Software Requirements Specification

Submitted By: Group 5

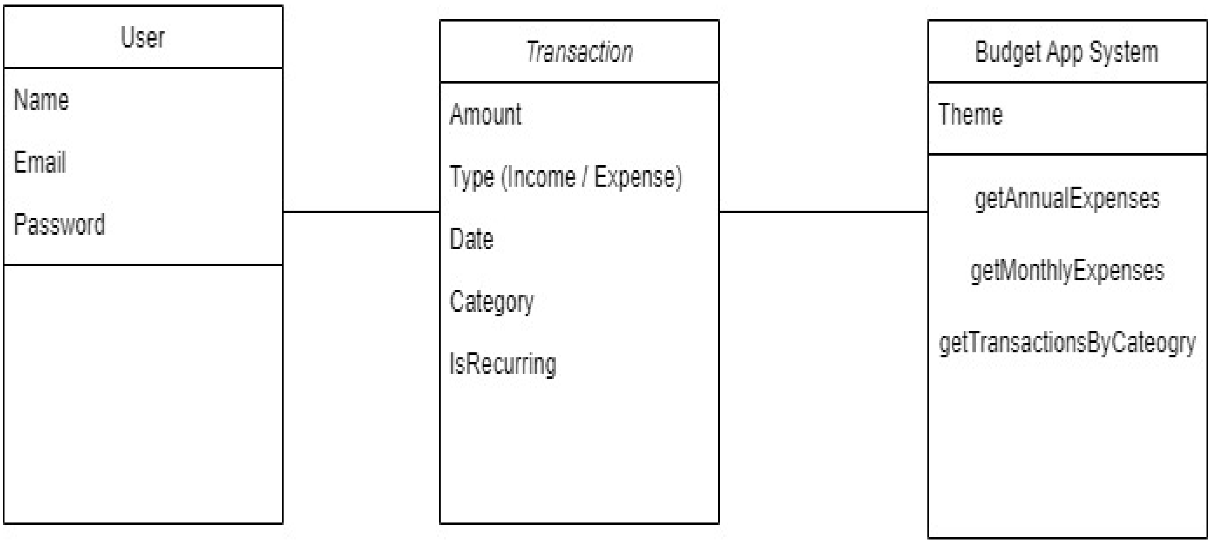
TABLE OF CONTENTS

1. Product Description

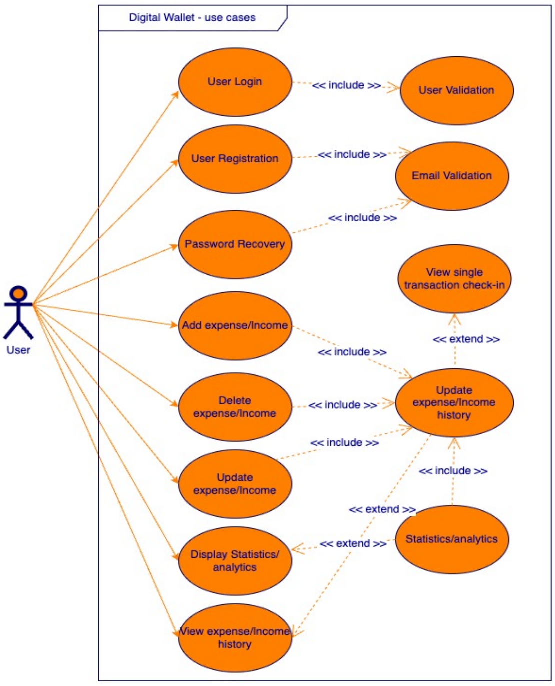
Digital Wallet

Digital wallet is a web app that helps you record all your financial transactions to get a better understanding of where your money is being spent. It gives you unique insights into your financial data, based on time periods, expense categories, and other filters. Now you can easily track exactly how your money is being spent.

