National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

# Mobile Security Challenges

## A Case Study of Mobile Financial Services

## Contributor

**Dr. V N Sastry**
Professor, IDRBT

# Table of
# CONTENTS

# Important **Abbreviations**

| | |
|---|---|
| DBT | Direct Benefit Transfer |
| PMJDY | Pradhan Mantri Jan Dhan Yojna |
| IMPS | Immediate Payment Service |
| AEPS | Aadhar Enabled Payment Setvice |
| UPI | Unified Payment Interface |
| BHIM | Bharat Interface for Money |
| BBPS | Bharat Bill Payment System |
| Bharat QR | Bharat Quick Response Code |
| NPCI | National Payment Corporation of India |
| NIPL | NPCI International Payments Ltd |
| IDRBT | Institute for Development and Research in Banking Technology |
| IIT | Indian Institute of Technology |
| REBIT | Reserve Bank Information Technology Pvt Ltd |
| IFTAS | Indian Financial Technology and Allied Services |
| MCX | Multi Commodity Exchange |
| NCDEX | National Commodity and Derivatives Exchange |
| CCIL | Clearing Corporation of India |
| RBI | Reserve Bank of India |
| TRAI | Telecom Regulatory Authority of India |
| DoT | Department of Telecommunication |
| MoC | Ministry of Communication |
| STQC | Standard for Testing and Quality Certification |
| DSCI | Data Security Council of India |
| NSE | National Stock Exchange |
| BSE | Bombay Stock Exchange |
| SEBI | Securities and Exchange Board of India |
| CDM | Cash Dispensing Machines |
| CCM | Cash Collecting Machines |
| CVM | Coin Vending Machines |
| NEFT | National Electronic Fund Transfer |
| RTGS | Real Time Gross Settlement |
| IFSMS | International Federation of Secure Mobile Services |
| PSP | Payment Service Provider |
| OWASP | Open Web Application Security Project |

1

# Introduction

Mobile Security is of paramount importance because of (i) exposure risk of Mobile Users Identity and misuse of Personal Data from the Mobile Device, (ii) large scale of Mobile User base covering almost the entire population getting threatened of new cybercrimes and (iii) unavoidable dependency of everyone on the mobile technology and mobile phone becoming the gateway for the digital world and digital personal assistant of the Mobile User.

As Bharat is progressing in a fast growth track to not only become a third largest world economy soon but is marching towards the goal of becoming the developed Nation before the Centenary Celebration of Independence in 2047 on account of its largest working youth and tech savvy population,  so through mobile phone technology everyone is expected to experience the digital transformation, digital infrastructure growth, effective utilization of resources, skills upgradation and interoperable mobile governance services in a seamless manner in the aspirational India in spite of natural and artificial disruptions. Mobile Technology will continue to play the most significant role in upliftment and growth. Mobile Device based Cyber Crimes are becoming rampant. There is urgent and greater need to focus on mobile security to preserve the continuation of public trust on digital services and reliability on every sectoral service offering.

The objective of this paper is to highlight the major challenges of mobile security that need to be focused by different entities involved in the mobile services ecosystem.  A Case study of mobile financial services specifically on mobile payments service is presented for illustration purpose and to demonstrate the various security measures being undertaken. This would help to understand and similarly develop secure mobile services to various other sectors.

# 2 Challenges

## 2.1 Roles and Responsibilities of Entities

It is to be ensured that the various entities involved in the mobile service ecosystem, such as mobile device manufacturer, mobile application developer, mobile network operator, mobile service provider, mobile app play store, security testing organization, government bodies providing mobile governance services, regulators and facilitators strictly follow their roles and responsibilities to offer secure public services in India and are held accountable for regulatory compliance and violations, if any.

## 2.2 Awareness and Skills Upgradation

Security is like cleanliness, which is every entity's responsibility. Lack of - digital literacy, awareness on security precautions, knowledge on technological changes, insecure use of mobile devices and social media by Mobile Users are giving easy way for targeted attacks and financial frauds. Continuous or Periodic Awareness Programs or campaigns for beginner, normal user and even for expert level user are necessary. User's knowledge on security precautions to be taken for mobile device security should be gradually upgraded to a mature level. If users are careful, many attacks on mobile device can be avoided, especially phishing and impersonating attacks. Mass scale awareness creation with demographically diverse and varied age group population is a big challenge. It is recommended for every sectoral entity offering mobile services to come forward to take the responsibility to conduct cyber and mobile security awareness programs or at least enable leaning through short videos or interactive games on mobile security tips to their employees of all levels, business partners and to their customers. Provide users with training on mobile communication security best practices. Teach them to recognize phishing attempts, avoid insecure public Wi-Fi networks, and maintain secure device configurations.

## 2.3 Understanding Security Clearly

Security is a subset of Risk Management of valuable assets, which if not taken care of, may lead to loss of value in terms of price, reputation, wealth, hygiene, time, data and deviation from achieving targets. Risks arise due to uncertainty and threat actors. Mobile Security Threats come from various threat actors known as Adversaries, Attackers, Hackers, Intruders, Interceptors, Impersonators, Eavesdropper, Malware, Spyware, Virus etc. The threat actors exploit the vulnerabilities in the protective mechanisms of the assets or the paths that lead to these assets. Mobile Security Vulnerabilities are weakness, gaps or loopholes in the protective mechanisms of digital assets, devices, interfaces and communication layers, which can be exploited by threat actors to gain unauthorized access to mobile device. Timely identification of the mobile security vulnerabilities, plugging and insulating them properly from threat actors or adversaries is a challenge.

