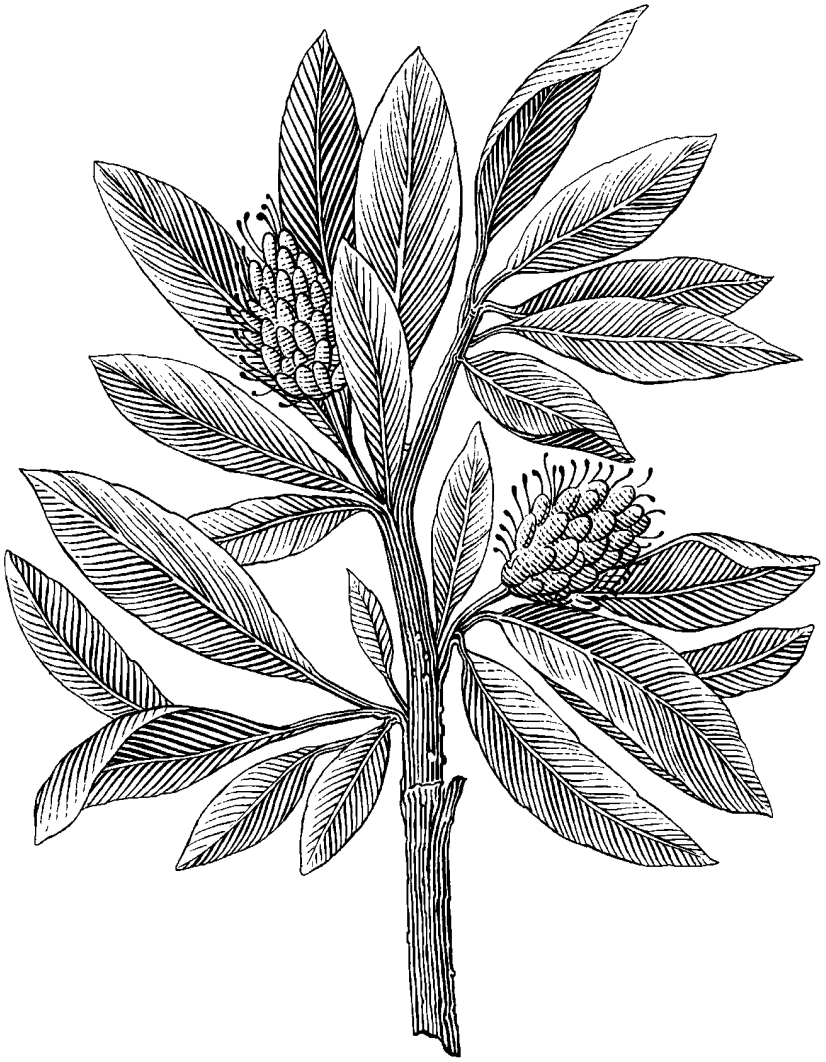
Linnéuniversitetet
Kalmar Växjö

Report

Assignment 2

2DV604



Semester: Spring 2024

Author1: Katarina Simakina
Email es225hi@student.lnu.se

Author2: Zejian Wang
Email zw222bb@student.lnu.se

Table of Contents

Task 1

Performance ASRs

1.During peak load, The LnUShop system must complete processes, including transactions, account updates, browsing listings and other tasks within 10 seconds to ensure a seamless shopping experience.

Motivation: High responsiveness during peak traffic time is essential for maintaining customer satisfaction and preventing transaction abandonment. If this is not achieved, users may experience delays that could lead to frustration leading to abandoned transactions, directly impacting sales and customer satisfaction.

2. The LnUShop must support at least 1000 concurrent user interactions per second at peak times without performance degradation.

Motivation: High throughput is necessary to handle the load during peak shopping time, such as textbook sales at the start of a semester. Failure to manage high traffic can result in slow service, transaction failures, and a decline in user satisfaction.

Security ASRs

1.ASR: The LnUShop system must incorporate mechanisms capable of proactively detecting various security threats, including but not limited to SQL injection attacks, cross-site scripting (XSS) and unauthorized access attempts.

Motivation: Implementing proactive threat detection is crucial for safeguarding the system against a wide range of security threats. By detecting before they can exploit vulnerabilities, the system can prevent data breaches, service disruptions and potential reputational damage. Without such measures, the system may be susceptible to attacks that compromise user data and undermine trust in the platform's security.

2. ASR: The LnUShop system requires an encryption mechanism to ensure security during data transmission and data at rest, such as SSL/TLS encryption for data transmission, AES encryption for data in storage.

Motivation: Given the LnUShop system involves transactions and personal data, ensuring data security during transmission and storage is necessary. This requirement directly impacts the architecture as it necessitates the integration of encryption mechanisms and protocols, influencing the choice of technologies and the design of the data storage and transmission components.

