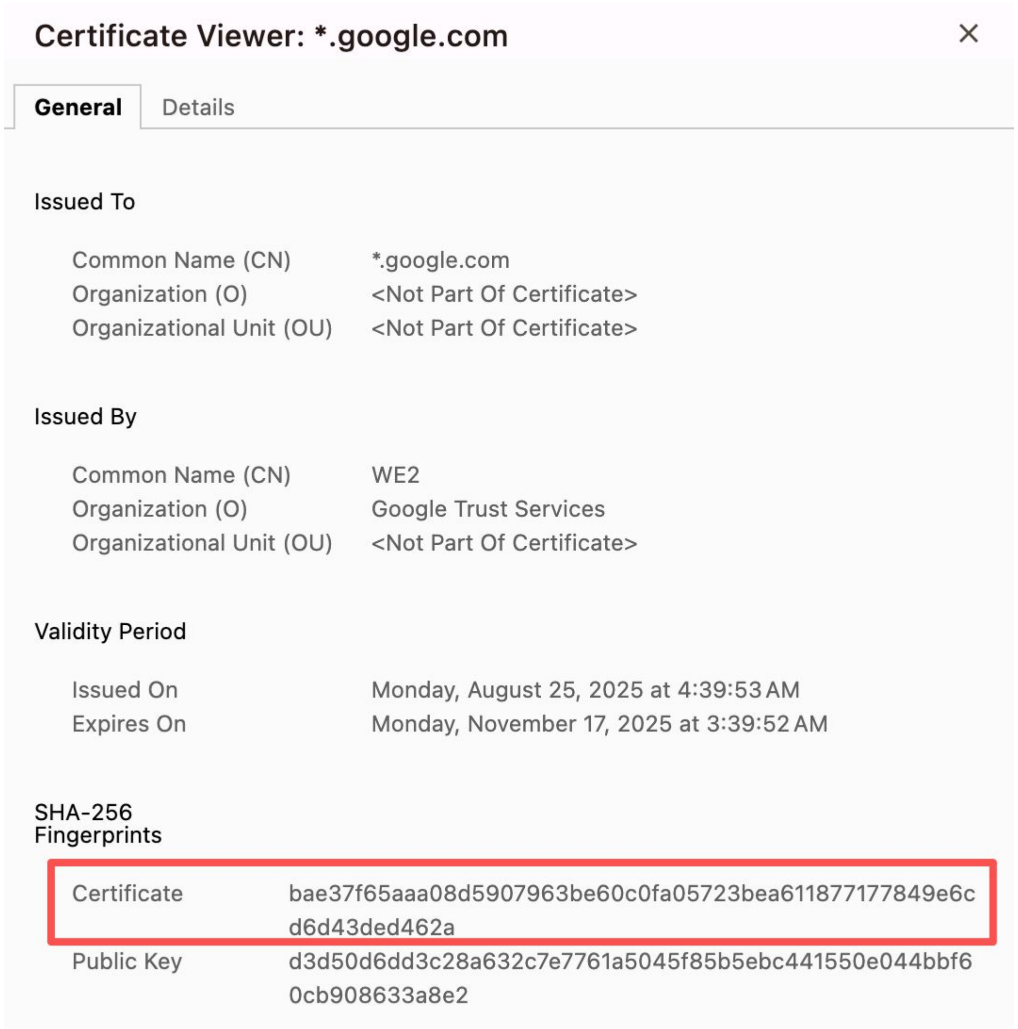


Certificate Viewer: *.google.com

Issued To

Common Name (CN)	*.google.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	WE2
Organization (O)	Google Trust Services
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Monday, August 25, 2025 at 4:39:53 AM
Expires On	Monday, November 17, 2025 at 3:39:52 AM

SHA-256 Fingerprints

Certificate	bae37f65aaa08d5907963be60c0fa05723bea611877177849e6cd6d43ded462a
Public Key	d3d50d6dd3c28a632c7e7761a5045f85b5ebc441550e044bbf60cb908633a8e2

Question 1:

How to generate the certificate ID？

Why we need certificate?

