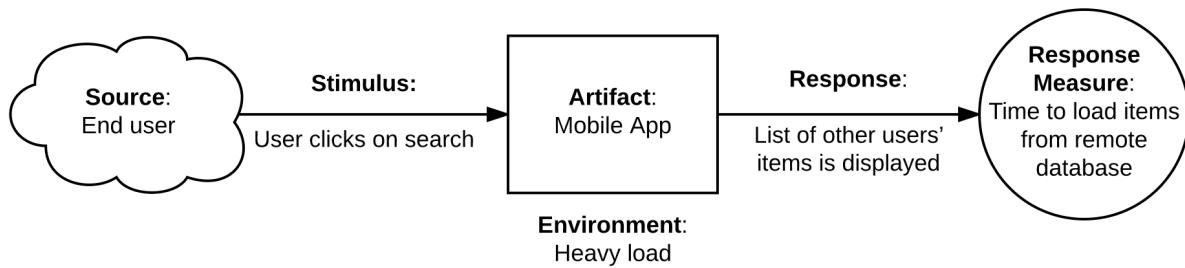
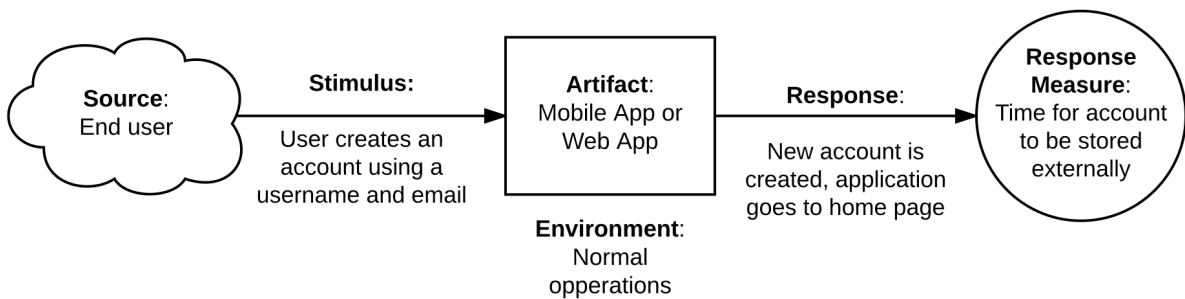


1.



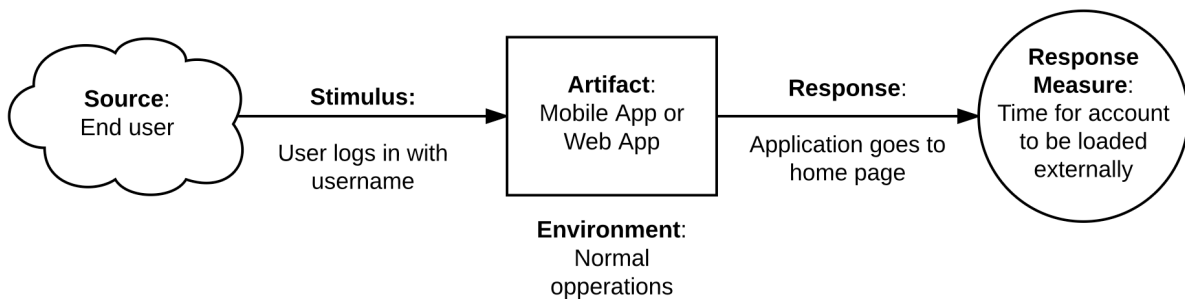
Risk: This scenario presents a risk because, according to the system ASRs, any task must take less than one second to complete, therefore there is nothing pointing out that this task accomplishes such requirement in this scenario. In addition, the tests presented time response bigger than 1 second and up to 5 seconds.

2.



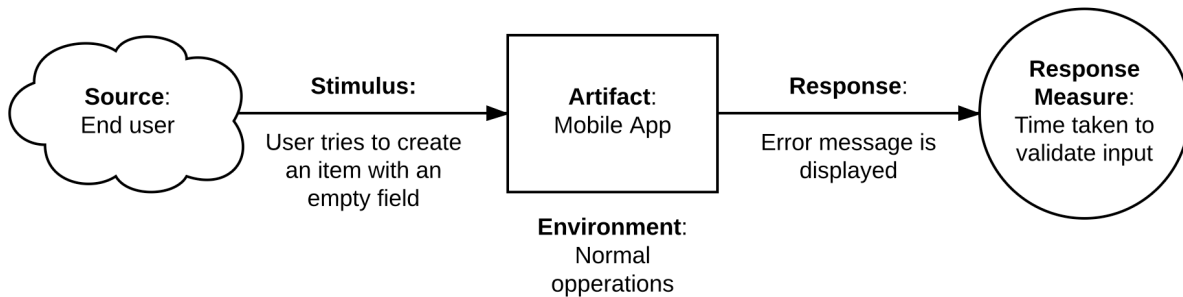
Risk: This scenario presents a risk because enabling users to create an account or log in without a secure authentication method, such as a password, poses a risk.

