Project Analysis

CMSC 495 6380

6/5/2021

Group 5

Summer Smith, Sean Dwyer, Keith Combs

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Date** | **Name** | **Description** |
| 6/5 | Summer | Created document with cover page, revision history table, and outline. Completed Input Data and Output Data sections. Added one possible enhancement. |
| 6/5 | Sean | Added Data Processing section and initial Subsystem descriptions. Added one additional enhancement. |
| 6/6 | Keith | Context Diagrams and Subsystem Diagram |
| 6/7 | All | Made final additions to Subsystems, revised design choices |
| 7/11 | Summer | Update interest accrual to mediate between logon and database |

**Input Data**

* Login credentials – Source: user web form
  + User ID
  + Password
* Registration information – Source: user web form
  + User ID
  + Password
  + Email
* Money transactions – Source: user web form
  + Choice of transaction (transfer, deposit, or withdraw)
  + Deposit amount
  + Withdraw amount
  + Transfer amount
  + Transaction confirmation or cancellation

**Output Data**

* Login status – Destination: rendered web page
* Transaction status (pending, canceled, complete) – Destination: rendered web page
* Account status – Destination: rendered web page
  + Savings balance
  + Checking balance
  + Interest percentages
  + Interest earned
* Alerts – Destination: rendered web page
  + Negative withdraw or transfer
  + Request transaction confirmation

**Data Processing**

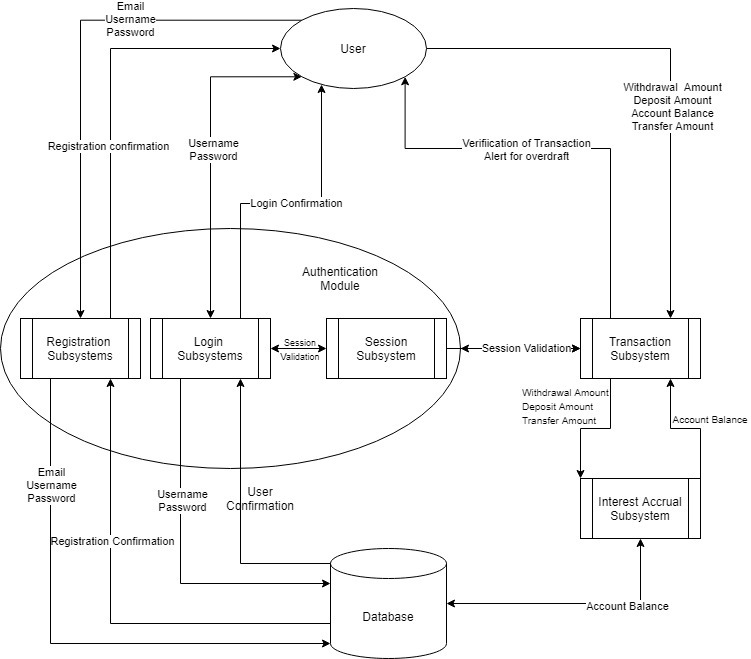
* Register new user ID, password hash, and email with new account (values set to 0)
  + Write new account record to database if successful
  + Display registration failure if user ID or email collides with existing accounts
  + Display registration failure if password fails to meet complexity criteria
  + Display registration success if registered
* Authenticate logon user ID and password hash against registered accounts
  + Display logon failure if user ID or password hash does not match
  + Display logon success if matched
* Track user authentication by webpage session
* Execute transaction based on user input:
  + Display request for confirmation or cancellation of transaction
  + Trigger execution based on user confirmation
  + Increase or decrease account by user input value for deposit or withdrawal respectively
  + Increase one account and decrease other account by user input value for transfer transaction
  + Retrieve balance of accounts and interest percentage and earnings for account status
  + Display resulting balances or requested information to user with transaction confirmation
  + Display alert for requested value resulting in overdrawn account, prompt for confirmation or cancellation
  + Continue with transaction if confirmed

**Context Diagram**

**Diagram

Description automatically generated**

**Subsystem Diagram**

****

**Subsystem Descriptions**

* Authentication Module
  + Registration Subsystem
    - Accepts user input for user ID, password, and email
    - Compares user ID and email against existing account records
    - Displays registration failure if user ID or email matches existing account
    - Analyzes password for appropriate complexity
    - Displays registration failure if password is insufficiently complex
    - Writes new account record to database with user provided user ID, password, and email, and with initial savings and checking values set to zero
    - Displays registration success
  + Logon Subsystem
    - Accepts user input for user ID and password
    - Compares user ID against existing account records
    - Displays logon failure if user ID does not match any existing account
    - Compares password hash to saved password hash of matched existing account
    - Displays logon failure if password hash does not match
    - Displays logon success
  + Session Subsystem
    - Tracks logon session
    - Provides logon verification to other subsystems before proceeding with transactions
* Transaction Subsystem
  + Accepts user input for transaction type
  + Displays request for additional information to users if necessary
  + Accepts user input for transaction values, if necessary
  + Prompts user for confirmation/cancellation before attempting transaction execution
  + Alerts user if the request transaction will overdraw an account, with prompt for confirmation/cancellation, will add overdraft fee if confirmed
  + Executes transaction by retrieving, updating, and writing updated values to databased, mediated by Interest Accrual Subsystem
  + Displays updated account balances to user post-transaction
* Interest Accrual Subsystem
  + Mediates between Logon Subsystem and the database
  + Detects if most recent interest accrual occurred more than 24 hours ago
  + If so, calculates daily interest against current principle and writes updated interest value to database
  + If interest accrual had been calculated within 24 hours, no changes are made

**Subsystem Mapping**

* Authentication Module
  + Registration Subsystem
    - Requirements 1, 3
  + Logon Subsystem
    - Requirements 1, 2, 4
  + Session Subsystem
    - Requirement 2
* Transaction Subsystem
  + - Requirements 1, 5, 6, 7, 8, 9, 11, 12, 13, 14
* Interest Accrual Subsystem
  + - Requirement 10

**Enhancements**

* Alerts for large withdraw or transfer (amount set by user)
* Transfer money between different users
* Open additional accounts per user (beyond savings/checking)
* Account sharing between users
* Administration page to edit accounts, interest rates, etc.
* Ability to close accounts
* Password reset
* Email alert functionality
* Two-factor Authentication
* More sophisticated overdraft system
* More sophisticated/varied interest system

**Risk and Risk Mitigation**

* Authentication and user session verification before access to restricted pages: Prevents unauthorized access to private user information
* Password complexity enforced at registration: Increases difficulty of both online and offline cryptographic attacks
* Password hash storage only, no plaintext passwords: Prevents easy compromise of user passwords, even if database is accessed
* Logon logging: Potential detection of online brute force attack via log auditing
* Web security automated vulnerability scanning: Confirm absence of susceptibility to a variety of web attacks, such as XSS or CSRF
* User education page: Included with registration success to inform users about appropriate security best practices