2. Context Model using UML Class Diagram



3. Use Case Diagram



4. Functional Features derived from Use Case Diagram

Feature Name	User Perspective	Description	Importance	Difficulty	Priority Score
Login authentication	Users enters their email and password to get access to their data.	Used to authenticate and authorize a user based on their stored credentials.	2	1	2
Transaction entry	User clicks a "+" button	Stores the transactions entered	3	2	6

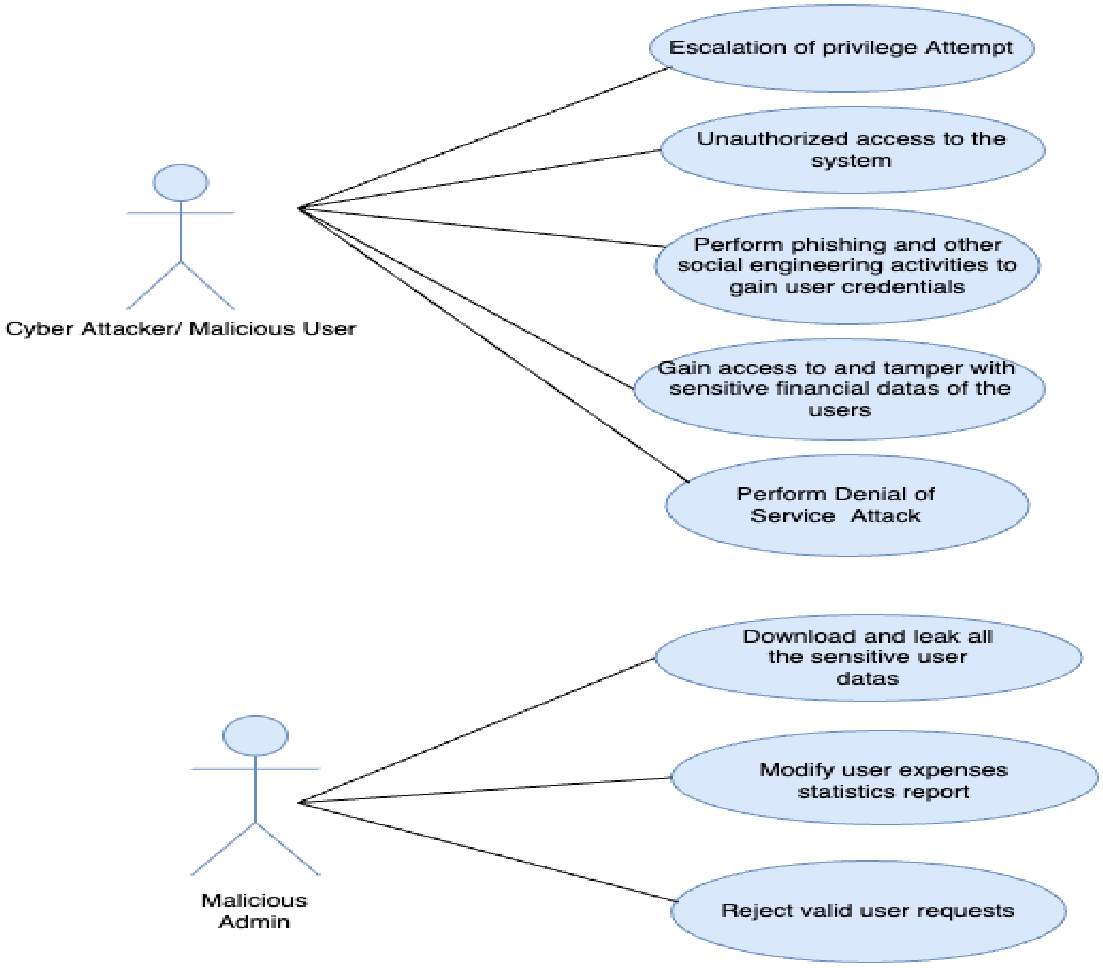
	and enters their transaction details	by the user into the database			
Transactions update	User can edit any entered transaction and update it with new values	This feature allows users to edit transactions while maintaining validity of all data and recalculating all totals	2	3	6
Analytics	User can view insights on their data.	This feature lets users check their total incomes, expenses, etc. over a period of time, and also sort, search, and filter their transactions based on categories or keywords.	3	3	9