## 2.4 Assessing the Intention of Threat Actors

A threat actor or adversary has malicious intention to identify the vulnerabilities or weakness or loopholes in the protective mechanisms of assets of Mobile Ecosystem and exploit them to gain unauthorized entry and access into user's Mobile Device to do mischievous activities. Stopping such actors is done through firewalls, anti-virus solutions, OS version upgrades, digital agents, AI tools etc. Although in the digital world it is impossible for a threat actor, whether insider or outsider, human or digital agent, to escape or get away unnoticed after committing a malicious activity provided proper security policies, continuous security monitoring, maintenance of logs for traceability and timely legal actions are followed. Trapping the threat actor using honey pots, use of event trackers and triggers, and maintaining traces of logs data for evidence can prove to be useful to get to the source and involved from behind in such culpable malicious activities.

## 2.5 Implementation of Security Goals Seamlessly

The Mobile Security Goals of Confidentiality, Integrity, Availability, Authentication, Authorization, Non-repudiation, Access Control, Traceability, Accountability, Trust and Reliability, which even though are well understood by people but the challenge is in their proper implementation and deployment in IT Systems by various entities of the mobile service ecosystem.

## 2.6 Secure SDLC and Security by Design of Applications

Mobile Ecosystem entities particularly Mobile Application developers should not only look into the required functionalities but follow the security by design philosophy and Secure Software Development Lifecycle (SSDLC) approach. These are necessary for new and existing mobile services to be re-designed with the UML diagrams embedding security goals to ensure end to end secure mobile transactions. It is to be ensured that secure coding practices are followed during the development of mobile apps, and regular security audits and vulnerability assessments are performed to identify and fix potential weaknesses in the mobile app's code.

## 2.7 Mobile Application Security

Ensure that the Mobile app is sandboxed so that it operates in isolated environments that prevent them from accessing unauthorized resources so as to reduce the risk of a compromised app affecting the security of other apps or the system. Use of Code Obfuscation Techniques and Reverse Engineering Protection techniques helps to protect against the de-compilation of an app and making it difficult for attackers to discover vulnerabilities. Regularly updating of mobile applications and operating systems helps to ensure they are protected from known vulnerabilities. Mobile OS updates typically include patches for security flaws that could be exploited in communication channels. Set up automated systems to manage the deployment of patches for mobile apps and operating systems to reduce the risk of leaving devices exposed to known security threats.

## 2.8 Multilingual Services to suit Indian Requirement

As India has multiple regional languages, in order to cater to wider spectrum of population, It is necessary to provide multi-lingual services in all the 22 National Languages in India. Bhashini Software of GoI is recommended for being used for the purpose. Multi-lingual mobile services may be provided across all mobile channels such as SMS, USSD, GPRS for Mobile Browser and Mobile Apps, Voice, IVRS and Multimedia services on 5G and 5G Advanced across all the mobile platforms. Language acts as a protective mechanism for the community users to safeguard from hackers as unknown code.

## 2.9 Location based Services preserving Privacy and Data Security

Location of a mobile user is identified by the location of the active mobile phone held along. Some mobile services may require location information of mobile user (i) to know delivery location for sending items ordered, (ii) to guide drivers of cabs or vehicles to reach to mobile user's correct location, (iii) to display travel route, traffic congestion, expected time, alternate routes and show nearby ATMs, hotels, places of visit etc., (iv) to help mobile banking apps to do dynamic authentication of transactions of the usual place of mobile user, (v) to do e-KYC or video-KYC of a mobile customer, (vi) to record it for specific purpose as digital evidence or for non-repudiation purpose etc.

Location information, co-ordinate data of current location, locations of places visited and the travel route history by the mobile user are critical which need to be kept confidential and should not be known or disclosed or seen by any unauthorized entity and to be protected from being misused. Mobile Users digital privacy and personal data of identity, location, traversed path and communication channels used are to be protected as per the Digital Personal Data Protection (DPDP) Act 2023 and subsequent rules in 2025. It is challenging to ensure that the consent and permission of a mobile user are taken to collect location information only when needed by the mobile user and stopped subsequently. Providers of Mapping services collecting location data should ensure that it is not used for any other purpose or AI agent.

Satellites play great role in the navigation services as Global Positioning System (GPS) location, such as Indian Regional Navigation Satellite System (IRNSS) called as Navigation with Indian Constellation (NavIC) by the Indian Space Research Organization (ISRO) to general public and authorized users. Emerging satellite services by external agencies as

Starlink need to comply to GoI regulations for mobile broadband services to protect the privacy of domestic mobile users as per the DPDP Act 2023.

## 2.10 Authentication Factors as per the risks of specific Sectoral Use Cases

It is to be ensured that in Mobile Service Ecosystem, four entities namely, Mobile User, Mobile Device, Mobile Application and Mobile Transaction channel are authenticated with proper authentication factors. Mobile User is verified by at least two of the three following factors of authentication (i) Knowledge factor or "what you know" like PIN, Password, relations, (ii) Possession factor or "what you have" like mobile phone or Card or wearable and (iii) Intrinsic factor or "what you are" like biometrics and behaviour aspects.

For Authentication user-id, password, OTP, biometric authentication of a mobile user using voice, face, fingerprint, iris, gait etc. captured by the inbuilt sensors of the smart mobile phone are useful. Mutual authentication helps to avoid man in the middle attacks by malicious entities such as intruders or impersonators. In case of direct authentication, authenticating entity itself registers and verifies, whereas in indirect authentication, these are done by other entities or third parties, so they should be trustworthy and tracked with proper service level agreements. For example, AADHAR based fingerprint or biometric authentication can be done by UIDAI indirectly for a Banking, Hospital or Vehicle License service transaction.

## 2.11 Supply Chain Service Composition using APIs and Micro-services

Mobile services have several component services, functions, micro-services and Application Program Interfaces (APIs) offered and executed by different entities within or outside India. For end-to-end secure mobile transactions, it is to be ensured that proper Service Level Agreements (SLA) between the provider and consumer are in place for their use and accountability and these are tested and certified to comply to fulfill security goals.

