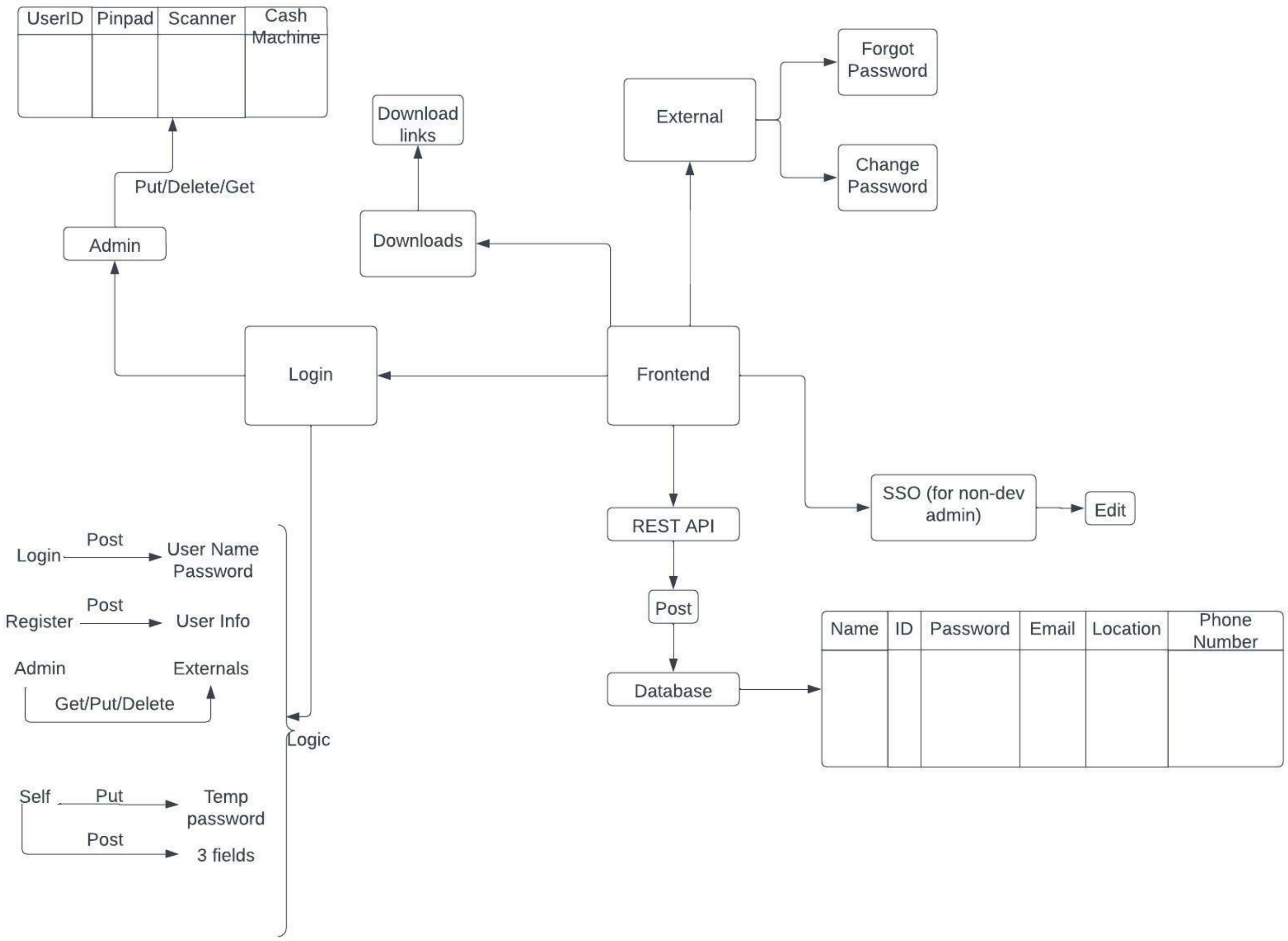
COSTL Developer Portal Documentation

Author: Jiawei Hao

Requirements

1) Role Assign: The portal should have the functionality to assign roles to its users. Roles include internal users, external users, and admins. For example, an internal user may have access to details on specific devices while an external user does not have such access. Method available: SSO.
2) Admin and user management: The ability to insert, update, and delete user/admin's information. Databases can be used to record information and access rights of each individual. Admin has the rights to query and modify the database. Method available: database.
3) Self-serve user: External users should be able to use "forgot password" and "change password" functionality.
4) Downloads: Users/devs should be able to download files within their access rights. Method available: download links.
5) Non developer edits: The ability to allow internal users (non-devs) to modify the content of the page. Method available: SSO.
6) Docker tests: The ability to run tests on Docker. This functionality should be implemented last.

Flow diagram



Database

Table 1: User Information

Name	UserID	Password	Email	Location	Phone Number
String	Integer	String	String	String	Integer

Table 2: User Access Rights

UserID	Pinpad	Register	Printer	Hand Scanner	Flatbed Scanner	Scale	Cash Washer
Integer	Bool	Bool	Bool	Bool	Bool	Bool	Bool

Table 3: User Roles

UserID	Role
Integer	String

API

Request Type	Data Type	Usage
Put	String	Users can change their passwords.
Post	Integer, String	When a user registers, the system creates the user's information in the database.
Put	String, Bool	An admin can create a user's access right.
Get	String, Bool	An admin can read a user's access right.
Delete	String, Bool	An admin can delete a user's access right.
Get	String	An user/admin can receive a link for download.
Post	String	The login creates the user's password.
Put	String	An user can have a temporary password (may not use this).
Post	String	An user can create 3 fields.
Get	Integer, String	An admin can read a user's information.
Put	Integer, String	An admin can update a user's information.
Delete	Integer, String	An admin can delete a user's information.

Scenarios/Restrictions

1) For security reasons, when a user changes password, the new password cannot be a password that has already been used by the user. This may not be a good idea because we need to store old passwords to compare to the new password, which can get passwords exposed.
2) A user cannot register more than once. We can limit one email or one phone number per registration only.
3) Only admins can have access to all devices. We can use a boolean variable "is_admin".
4) Admin may accidentally modify or delete an user's information. We can add a double confirmation feature to prevent such accidents.
5) When a user requests to change the password, the process should be secure and trustable. We can either use the walmart domain to send an email (complicated procedures) or use security questions for changing the passwords.
6) To distinguish different users, we can use SSO for admin/staff login and email and passwords for external user login.