LULEÅ UNIVERSITY OF TECHNOLOGY

A dynamic web system: Lulea Newspaper

Max Lütkemeyer
Juliana Carolina Sanchez Duarte

docker

Express JS

handlebars

N

TS

Prisma

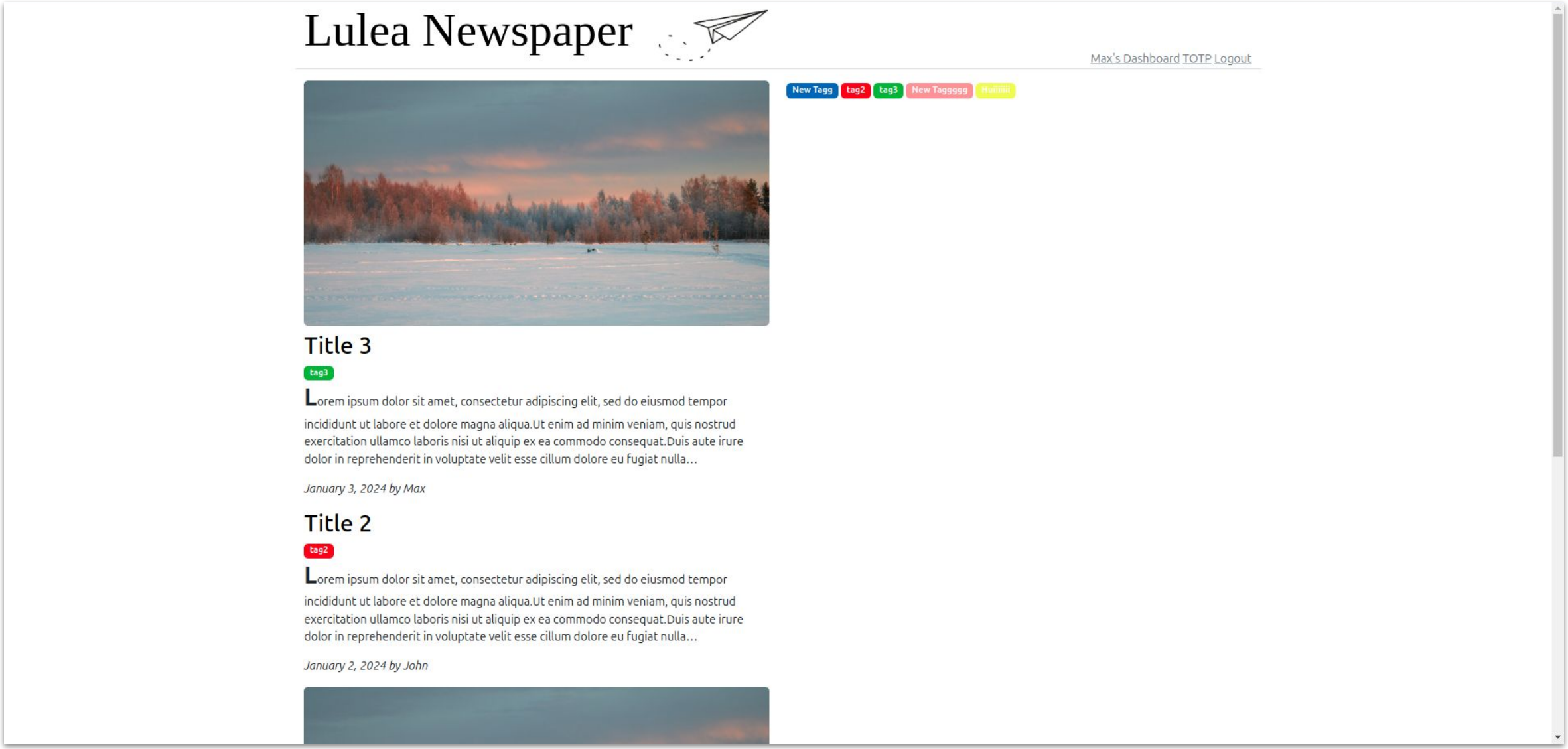