## 2.12 Layer wise Mobile Device Security

It is to be ensured that each of the 5 layers of the security capability framework of the smart mobile device namely, (i) the hardware at the bottom layer such as chip, flash, baseband, (ii) operating system above it such as Android or i-OS, (iii) peripheral interface involved with OS and hardware such as sensors, IoT connectivity, SIM, touch pad, database, (iv) application software layer on top such as installed apps, mobile browser, library and (v) the user data protection layer involved with hardware, OS and application software such as encryption/decryption, password and secure data storage are all tested to be secure and updated to ensure no known vulnerabilities. SIM being the gateway for the mobile device connectivity to the external world, is a potential target by adversaries to steal mobile user identity and commit frauds, so it needs to be properly protected.

## 2.13 End to End Security through Mobile Communication Channels

Ensuring the security of mobile communication channels is essential to protect sensitive information from interception, tampering, and unauthorized access. Mobile devices support various communication channels such as cellular networks (2G to 5G Advanced), Wi-Fi, Bluetooth, and messaging apps to transmit data, which can be vulnerable to various types of attacks, such as eavesdropping, man-in-the-middle (MITM) attack and spoofing. These mobile channels of wireless communication are categorized as :

| Mobile Communication | Short Range | Long Range |
|---|---|---|
| **Voice Channels** | Call, App Based, WiFi, BLE, Zig Bee, Embedded Wireless Mike and Speaker etc. | 2G to 5G Advanced, 6G, Satellite, VoIP, Call Centre etc. |
| **Data Channels** | SMS, USSD, RFID, NFC. Messaging Apps etc. | SMS, USSD, LoRA, Messaging Apps etc. |
| **Multimedia Channels** | Digital Audio and Video through WiFI, BLE and Mobile Apps as Shareit etc. | 3G to 5G Advanced, 6G, Satellite Phone, Dish Antenna, Mobile Broadband, Mobile Apps as WhatsApp etc. |

As mobile communication is an integral part of many business and personal activities, ensuring its security requires a holistic approach, combining technology, best practices, and user awareness. It is important to test, verify and certify that the security specifications of standards of these mobile communication channels of wireless communication are complied to the latest specifications before they are made available for public use and are upgraded from time to time, which is the responsibility of TRAI, MoC, DoT, TEC, TSDSI, BIS, STQC, DSCI, COAI, IAMAI, IFSMS, Mobile Telecom Operators and Mobile Device Manufacturers.

For secure mobile communication, ensure the following End-to-End Encryption (E2EE); Transport Layer Security (TLS); Wi-Fi Encryption using Wi-Fi Protected Access 3 (WPA3); Virtual Private Network (VPN) which encrypts the data traffic between the mobile device and the VPN server, preventing eavesdropping or MITM attacks on open networks; 5G Security, Multi-Factor Authentication (MFA), O-Auth and OpenID Connect to securely manage authentication without sharing sensitive credentials and protecting user accounts from unauthorized access; Signal Protocol for secure messaging based on strong encryption;

Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) for Emails encryption of messages and attachments; Certificate Pinning to embed a specific certificate or public key into the mobile app to check during the communication, whether the server's certificate matches the pinned certificate so as to prevent Man-in-the-Middle (MITM) Attacks which may use fraudulent certificates; Use of DNS over HTTPS (DoH) or DNS over TLS (DoT) to protect DNS queries from being intercepted or altered by attackers, which ensures that the mobile device can securely resolve domain names without exposing the query to attackers; continuous monitoring of mobile device traffic to identify suspicious activity, such as data exfiltration attempts or unusual communication patterns; Intrusion detection systems (IDS) or mobile threat detection solutions can alert administrators to potential security threats; Anomaly detection helps to identify unusual behaviours as sudden spike in traffic or abnormal destination IPs in mobile communications can indicate a security breach or attack; Bluetooth communications should be encrypted, and the device should only pair with trusted devices. Disable Bluetooth when not in use to reduce the attack surface and prevent unauthorized pairing or data interception; NFC communication is protected using encryption and that mobile device only accept communication from trusted sources. Use NFC-based payment systems (e.g., Apple Pay, Google Pay) that implement strong security protocols like tokenization; use Anti-Phishing software on mobile devices to detect and block malicious links, emails, and SMS messages; Enable features like URL filtering and domain blacklisting to reduce the likelihood of phishing; use mobile spam filters for SMS and email to prevent malicious links from being delivered through these communication channels.

## 2.14 Mobile Cloud Services Availability and Data Security

Ensuring mobile cloud security is critical because mobile devices access, store sensitive data and applications hosted on cloud environment. Proper service level agreement between the cloud service provider and mobile user is necessary to avoid data breaches, unauthorized access, and network vulnerabilities. It should also mention how the data privacy is ensured and if revoked, how it is deleted or passed onto the authorized person as per the consent of the Mobile User.