5. Bi-directional traces between features and use cases

Use Case name --> **Feature name |** **V**	Login authentication	Transaction entry	Transactions update	Analytics
Allow password recovery if password is forgotten	X			
Compute income and expense for a given period of time				X
One-click to add income and expense		X		
One-click to update existing transaction entry			X	

Send one time password to verify Email	X			
Display income and expense for a given period of time				X
Validate User ID and password for existing user to login	X			
List all transaction				X

6. Abuse Case Diagram


Escalation of privilege Attempt
Unauthorized access to the system
Cyber Attacker/ Malicious User
Perform phishing and other social engineering activities to gain user credentials
Gain access to and tamper with sensitive financial datas of the users
Perform Denial of Service Attack
Download and leak all the sensitive user datas
Malicious Admin
Modify user expenses statistics report
Reject valid user requests

7. Security Scenario

7.1

Source	Unknown Identity external to the system (Cyber Attacker)
Stimulus	Tries to perform phishing activities to gain user credentials.
Artifact	Web application, Database
Environment	Under normal operations
Response	System identifies suspicious activity and locks user while also logging the activity.
Response Measure	99% of the services are still available to the system.

7.2

Source	Unknown Identity external to the system (Cyber Attacker)
Stimulus	Tries to tamper with sensitive financial data of the users.
Artifact	Web application, Database
Environment	Under normal operations
Response	

	System identifies suspicious activity and locks user while also logging the activity.
Response Measure	99% of the services are still available to the system.

7.3

Source	Unknown Identity external to the system (Cyber Attacker)
Stimulus	Tries to perform a DDoS attack.
Artifact	Web application, Database
Environment	Under normal operations
Response	System identifies suspicious activity and locks user while also logging the activity.
Response Measure	If DDoS is successful, system will not be available

7.4

Source	Malicious Admin
Stimulus	Download and leak sensitive user data.
Artifact	Web application, Database

Environment	Under normal operations
Response	System identifies suspicious activity and logs activity. Reports and blocks malicious admin.
Response Measure	99% of services are still available to system.

7.5

Source	Malicious Admin
Stimulus	Tries to Modify user data.
Artifact	Web application, Database
Environment	Under normal operations
Response	System identifies suspicious activity and logs activity. Reports and blocks malicious admin.
Response Measure	99% of services are still available to system.

7.6

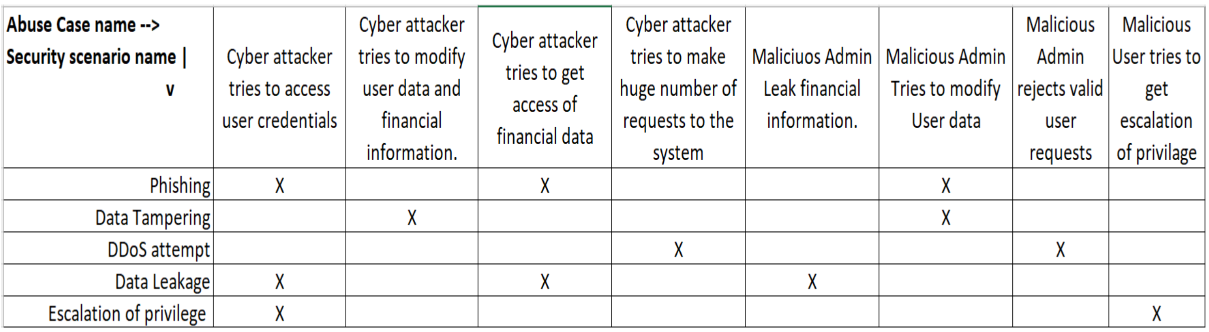
Source	Malicious Admin
Stimulus	Tires to reject valid user request

Artifact	Web application, Database
Environment	Under normal operations
Response	System identifies suspicious activity and logs activity. Reports and blocks malicious admin.
Response Measure	99% of services are still available to system.

