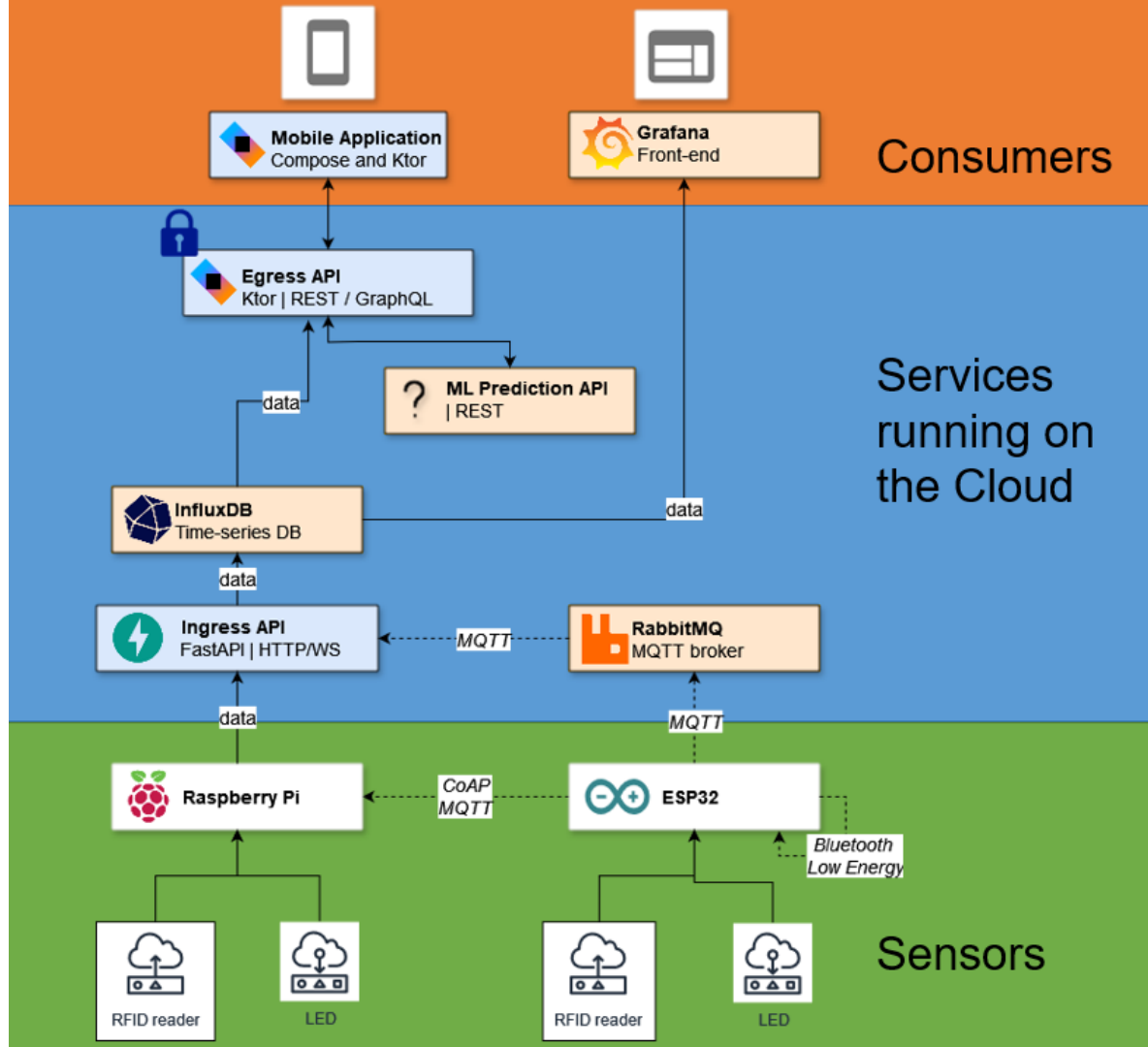


Lab 5 Egress: Part2 – Securing Web Services

Cloud and mobile applications



Goals

1. Provide basic authentication to your egress API using JSON Web Tokens (JWT)
2. Register and log users in using a database in the cloud

@Home: Preparation

- **No checklist on Ufora this time**
- Check if you can access MariaDB in cluster
- Go through Ktor's JWT Tutorial
 - We will use JSON Web Signatures to encrypt JSON data structures to create API tokens

In Lab: Tutorials

- Patch code into existing egress
- Code walk-through
 - User registers with unique username and password
 - Upon user login, check credentials, then generate token
 - Tokens will be used to authorize users before they GET egress endpoints defined in last lab
- Most important files
 - `/server/modules/security/Auth.kt`
 - `/services/auth/SessionManager.kt`
 - `/services/auth/UserManager.kt`

In Lab: TASK 1

- Configure JWT
 - Write verify, validate, and challenge functions
 - In `/server/modules/security/Auth.kt`

In Lab: TASK 2

- Registration
 - In `/server/modules/security/Auth.kt`, fill in `post("/register")` function
 - In `/services/auth/SessionManager.kt`, fill in `createAccount` function
 - Validate credentials by communicating with database (use `/services/auth/UserManager.kt`)

In Lab: TASK 3

- Login
 - In `/server/modules/security/Auth.kt`, fill in `post("/login")` function
 - In `/services/auth/SessionManager.kt`, fill in `processLogin` function
 - Validate credentials by communicating with database, then generate token.

In Lab: BONUS TASK 4

- Problem: bad actors spam login endpoint to hack accounts
- Backoff/ban IP address that makes too many requests
 - In `/server/modules/security/Backoff.kt`, fill in `BackoffPlugin` code
 - Use code in `/services/auth/RateLimiter.kt`

Material to submit

- Archive (Lab5_FamilyName_FirstName.zip): **due 1 May @10:00**
 - Lab report in .pdf over **both Part1 and Part2**
 - Screenshots or problems with preparation sections
 - Explanation of code
 - Screenshots of task results
 - Questions of both Part1 and Part2
 - Source code
 - Just /src folder is sufficient
 - Video of task results (if applicable)

Ing. Tom Windels

PhD student

Tom.Windels@UGent.be

Dr. Jennifer B. Sartor

Onderwijsbegeleider

Jennifer.Sartor@ugent.be