Final Security Mechanisms Report

Mobile Platform	iOS App
Application domain type	m-Health
Authentication	Yes
Authentication schemes	Biometric-based authentication ; Factors-based authentication
Has DB	Yes
Type of database	SQL (Relational Database)
Which DB	SQLite
Type of information handled	Personal Information ; Confidential Data ; Critical Data
Storage Location	Remote Storage (Cloud Database)
User Registration	Yes
Type of Registration	Will be an administrator that will register the users
Programming Languages	C/C++/Objective-C
Input Forms	Yes
Upload Files	No
The system has logs	Yes
The system has regular updates	Yes
The system has third-party	Yes
System Cloud Environments	Private Cloud
Hardware Specification	Yes
HW Authentication	Basic Authentication (user/pass)
HW Wireless Tech	3G ; 4G/LTE ; 5G ; Bluetooth ; Wi-Fi ; GPS ; RFID ; NFC
Device or Data Center Physical Access	Yes

Security Backup Mechanisms

Security Backup Mechanisms for cloud-based mobile apps are procedures to keep data safe and secure in the event of an emergency, such as a computer crash, a user error, or a malicious attack. These mechanisms can include:

â€¢ Access Control: Access control restricts the access of certain parts of the application, such as confidential data or the applicationâ€™s backend, in order to limit the potential damage caused by malicious activities.

â€¢ Data Encryption: Data Encryption scrambles application data into an unreadable format, making it impossible to access without the decryption key.

â€¢ Password Hashes: Password Hashes are securely stored versions of the usersâ€™ passwords to prevent malicious activities such as credentials theft.

â€¢ Tokenization: Tokenization is a mechanism that replaces sensitive data with a token to reduce the risk of data theft.

â€¢ Backup System: A backup system can be used to store application data in separate, secure locations. This data can be used to restore the application to its former state in the event of a disruption.

Backup Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer
Backup	iOS	iTunes Backup	Syncs with iTunes for off-site backup	7 - Application
Backup	Android	Google Drive	Google's cloud solution for data storage and backup	7 - Application
Backup	Android	Third-party cloud solutions	Solutions such as Dropbox, OneDrive and iCloud Drive	7 - Application
Backup	All	Local Backup	On-site backups saved on the device's internal storage	1 - Physical
Backup	All	External Storage Backup	Off-site backups saved to external devices such as external hard drives and USB drives	1 - Physical

Security Audit Mechanisms

A Security Audit Mechanism is an automated or manual process which evaluates cloud-based mobile apps for security issues. It may include verifying the integrity of the code, inspecting system configurations, testing user authentication and authorization controls, and ensuring that the system is following best practices such as encryption, patching, and regular system updates. A Security Audit Mechanism can also identify potential security weaknesses and provide recommendations for mitigating these. Furthermore, a Security Audit Mechanism can perform performance and reliability checks, as well as other security checks such as penetration testing, infrastructure testing, and security vulnerability scanning. By utilizing these security audit mechanisms, organizations can ensure their cloud-based mobile apps are safe and secure.

Audit Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer
Authentication	iOS	Appleâ€™s App-ID and two factor authentication	A two-factor authentication and App-ID system used by Apple to verify and authenticate applications running on its iOS mobile platform	Application
Authorization	iOS	Access control list (ACL)	A tool used to manage user access to various parts of a mobile application, such as data or services	Application
Data Protection	Android	Google Play Store	Googleâ€™s Play Store protects uploaded applications from malicious code before it is distributed on the platform	Presentation
Auditing	iOS	App Store	The App Store provides an audit trail of all applications downloaded, to ensure proper users have the correct permissions to access applications	Application
Data Validation	Android	Android Content Providers	Android content providers are used to securely store data and detect malicious code before it is passed to applications running on the platform	Application

Cryptographic Algorithms Mechanisms

Cryptographic algorithms are used to ensure data confidentiality, authenticity, integrity and non-repudiation in cloud-based mobile apps. To achieve these goals, cryptographic algorithms are often used in combination with mechanisms, such as Digital Signatures, Secret Key Cryptography and Public Key Cryptography.

Digital Signatures validate the identity and authenticity of communications, while Secret Key Cryptography algorithms like AES, DES and 3DES protect transmitted data through the use of encryption. Public Key Cryptography algorithms like RSA, ECDSA and Diffie-Hellman can also be used to authenticate, encrypt and exchange secret keys between the mobile device and the cloud provider. In addition, protocols such as SSL / TLS can add an extra layer of security while protecting and verifying the communication and providing message integrity.

