Cloud-based Health-care Apps

January 10th, 20213

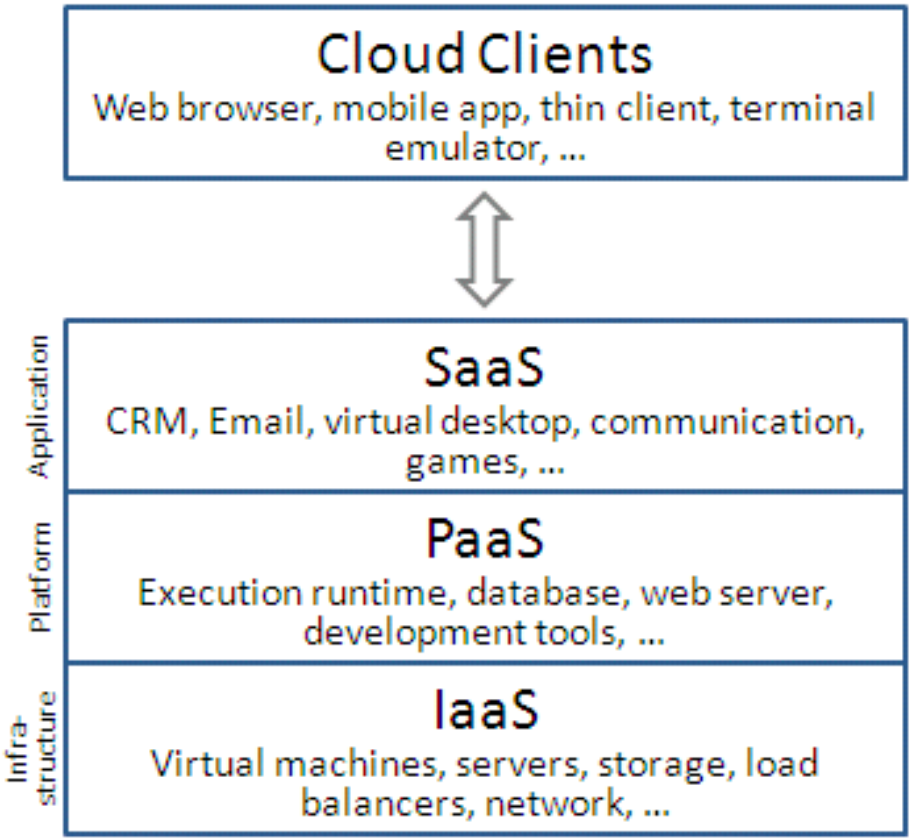
Thomas Hildebrandt,
Software, Data, People & Society
Datalogisk Institut Københavns Universitet

KØBENHAVNS UNIVERSITET

Todays lectures

- Security and privacy issues (in particular for Cloud computing)
- Mandatory Assignment 2 + 3