LULEÅ UNIVERSITY OF TECHNOLOGY

maxltk-4@student.ltu.se

sanjul-4@student.ltu.se

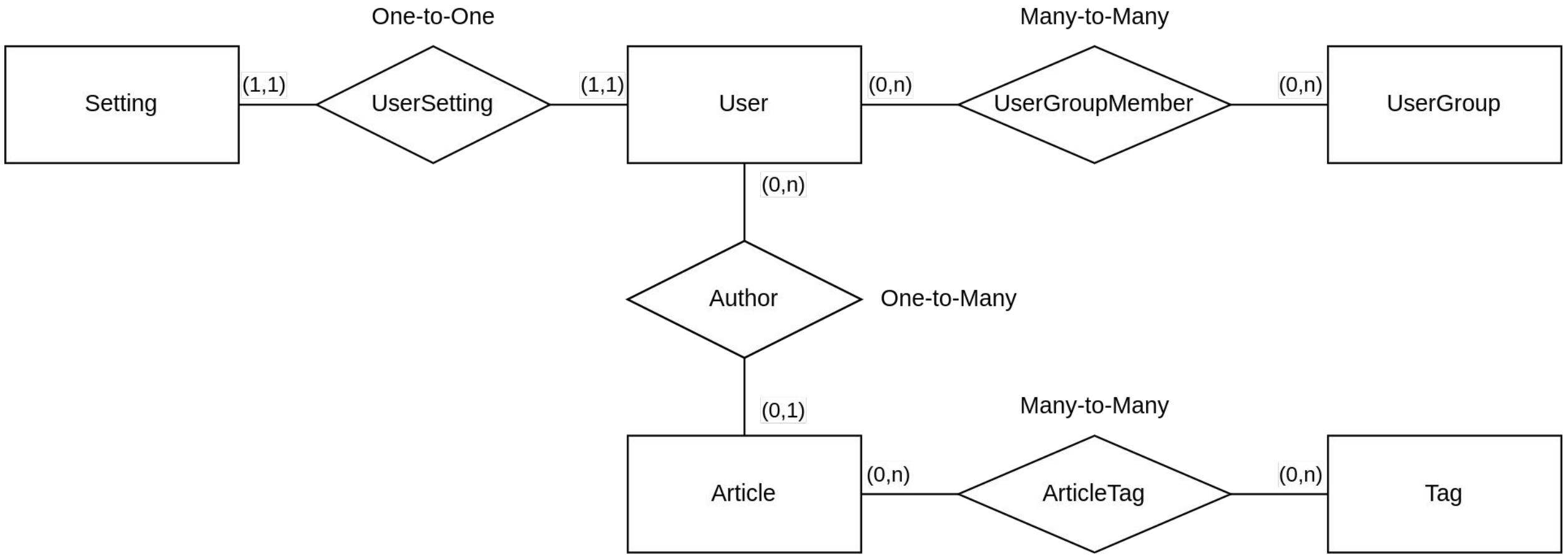
Overview

We built a newspaper website with dynamic loaded articles and a user system.



