Iteration 3: Addressing Quality Attribute Scenario Driver (QA-4)

In this iteration , the design phase, the outcomes of the actions completed in each of the ADD phases are presented. We now begin to think about the fulfilment of some of the more essential quality attributes, based on the fact that users may store private financial information on the site. This iteration concentrates on one of the quality attributes possibilities that is QA-4.

Step 2: Establish Iteration Goal by Selecting Drivers

This iteration , we focus on the QA-4 quality attribute scenario: User's will store private financial information on the site to buy and sell art . Therefore the system should encrypt the private information of it's users like login and financial information.

Step 3: Choose One or More Elements of the System to Refine

For this iteration we will be choosing Database Server and Web Server elements to refine . These are the two elements within the deployment plan that can be controlled in order to fulfill the security attribute.

Step 4: Choose One or More Design Concepts That Satisfy the Selected Drivers

The following table summarizes the selection of design decisions in this iteration:

Design Decisions and Location	**Rationale and Assumptions**
Implementing authenticate actors technique by having a login system and password	The website may be able to authenticate users by ensuring that user or computer is who they claim to be . Users/computers are required to have their passwords and a username to enter the access all the features if website

Using Encrypt Data technique by securing credentials in configuration files and using cryptographic algorithms .	The website must exchange the financial information with the payment system securely. Also users' financial information should be encrypted .
Implementing change default settings technique .	The website may force the users to change the default password settings by popping up a password change web page .

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

The instantiation design decisions made in this iteration are summarized in the following table:

Design Decisions and Location	**Rationale and Assumptions**
Authenticate actors by having them enter their unique username and password on the login page before accessing the website.	The website using login technique will help to authenticate users and will ensure that the user's information is saved and being accessed by the right user.
Establishing a cryptographic algorithm to ensure secure exchange of the information between the website and external payment system . Configurating files for the database .	A cryptographic algorithm can be used in the website to help exchange of financial or other confidential information securely between the system's.
Establish the change default settings by having a webpage which will pop-up if the user is login in for the first time.	Changing default settings should be mandatory to access the website if the user is login in the website for the first time .

Step 6: Sketch Views and Record Design Decisions

In this step , the deployment diagram that was made in iteration 1 is refined.

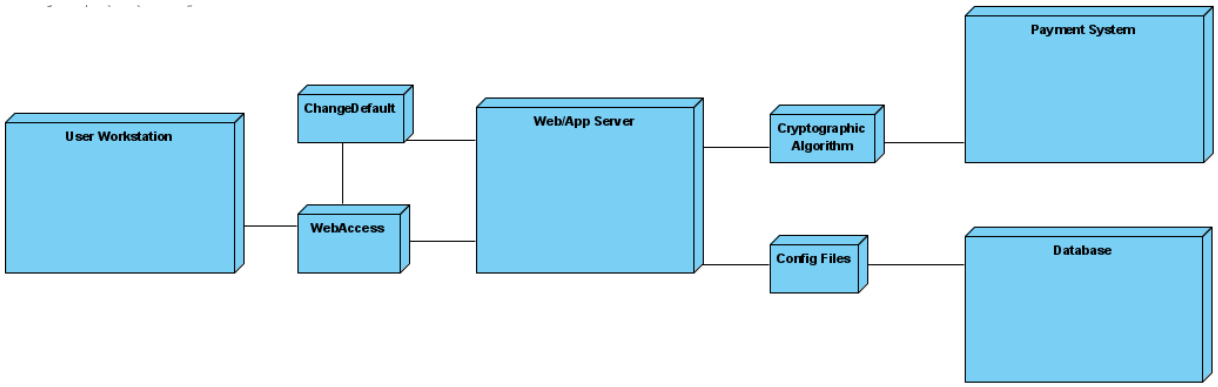

Figure 11:Refined Deployment Diagram

The following table summarizes the new elements that were not introduced in deployment diagram in iteration 1 :

Element	**Responsibilities**
WebAccess	This takes user to the login webpage where the user will login using his username and password
ChangeDefault	This will take those users who are using the website for the website and will let users change the default settings of the website along with the password and username.
Cryptographic Algorithm	This will ensure that the exchange of data between the webserver and payment system is secured and there is no misuse of the data.
Config Files	This helps in encrypting the database files by configuring them , hence securing them from hackers.

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

The focus of this iteration was on QA-4. The following table shows how the design decisions that were taken during this iteration affected the drivers.

Not Addressed	Partially Addressed	Fully Addressed	Rationale
	UC-2		No relevant decisions made.
	QA-2		No relevant decisions made.
	QA-4		By introducing authenticated actors and changing default settings techniques we can monitor any abnormal activities on the website and reduce the probability of any malicious use by keeping users aware, and have control, of the security settings. Also using encryption for exchanging data between the payment system and for the users' information in the database will help protect users' information from data breaches.
	QA-6		No relevant decisions made.
QA-7			No relevant decisions made.
CON-1			No relevant decisions made.
	CON-2		No relevant decisions made.
CON-3			No relevant decisions made.
CON-4			No relevant decisions made.
		CON-5	Modules associated with all of the use cases have been identified