Cryptographic Algorithms Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer	Use for coding	Use for runtime
Integrity	Android	HMAC-SHA256	A cryptographic hash function based on SHA256 that combines a shared secret and the message	7	Yes	Yes
Confidentiality	iOS	AES-128	AES with 128 bit key size that supports authenticated encryption	6	Yes	Yes
Authentication	iOS	ECDSA	Elliptic Curve Digital Signature Algorithm that provides digital signatures	7	Yes	Yes

Biometric authentication mechanisms in cloud-based mobile apps are methods of authentication relying on the physiological characteristics of a user as a method of accessing the device or application. Examples of popular biometric authentication technologies available for cloud-based mobile devices are fingerprint scanning, facial recognition, and voice recognition. These technologies use advanced algorithms to validate a userâ€™s identity based on the physiological traits unique to each individual. By using these methods, companies and app developers can increase the security of their cloud services while preventing unauthorized access.

Biometric Authentication Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer
Authentication & Access Control	Android	Facial Recognition	Hardware based biometric authentication that uses the device front facing camera to snap a picture of the user's face and match it against stored images	Application

Authentication & Access Control	iOS	Voice Recognition	Software based biometric authentication that uses the device microphone and internal software to capture the user's voice and match it against stored audio	Application
Encryption & Decryption	Android	2-Factor Authentication with PIN & Pattern	Combined hardware and software based authentication that requires the user to enter a PIN and draw a pattern on a defined pattern grid.	Presentation
Encryption & Decryption	iOS	Retina Recognition	Hardware based biometric authentication that uses the device front facing camera to obtain a high-resolution picture of the user's eye and matches it against stored images	Application
IDS & IPS	Android	Fingerprint Scan	Hardware based biometric authentication that uses the device built-in fingerprint scanner to scan the user's fingerprint and match it against stored images	Application
IDS & IPS	iOS	3-Factor Authentication with PIN, Pattern & Password	Combined hardware and software-based authentication that requires the user to enter a PIN, draw a pattern on a defined pattern grid, and enter a password	Presentation

Factors-based authentication mechanisms in cloud-based mobile apps are methods used to securely access digital resources. They involve the use of two or more authentication factors, such as something that a user knows (e.g., a password), something that a user has (e.g., an authentication code sent to a mobile device), and/or something that a user is (e.g., a biometric scan). Factors-based authentication can help protect mobile apps by providing an extra layer of security, making it less likely that someone unauthorized can access sensitive user data.

Factors-based Authentication Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer	To Use
Data Security	iOS	Two-factor authentication	Confirming identity by combination of two unique factors	Application	Coding Phase and Runtime
Privacy	Android	Biometric authentication	Confirming identity by using biometric methods	Application	Coding Phase and Runtime
Account Access	iOS	User ID & Password	Confirming identity by using combination of user ID and password	Application	Coding Phase and Runtime

Cryptographic Protocols Authentication Mechanisms

Cryptographic protocols mechanisms for cloud-based mobile apps refer to the cryptographic techniques used to protect data and communications between user devices and cloud-services. The protocols involve the encryption of data and messages with symmetric and asymmetric algorithms, the digital signing of messages, the authentication of users, the establishment of secure tunnels, and the use of secure hashing and salting. The goal is to ensure that, if a malicious person attempts to intercept the headers or payload of a cloud-based mobile app, they will be unable to access valuable information.

Cryptographic Protocols Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer
Authentication	iOS	OAuth	OAuth is an open-standard authorization protocol for allowing access to a protected resource	Application layer
Encryption	Android	TLS	Transport Layer Security (TLS) is a cryptographic protocol used to provide secure communications over a computer network	Transport Layer

Integrity	iOS	SHA-1	Secure Hash Algorithm (SHA-1) is a cryptographic hash function used to generate a 160-bit hash value	Application layer
Non-repudiation	Android	HMAC	HMAC is a cryptographic mechanism used to verify the integrity of a message by using a secret key	Application layer

Access Control Mechanisms

Security Access Control Mechanisms (SACMs) are the technical and administrative strategies and tools used to protect cloud-based mobile apps from unauthorized access to confidential data and systems. These mechanisms are designed to restrict access to certain users, manage user privileges, authenticate user accounts, and authorize access requests. Examples of SACMs include multi-factor authentication (MFA), biometric authentication, single-sign-on (SSO), role-based access control (RBAC), application-level encryption, and least privilege access. SACMs allow organizations to properly control who has access to what resources and strictly enforce principles of confidentiality, privacy, and data security.

Access Control Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer
Data confidentiality	Android	RSA Encryption	Encryption of data with public and private keys	Application
Data integrity	Android	Hashing	Use of a hash algorithm such as SHA-2 to ensure that data is not tampered with	Transport
Account Management	iOS	Two-Factor Authentication	Use of two-factor authentication to verify user access	Presentation
Data access control	iOS	Role-Based Access Control (RBAC)	Defines levels of access based on user roles	Application
Resource authorization	iOS	Authorization Token	Generates a token at the end of a successful authorization process which is used to grant permission	Application

Inspection Mechanisms

An inspection mechanism is a process or tool used to ensure that cloud-based mobile apps meet certain quality and security requirements. Inspection mechanisms involve thoroughly evaluating the source code, architecture, and security of the app to ensure it meets the desired standard. Examples of inspection mechanisms include static code analysis, application security testing, architectural design reviews, and penetration testing. These inspection mechanisms help identify any weaknesses, vulnerabilities, or security issues in the app before it is deployed in the cloud.