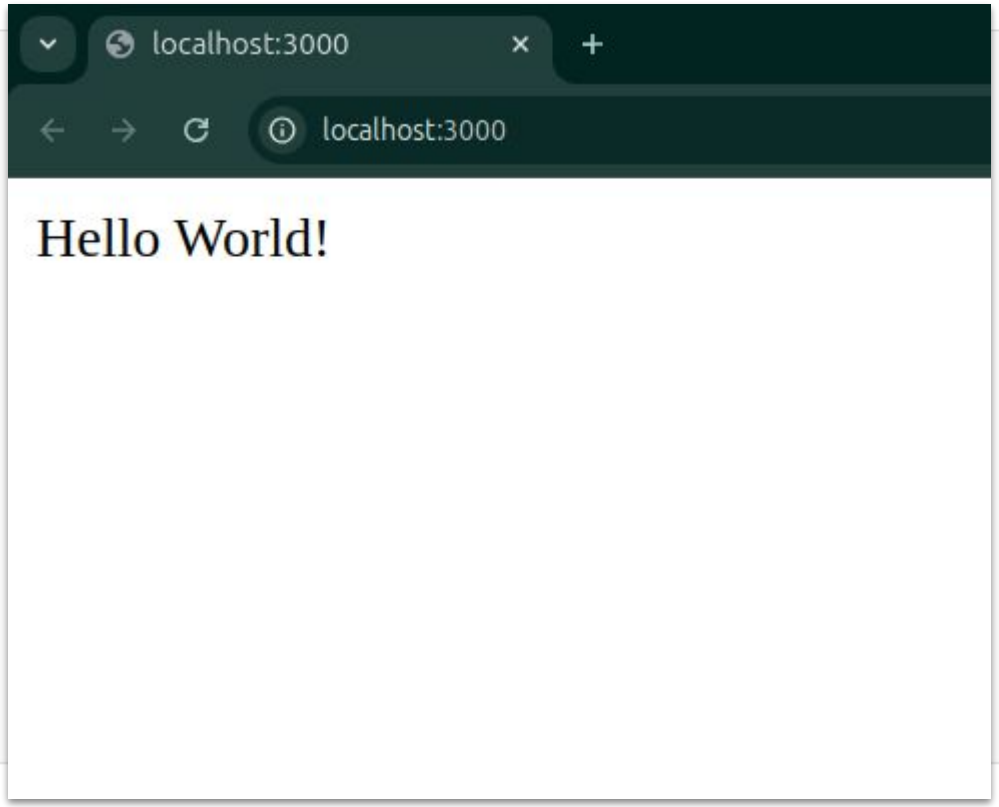
Data model

Lulea Newspaper uses a simple data model with 5 entities and 4 relationships!



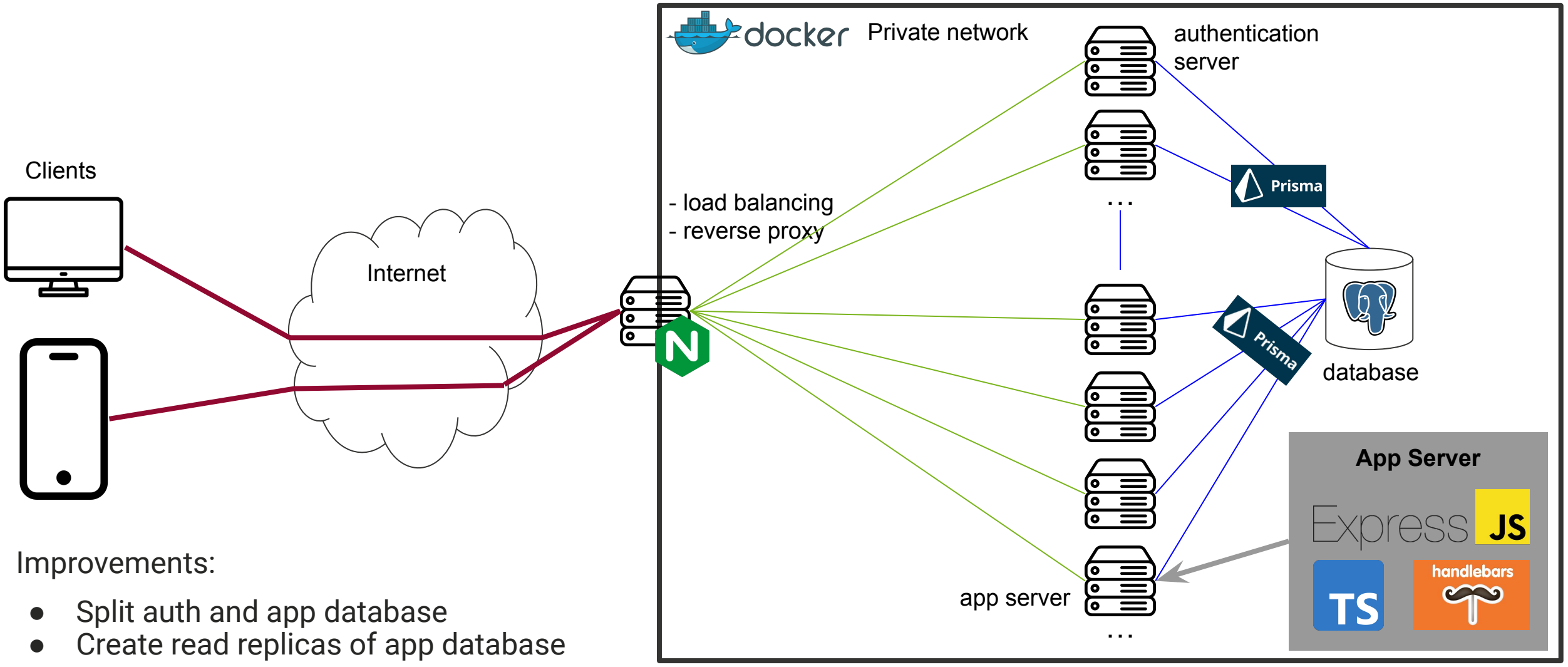
Express.js Hello World example


```
const express = require('express')
const app = express()
const port = 3000

app.get('/', (req, res) => {
  res.send('Hello World!')
})

app.listen(port, () => {
  console.log(`Example app listening on port ${port}`)
})
```