The cloud provider should implement Role-Based Access Control (RBAC) to restrict Mobile user access to only the cloud resources and data which is authorized to be used. This reduces the potential damage caused by unauthorized access. Single Sign-On (SSO) solution may allow users to access mobile cloud applications with a single set of credentials while maintaining security across multiple services. Securing mobile cloud environments involves a comprehensive approach that combines encryption, access control, mobile device management, API security, threat defence, and cloud-specific security best practices. By implementing robust security policies, using encryption, monitoring cloud activity, and educating users, organizations can minimize the risks associated with mobile cloud security. Regular audits and updates, along with proper governance and a Zero Trust security model, will further ensure that cloud resources remain secure from evolving threats. Ensure that cloud services (e.g., IaaS, PaaS, SaaS) are secured with the latest security features, such as encryption, firewall rules, and access controls. Cloud providers should offer robust security frameworks and compliance certifications (e.g., ISO 27001, SOC 2, GDPR). Ensure that data is stored in locations that comply with legal and regulatory requirements (e.g., GDPR, HIPAA). This is particularly important for organizations operating across different regions with varying data privacy laws. Maintain detailed logs of user activity and access to cloud resources. These logs should be regularly reviewed for suspicious activity and potential security breaches. Implement automated security monitoring tools to detect anomalies, unusual behaviour, and potential threats to cloud resources accessed via mobile device. Regularly generate compliance reports that demonstrate adherence to security standards, industry regulations, and internal policies. This is essential for audits and for maintaining cloud security. Implement a Zero Trust security model, where no device or user is trusted by default, regardless of whether they are inside or outside the network. Every access request to cloud resources is verified and authenticated, ensuring strict controls. Break down cloud networks into smaller, segmented areas, and apply security policies individually for each segment to limit the attack surface. Educate employees about the importance of downloading apps from trusted sources (e.g., Google Play, Apple App Store) and the risks associated with third-party or unverified apps. Implement a comprehensive disaster recovery plan that includes mobile devices and cloud systems, ensuring continuity of operations in the event of a security incident.

Users should understand the shared responsibility model in cloud security, where the cloud service provider is responsible for securing the infrastructure, while the organization which provides services on the cloud is responsible for securing data and applications running on the cloud. Regularly train mobile users on the risks of accessing cloud resources from mobile devices, how to avoid phishing attacks, the importance of strong authentication, and how to recognize suspicious behaviour. Ensure that data accessed and stored in cloud environments is regularly backed up and stored securely. In case of a data breach or cyberattack, these backups can be used to restore systems and data quickly.

## 2.15 Classification of Mobile Services, APIs and Micro-Services

The classification and indexing of mobile services, APIs, and microservices are essential for ensuring efficient organization, discovery, and integration of software systems. By categorizing services based on functionality, versioning, dependencies, and other attributes, organizations can optimize the discovery and integration of services. Implementing efficient classification and indexing systems using the right tools ensures better management, faster development cycles, and improved collaboration across teams. Important factors that need to be considered for Classification and Indexing are (i) Consistency in naming conventions, categorization, and documentation standards to make it easier for teams to understand and use services, (ii) Automation as the process of indexing APIs and microservices using tools like CI/CD pipelines, service discovery mechanisms, and API gateways to reduce manual errors and ensure real-time updates, (iii) Version Control to track versions of services, APIs, and microservices to maintain backward compatibility and support seamless integration, (iv) Tagging of labels to classify services based on functionality (e.g., "payment", "user-authentication", "geo-location") for easier filtering and search, (v) Security and Access Control for the services and APIs to ensure only authorized users can access and index them, (vi) Documentation for clear and consistent documents to support onboarding of new developers and maintain service usability.

To effectively manage classification and indexing, developers and organizations typically use specialized tools and platforms to automate and optimize the process. Some sample tools are (i) For API Gateways, tools as Kong, Apigee, AWS API Gateway provide centralized management of APIs and allow for the classification, routing, and indexing of APIs which can automatically track versions, monitor traffic, and handle authentication, (ii) For Service Discovery, tools as Consul, Eureka, Kubernetes Service Discovery provide indexing of microservices in a cloud-native environment ensuring services are easily discoverable by other services in the ecosystem, (iii) For API Management Platforms, tools as Postman, SwaggerHub, WSO2 API Manager provide support to catalogue, classify, and index APIs. They also facilitate documentation, testing, and collaboration across teams, (iv) For Service Catalogues, tools as ServiceNow, Red Hat OpenShift provide catalogue of services as APIs, mobile services, and microservices and allow users to classify, index, and monitor service performance.

### (A) Classification of Mobile Services, API and Micro-Services

Classification is the process of organizing and categorizing services based on their functionality, purpose, scope, and other relevant attributes. This ensures that mobile services, APIs, and microservices can be easily discovered and utilized in the appropriate context. By properly classifying these services, developers can quickly discover and integrate the required resources, manage dependencies, and optimize the system's performance and mobile users can know what is available and to how to search in an orderly manner.

**(i) Mobile Services may be classified** as (i) User-Centric Services focusing on the user's interaction with the mobile app, such as authentication, profile management, and notifications for example User authentication, push notifications, payment services, (ii) Location-Based Services that provide location-specific functionality, often using GPS or other location data, such as  Geolocation services, mapping services, weather services, (iii) Data Syncing Services which manage data synchronization between the mobile device and cloud services or databases such as Cloud storage sync, offline data sync, real-time data updates, (iv) Device Services that interact with the mobile device's hardware, for example camera services,  sensor based accelerometer services and fingerprint authentication and microphone.

**(ii) Application Programming Interfaces (API)** are classified as (i) Public APIs: These APIs are exposed to third-party developers and are typically used for broader integration with external services such as Payment gateway APIs and weather data APIs, (ii) Internal APIs: These APIs are used internally within the organization, typically for communication between microservices or different layers of the application stack such as REST APIs for communication between the front-end and back-end servers, (iii) Private APIs: These are similar to internal APIs, but they are more restricted and used for specific, high-security use cases within the organization such as APIs that access sensitive data or perform critical operations that are isolated from general access.

**(iii) Microservices are classified** as (i) Business-Oriented Microservices: These microservices encapsulate business logic, domain-specific functionality, and processes such as Order processing microservice, payment processing microservice, (ii) Infrastructure-Oriented Microservices: These microservices provide support functionality like authentication, logging, monitoring, and resource management, for example Authentication microservice and logging microservice and (iii) Integration-Oriented Microservices: These handle communication between different services or external systems such as API gateway, data processing microservice, integration with third-party APIs.

## 2.16 Indexing of Mobile Services, APIs, and Microservices

Indexing refers to the process of creating a catalogue or repository that stores metadata and attributes for each service, making it easier to search, retrieve, and manage these services. Proper indexing ensures that the services are efficiently searchable, traceable, and integrated within larger architectures.

