**Mobile Applications**

1. IDEs:

Android: Android Studio, Visual Studio – Xamarin, Unreal Engine, PhoneGap, Corona, CppDroid, AIDE, IntelliJ IDEA.

iOS: Xcode, Swift and Appcode

(Swift: Swift is a general-purpose, multi-paradigm, compiled programming language developed by Apple Inc. for iOS, macOS, watchOS, tvOS, Linux and z/OS. Swift is designed to work with Apple's Cocoa and Cocoa Touch frameworks and the large body of existing Objective-C code written for Apple products.

Xcode is IDE, Swift is language)

Windows: Visual Studio

1. Offline database for mobile – SQLite, Realm DB, ORMLite, CouchDB

It is useful as we can store user info, etc inside the device memory itself.

1. Stores to publish apps:

Android: Play store, Amazon Appstore, Mobogenie, 1Mobile, SlideME

iOS: Apple store

Windows: Windows store

1. Mobile app Security:

**Hackers with malicious intent can:**

* Inject malware into apps and onto devices where it can access data, store keystrokes, and steal screen lock passcodes
* Tamper with or copy your app’s code and reverse-engineer a spoof app containing malware
* Intercept sensitive information traveling over the airwaves
* Steal customer data for identity theft or fraud purposes
* Get hold of intellectual property and private business assets
* Access your IP or compromise your company’s back-end network

1. Security Measures:
2. SECURE YOUR APP’S CODE FROM THE GROUND UP. (encrypt app code by obfuscation or minification)

Obfuscation: obfuscation is the deliberate act of creating source or machine code that is difficult for **humans** to understand. Like obfuscation in natural language, it may use needlessly roundabout expressions to compose statements.

Eg. PHP – Base64, eval(), GLOBAL()

Javascript – Base64, EVAL

### SECURE YOUR NETWORK CONNECTIONS ON THE BACK END. (cONTAINERIZATION, vpn, ssl)

### PUT IDENTIFICATION, AUTHENTICATION, AND AUTHORIZATION MEASURES IN PLACE. (OAUTH2, JSON WEB TOKENS, OPEN-ID CONNECT)

### BE MINDFUL OF HOW CUSTOMER DATA IS SECURED AND IMPLEMENT A GOOD MOBILE ENCRYPTION POLICY. (FILE LEVEL ENCRYTION, DATABASE ENCRYPTION, KEY MANAGEMENT)

### HAVE A SOLID API SECURITY STRATEGY IN PLACE. (identification, authentication, authorization)

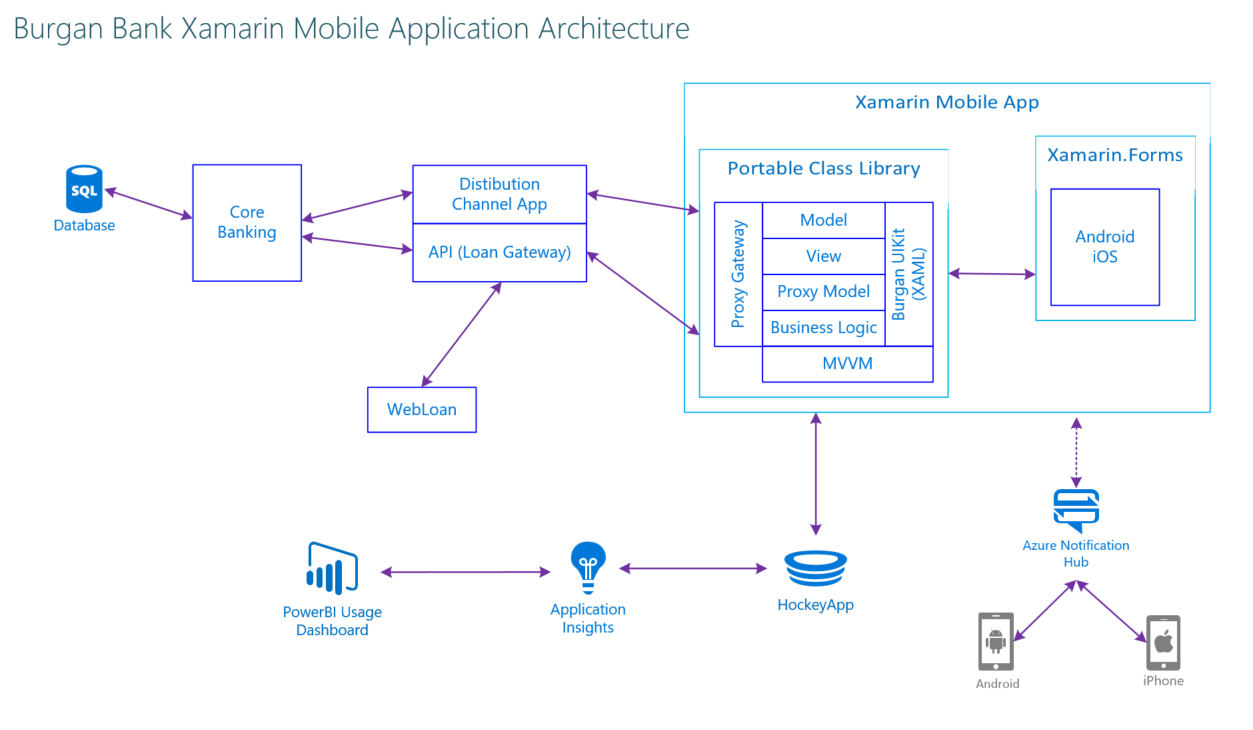
### TEST YOUR APP SOFTWARE—THEN TEST AGAIN. (Penetration testing)

