ASSET CONTROL SYSTEM

Author (s):

1. Dinesh Chowdary Guduru
2. Aditya Bikki
3. Sriyuktha Sakhamuri
4. Thanmai Bvsma
5. Manvitha Ayinampudi

Major User Stories: Fundamental Features and Authentication

Selected Template: System Analysis Use Case Template

Use Case:

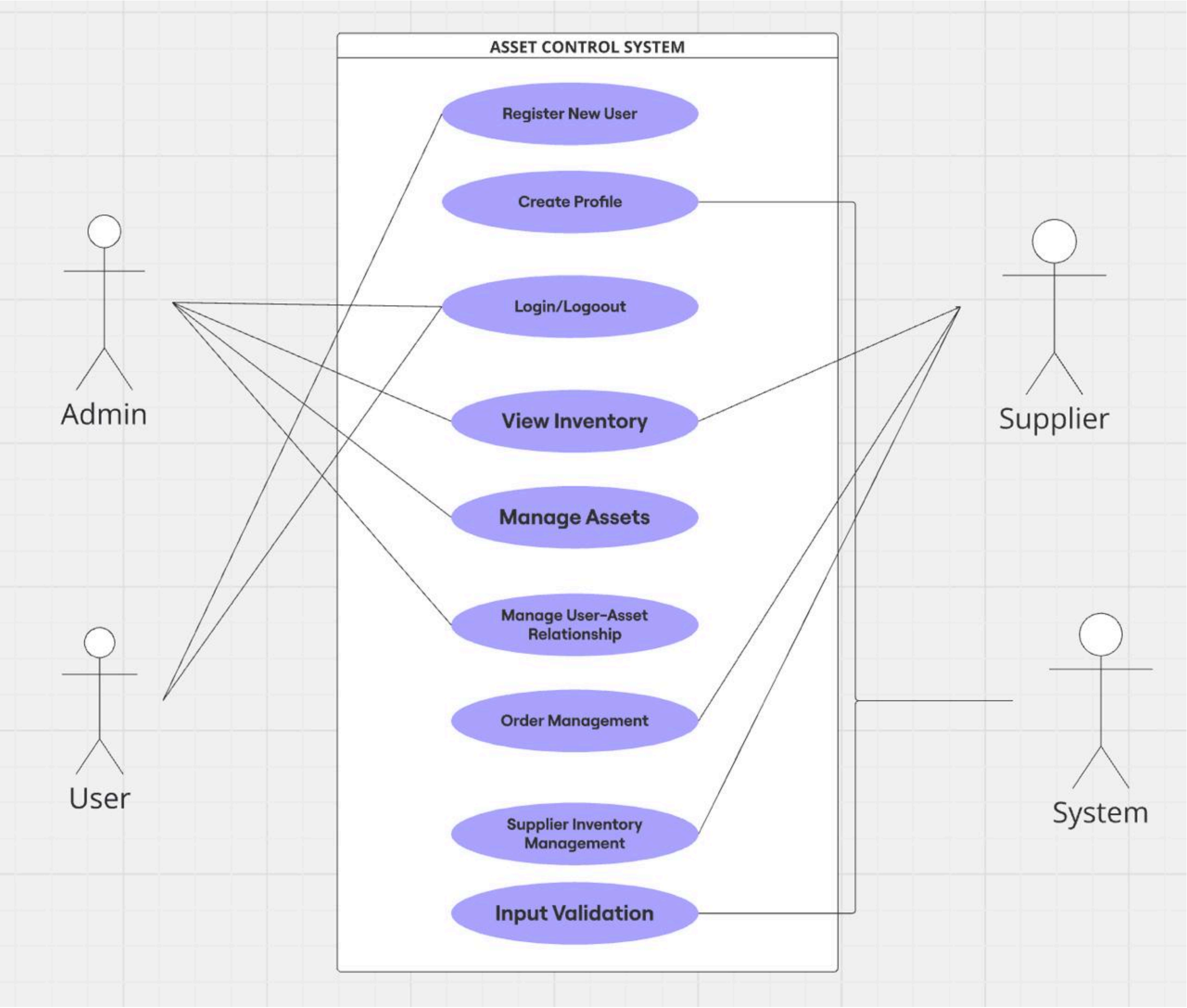
USE CASE NAME:	Fundamental Features and Authentication	**USE CASE TYPE** **Business Requirements:** □ **System Analysis:** ☑
USE CASE ID:	1	
PRIORITY:	High(1)	
SOURCE:	Customer	
PRIMARY BUSINESS ACTOR	User	

PRIMARY SYSTEM ACTOR	Authentication System	
OTHER PARTICIPATING ACTORS:	Database System	
OTHER INTERESTED STAKEHOLDERS:	System Admin	
DESCRIPTION:	This use case describes the implementation of a basic user authentication system including login/logout functionality, secure password handling, and management of asset control with login and logout capabilities.	
PRE-CONDITION:	● User has an existing account. ● The system is operational and connected to a secure database. ● Password encryption is in place.	
TRIGGER:	The user initiates the authentication process by attempting to log in and also when the user attempts to log out of the system.	
TYPICAL COURSE	**Actor Action**	**System Response**
OF EVENTS:	**Step 1**: The user navigates to the login place.	**Step 2**: The system displays the login form.
	Step 3: The user enters a username and password	**Step 4**: The system encrypts the database.

	Step 5: The user clicks the login button.	**Step 6:** If the credentials are correct, the system grants access and redirects the user to the asset control system.
	Step 7: The user performs asset control tasks.	**Step 8:** The system securely manages the assets.
	Step 9: The user clicks the logout button and redirects to the login page.	**Step 10:** The system logs the user out and redirects to the login page.
ALTERNATE COURSES:	If the user enters an invalid username or password: ● The system displays an error message and prompts so that the user can retry. If the user forgets their password: ● The system offers a "Forgot Password" option to reset it via email.	
CONCLUSION:	Users are able to securely log in, manage assets and log out of the system securely.	
POST-CONDITION:	The user is logged out and the session is terminated. The system maintains user sessions securely until logs out.	
BUSINESS RULES	● User passwords must be encrypted before storage. ● Multiple failed login attempts should be locked. ● Error messages must be displayed for failed login attempts.	
IMPLEMENTATION CONSTRAINTS AND SPECIFICATIONS	● Ensure compliance standards for password storage. ● Use industry-standard encryption algorithms for password storage. ● Ensure secure communication channels like HTTPS.	

ASSUMPTIONS:	- Users have unique usernames and passwords. - The database is secure and accessible. Users are responsible for maintaining the confidentiality of the login credentials
OPEN ISSUES:	- Inconsistent authentication workflow. - Inconsistency in maintaining persistence.

Use Case Diagram:


ASSET CONTROL SYSTEM
Register New User
Create Profile
Login/Logout
View Inventory
Manage Assets
Manage User-Asset Relationship
Order Management
Supplier Inventory Management
Input Validation
Admin
User
Supplier
System