**(i) Indexing of Mobile Services** has the following key attributes (i) Service Name and Description of functionality, (ii) Version number of the mobile service for ensuring backward compatibility, (iii) Endpoint Details as endpoint URL and relevant request/response formats, (iv) Platforms supported by the service as iOS, Android, Web, etc., (v) Dependencies of mobile services as payment gateway services and  authentication, (vi) Security protocols used by the mobile service as OAuth, JWT, API keys and (vii) Service Documentation with Links to  developer guides.

**(ii) Indexing of APIs** has the following key attributes (i) API Name and Version for easy tracking, (ii) API Endpoints, methods used as GET, POST, PUT, DELETE and URLs to be listed, (iii) Authentication and Authorization Methods for securing the API, such as API keys, OAuth tokens, or JWT, (iv) Rate Limiting Information about API rate limits and any quota restrictions, (v) Data Formats Supported such as JSON, XML, or Protocol Buffers,(vi) Standardized error codes and possible response messages, (vii) API Documentation Links, Swagger files, or OpenAPI specifications, (viii) Service Dependencies Information on which backend systems or services the API interacts with.

**(iii)Indexing of Microservices** has the following key attributes (i) Service Name of the microservice, its purpose and functionality as payment processing and user authentication, (ii) API Interfaces Details of the APIs exposed by the microservice, including endpoints, input/output data formats, and security mechanisms, (iii) Service Dependencies list of other services or external systems that the microservice communicates with, (iv) Deployment Details about how the microservice is deployed as  containerized using Docker, serverless, Kubernetes-based, (v) Health Checks and Monitoring Metrics for the health of the microservice, uptime, performance, and monitoring information, (vi) Version of the microservice to track updates and ensure backward compatibility, (vii) Service-Level Agreements (SLAs) for the microservice's availability, performance, and response times expected, (viii) Technology Stack and frameworks used to build the microservice as Node.js, Spring Boot, Python Flask, (ix) Security and Compliance features, such as encryption, data access policies and compliance standards.

## 2.17 Open-Source Development, Support and Sustainability

Open-source development brings transparency, flexibility and collaborative development of secure mobile applications and services in spite of potential risks as inadequate maintenance, insecure coding practices, and third-party dependency vulnerabilities. To mitigate these issues, open-source mobile projects prioritize secure coding, regular updates, security audits, proper authentication, and privacy compliance. Developers should stay informed about the latest security trends, use automated security tools, and ensure that their contributions to open-source projects follow best practices for mobile security.

Some open-source development issues related to mobile security are (i) lack of Regular Updates on open-source libraries, frameworks, maintenance and support on regular patches, and vulnerabilities, (ii) ensuring secure coding practices are part of the contribution guidelines for open-source projects, (iii) thorough formal security audits and periodic reviews, (iv) many open-source mobile apps may not properly handle authentication, such as improper session management, inadequate password policies, or failure to implement multi-factor authentication (MFA), (v) thorough evaluation of third-party libraries and dependencies before integrating them, (vi) following current best practices of cryptography, such as

AES-256 encryption for data storage, TLS 1.2+ for secure communication, and proper key management using secure hardware as Trusted Execution Environments or Secure Element for storing private keys under CCA, (vii) apps should limit to requesting only the necessary permissions and avoid  access to sensitive resources, and securely configure APIs, databases, and services to prevent unauthorized access, (viii) Open-source mobile apps might expose insecure APIs that are vulnerable to attacks like man-in-the-middle (MITM) or insecure data transfer, (ix) Use of code obfuscation and minification techniques to make reverse engineering more difficult. Tools like ProGuard (for Android) or iOS-specific obfuscation methods can help protect intellectual property and reduce the risk of attacks, (x) avoid collecting more personal data than necessary or mishandle user data. Inadequate privacy controls could violate regulations like DPDP Act 2023. Follow privacy best practices such as anonymizing data, minimizing data retention, and being transparent about data collection and usage (xi) open-source projects may lack proper governance structures, leading to issues with code quality, decision-making, and accountability. So establish clear governance structures for open-source projects, with defined roles for maintainers, contributors, and security auditors, (xii) Open-source contributors may not always be aware of the latest security threats and best practices for mobile security. So encourage ongoing security training for open-source contributors, provide security resources and guidelines, and raise awareness about mobile security threats. Regularly update documentation to highlight security concerns.

## 2.18 Mobile Device Management for Security and Data Protection

Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) Security Solution is critical for protecting corporate data on Mobile Devices as smartphones, tablets, and laptops within an enterprise environment and to ensure compliance to security standards. A user can use the mobile phone to remotely connect to the work computer, check email, or troubleshoot issues even if physically not present at the office.  The security of mobile devices within an MDM solution should focus on protecting the devices, the data they carry, and the networks they connect to. Combining strong authentication, encryption, network security, app management, and continuous monitoring forms a comprehensive security strategy for managing mobile devices. Also staying current with security patches and training users in secure mobile usage is vital for ensuring long-term security.