3.



Trade-off: Allowing users to log in to a system using only their username creates a trade-off between security and usability. While it improves usability by eliminating the need to remember a password, it reduces security since there is no second factor of authentication to verify the user's identity.

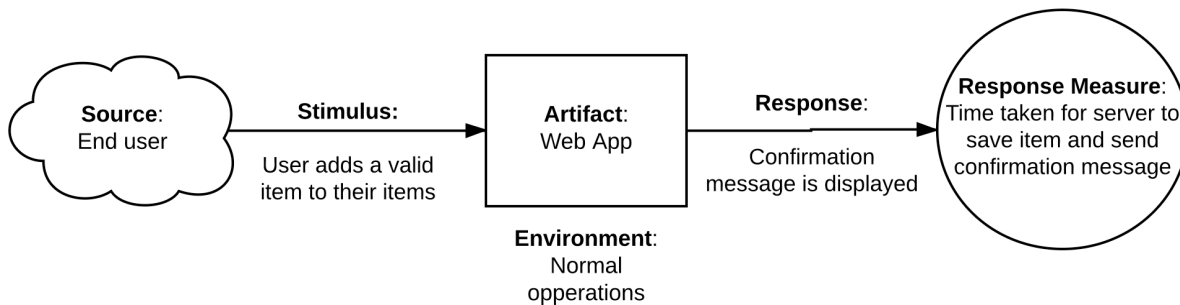
4.



Non-risk: This scenario does not pose any immediate risk, since the system successfully manages the potentially risky stimulus by providing clear feedback to the user.

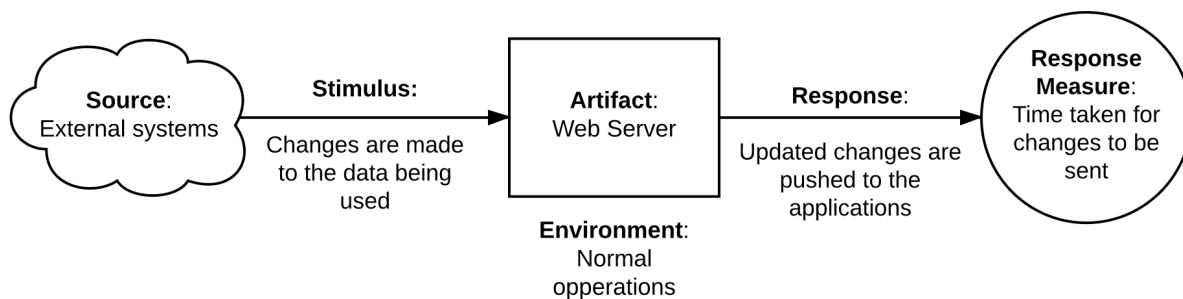
However, it is important to note that this scenario may impact usability. If the system displays a generic error message, it could lead to confusion or frustration for the user, resulting in a poor user experience.

5.



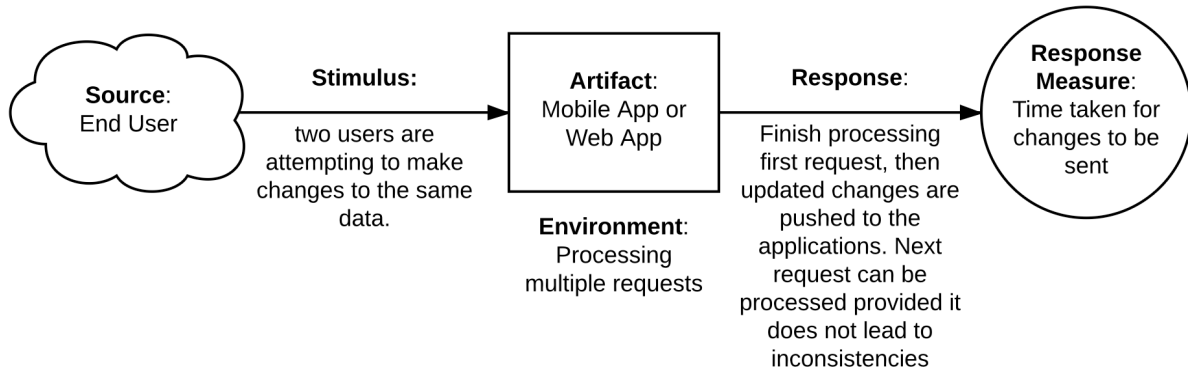
Non-risk: This scenario presents no risk for the system. The operation was completed successfully, and the response time was less than one second.

6.



Sensitivity-point: This scenario is considered a sensitivity point due to its potential impact on data integrity, as a change from an external system can cause inconsistencies in the data during concurrent operations. To minimize the potential impact of this scenario, a synchronization mechanism that ensures data and resources remain up to date can be implemented.

7.



Non-risk: Since the system processes multiple requests sequentially, it synchronizes the operations and leads to consistent resources on each operation, resulting in an expected running.

