Enhancement Two: Algorithms and Data Structure

A. The Artifact Description

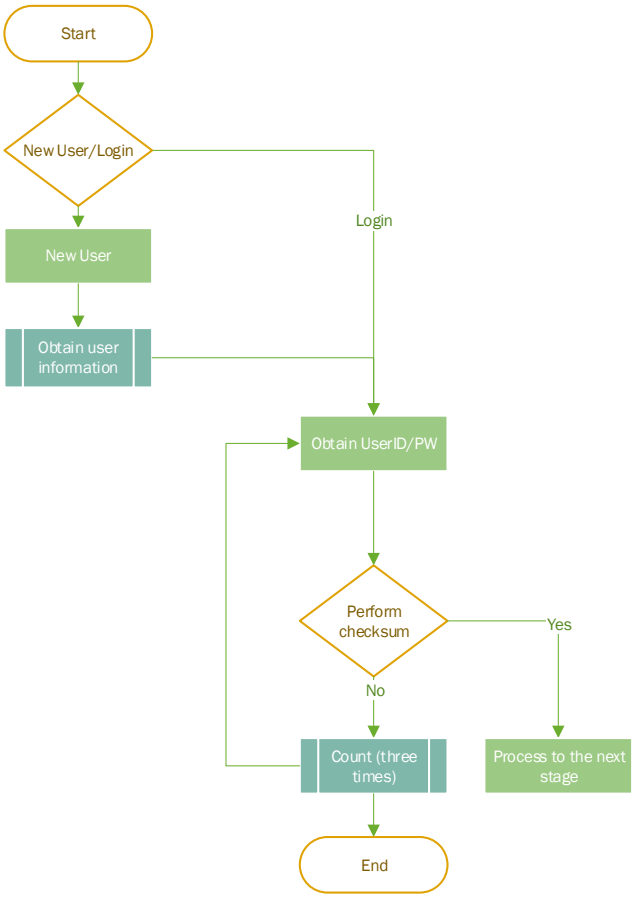
Part of the project was to expand the capability of the Travel SNHU application allows the user to store user information. I would like to integrate the hashing and MD5 for user information such as a password. This will provide security features to protect users information and identity.

B. Inclusion of the Artifact Justification

The inclusion of artifact offers protection to user account and identity. In the first assignment 1-4, I was going to use either MD5 or SHA-1 for hashing algorithm for password checksum. Since MD5 is believed to be not a secure hashing algorithm, because it is susceptible to collision occurrences. SHA-1 is a better choice for hashing algorithm in this case. SHA1 (160 bit) are cryptographic hash functions used to encrypt information by generating a hash based on the passed byte structure (Denzel, 2010).

C. Reflect on Enhancement Process

As planned in assignment module one, the workflow for password checksum depict in the flow chart.



The user either create new account

1. Create new account or login
2. If new user, obtain information
3. Store userID and hashed password
4. then login

Login will verify their password in the SHA-1 authenticate as follow:

1. User enter UserID and Password
2. The entered password is hashed and authenticate against the stored password
3. If success, proceed to the next process.
4. If failed the authentication, repeat step 2 to login. User will have three attempts. Terminates when exhaust 3 times.

D. D. Reflect on the process of enhancing and/or modifying the artifact. What did you learn as you were creating it and improving it? What challenges did you face?

I have to modify the flow chart from the initial proposed in module one. The modification is adding a create new user function. I have a little hard time of deciding on checksum authentication between MD5 and SHA-1. Since MD5 has encountered collision and believe to be unsecured, I settle for SHA-1. SHA1 is a better secure hashing algorithm, although both principles are somewhat the same concept. Though MD5 is not 100% secure in general both methods are very efficient and widely use for hashing password.

Reference

D. Denzel. (Jun 2010), Generating MD5 and SHA1 checksums for a file. Retrieved from: https://dzone.com/articles/generating-md5-and-sha1