Some best practices for ensuring strong MDM security are (i) Use containerization or app sandboxing to separate corporate data from personal data on mobile devices, ensuring that sensitive information is isolated and secure, (ii) Implement remote wipe and lock capabilities to ensure that data can be erased from a device if it is lost or stolen, (iii) Implement data loss prevention (DLP) mechanisms to monitor and control sensitive data used and shared across mobile devices and cloud platforms, (iv) Restrict the storage of sensitive information on personal cloud storage services and instead enforce the use of secure, company-approved cloud storage solutions that comply with security policies, (v) Deploy mobile threat defence solutions that can detect and prevent threats such as malware, phishing attacks, and rogue apps from compromising mobile devices, (vi) Ensure that mobile devices are equipped with antivirus or antimalware software and integrate Mobile Threat Défense solutions to detect and mitigate advanced mobile threats, such as malware and phishing attacks to detect malicious activities that may target devices accessing cloud applications, (vii) Regularly update and patch mobile operating systems and applications to close any security vulnerabilities that may be exploited by attackers, (ix) Implement strong  multi-factor authentication (MFA) for device access to prevent unauthorized entry with strong password policies, fingerprint recognition or face ID for unlocking device, (x) Use VPNs or SSL/TLS encryption to protect sensitive information when transmitted over the internet. (xi) Set up geofencing so that devices are automatically locked or wiped if they leave designated safe areas, (xii) Only allow trusted apps or white listed apps from known sources, and block unapproved or blacklisted apps which may cause threats and control the permissions granted, (xiii) Use containerization or sandboxing to isolate work-related apps and data from personal apps, reducing the risk of cross-contamination, (xiv) Implement controls to detect and block jailbroken or rooted mobile devices from accessing corporate resources.

## 2.19 Centralized vs Distributed Mobile Services

It is a challenge to offer all mobile governance services of all sectors into a single trusted mobile app such as UMANG. Whether distributed multiple mobile apps offerings in each sector for public utility should continue as status quo or converge to single PAN India mobile app in each sector is a challenging question to be debated. Hence it is important to look into the advantages and disadvantages of both centralized and distributed mobile services approach briefly given below.

### (A) Centralized Services – Advantages and Disadvantages

Centralized mobile services refer to mobile platforms or applications that are provided, managed and controlled by a single central authority or organization. They offer a streamlined, secure, and consistent user experience, making them ideal for many users who prioritize convenience, ease of use, and security. In a centralized approach, the service provider has control over user data, services, security, and updates. Examples are Android Apps available at Play Store of Google, iOS Apps available at App Store of Apple, AWS Cloud of Amazon, mobile banking Apps for its customers by respective banks, AADHAR Authentication etc.

Providers of Centralized mobile service have the following advantages (i) enforcing policies across all users strictly to provide consistent security, standardized service quality, security updates, bug fixes, and pushing patches to users quickly to reduce the time windows for potential attacks. For example, Indian Mobile Seva Platform has security measures in place to test and review mobile apps of public and private organizations and of individuals for malware or vulnerabilities detection before they are publicly made available to mobile users, (ii) providing consistent user interfaces (UIs) and user experiences (UX) across apps and services, leading to better navigation and usability, (ii) providing interoperable services with seamless integration across various devices. Users can easily synchronize data, apps, and services across multiple devices (e.g., smartphones, tablets, smartwatches, etc.), (iii) provide users with a single point of contact for troubleshooting, customer support or publishing APIs.

Providers of Centralized mobile services have the following disadvantages (i) users often have limited control over how their data is used, stored, or shared, (ii) single point of failure or any data breach may lead to exposure of large amounts of user data which could be misused or exploited, (iii) not providing customized or personalized mobile experience, (iv) restricting flexibility of choice, (iv) monopoly in market and sudden price rise , (v) abiding government regulations and political pressure to enforce censorship or limit access to certain information or services such as removing apps or content from app stores, (vi) lack of Transparency and prioritizing own interests.

### (B) De-Centralized Services – Advantages and Disadvantages

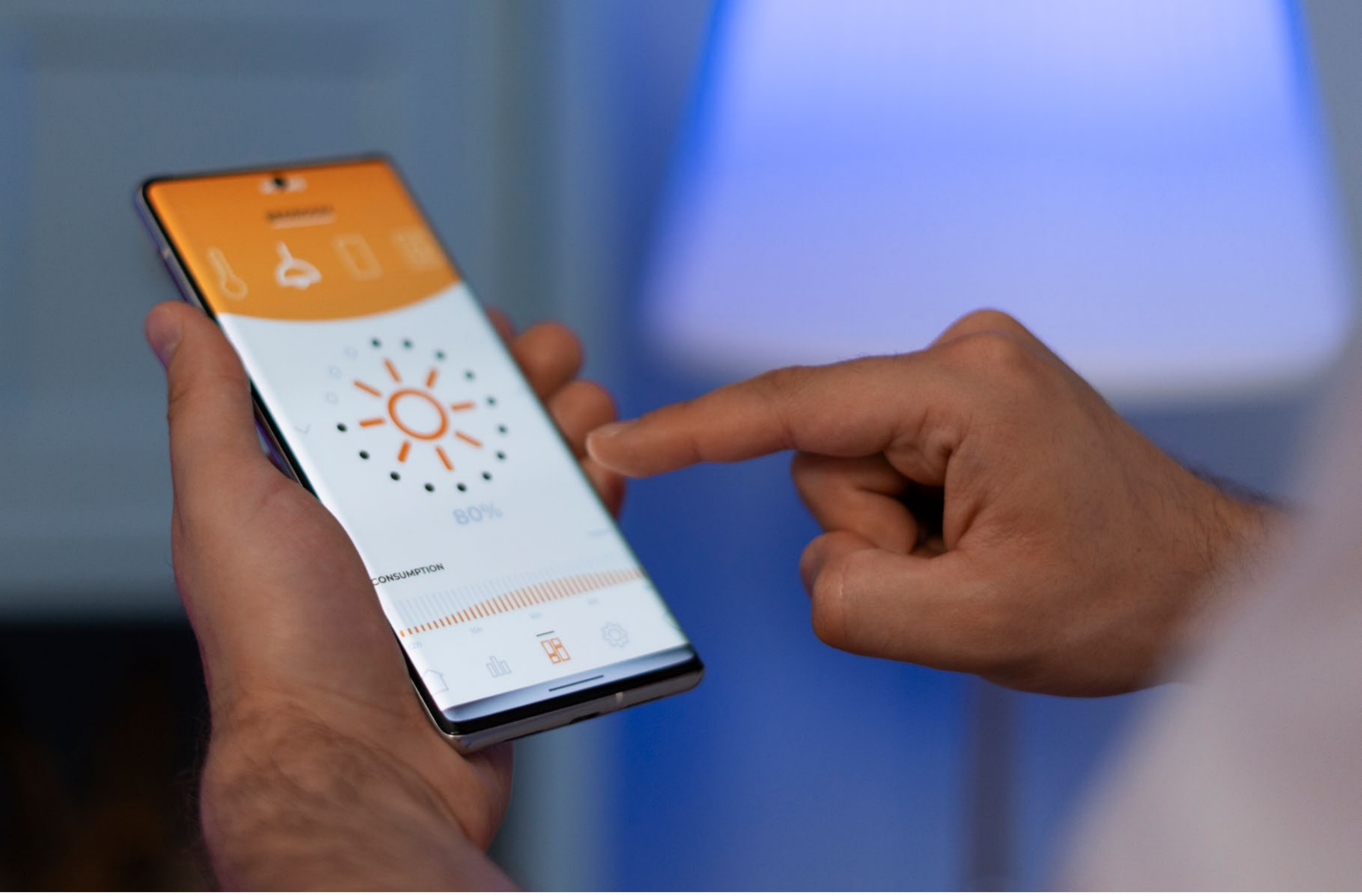
Distributed mobile services refer to a system where services and data are spread across multiple nodes or devices, rather than being centralized in one location or controlled by a single authority. These types of services often leverage technologies like blockchain, peer-to-peer networks, decentralized cloud computing, innovation of startups. For users who are concerned about privacy, customization, and a decentralized approach, decentralized mobile services may be suitable.