Task 2

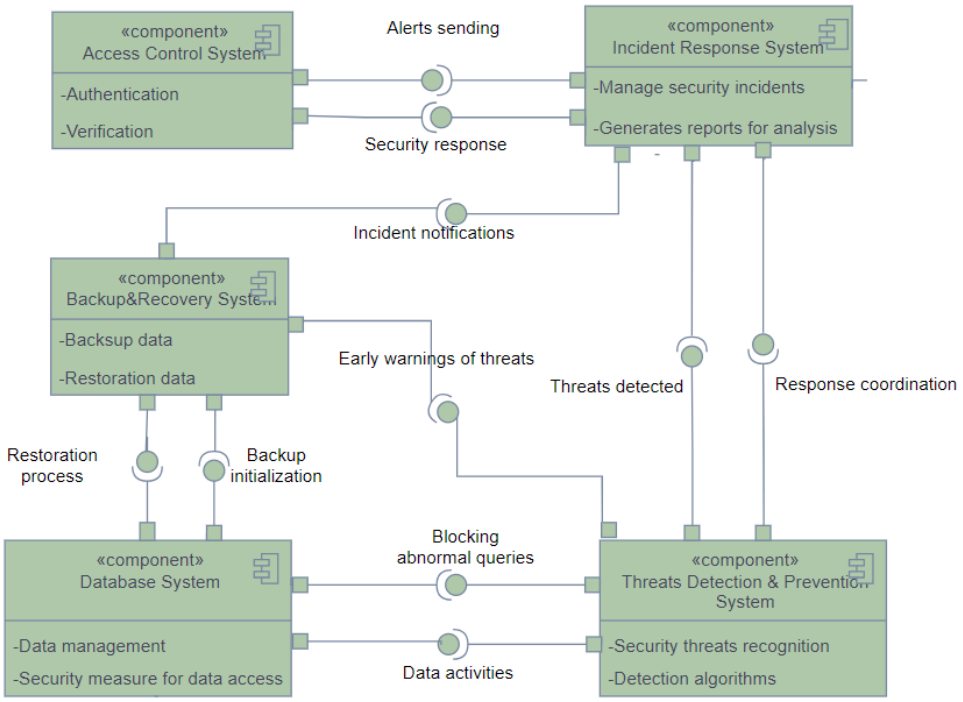
Security ASR

ASR: The LnUShop system must incorporate mechanisms capable of proactively detecting various security threats, including but not limited to SQL injection attacks, cross-site scripting (XSS) and unauthorized access attempts.

Portion of Scenario	Possible Values	Rationale for Variants
Source	SO1: External Threat Actors: Malicious individuals or entities attempting to exploit vulnerabilities in the LnUShop system. SO2: Internal Threats: Threats posed by employees or authorized users with malicious intent.	Identifying the source as security threats helps to specify the potential attackers and their motivations for attacking the system, providing insight into the types of threats the system must defend against.
Stimulus	ST1: Injection Attack: Attempts to inject malicious code or commands into the system, such as SQL injection by SO1. ST2: XSS Attack: Attempts to inject malicious scripts into web pages viewed by other users by SO1, SO2. ST3: Unauthorized Access Attempt: Attempts to gain unauthorized access to restricted areas or sensitive information by SO2.	Defining the stimulus as security breach attempts clarifies the specific actions that trigger the security mechanisms within the LnUShop system, helping to identify and respond to potential threats effectively.
Artifact	A1: Access Control System: This artifact encompasses the mechanisms and policies used to control access to the database, including user authentication, authorization, and privilege management. A2: Backup and Recovery System: This artifact represents the system or process responsible for backing up database data and ensuring its integrity and availability in the event of data loss or corruption. A3: Threat Detection & Prevention System: This artifact monitors and analyzes activities in real-time to detect and alert administrators to suspicious or unauthorized activities;detects security threats and blocks suspicious queries.	The selection of these artifacts is driven by their critical roles in ensuring the security and integrity of the LnUShop system. Access Control Mechanisms are fundamental for regulating user access and privileges, safeguarding sensitive data from unauthorized access. The Backup and Recovery System is necessary for data resilience, ensuring that in the event of data loss or corruption, the system can be restored to a consistent state. Threat Detection & Prevention System provides real-time visibility into activities, enabling the detection and

	A4: Incident Response Service: This artifact manages responses to security incidents and logs incidents for further analysis.	response to potential security threats or unauthorized actions. Together, these artifacts form essential components of the system's security infrastructure, contributing to its overall resilience and protection against security breaches.
Environment	E1: Normal Operating Conditions: Represents typical system operation without active security incidents. E2: Incident Response Mode: Indicates situations where security incidents are detected and response mechanisms are activated.	Describing the environment as operational conditions helps to contextualize the scenarios in which security threats may occur, allowing for appropriate responses strategies.
Response	R1: Automated Threat Detection: Automated systems and algorithms detect, mitigate and block security threats in real-time. R2: Manual Investigation and Response: Security personnel investigate detected threats and take manual actions to mitigate them.	The response represents the actions taken by the LnUShop system to mitigate security threats and protect against potential breaches. Variants like automated threat detection and manual investigation are the mechanisms employed for threat mitigation.
Response Measure	RM1: Detection Rate: Percentage of security threats detected by the system. RM2: Detection Time: Time taken to identify the security threats and the initiation of appropriate actions to respond to the threats.	Defining response measures like threat detection rate and detection time helps to assess the effectiveness of the security mechanisms in place and identify areas for improvement in the system's security posture.