Architecture

The system is scalable to handle a big amount of users.



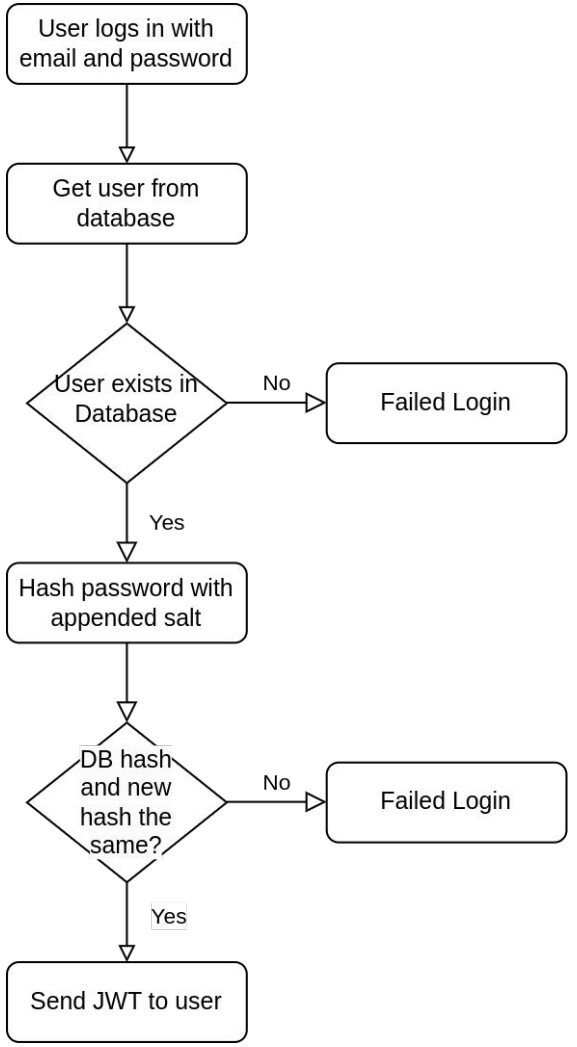
Improvements:

- Split auth and app database
- Create read replicas of app database

Users provide email and password and we compare hash values

password_hash = script(password+salt)

- Login with email and password
- Only password hashes are stored in database
  - Data we are responsible for is less critical
- scrypt is used as a hash function (very slow!)
  - Attackers need more time to generate hashes
  - Implemented in node.js standard libraries
- A salt is added before the hash
  - Instead of hashing the password, we hash pw+salt
  - salt is stored in database
  - If the hashes are leaked, attackers cannot just compare hash values with already computed ones



RFC 7914 https://datatracker.ietf.org/doc/html/rfc7914

Authorization

Access to resources is based on groups and userIDs and is implemented with Json Web Tokens (JWT)

- JWT's are used to represent claims to be transferred between two parties
- Content is readable, but modification can be detected!