Cloud computing

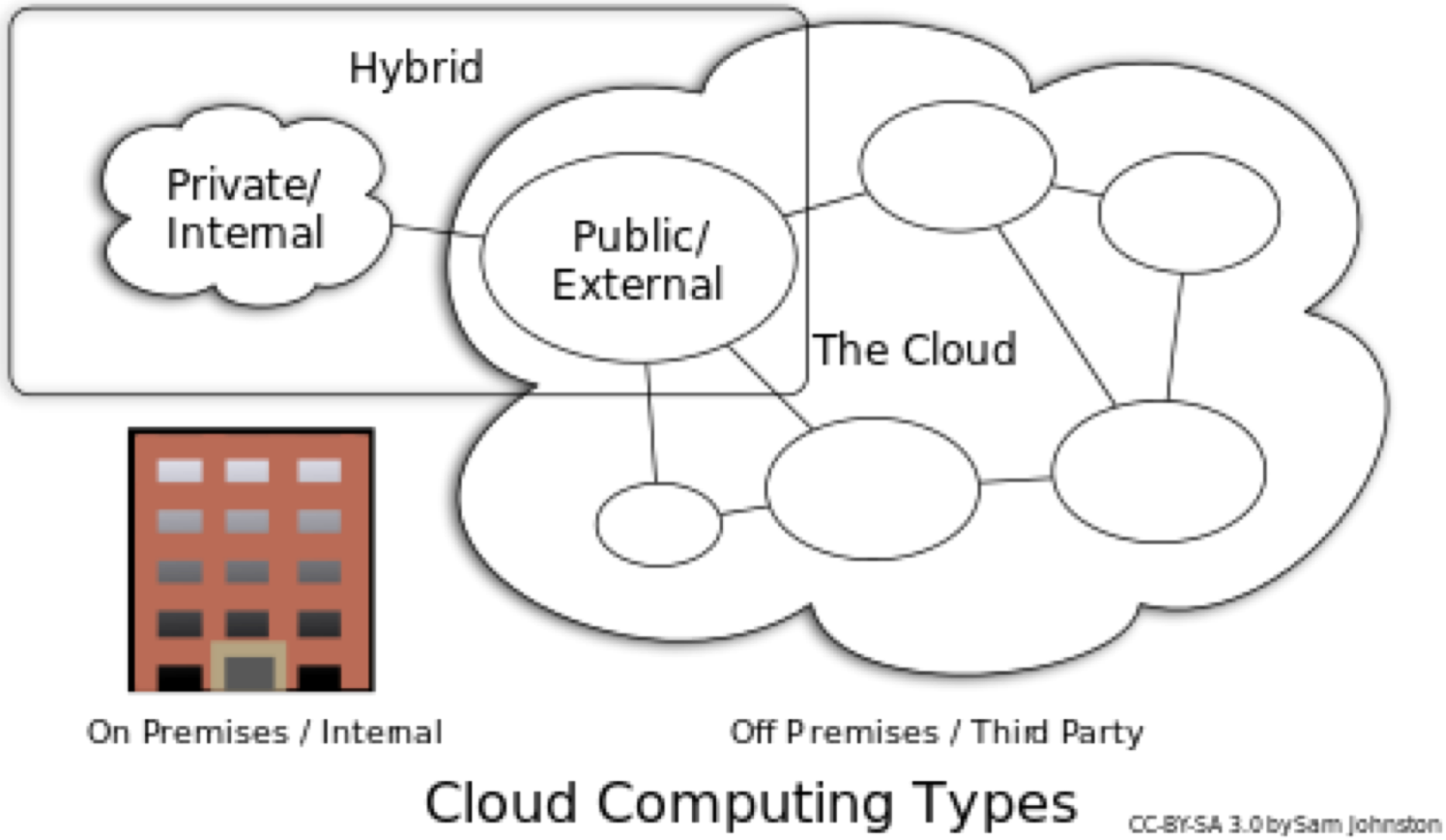


Examples:
KMD Workzone, Office 365, GMAIL, Instagram, Twitter,⋯
DCRSolutions (design portal, active repository)

Examples:
AWS RDS, Azure SQL Database, Azure Machine Learning

Examples:
Azure SQL Virtual Machine

Public, Private, Hybrid Clouds



Benefits of Cloud Computing

- Prepared for change and scalability
- Outsourced hardware & infrastructure management and security

Possible problems using cloud services ?

- Technical (and political) dependency on an external company
- Different uses of terms in contracts (e.g. what is a data loss ?)
- The service provider becomes *data processor* under GDPR
- Schrems I and II
  - 2013: Maximillian Schrems files first complaint to Irish Data Agency on Facebook datatransfer from EU to US.
  - 2015: EU court decides (Schrems I). Safe Harbour replaced with Privacy Shield agreement
  - 2020: New complaint from Schrems leads to new EU court decision (Schrems II)
  - EU standard clauses can only be used if protection, e.g. also against secret service, is guaranteed

EU General Data Protection Regulation (GDPR)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- Took effect from May 25th, 2016.