Distributed mobile services have following advantages (i) As data is not stored in a central server but rather across multiple devices or nodes. This reduces the risk of data centralization and gives users more control over their own data, (ii) Reduced Surveillance and reduced censorship on tracking users' activities across different services, (iii) There is no single point of failure ensuring greater reliability, (iv) Lower costs for infrastructure, efficient resource sharing and improved fault tolerance.

Distributed mobile services have following disadvantages (i) Managing and coordinating a distributed system can be more complex than centralized services, (ii) Scalability and performance challenges and as more users join delays may happen, (iii) Lack of accountability, (iv) Legal complexities if data is spread across different countries and jurisdictions, (v) User Experience and Usability Issues may be more complicated to handle, (vi) local storage, edge based services and their maintenance may become costlier.

## 2.20 Mobile Seva Platform for Mobile Governance and Innovation

The Mobile Seva Platform (MSP) set up by MEITY, GoI is a central trusted repository of mobile apps, APIs and microservices of all sectors of Digital India developed in Bharat by Govt., public and private organizations, MSME and individuals. Security Testing of the Mobile Apps is done before the mobile app, APIs and Microservices are made available for public use. By ensuring the security of mobile applications and the services it provides, Mobile Seva platforms can help protect user data, facilitate secure access to services, and manage authentication, authorization, Anti-Phishing and Fraud Prevention. Mobile Seva platform provides APIs for integration with third-party systems as banks, IRCTC and service providers. The APIs are secured using OAuth and API keys to ensure that only authorized systems can access the platform's resources. These APIs are also monitored for any unusual activity or security vulnerabilities. The platform may add real-time monitoring capabilities to detect and respond to any mobile security incidents or breaches, ensuring that appropriate actions can be taken promptly. To prevent abuse, Mobile Seva platform implements rate limiting and throttling mechanisms, which restrict the number of requests that can be made to the platform within a given time period. Mobile Seva platform hosted on secure distributed cloud infrastructure is managed by CDAC/MEITY following best security practices and policies. This includes using firewalls, intrusion detection systems (IDS), and access control lists (ACLs) to secure data and services. Mobile Seva Platform contributes to mobile security by implementing a range of security features that protect both the user and the platform. CDAC's M-Kavach 2 app or latest version is very useful to protect mobile device for Mobile Users, which is recommended for download from play store or mobile seva platform and use. MSP ensures secure communication, user authentication, data privacy, and compliance with regulatory standards, as well as providing secure access to services. By integrating modern security practices like encryption, multi-factor authentication, API security, and



fraud detection, it ensures that sensitive data is protected, services are not misused, and users can trust the platform. As mobile-based services grow in popularity, especially for public services, maintaining robust mobile security through platforms like Mobile Seva is essential for fostering trust and encouraging the adoption of these services.

## 2.21 System Integrators for intra-enterprise and public mobile services

System integrators (SIs) play a crucial role in mobile security, particularly when integrating complex mobile security solutions within an organization's IT ecosystem. They act as the bridge between various mobile technologies, enterprise systems, and security frameworks, ensuring that all components function together seamlessly while maintaining a high level of security.

System integrators offer end-to-end mobile security solutions that integrate mobile devices, applications, and backend infrastructure into a cohesive and secure environment. They bridge the gap between disparate systems, ensuring that security policies are enforced across all levels. From planning and risk assessment to real-time monitoring and incident response, system integrators ensure that mobile devices and applications are secure, compliant with regulations, and protected against threats. Their expertise in integrating complex security technologies and frameworks is vital in keeping mobile environments safe and resilient to evolving threats. System integrators are responsible for scaling mobile security solutions to accommodate increasing numbers of devices, users, and transactions without compromising performance or security. Integrators must ensure that the security measures implemented do not degrade the mobile user experience. This means ensuring that encryption, authentication, and other security processes are efficient and do not impact the mobile app's responsiveness or functionality.

