Project Design

CMSC 495 6380

6/5/2021

Group 5

Summer Smith, Sean Dwyer, Keith Combs

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Date** | **Name** | **Description** |
| 6/13 | Summer | Created document with cover page, revision history table, and outline.  Initial pseudocode for interest accrual subsystem. |
| 6/14 | Summer | Create event trace diagram for interest accrual subsyem |
| 6/14 | Sean | Added event trace diagrams and pseudocode for authentication subsystem |

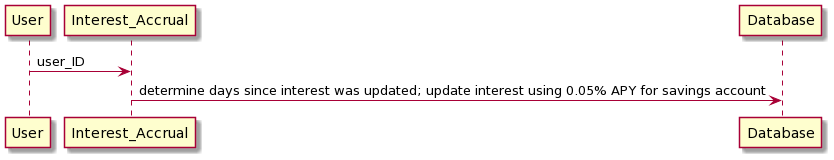
**Event Trace Diagram**

*Scenario 1:*

Description: the user logs in and the interest accrual system updates the interest value if it hasn’t been updated that day.

Pre-Condition: user is logged in.

Post-Condition: interest value is updated to reflect total interest (as of today).

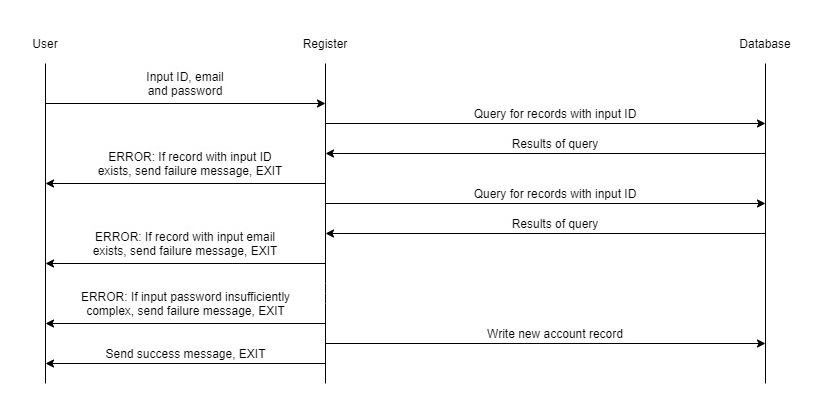


*Registration Scenario:*

Description: User enters user ID, password, and email address and is registered by the app as a new account.

Precondition: The web app is running and accessible.

Post-condition: A new database record has been made with the entered user ID, password, and email address, and account values have been initialized to zero; the user is notified of registration success.

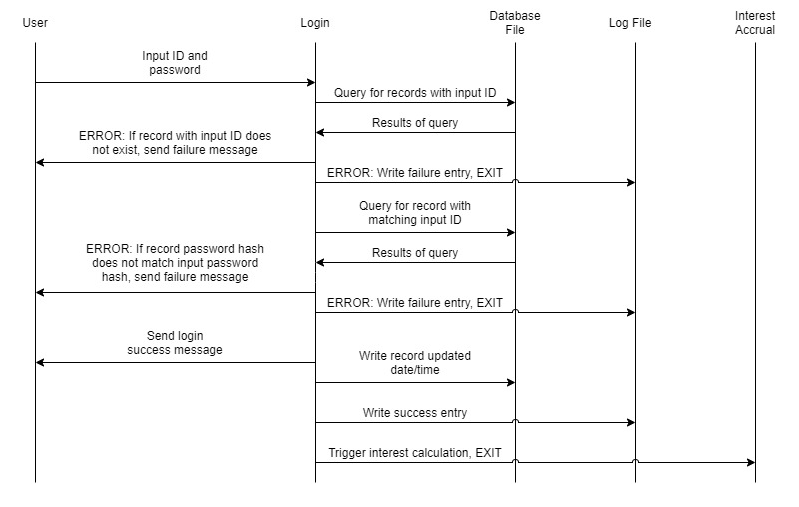
****

*Login Scenario:*

Description: User enters user ID and password, and is logged on if matched to an existing account.

Precondition: The web app is running and accessible; the user has previously been registered in web app.

Post-condition: User is notified of logon success and redirected to home; user session is recorded as logged in; logon attempt is logged; interest accrual is triggered.

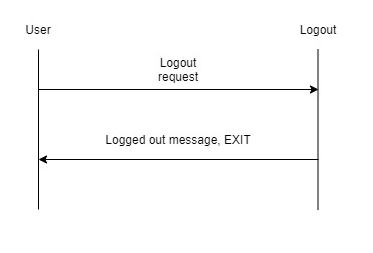


*Logout Scenario:*

Description: User triggers logout.