Task 3



Access Control System:

Responsibilities: Manages user authentication processes, including password verification, session management, and role-based access control.

Provides interfaces:

Incident Response system: provides alerts for suspicious authentication activities.

Requires interfaces:

Incident Response system: requires incident notifications for authentication-related issues.

Threat Detection & Prevention System:

Responsibilities: detects security threats such as SQL injection and XSS attacks using recognition and detection techniques;monitors processes in real-time for suspicious activities, utilizing predefined rules and machine learning models.

Provides interfaces:

Database system: provides alerts for detected threats and blocks abnormal queries.

Incident Response system: provides information on detected threats for immediate action.

Backup and Recovery system: provides early warnings and information about potential threats for necessitate data backup or restoration effort to maintain data integrity.

Requires interfaces:

Database system: requires detailed query analysis to identify potential threats.

Incident Response system: requires incident notifications for detected threats for appropriate response and resolution such as initiating recovery protocols.

Database System:
Responsibilities: Manages data storage, retrieval and manipulation while implementing security measures to prevent SQL injection and ensure data integrity.
Provides interfaces:
Backup&Recovery system: provides the initiation of backup procedures and orchestrates the execution of data restoration commands.
Threat Detection&Prevention system: provides access for query analysis to detect potential threats.
Requires interfaces:
Threat Detection & Prevention system: requires query analysis to identify security vulnerabilities such as SQL injection areas susceptible to data breaches.
Backup and Recovery system: requires backup initiation and restoration commands to ensure data integrity and continuity.

Backup and Recovery System:
Responsibilities: Handles regular data backups and provides restoration functionalities in case of data loss or corruption.
Provides interfaces:
Database system: provides backup and restoration processes for ensuring data resilience against security breaches.
Requires interfaces:
Database system: requires data backup and restoration to maintain data integrity.
Incident Response system: requires incident notifications related to data recovery actions for immediate response and resolution.
Threat Detection & Prevention System: requires alerts and information on potential threats to create backups before potential breaches.

Incident Response system:
Responsibilities: Manages responses to security incidents, including threat isolation, mitigation actions and incident logging for further analysis.
Provides interfaces:
Access Control system: provides user authentication data for incident correlation.
Threat Detection & Prevention system: provides alert notifications for incident response coordination.
Backup & Recovery system: provides alerts for data recovery actions.
Requires interfaces:
Access Control system: requires incident notifications related to authentication issues for correlation and response..
Threat Detection & Prevention system: requires incident notifications for detected threats for appropriate response and resolution.

Task 4

For the Performance Architecturally Significant Requirements for the LnUShop system, initially we navigate through a design space that considers two architectural strategies.

Architecture Considerations
The primary goal is to ensure that the system can handle peak loads efficiently and manage a high number of concurrent user interactions without performance degradation and ensure response times within 10 seconds for various user actions.

Options: *Monolithic Architecture, Microservices Architecture.*
Option chosen: Microservices Architecture
Motivation: It is a decentralized approach, where each service (e.g., user registration, search and filter, transactions) is developed, deployed, and scaled independently. This architecture can more readily adapt to varying loads, improving the system's ability to maintain performance under stress, distributing the load more effectively and ensuring responsiveness.

Database Management and Caching Strategy Considerations
Within the chosen *Microservices* frame, we further explore *Database Management options and Caching Strategies,* which are the read and write operations with a need for high concurrency:

***Database Management*:**
Options: Traditional relational databases, NoSQL databases.
Chosen option: NoSQL databases
Motivation: NoSQL databases provide much more advantages for unstructured data and high-volume transactions to meet the performance requirements.

***Caching Strategies*:**
Options: In-memory data stores like Redis, Content Delivery Network (CDN) Caching.
Option chosen: In-memory data stores.
Motivation: It can cache frequently accessed data, such as product listings and user profiles, significantly reducing response times for read-heavy operations, meeting the performance requirements.

Conclusion
The architectural discussion through the design space for the LnUShop system concludes with the selection of a Microservices Architecture, complemented by selecting NoSQL from Database Management strategies and in-memory Caching Strategy, this architecture is aimed to meet the performance ASRs, providing an efficient system capable of delivering a good shopping experience even during peak periods. Each decision in this funnel narrows the design space, focusing on solutions that best suit the system’s performance goals.