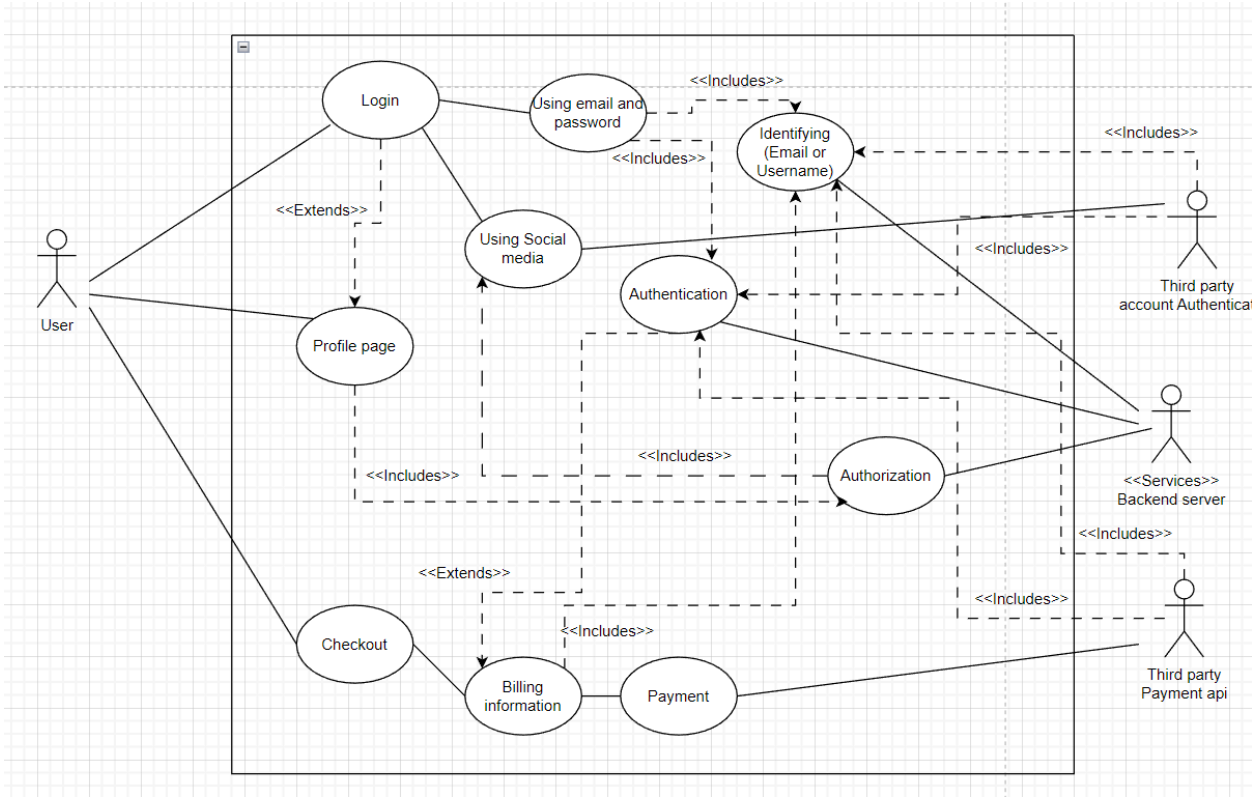
Assignment 2

Martin Fontin mf223ub@student.lnu.se

Part1

A user can Login with either Email and password or using a social media account
Login using email and password Extends from Identifying and Authentication since both are required from the user to login. Login in using social media accounts uses a third party to Identify the users, but also if the user is not logged in to that social media account they also need to be authenticated. If a user wants to visit the profile page the user needs to be logged in, if the user is not already logged in the user has to login, after that the user can be Authorized. Lastly, the checkout page only Includes Identifying when a user enters billing information, but if the user is already logged in the server can fetch billing information using its user's session by authentication. Also the payment is provided by a Third party payment api.



Part 2

QAS 1

Source: Unidentified user
Stimulus: Attempts to login to another user's account
Artifact: Login service
Environment: Online, Normal operation
Response: The system detects attempted login attempts and logs it.
Response measure: System notices failed login attempts and locks the account in question.