- We store: user_id, name, email and groups

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
J1c2VyX2lkIjoiMSIsIm5hbWUiOiJKb2huIERvZ
SIsImVtYWlsIjoiam9obkBsdHUuc2UiLCJncm91
cHMiOlsiYXV0aG9yIiwiYWRtaW4iXX0.Fj7DDBD
EgUSsTJfrL4waxCymID-OTUEr091cAh3X5zA
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

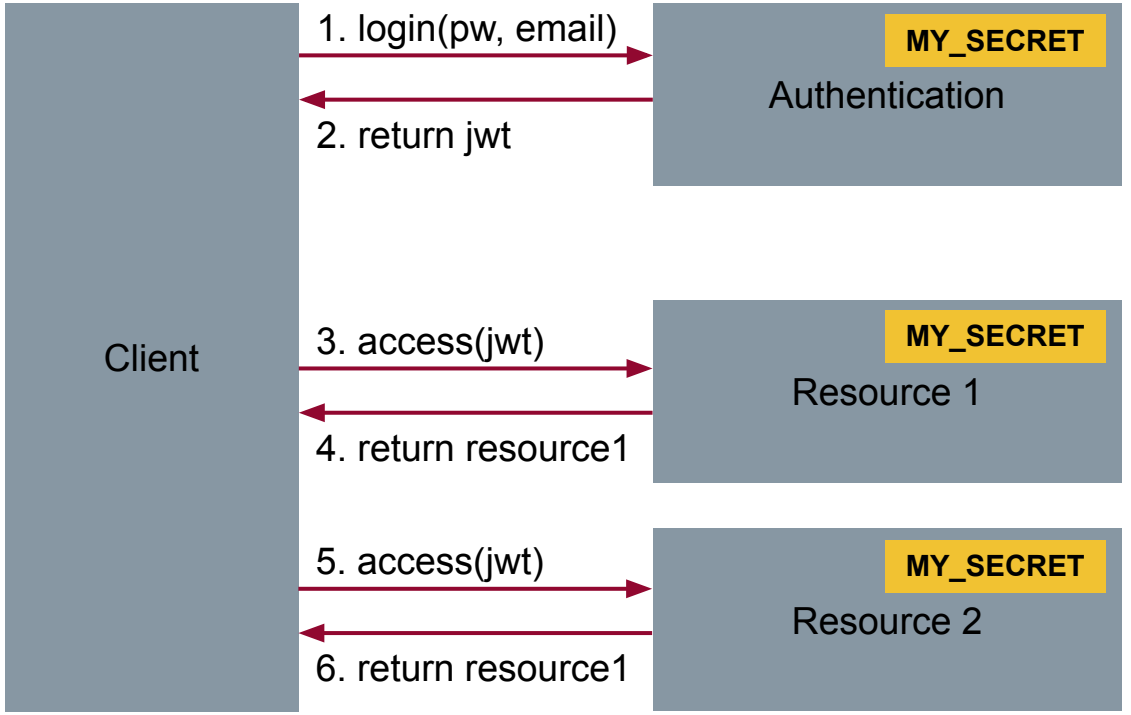
```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "user_id": "1",
  "name": "John Doe",
  "email": "john@ltu.se",
  "groups": ["author", "admin"]
}
```