Inspection Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer
Integrity	Android	ProGuard	Code obfuscation	8
Confidentiality	iOS	Secure store	Keychain security	7
Authentication	Android	SafetyNet API	Attest the device integrity	7
	Android	Android Keystore	Keystore security	7
	iOS	Apple push notification service (APNS)	Authentication message	7
Data Validation	Android	DX Guardrail	Verification of data model	7
	iOS	SwiftLint	Static analysis	7# Logging Mechanisms

An inspection mechanism is a process or tool used to ensure that cloud-based mobile apps meet certain quality and security requirements. Inspection mechanisms involve thoroughly evaluating the source code, architecture, and security of the app to ensure it meets the desired standard. Examples of inspection mechanisms include static code analysis, application security testing, architectural design reviews, and penetration testing. These inspection mechanisms help identify any weaknesses, vulnerabilities, or security issues in the app before it is deployed in the cloud.

Logging Mechanisms Examples:

Security Requirement	Mobile Plataform	Mechanism	Description	OSI Layer
Authentication	iOS	DeviceCheck	DeviceCheck enables customers to securely store small bits of data on Apple devices during the coding and runtime phases	Application

Access Control	iOS	KeyChain	Appleâ€™s Keychain, is a encrypted storage system that primarily stores passwords, certificates, and encryptionkeys	Application
Auditing	Android	Syslog	System logging mechanism for capturing and persistently logging system and audit-specific events in the Android OS	Transport
Logging	Android	LumberJack	Logging mechanism for logging the events for mobile applications	Application

Device Detection Mechanisms

Security Device Detection Mechanisms in Cloud-based mobile apps are technologies responsible for detecting the mobile device that is used to access the application. The mechanisms can vary from OS-level or device-level properties and can include biometrics such as facial recognition, fingerprint scanning, and voice recognition. These mechanisms allow cloud-based mobile apps to detect the device used and ensure that only authorized devices are able to access the app, providing an extra level of security against potential malicious activity.

Device Detection Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer
Coding Phase	iOS	Mobile App Wrapping	A tool used to secure enterprise apps	Application
Coding Phase	Android	App Reverse Engineering Protection	A technique used to protect code from reverse engineering	Application
Runtime	iOS	Jailbreak Detection	Detects if the device is jailbroken or not	Application
Runtime	Android	Root Detection	Detection of rooted devices	Application

Physical Location Mechanisms

Security physical location mechanisms are applied to cloud-based mobile apps to ensure that user data is not accessed or stored from locations outside of an approved geographic region. These mechanisms include technologies such as geofencing and IP address tracking. Geofencing verifies that user data is being accessed and stored within a predetermined geographic area by creating a virtual fence around the area. IP address tracking allows mobile apps to identify the geographical location associated with a particular IP address in order to verify that a user is located in the approved geographic area. These security location mechanisms are essential for cloud-based mobile apps, as they help prevent unauthorized access to user data from malicious actors located in remote locations.

Physical Location Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer
Authenticated Access	iOS	Biometric Scanner	Uses user's fingerprints as part of the authentication process	Physical
Data Integrity	Android	Transparent Encryption	Files are encrypted transparently and automatically	Network
Data Availability	Both	Secure Boot & Root	Ensures that all parts of system are authenticated and verified	Physical
Data Confidentiality	iOS	App sandboxes	Prevents unauthorized access to specific files	Application
Data Security	Android	Full Disk Encryption	Encrypts all data on device	Network

Confinement Mechanisms

Security Confinement Mechanisms in Cloud-based mobile apps refer to the various measures put in place by app developers to help ensure the security and integrity of data within the app. These mechanisms might include measures like authentication requirements, security protocols, encryption, tokenization, application sandboxing, and isolated virtual machines. These measures help limit the risk of data theft or compromise within a cloud-based mobile application.

Confinement Mechanisms Examples:

Security Requirement	Mobile Platform	Mechanism	Description	OSI Layer
Vulnerability Protection	Android	Flask	Flask is a Python web development framework used to protect against malicious code injections	Application Layer

Isolation of Data	iOS	Security-Enhanced Linux (SELinux)	SELinux is a Linux kernel security module used to isolate code from its data	Network Layer
Security of Data	Blackberry	BitLocker	BitLocker is a Windows data encryption system meant to protect data while it is stored	Data Link Layer
Secure Communications	Symbian	IPsec	IPsec is a protocol suite used in secure communication by authenticating and encrypting data	Presentation Layer
Secure Data Transfer	Palm	DM-Crypt	DM-Crypt is a drive encryption system meant to protect data while it is transferred	Session Layer