Microsoft Authenticator

Question 2:
2 factors
Or 3 factors？

The Answer should be 2 factors, because the UM server does not require facial regnization.

Question 3:

Why hash code can not be the digital signature??

And why need private key to encrypt it?

csc116 Access Control: Role-based Access Control, Fine-grained Access Control

What is Access Control?

Definition: **Restricting unauthorized access to systems/data.**

Importance: Security, compliance, data protection

Data Privacy

5 Access Control Methods

- **Discretionary Access Control (DAC)**: The owner of the resource decides who gets access, e.g., file sharing permissions in Windows.
- **Mandatory Access Control (MAC)**: Access is determined by a central authority based on classifications. **Example: Military or government systems.**
- **Role-Based Access Control (RBAC)**: Access is based on the user's role within an organization. **Example: Admins have more privileges than regular users.**
- **Attribute-Based Access Control (ABAC)**: Access is granted based on a combination of attributes (e.g., time of access, location, or like majors). Also, named **fine-grained access control.**

Fine-grained access control

Fine-grained access control allows for **very detailed, specific rules** about who can access what, under precise conditions.

“Only employees in the Finance department can access payroll data, but only during business hours and from a secure company device.”

“A doctor can access patient records, but only for patients assigned to them and only from within the hospital network.”

Question 1：In a military database, documents are labeled as "Top Secret," "Confidential," or "Public." Only users with the appropriate security clearance can access certain documents, regardless of their role.

Which access control model is being used?

A) Role-Based Access Control (RBAC)

B) Discretionary Access Control (DAC)

C) Mandatory Access Control (MAC)

D) Attribute-Based Access Control (ABAC)

Question 2：A hospital system allows doctors to access patient records only if they are the primary physician assigned to that patient, and only while they are inside the hospital premises.

Which access control model is being used?

A) Discretionary Access Control (DAC)

B) Role-Based Access Control (RBAC)

C) Attribute-Based Access Control (ABAC)

D) Mandatory Access Control (MAC)

Authorization and Access Control

1. **Access Control**
   This is a broader concept that refers to the entire process of **managing and restricting access to resources**.

   It includes:

- **Authentication**: Verifying the identity of a user, such as through passwords, biometrics, or multi-factor authentication.
- **Authorization**: After authentication, determining what resources the user is allowed to access and what actions they can perform.
- **Auditing**: Monitoring and recording access activities to detect and respond to anomalies.

Access Control

- **Authentication:** When a user tries to log into the EHR system, they must verify their identity using their university credentials, such as a username and password, or even multi-factor authentication (e.g., using a secure token).
- **Authorization:** Once authenticated, the system checks what specific permissions the user has. For example:
    - Medical students may be authorized to view patient records but cannot edit or delete them.
    - Professors and licensed physicians may have authorization to both view and update patient records.
- **Auditing:** Detecting unauthorized attempts or suspicious activities.