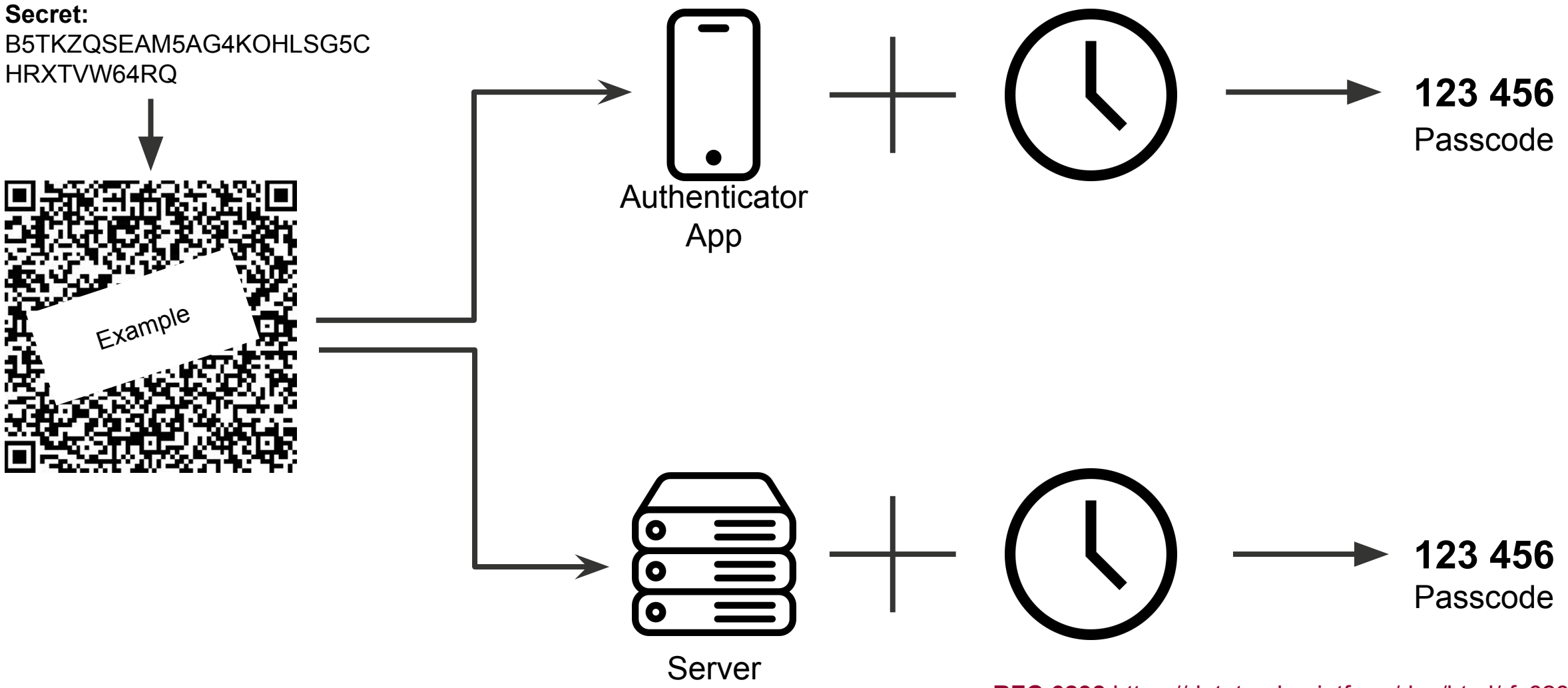
VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  MY_SECRET
) ☑ secret base64 encoded
```



RFC 7519 https://datatracker.ietf.org/doc/html/rfc7519

Time-based One-Time Passwords (TOTP): A 2FA solution with symmetric key cryptography and offline support



RFC 6238 https://datatracker.ietf.org/doc/html/rfc6238

References

[1] Django Software Foundation . 2024. Django makes it easier to build better web apps more quickly and with less code. https://www.djangoproject.com/

[2] Docker Inc. 2024. Docker, Develop faster. Run anywhere. https://www.docker.com/

[3] Google Cloud. 2024. Google Cloud Storage: Node.js Client. https://cloud.google.com/nodejs/docs/reference/storage/latest

[4] Héctor Molinero Fernández. 2024. One Time Password (HOTP/TOTP) library for Node.js, Deno, Bun and browsers. https://www.npmjs.com/package/otpauth

[5] Internet Engineering Task Force (IETF). 2024. JSON Web Token (JWT) RFC 7519. https://datatracker.ietf.org/doc/html/rfc7519

[6] Microsoft. 2024. TypeScript is JavaScript with syntax for types. https://www.typescriptlang.org/

[7] OpenJS Foundation. 2024. Crypto documentation. https://nodejs.org/api/crypto.html#crypto

