Soen 423 Project Documentation

By

Kadeem Caines: 26343600

John Libera: 27728085

John Bakalis:

Jordan Cassivi:26787819

**Introduction**

As a team of 4, we will be working on extending our Distributed Health Care Management System which consisted of Patient and Admin clients remotely executing methods in specific city hospital servers via CORBA. We will be testing it to tolerate either a single software (non-malicious Byzantine) failure or be highly available under a single process crash failure using active replication. This document will describe the architecture, classes, methods and implementations used in order to configure this system

**Design Description/Overall architecture**

**Implementation Details**

**Distributed Computing Paradigms**

* Client-Server

**Packages**

* Client
* Replicas
* ReplicaManager
* UDP
* IDL
* Front End
* Sequencer
* Corba (IDL)

**Data Structures**

-Array List

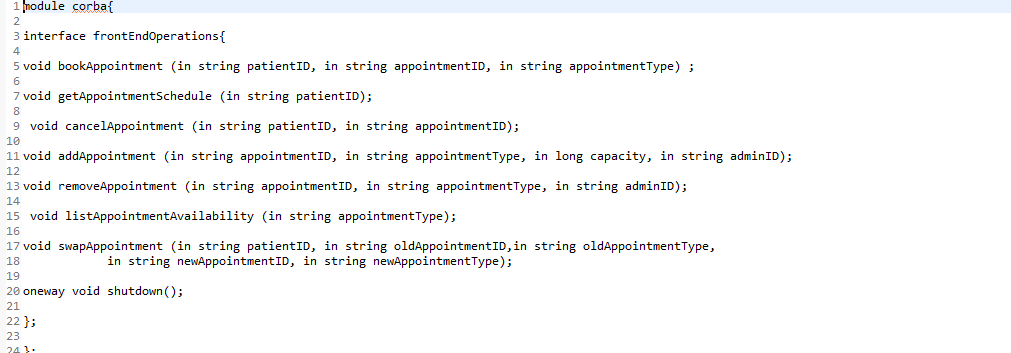
-HashMaps

**Distribution of Tasks**

|  |  |
| --- | --- |
| Task | Student |
| Front-End (Student 1) | Kadeem |
| Replica Manager (Student 2) |  |
| Failure-free Sequencer (Student 3) |  |
| Test Cases + Client Program (Student 4) | John Libera |

**Corba**

We will be using CORBA for all RPC calls. Our methods are defined in the IDL following IDL file:



**Communication**

* UDP: communication between the server, the RM, the sequencer will all be done via UDP since it is faster than transferring messages since it does not have to establish a link with each component first. UDP will be tested to the point where minimal packet loss is implemented. Even though this is not a real distributed system, packet loss in general is still possible.
* Reliable Multicast:

**-Client:**

The client will ultimately be responsible to speak with the frontend using CORBA. During its startup, it greets the user and ask them what city they are from. Once selected, the system now asks if the user is an admin or patient. It then assigns them a unique ID. Afterwards, it will validate the ID and lookup the frontend remote object by implementing the server interface for each region.

**-Front end**

The purpose of the frontend is to manage the communication between the client and sequencer. It gives the clients a failure free interface to branch the servers to allow them to perform patient as well as administrative operations. The frontend will register itself as the regional server as a remote object with CORBA and will wait on requests from the clients. It contains all of the corba methods of Corba IDL file. When requests are received, they are then forwarded to the sequencer. Frontend component then waits for the replicas to send their responses, Where it can make a decision about which response is correct and send it back to waiting client. If in the event that the replica detects a fault, the frontend will send a message to the replica managers to inform them of that fault.

**-Replicas**

Each of our replicas from assignment 2 will be running on different machines. These replicas (or server processes) will have their own RMs and will send back confirmation messages (via UDP) to the Front end. The replicas will each contain our implementations of the patient/admin and hospital server DHCM and will have their own UDP system for specific methods (listing available appointments and swapping appointments). The overall purpose of multiple replicas is to simulate the distributed system, where if one of the replicas fail, the system as a whole can still function and be available.

**-How we will simulate a Byzantine Failure**

Since this is but a simulation of a distributed system, we are not expecting a hardware type of byzantine failure for any of the replicas. We will be focusing on a software type of failure, one where incorrect data is sent back to the client. If one replica out of the 4 does not have data that matches the other 3, then the system will continue as normal. We will manually create a byzantine failure by sending incorrect data.

**-Sequencer**

The sequencers job is to receive requests from the frontend and provide them with a sequence ID. This identifier will need to auto-incremented and will need to act as a way to ensure that all replicas execute the operations in the correct order. The moment each request has an ID, it multicasts to all the replicas. Locations inside the replicas should receive the request as determined by the request manager ID. The message sent should also be stored in a history log in which is can be played back in the event of a replica failure.

**-Replica Manager**

The purpose of the replica manager is to manage a single replica. In other words, it’s primarily responsible for restarting its replica if the frontend thinks it is misbehaving. It will also need to know how to plant need data into a restarted replica so that it would be in the same state as the other replicas.

**Communication between these components (may need to show with diagram)**

Client→ Frontend

Frontend→ Sequencer

Sequencer→ Replicas

Replicas→ Main Server

Replicas→ Frontend

Frontend→ Client

Frontend→ Replica Manager

Replica Manager→ Replica

**Recovery from Failure**

* Software Byzantine Failure:

If any of the replicas produce an incorrect result, the frontend will inform the replica manager about it so that replica can be restarted.

* Single Process crash failure:

Single process failure will lead to the replica giving incorrect data or timing out with the frontend. Leading the frontend asking the associated replica manager to restart the replica that is failing.

* Error recovery:

The sequencer will keep an in-memory log of all the sent messages. After a replica is restarted, its replica manager will ask the sequencer to replay the log to its replica in order to catch up with the state of the other replicas in the system.

**UML**

**Test cases**

**Difficulties**

In general, our biggest issue was actually figuring out how to code each segment and

have each one communicate with one another properly.