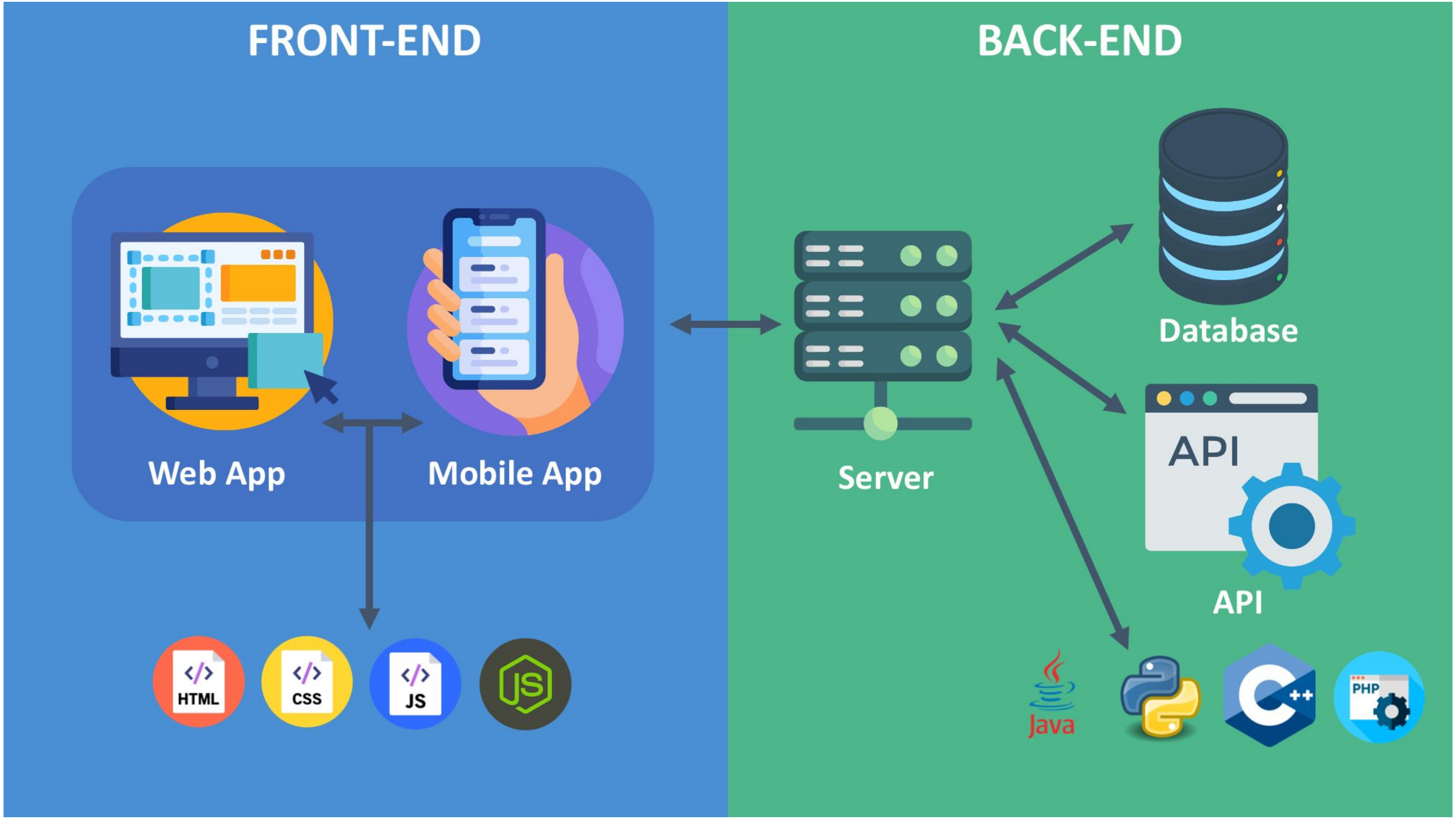
Access Control is the overall process that includes verifying identities, assigning permissions, and monitoring activities. (Much broader)

Authorization is the step that **determines what resources and actions** an authenticated user can access within the system.

Principle of Least Privilege

The **Principle of Least Privilege (PoLP)** is a fundamental cybersecurity concept that states **users, applications, and systems should be granted the minimum level of access—or permissions—necessary to perform their specific tasks** and nothing more.