[8] OpenJS Foundation. 2024. Fast, unopinionated, minimalist web framework for Node.js. https://expressjs.com/

[9] OpenJS Foundation. 2024. Jest is a delightful JavaScript Testing Framework with a focus on simplicity. https://jestjs.io/

[10] OpenJS Foundation. 2024. Node.js Test Runner Documentation. https://nodejs.org/en/learn/test-runner/introduction

[11] OpenJS Foundation. 2024. Run JavaScript Everywhere. https://nodejs.org/en

[12] OpenJS Foundation. 2024. Scrypt documentation. https://nodejs.org/api/crypto.html#crypto_crypto_scrypt_password_salt_keylen_options_callback

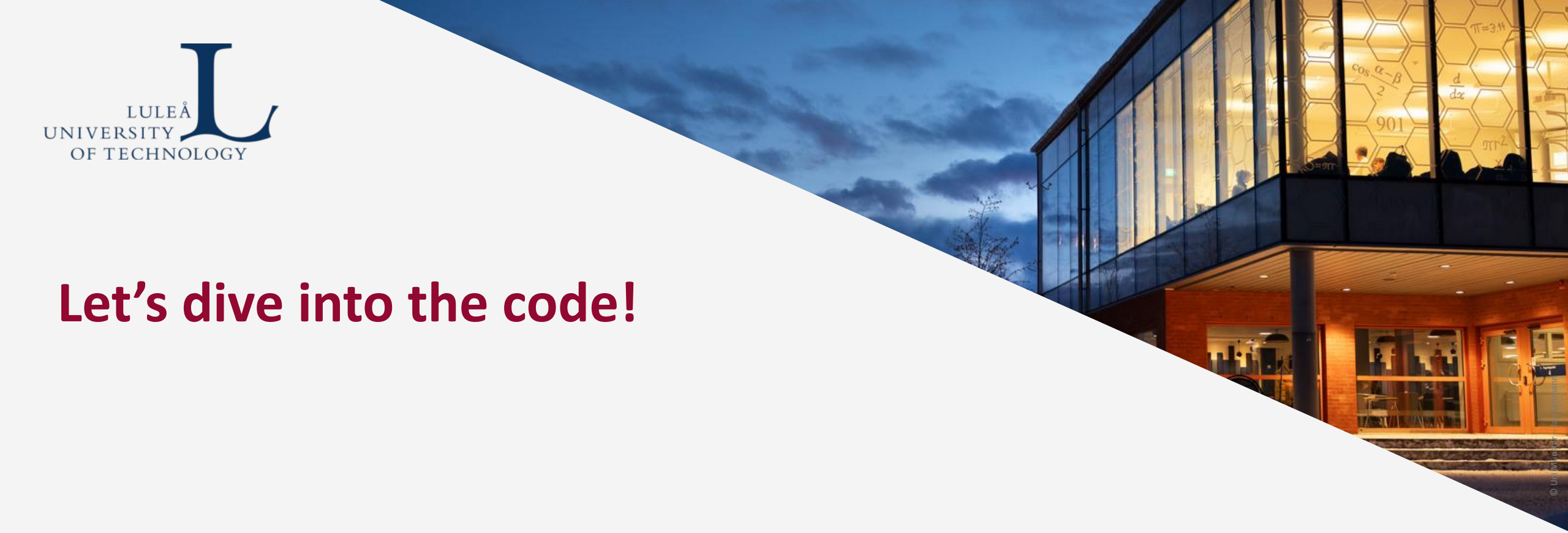
[13] Prisma Data, Inc. 2024. Build data-driven applications — with a great DX. https://www.prisma.io/

[14] Skokan, Filip. 2024. jose is JavaScript module for JSON Object Signing and Encryption. https://github.com/panva/jose

[15] Sysoev, Igor and F5-Inc. 2024. nginx, an HTTP web server, reverse proxy, content cache, load balancer, TCP/UDP proxy server, and mail proxy server. https://nginx.org/

[16] The PostgreSQL Global Development Group. 2024. PostgreSQL: The World's Most Advanced Open Source Relational Database. https://www.postgresql.org/

LULEÅ UNIVERSITY OF TECHNOLOGY



Let’s dive into the code!

LULEÅ UNIVERSITY OF TECHNOLOGY

maxltk-4@student.ltu.se

sanjul-4@student.ltu.se