- Regulates the processing of personal data and rights for data portability

- Key elements of the EU GDPR:
  - Introduces the roles: *Data controller* and *Data processor*
  - Data minimization (Article 5)
  - Right to be forgotten (Article 17)
  - Right not to be subject to fully automated decisions (Article 22)
  - Pricacy/data-protection by design (Article 25)

Data controller & Data Processor

Data Controller:

"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; "

Data Processor:

" a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; "

Data minimization (Article 5)

Personal data shall be:

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

Right to erasure ('right to be forgotten') (Article 17)

- The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Automated individual decision-making, including profiling (Article 22)

- The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Data protection by design and by default (Article 25)

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Transfer to countries outside EU/EØS (3rd part countries)

Følgende lande er p.t. godkendt af EU-Kommissionen som sikre tredjelande:

- Andorra
- Argentina
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Schweiz
- Storbritannien
- Sydkorea
- Uruguay

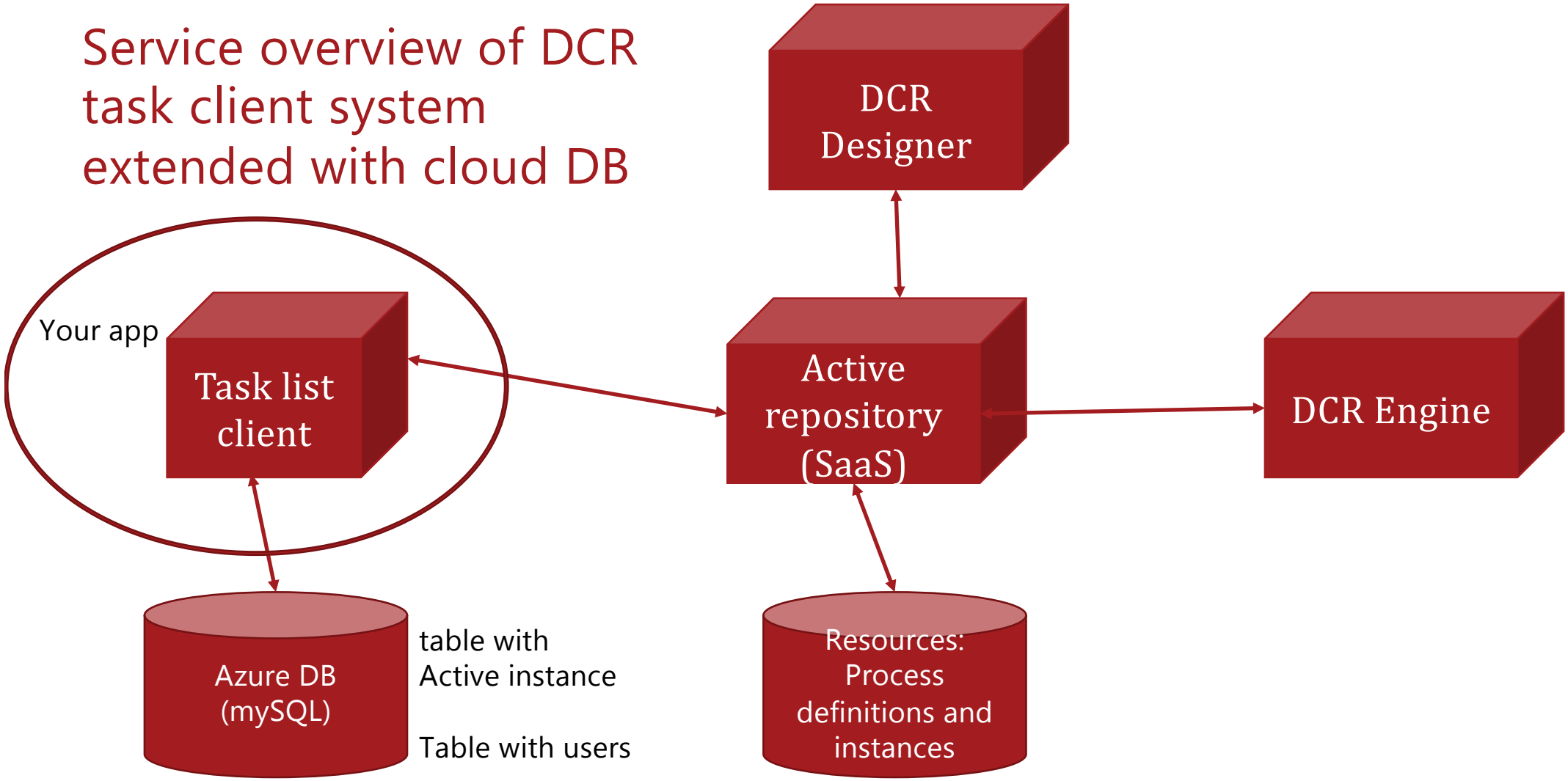
Endvidere er følgende områder og sektorer i tredjelande godkendt som sikre:

- Canada: Modtagere omfattet af den canadiske Personal Information Protection and Electronic Documents Act (PIPEDA)
- Færøerne: Modtagere omfattet af den færøske lov om behandling af personoplysninger. Overførsler til rigsmyndighederne på Færøerne er ikke omfattet.
- Japan: Modtagere omfattet af den japanske Act on the Protection of Personal Information (APPI)
- USA: Modtagere certificeret under EU-U.S. Data Privacy Framework

Security mechanisms

- Encryption (symmetric and asymmetric) used on data in transit and/or rest
- User authentication and Access control, e.g. RBAC (Role based access control)
- Anonymization and Pseudonymization

Service overview of DCR task client system extended with cloud DB



Assignment 2

In this exercise you set up a Relational Database in the Azure Cloud and connect to it from your app.

Concretely, set up the MySQL RDS.

Create two tables in the database. The first table should have rows containing DCR emails and roles. The second is a table where each row contains the graph id, a simulation id of a DCR process in the active repository and a name of the process instance. You may also add additional rows (e.g. a longer textual description of the process containing for instance the name of the person to which the process applies).

Minimal version:

Modify your tasklist app such that it

- loads an instance from the database if there is one and show a button "terminate" instead of "start instance". The terminate button should delete the current simulation in the database when pressed, but only if there are no pending activities
- only shows the tasks relevant for the user role
- stores the simulation for the new instance in the database when it is created

Connecting to the database from your app

```python
import mysql.connector
from mysql.connector import errorcode

import httpx
import xmltodict
```

```python
config = {
    'host': 'tasklistdatabaset.mysql.database.azure.com',
    'user': 'tilman',
    'password': [redacted]
    'database': 'tasklistapp',
    'client_flags': [mysql.connector.ClientFlag.SSL],
    'ssl_ca': 'DigiCertGlobalRootG2.crt.pem'
}
```

```python
create_table_string = '''CREATE TABLE IF NOT EXISTS `instance` (
  `GraphId` varchar(255) NOT NULL,
  `SimulationID` varchar(255) NULL,
  `IsInValidState` tinyint(1) DEFAULT NULL,
  PRIMARY KEY (`GraphId`)
);'''
```

```python
def execute_query(sql_query):
    res = None
    try:
        conn = mysql.connector.connect(**config)
        print("Connection established")
    except mysql.connector.Error as err:
        if err.errno == errorcode.ER_ACCESS_DENIED_ERROR:
            print("Something is wrong with the user name or password")
        elif err.errno == errorcode.ER_BAD_DB_ERROR:
            print("Database does not exist")
        else:
            print(err)
    else:
        cursor = conn.cursor(buffered=True)
        cursor.execute(sql_query)
        if sql_query.startswith("SELECT"):
            res = cursor
        else:
            conn.commit()
        cursor.close()
        conn.close()
    return res
```

execute_query(f"INSERT INTO `tasklistdatabase`.`instance` VALUES ({self.graph_id_input.text},{self.simulation_id},{is_accepting})")

Assignment 2 + 3

What to hand in:

- a small report with
  - an introduction (1/2) page giving an overview,
  - a 2 page description of the code you made,
  - a 1/2 page conclusion reflecting on what was done and what problems that is in the design,
  - an appendix containing a sequence of screen shots of an example run.
- a folder of your code (remove your password to the database)

Extra for assignment 3:

Add a reflection section (3 pages) where you reflect on
1) why using process-aware information systems for healthcare apps in general
2) the use of declarative process modelling and DCR
3) security and privacy concerns (GDPR)