How to implement Role-based Access Control？



FRONT-END

BACK-END

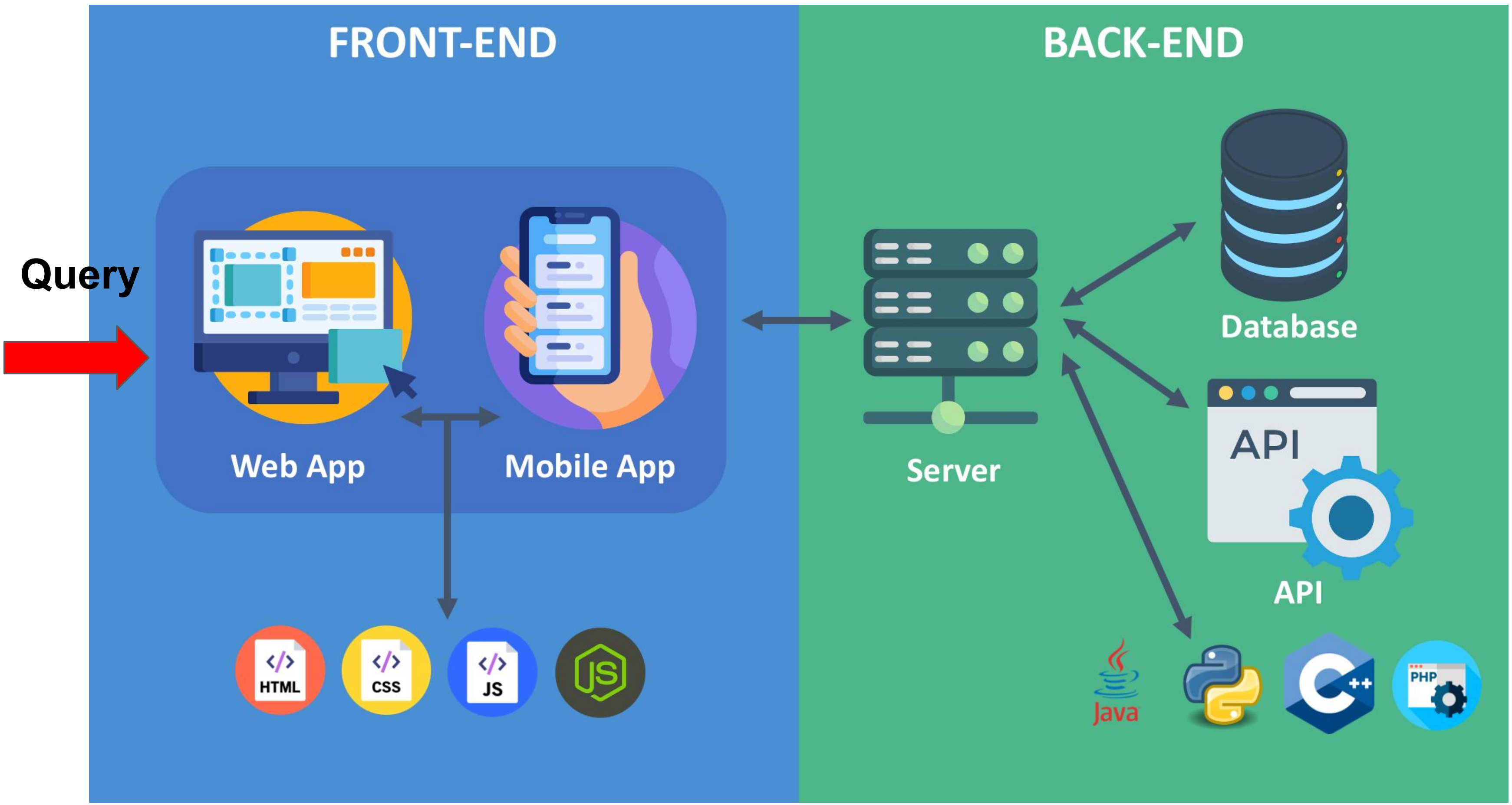
Web App

Mobile App

Server

Database

API

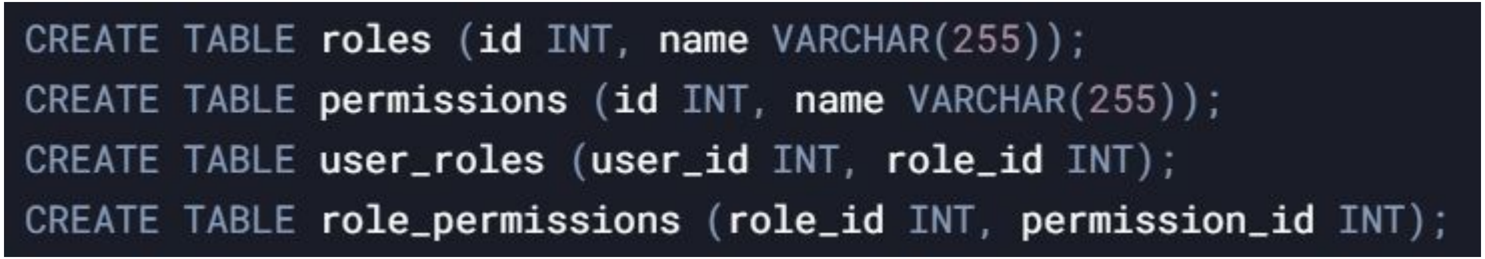

Query

FRONT-END
BACK-END
Web App
Mobile App
HTML
CSS
JS
Server
Database
API
API
Java
PHP

Design an Access Control Database

Access Control Lists (ACL)

- **Users**: Store user details (e.g., `id`, `username, hash_password`).
- **Roles**: Define roles (e.g., `admin`, `patients, nurses, doctors`).
- **Permissions**: List actions (e.g., `read`, `write, update, remove`).
- **User_Roles**:
- **Role_Permissions**:



```
CREATE TABLE roles (id INT, name VARCHAR(255));
CREATE TABLE permissions (id INT, name VARCHAR(255));
CREATE TABLE user_roles (user_id INT, role_id INT);
CREATE TABLE role_permissions (role_id INT, permission_id INT);
```

Question：

If a web system with low quality access control, and the attackers modified the EHR patient records.

What is the next step if you are a developer?

Data Backup and Disaster Recovery

Data Backup and Disaster Recovery are essential components of cybersecurity, particularly in environments like healthcare where data loss can directly impact patient care and organizational operations.

Data backup refers to the process of creating copies of important data and storing them in a separate, secure location. This ensures that if the original data is lost, corrupted, or compromised (due to hardware failure, human error, cyberattacks like ransomware, or natural disasters), you can restore it from the backup.

