Q1:

Software Requirements Specification

for

Bird Boarding Booking System

Version 1.0 approved

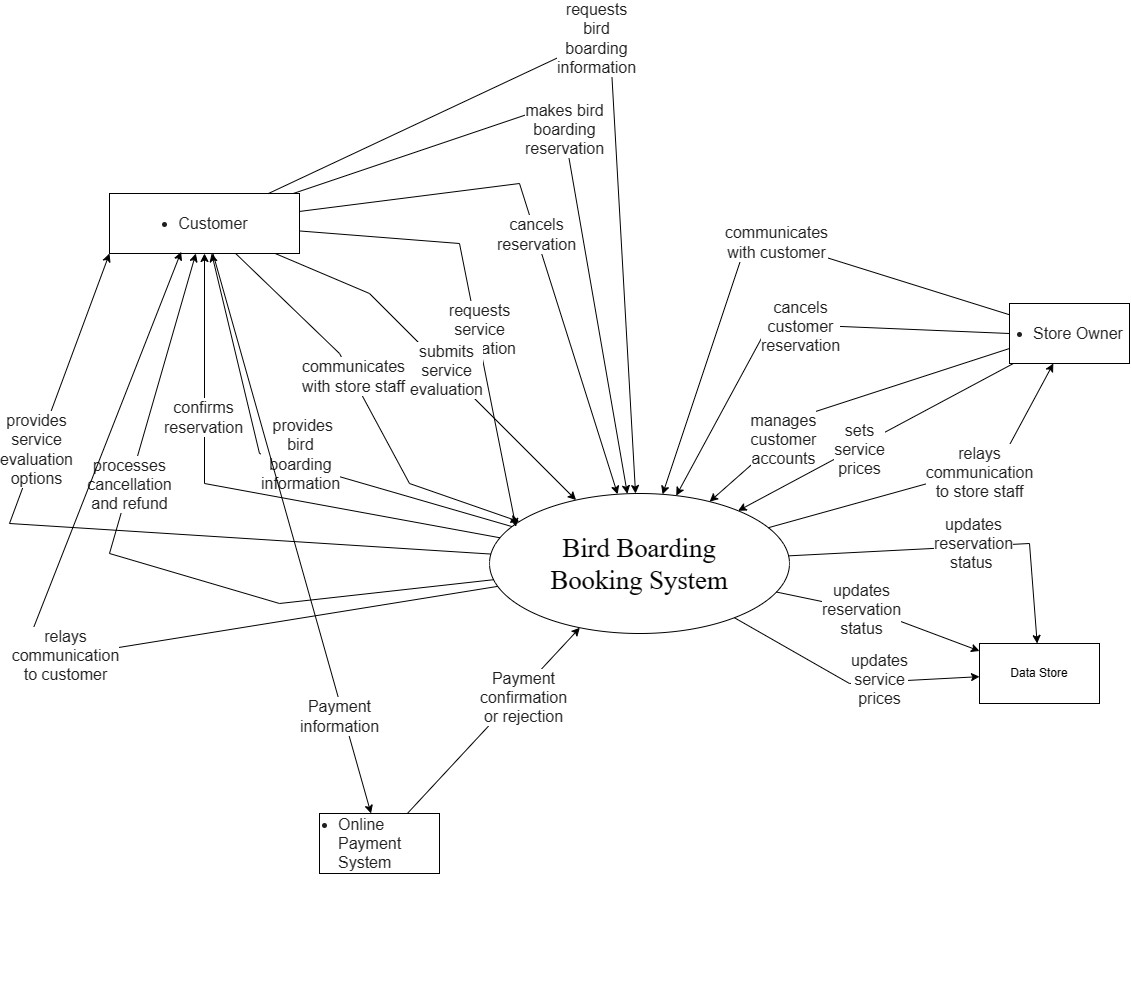
Prepared by

Nguyen Van A

Campus ?

02/04/2024

Q2:



Q3:

< Student must replace this line

Notes:

1. Draw the correct syntax to describe the use case diagram (0.4 point)
2. List the name of >= 4 actors and brief descriptions (0.8 point)
3. Draw use cases and brief descriptions (2.8 points)

>

<Student must replace this line, answer Q3 by drawing 1 use case diagram that reflect this exam paper and copy and then paste the image of that use case diagram here>

< Student must replace this line, **briefly describe** the actors of the diagram by fill the content to below table>

|  |  |  |
| --- | --- | --- |
| **#** | **Actor** | **Description** |
| 01 |  |  |
| 02 |  |  |
| 03 |  |  |

< Student must replace this line, **briefly describe** the use cases of the diagram by fill the content to below table>

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Use Case** | **Actors** | **Description** |
| UC-01 |  |  |  |
| UC-02 |  |  |  |
| UC-03 |  |  |  |

Q4:

|  |  |  |
| --- | --- | --- |
| ID | Rule Definition | Use cases |
| BR-01 | Only one customer's birds can occupy a cage at a time. | UC-01, UC-02 |
| BR-02 | The boarding price is reduced by 50% for each additional bird placed in the same cage. |  |
| BR-03 | Customers receive a 50% refund for cancellations before the deadline, and no refund after. |  |
| BR-04 | New customer accounts require approval by store staff or owner before login. |  |
| BR-05 | After 5 consecutive failed login attempts, the customer's account is locked for security reasons. |  |

**Q5:**

a. Security (Usability):

* Password Strength: The system should require passwords for customer accounts to be a minimum of 12 characters in length and include a combination of uppercase and lowercase letters, numbers, and symbols.
  + Explanation: A minimum password length of 12 characters is considered more secure than 8 nowadays. Enforcing a combination of character types makes passwords harder to crack through brute-force attacks.
  + Testing: Testers can verify password requirements by attempting to create accounts with passwords that don't meet the criteria. The system should prevent account creation with weak passwords.
* Secure Communication: The system should implement secure communication protocols (HTTPS) to protect user data during transmission. This can be verified by testers using browser developer tools to inspect network traffic and ensure data is encrypted (HTTPS instead of HTTP) during login, registration, and other sensitive actions.

b. Performance (Availability):

* System Uptime: The system should be available at least 99.5% of the time during peak hours (e.g., weekends, holidays).
  + Explanation: 99.5% uptime translates to a maximum downtime of 21.6 minutes per week, which is a reasonable target for a business-critical system.
  + Testing: Testers can use automated monitoring tools to track system uptime over a period of time. Analyzing these metrics will reveal if the uptime target is being met.
* Response Time: The system response time for user actions (searches, bookings, etc.) should be less than 3 seconds on average.
  + Explanation: A 3-second response time is considered a good benchmark for user experience. Longer delays can lead to frustration and cart abandonment.
  + Testing: Testers can utilize performance testing tools to simulate user load and measure response times for various functionalities. Analyzing these results will indicate if the system meets the performance target.