les appareils des utilisateurs se connecteraient automatiquement au routeur dans la pièce dès qu'ils y entrent. Un firmware custom roulant sur le routeur pourrait faire l'acquisition des adresses MAC des appareils des utilisateurs, de la même façon que le beaconning récupère le UUID Bluetooth. Le reste du système pourrait alors fonctionner de façon identique. Cela demande des coûts supplémentaires pour les routeurs, mais ne demande pas d’ESP et ne demande aucune installation de logiciels de la part des utilisateurs pour qui tout le système est transparent.

Sécurité informatique

- Les risques les plus importants sont au niveau de l'anonymité des données de l'utilisateur. Dans un premier lieu, les données telles que le nom et le numéro de téléphone associés à un UUID bluetooth sont très critiques, et la base de donnée de l'archive doit être bien sécurisée. Même sans accès à des données identifiantes, simplement suivre les mouvements d'un utilisateur en connaissant la suite des emplacements où le UUID de son appareil Bluetooth a été connecté peut être dangereux comme données. Autant les données de position que des données identifiantes (nom et # tel) sont donc disponibles sur des interfaces Web dans l'architecture proposée.

- En ce moment, aucune authentification n’est nécessaire pour accéder aux interfaces web où les données sont disponibles.
- Les données sont envoyés en clair via MQTT
- Les données ne sont pas détruites une fois leur durée de vie dépassée