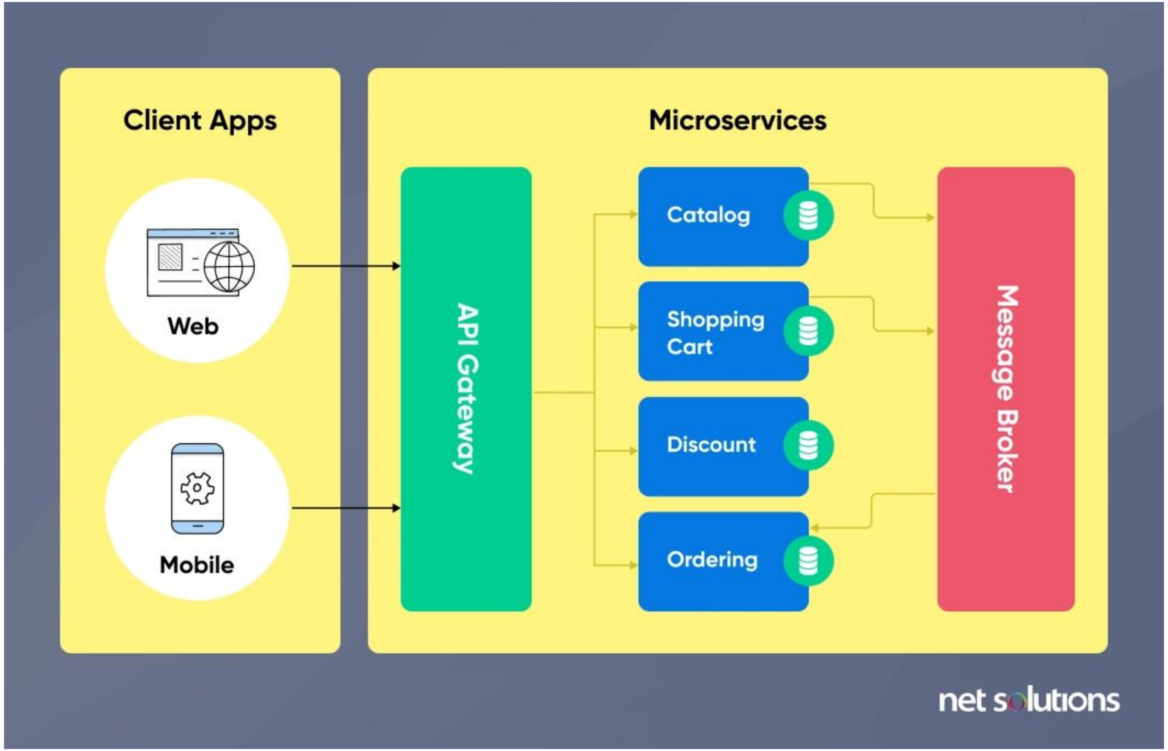
Data backup and Local Storage

Local storage is a dedicated backup drive at your place of business where you make Full, Incremental, or Differential copies of your data.

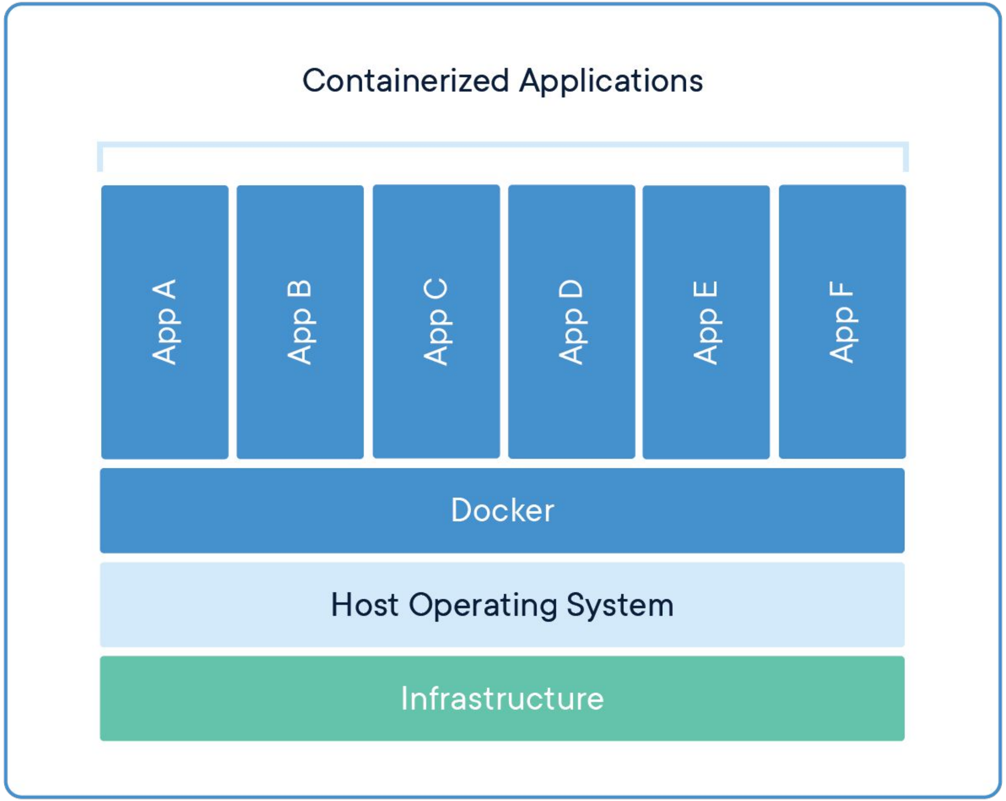
Data backup and Cloud Storage

Cloud Storage is a virtual platform that provides off-site, scalable storage resources, dynamically provisioned per the business’s technical requirements.