7.7

Source	Malicious User
Stimulus	Tires to gain vertical escalation of privilege
Artifact	Web application
Environment	Under normal operations
Response	System identifies suspicious activity and logs activity. Reports and blocks malicious user.
Response Measure	99% of services are still available to system.

8. Bi-directional traces between these security scenarios and abuse cases



Abuse Case name --> **Security scenario name |** **v**	Cyber attacker tries to access user credentials	Cyber attacker tries to modify user data and financial information.	Cyber attacker tries to get access of financial data	Cyber attacker tries to make huge number of requests to the system	Maliciuos Admin Leak financial information.	Malicious Admin Tries to modify User data	Malicious Admin rejects valid user requests	Malicious User tries to get escalation of privilage
Phishing	X		X			X		
Data Tampering		X				X		
DDoS attempt				X			X	
Data Leakage	X		X		X			
Escalation of privilege	X							X

9. Abuse Case Descriptions

9.1 Abuse Case Textual Description

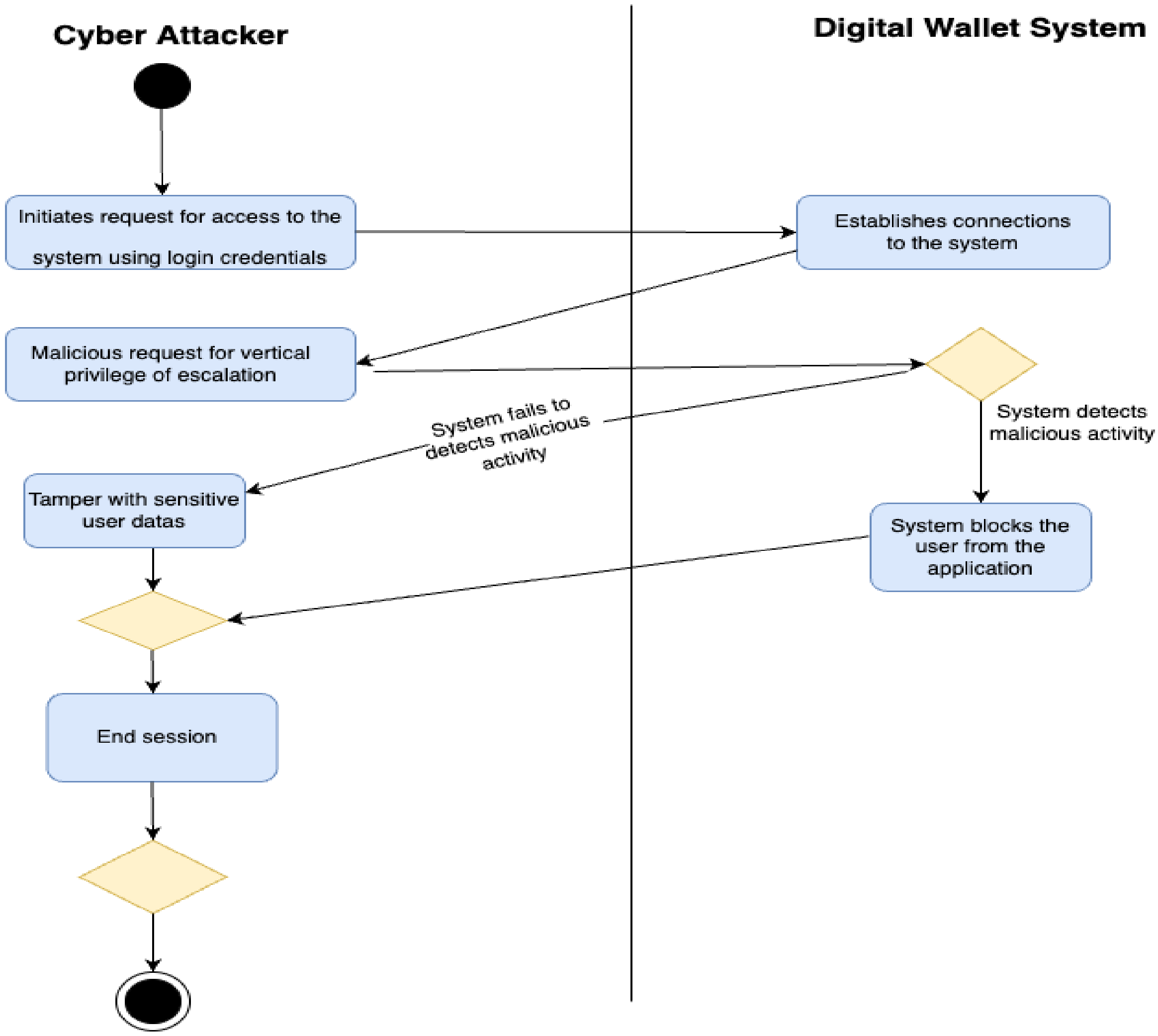
Name: Download and leak all the sensitive user datas
Actors: Malicious Admin
Trigger: Malicious admin has access to the database where all the user datas are stored
Preconditions: Malicious admin has access to the login credentials to the database server
Postconditions:

Successful postconditions: Malicious admin fails to have access to the user datas and all other admins are notified via email about the failed attempt to access user datas.

Failure postconditions: Malicious admin has access to all the user datas and is able to leak the sensitive information.

9.2 Abuse Case Graphical Format:

Abuse case: Gain access to and tamper with sensitive financial datas


Cyber Attacker
Digital Wallet System
Initiates request for access to the system using login credentials
Establishes connections to the system
Malicious request for vertical privilege of escalation
System fails to detects malicious activity
System detects malicious activity
Tamper with sensitive user datas
System blocks the user from the application
End session

10. Quality Attributes and Required Scenarios / Utility Table

Quality attribute	**Quality Scenario name**	**Quality Scenario brief description**	**Quality Scenario utility**	**Estimated Quality Scenario development difficulty or risk**	**Scenario priority score**
Security	Encrypt all the user datas with an encryption algorithm	All of the user datas stored in the system should be encrypted so that unauthorized access does not result in data leak.	3	2	6
Scalability	Ability to serve 100000 concurrent users at a time	The system should be able to serve 100000 users at a time without degrading its performance	2	2	4
Performance	The system is able to perform user requests accurately	The digital wallet application should be able to understand and perform the task the user is requesting accurately.	3	2	6
Availability	The system is available to use at all times	The digital wallet application should not have any downtime	3	2	6
Usability	The user is able to search the expenses by month	The digital wallet application should be able to have the functionality to display the expenses of users filtered by months	2	2	4

11. Quality scenarios using SEI

11.1

Scenario Name	Security
Source	Internal stakeholders
Stimulus	Encrypt all user data with encryption algorithm
Artifact	Digital wallet Web application
Environment	Under normal operations, run time
Response	All data stored will be encrypted and safe from attacks.
Response Measure	99% of data is secure

11.2

Scenario Name	Performance
Source	User

Stimulus	All requests are handled in a timely and accurate manner.
Artifact	Digital wallet Web application
Environment	Run time
Response	Negligible delay and negligible inaccuracy.
Response Measure	99% of system response is accurate and timely.

11.3

Scenario Name	Availability
Source	Internal stakeholders
Stimulus	System available all the time
Artifact	Digital wallet Web application
Environment	Run time

Response	System is available 24*7
Response Measure	0% down time.