QAS 2

Source: A user
Stimulus: Attempts to access
Artifact: Administrator dashboard
Environment: Online, Normal operation
Response: Unauthorized access
Response measure: Log ip address of unauthorized user, and other information about the failed access attempt. Also blocks the ip address.

QAS 3

Source: A unidentified user
Stimulus: Attempts to create multiple accounts during a short time frame.
Artifact: Login service
Environment: Online, Normal operation
Response: Block Ip address from creating accounts but also limiting the IP
Response measure: Log the accounts created and block them. Also flag the ip address in the system.

Part 3

When an unidentified user attempts to login to another user's account the **Identification & authentication** requires the database to confirm the identification and password from users. If it fails it requires the **log component** to log the failed authentication attempt.

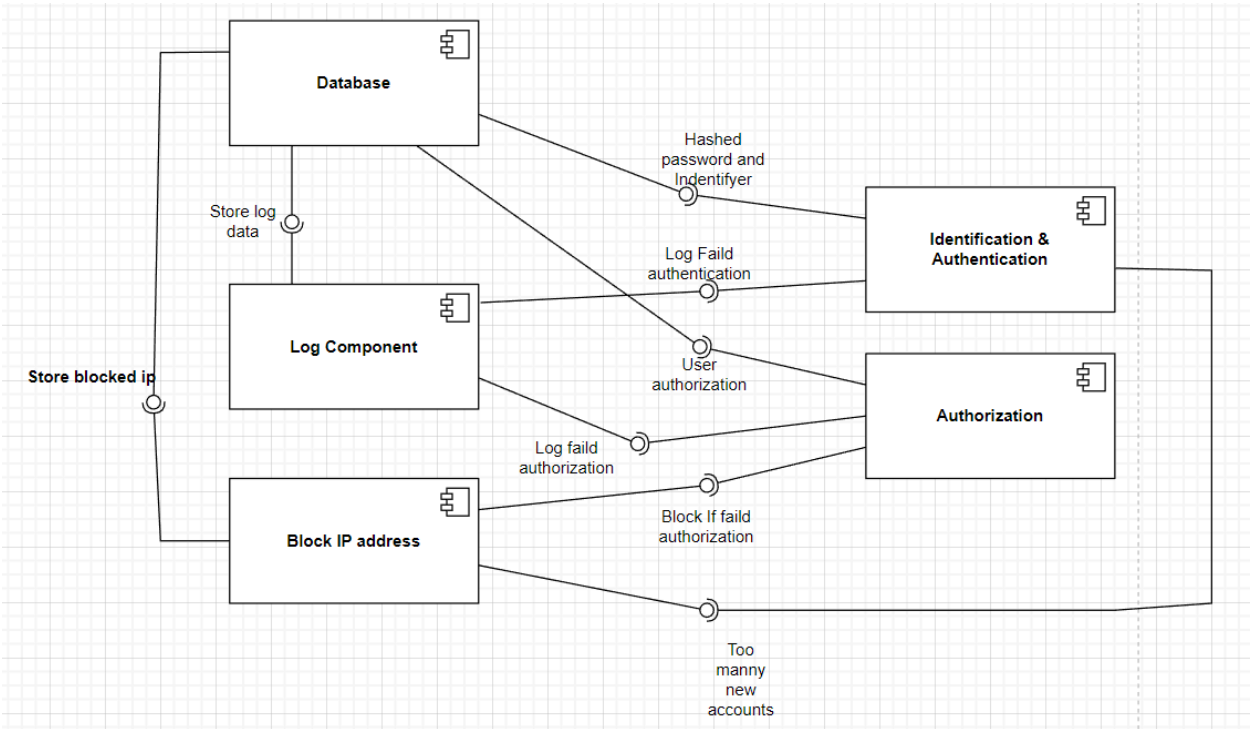
When a user attempts to access the administrator dashboard the **Authorization** component requires the **database** component to check users privileges to decide if a user should be authorized or not. On a failed authorization the component requires both the log component to log the failed authorization attempt and the **Block Ip Address** component to block the user from trying to access the service.