Distributed Storage Systems for Micro-Services

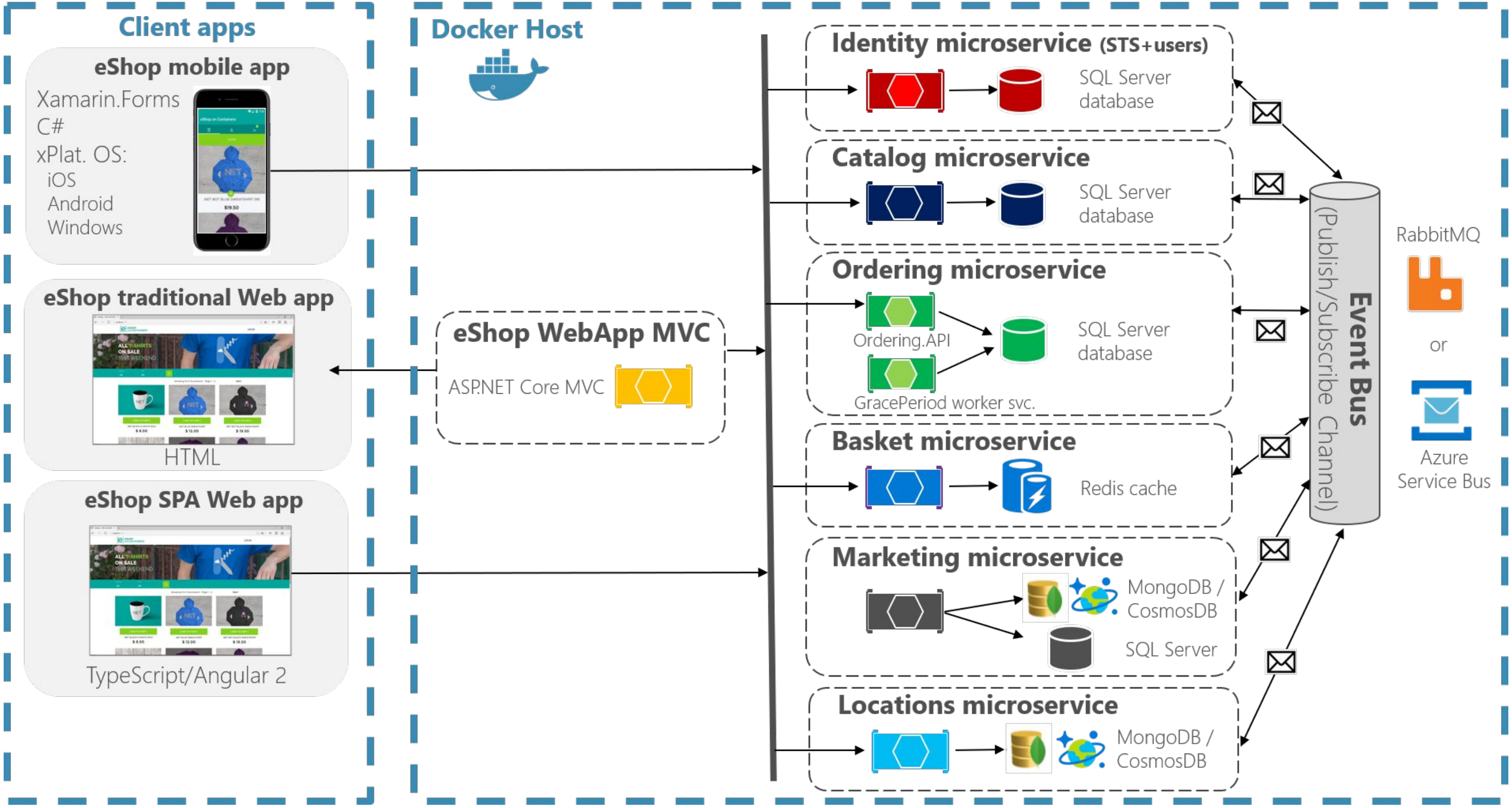


Docker Container



eShopOnContainers reference application

(Development environment architecture)



Amazon Distributed Data Centers

https://www.datacentermap.com/c/amazon-aws/datacenters/

Conclusions

Distributed storages can mitigate the whole databases be attacked.

It separates the whole services into different micro-services to improve the development speed.