NWEN304 Interim Presentation

Turtles all the way down

Colin Greg

Frontend

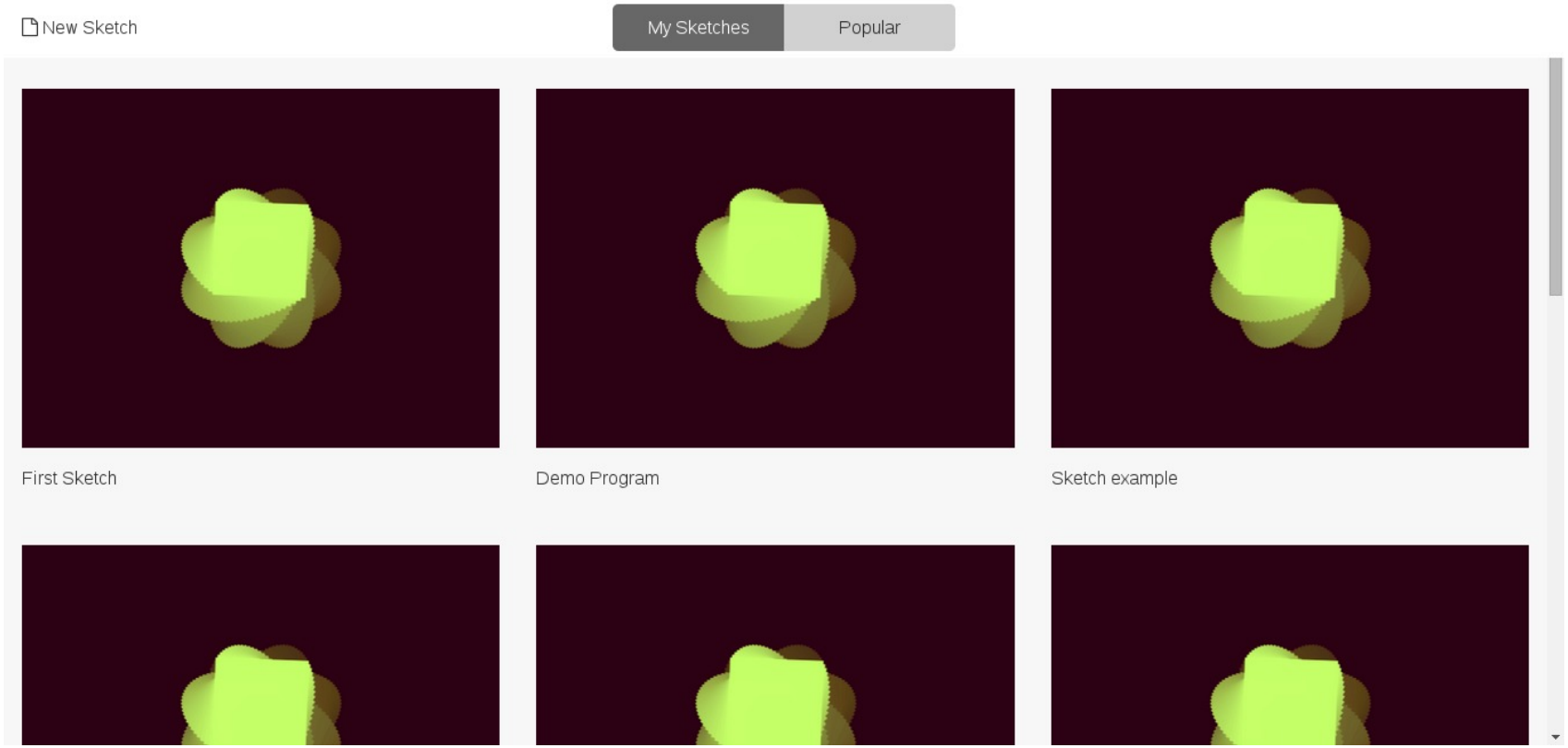

Figure: Sketch Browser

Frontend

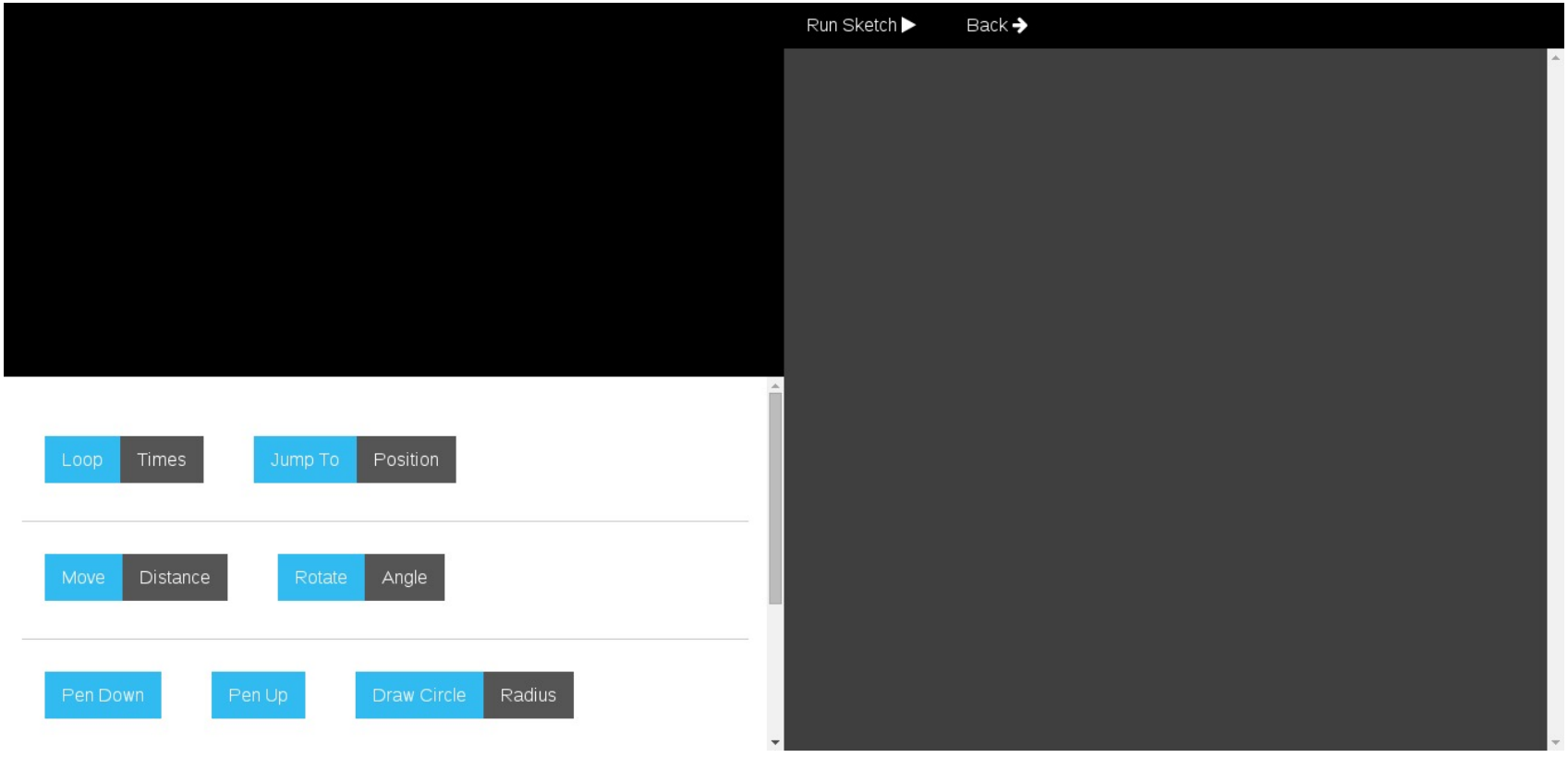

Figure: Sketch Editor

Frontend

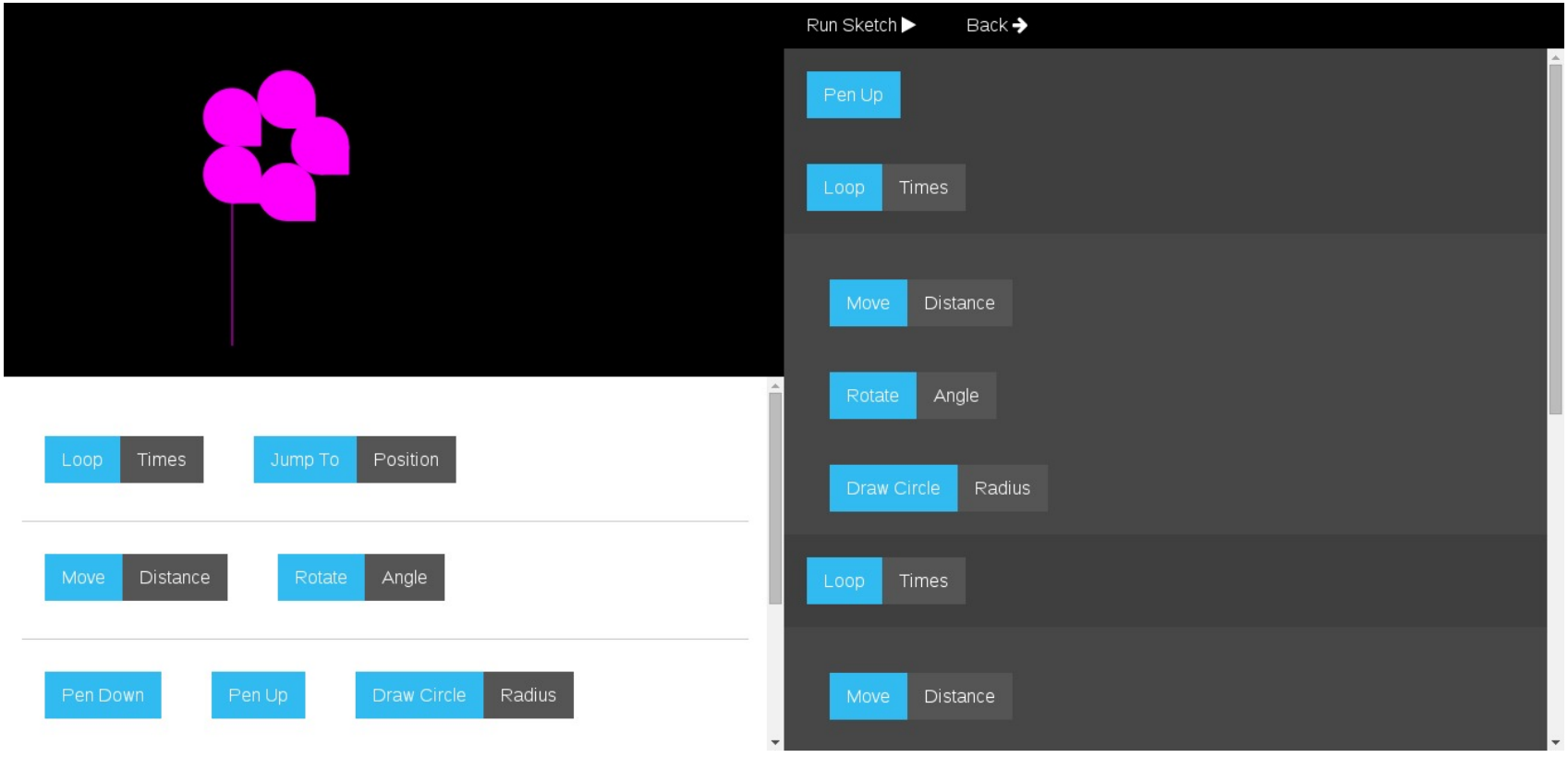

Figure: Sketch Editor with Contents

System Architecture

- Hosted on Heroku.
- Logical tier is NodeJS.
- Data tier is PostgreSQL.
- Preview images stored on Amazon S3

Issues

Scalability

- Stateless protocol.
- Client side computation.
  - Sketches are rendered client side
  - Images are encoded on the client side.
- Caching
  - User sketches are stored locally, as well as the server side

Security

- SQL text Input presented to PostgreSQL is parametrized to sanitize and avoid SQL injection.
- Escaping on the client side to avoid XSS.

We have identified the need to provide authentication of devices to prevent unauthorized access to user data.

Potential Vulnerabilities

- Issues with binary blob for preview images
- XSS issues with user created sketch names
- CORF attacks due to the nature of the NodeJS backend

Reliability

- Running on Heroku.
- Testing
- Strategies for dealing with DOS
  - Rate limiting?
  - Data constraints?

Privacy

- Where we can, we have avoided coming into contact with private data
- Only store UUID which links back to device
- This UUID is masked behind a randomly chosen name and is never shown to any client

Testing

- CURL scripts for automated testing of routes
- Fuzzing to attempt to discover vulnerabilities
- Stress testing for reliability

Still to do?

- Integration between client and server side
- Potentially sharing of sketches on social media

Responsibilities