

Project Group Members (Course Group 13):

Poojah Karunakaran (100618754)

Kevin Erskine (100762922)

Ivan Bisol (100701735)

Misha Larionov (100743093)

Step 2: Establish Iteration Goal by Selecting Drivers

For this iteration the quality attribute that is being focused on is QA-3. The quality attribute scenario is to ensure that the security and privacy of the system is maintained. That sensitive information is not able to be accessed by anyone except the appropriate people.

Step 3: Establish Iteration Goal by Selecting Drivers

For this security and privacy scenario, the elements that will be refined are the physical nodes that are identified in during the first iteration:

- Website Application Server
- Database Server

Step 4: Establish Iteration Goal by Selecting Drivers

Design concepts used in this iteration are presented in the following table:

Design Decisions and Location	Rationale
Implementing Password Hashing	Implementing password hashing in the system will increase security. The password of the buser being replaced by a random string will make it incredibly difficult for anybody to access and steal that password.
Encryption of Sensitive Data	Sensitive data that is submitted by the user will be encrypted to help keep all information secure. By scrambling all strings and keeping the key with the correct persons will increase the security and privacy of the system.
Validation of User Entered Data	Validating user data before sending to the database will increase the security and privacy of the system by ensuring the appropriate information is being submitted.

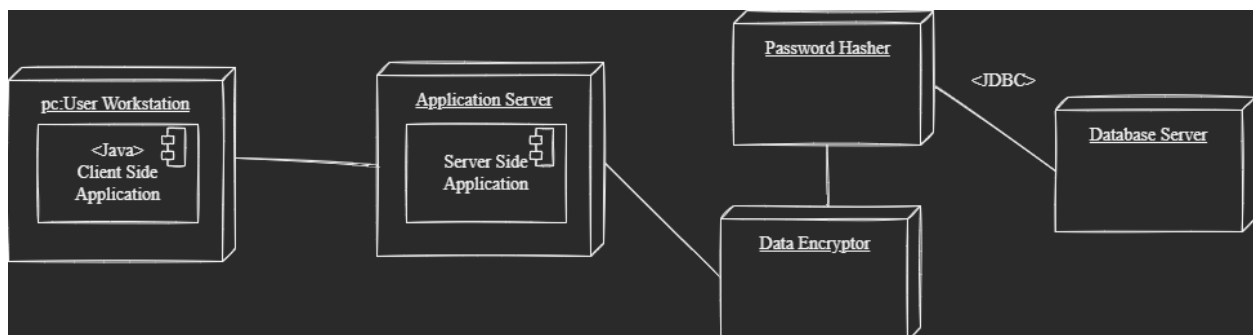
Step 5: Instantiate Architectural Elements, Allocate Responsibilities, and Define Interfaces

The instantiation design decisions are summarized in the following table:

Design Decisions and Location	Rationale
Implement password hashing after user submit information to database	Implementing password hashing will ensure that even if an unauthorized person is able to access the user's password, the information will be useless to them. This is implemented as the information is being sent to the database from the form on the website.
Encryption of all sensitive data such as emails, credit card numbers, addresses, etc. in the database	The information of the user stored on the database is encrypted so that all info is not usable by any unauthorized persons. This is implemented in the database and the authorized and appropriate persons only have access to the key.
Validating all fields before submitting to stop SQL injection	Before any information is sent to the database, the fields are validated and ensure that no SQL injection methods are being used to attack the information in the database.

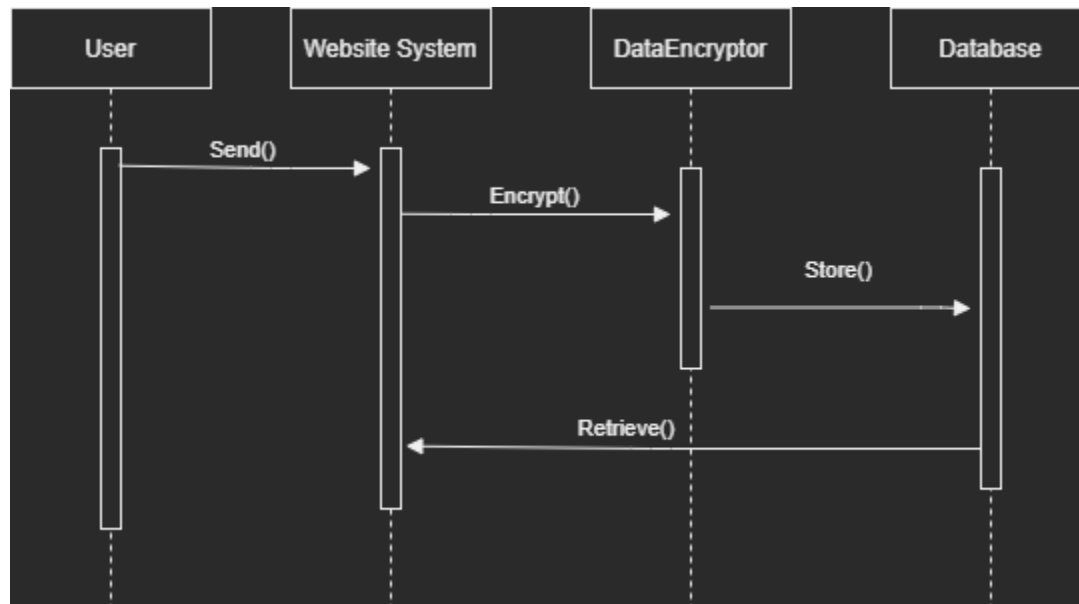
Step 6: Sketch Views and Record Design Decisions

Diagram below shows a deployment diagram that includes the introduction of password hashing and data encryption in the system.



All newly introduced elements in this diagram has been listed previously, therefore no table has been created

The UML sequence diagram shows how the data encryptor is introduced into the system. This shows how the data sent from the user is then sent to the website system and then encrypted by the data encryptor, finally is then stored in the database. This diagram supports QA-3 (security and privacy) and UC-1 (secured database). This diagram shows the communications between the several elements introduced into the system.



Step 7: Perform Analysis of Current Design and Review Iteration Goal and Achievement of Design Purpose

Not Addressed	Partially Addressed	Completely Addressed	Design Decisions Made During the Iteration
		UC-6	This iteration has addressed the need for all users to be registered properly
		UC-7	Field validation has been implemented in this iteration successfully to avoid things such as SQL injection
	QA-2		No relevant decisions made. As

			the requirements to meet in usability will be addressed in later iterations
		QA-3	This iteration addresses the security and privacy concerns and implements the necessary modules to address those concerns
		CON-2	This iteration addresses the security and privacy concerns and implements the necessary modules to address those concerns
	CRN-3		Relevant tasks has been allocated among developers, more tasks to allocated for later iterations