### USERS: PROTECT YOUR DEVICES. (don’t root or jailbreak as it negates the built in security measures and hence your device becomes vulnerable)

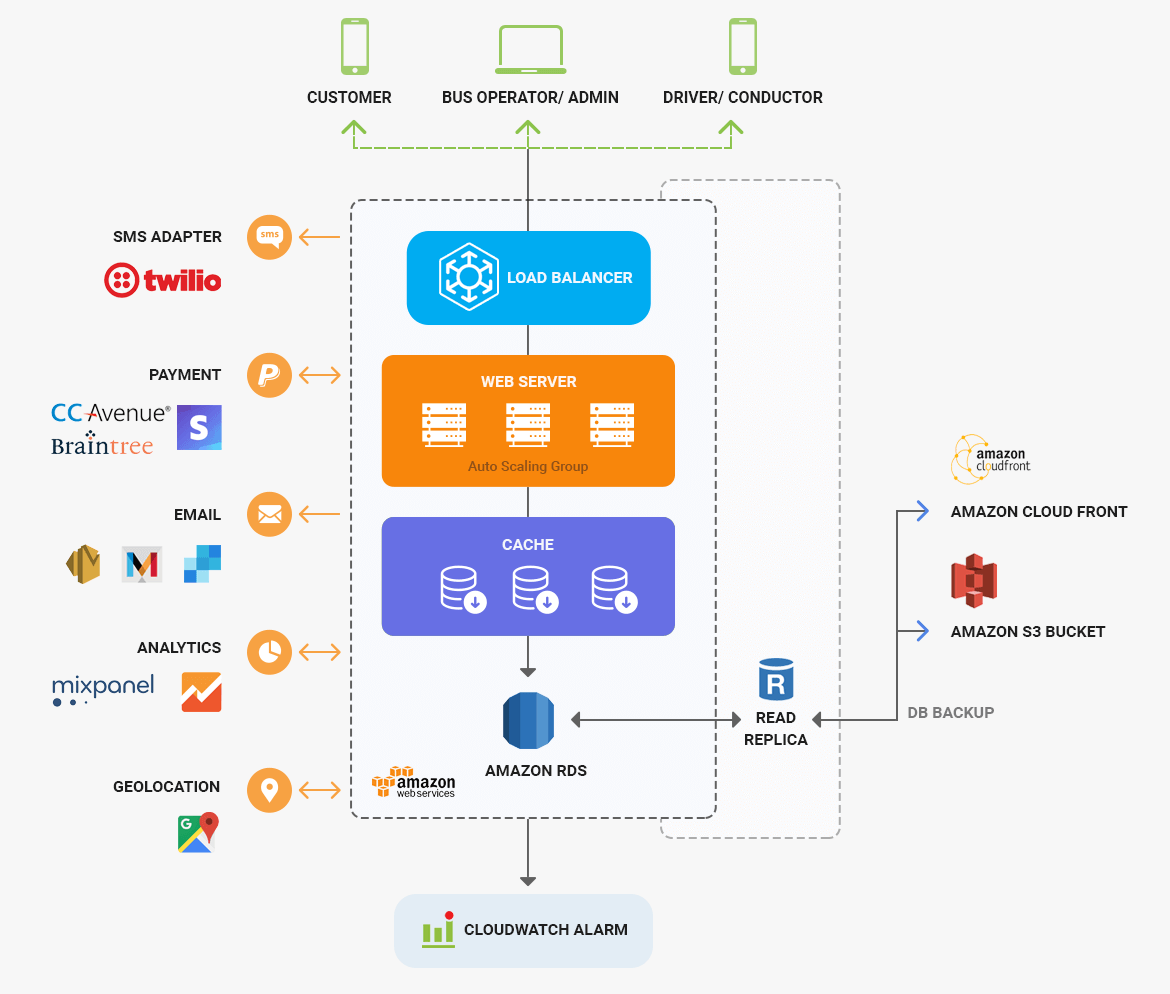
### IF YOU’RE AN ENTERPRISE ORGANIZATION WITH A BYOD (BRING YOUR OWN DEVICE) POLICY, USE EXTRA CAUTION.

### Mobile Software Architecture:Related image

1. Banking Architecture:



Reservation Architecture:



Today -

Payment Gateway and architecture

Types of Payment options(India and abroad)

Embedded Programming - Automotive

AR, VR – Mobile

Thursday – IOT

Friday – 3D Painting

Monday – Big data analytics

Tuesday - Digital Marketing – components, tasks

Wednesday - Gaming

After that –

Telecom(If interested)

Media and Animation

Simulations, CAD,CAM, Design

AI