When an unidentified user attempts to create multiple accounts the **Identification & authentication** component requires the **Log component** to log the multiple accounts but also requires the **Block ip address** component to be able to block that user from creating more accounts.

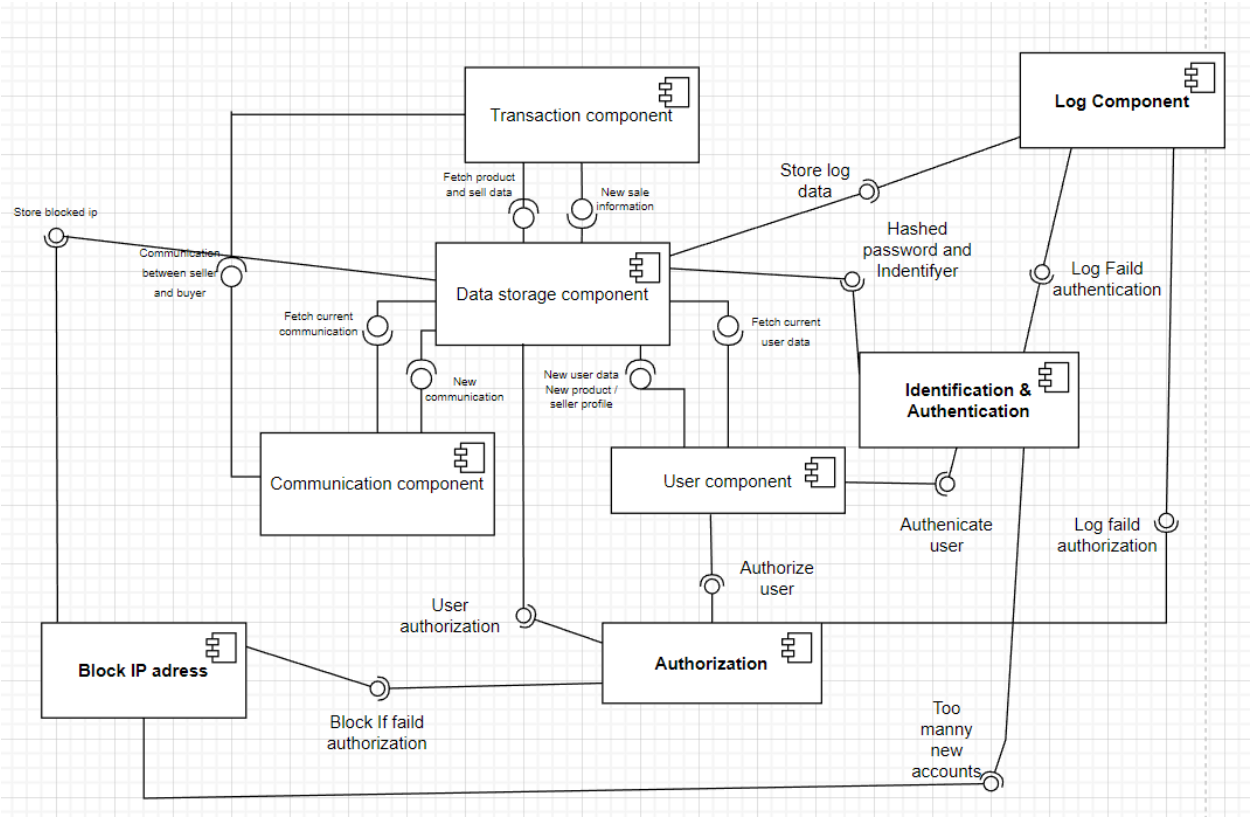
Log Component provides Logging of failed authentication attempts to the **Identification & authentication** component, but also provides logging of failed authorization to the **Authorization** component. To be able to log the attempts the component requires the **database** component.

Block IP address provides blocking of an ip address if an user fails at authorization. It also requires the **database** to store the blocked ip address.

The **database** component provides storage of data from the **Log component** but also provides the **block ip address** component.



Part 4



Adaptations

Removed the database component from part 3 diagram and connected its interfaces to the Data storage component

Added relations between Users component and Authorization and (Identification & Authentication) components