Precondition: The web app is running and accessible; the user is logged in.

Post-condition: User is notified of logout; user session is cleared.

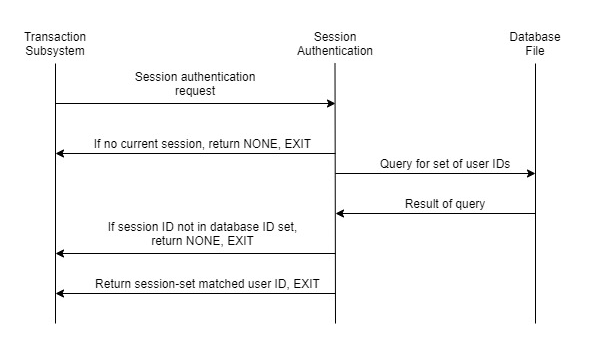


*Session Scenario:*

Description: Current session is verified as logged in.

Precondition: The web app is running and accessible; the user has logged in successfully.

Post-condition: Session logon status is returned.

****

**Class Design**

1. Authentication Subsystems

Class register {

database.connect() // standard library database API

Void register() {

user\_ID = request.form(“User ID”) // framework feature

password = request.form(“Password”) // framework feature

email = request.form(“Email”) // framework feature

user\_set = database.fetchall(“User ID”) // standard library database API

if user\_ID in user\_set {

render(“Registration failure”) // framework feature

return

}

email\_set = database.fetchall(“Email”) // standard library database API

if email in email\_set {

render(“Registration failure”) // framework feature

return

}

if not check\_password(password) {

render(“Registration failure”) // framework feature

return

}

database.execute(user\_ID, hash(password), email, checking=0, savings=0, interest=0) // standard library database API

database.commit() // standard library database API

database.close() // standard library database API

render(“Registration success) // framework feature

redirect(“Login page”) // framework feature

return

}

bool check\_password(password) {

if(password length > 12 AND

password uppercase >= 1 AND

password lowercase >= 1 AND

password numbers >= 1 AND

password special characters >= 1) {

return true

}

return false

}

string hash(password) {

return sha256\_crypt(password) // framework feature

}

}

NOTE: Logout Scenario/functionality is trivial and is included in this class as a simple method; a logged in user will simply have their session cleared and be notified of logging out. An authenticated user will be unable to access the logout page in the first place.

Class logon {

Void login() {

session.clear() // framework feature global

user\_ID = request.form(“User ID”) // framework feature

password = request.form(“Password”) // framework feature

user\_set = database.fetchall(“User ID”) // standard library database API

if user\_ID not in user\_set {

render(“Login failure”) // framework feature

log(IP, user\_ID, hash(password), time, “failure”)

return

}

stored\_hash = database.fetch(user\_ID)[“password”] // standard library database API

if hash(password) != stored\_hash {

render(“Login failure”) // framework feature

log(IP, user\_ID, hash(password), time, “failure”)

return

}

session.set(user\_id) // framework feature global

render(“Login Success”) // framework feature

redirect(“Home page”)

log(IP, user\_id, hash(password), time, “success”)

return

}

Void logout() {

Session.clear() // framework feature global

Render(“logged out”) // framework feature

Redirect(“Login page”) // framework feature

Return

}

string hash(password) {

return sha256\_crypt(password) // framework feature

}

Void log(ip, id, hash, time, status) {

Open(log\_file)

Writeline(ip, id, hash, time, status)

Close(log\_file)

}

}

Class session\_authentication {

String verify() {

user\_id = session.get(“user\_id”) // frame feature global

if user\_id = None {

return None

}

user\_set = database.fetchall(“User ID”) // standard library database API

if user\_ID not in user\_set {

return None

}

return user\_id

}

}

1. Transaction Subsystems
2. Interest Accrual Subsystem

Class Interest {

database.connect() //standard library database API

APY = .005

APD = APY/365

Void interest(user\_ID){

delta = date.today() – database.fetchall(user\_ID)[“last\_updated”]

if delta.days > 0{

collect\_interest = (APD \* delta.days) \* database.fetchall(user\_ID)[“savings”]

new\_interest = database.fetchall(user\_ID)[“interest”] + collect\_interest

database.execute(user\_ID, interest = new\_interest, last\_updated = date.today()) //standard library database API

log(IP, user\_ID, time, “interest updated”)

database.commit() //standard library database API

}

database.close() //standard library database API

return

}

**Risk and Risk Mitigation**