Security is an ongoing concern, and system integrators need to manage and improve mobile security throughout its lifecycle. This involves staying up-to-date with the latest security threats and patches, integrating new security technologies, and ensuring that the mobile security

## 2.22 Security Testing of Mobile Device, Mobile Communication and Mobile Services

Mobile Security Testing is necessary to assure that the mobile device hardware, Firmware, Mobile OS, mobile communication channels, mobile interfaces, mobile browser, Mobile device library functions, APIs, Micro-services and mobile apps etc. within the mobile device are secure and are able to counter the various emerging threats and vulnerabilities. Every organizational entity should have IT Security Policy, organizational structure to take up the task of assessing/vetting the mobile security and Mobile Security Operational Guidelines.

There are various mobile security testing standards available whose latest versions are to be followed. An organization or Security Testing Lab undertaking the mobile device security testing and app vetting needs to have Administrator, Test Engineer, Test Managers, Quality Assurance (QA) Manager/QA Engineer.

## 2.23 Mobile Forensics:

Mobile forensics as part of Digital Forensics is important to collect/recover evidence from Mobile Device in case of a cybercrime. Cryptanalysis is an important aspect and its implementation must be assessed for security assurance. Mobile Security Labs in each district may be set up and state level Mobile Forensics Labs be modernized.

## 2.24 Mobile Security Standards – Adoption, Audit and Compliance

Entities of the mobile service ecosystem, should follow the related standards such as (i) Mobile Phone Handsets Safety Requirements (IS 16333, Part-1, 2015 & BIS, reaffirmed 2021), (ii) Mobile Device Security Standard (Part-1 to 4), BIS, Dec 2021, (iii) OWASP Top 10 Mobile Security Risks, Release 2024 or latest one, (iv) OWASP MASVS, Version 2.1.0 released on January 18, 2024, (v) CIS (Centre for Internet Security) Benchmarks (Google Android v1.5.0 - 09-26-2023 and Apple iOS 17 v1.1.0 - 04-30-2024 ) or latest ones, (vi) SANS Mobile Device Checklist & Security Consensus Operational Readiness Evaluation (SCORE) Security Checklist, (vii) NIST SP 800- 163r1 (2019): Vetting the Security of Mobile Applications, (viii) ISO/IEC 27001 (2022): Information security, cybersecurity and privacy protection- Information security management systems- Requirements.

## 2.25 Mobile based Security Attacks and Cyber Crimes

Mobile Users are becoming victims of Financial Frauds, Cyber Crimes, Extortion, Digital Arrest etc. It is a big challenge to protect Mobile Users from Mobile Security attacks and Cyber Crimes and strictly punish the culprits with speedy trials otherwise trust on the mobile ecosystem may degrade.

## 2.26 Light Weight Cryptography for Mobile Services

Cryptography plays important role in securing the mobile user's data - even if attackers have physical access to the user's mobile device. Cryptography Techniques used such as random number generation, encryption/decryption, signature generation, symmetric key generation, asymmetric key generation, hashing etc. should be standard based, foolproof and only be used with their security certified APIs. Due to mobile phones limitations of processing, storage and battery power, light weight cryptography algorithms are suggested such as ECC (Elliptic Curve Cryptography) and ECDSA (Elliptic Curve Digital Signature Algorithm). NIST standard and CCA Specifications may be followed.

### 2.27 Quantum Safe Cryptography Readiness for Secure Mobile Services

It is perceived that continuing with the conventional cryptography techniques, which are in practice today in mobile services, has great threat in near future due to Quantum Computers which have higher potential and efficiency to break them. It is therefore advisable to investigate the use of Quantum-safe cryptography or post-quantum cryptography (PQC) techniques as per Indian sectoral service requirements, which would remain secure even in the presence of powerful quantum computers and would secure mobile user data against potential attacks from quantum computers. Popular PQC based mathematical approaches are Lattice-based cryptography, Code-based cryptography, Hash-based cryptography, Multivariate polynomial cryptography and Isogeny-based cryptography. MEITY, DoT, TEC, DRDO and SETS have demonstrated the use of Quantum Safe Cryptography in specific sectoral use cases as per Indian context. IDRBT is working on PQC use cases to strengthen security of BFSI Sectorial services and Mobile Banking Services in India.

### 2.28 Regulatory Compliance of Sectoral Mobile Services

Every Mobile Service ecosystem entity is responsible and accountable for the actions that it has performed as per its role, rules of service and prescribed guidelines for ensuring Secure Mobile Services and Data Protection. Mobile Security Standards, Guidelines and Best Practices issued by Standard Organizations, Regulators and Trusted Entities of specific sectors are to be followed and complied. The mobile user consent mechanism and grievance redressal for tackling issues related to data privacy are to be followed as per the DPDP Act 2023. Designated and authorized bodies of the respective regulators of service verticals and enforcement agencies should monitor, do periodic technology and social audit and ensure compliance to Mobile Security Standards and Guidelines, Digital Personal Data Protection Act and associated rules along with other related Government regulations, guidelines, standards and best practices in place.

### 2.29 User Experience and Complaints Redressal Mechanisms

In order to provide efficient and secure mobile services for better User Experience (UE), developers and providers should look into the essential features supported by a mobile device and its various user interfaces (UI). This includes focusing on the possible risks from mobile phone platforms, channels, applications, browsers, databases, processors, SIM etc. and corresponding protection mechanisms.

Service providers should guarantee service availability for public or authorized mobile users and specify the conditions in their Security Policy including eligibility of authorized users, language for better user experience and filter out disruptors or denial of service attackers through periodic monitoring. Cookies let one to navigate between pages efficiently as they store mobile user preferences to improve user experience of a website. If the cookies show abnormal behaviour in terms of their functionality and security, then the sourc website originating such cookies may be blacklisted from public use in India.

The mobile user consent mechanism and grievance redressal for tackling issues related to data privacy are to be followed as per the DPDP Act 2023. Mobile Security related grievance and redressal mechanism should be included by all providers of Mobile services along with Customer contact numbers and email id for registering user complaints and suggestions in all Mobile Applications.

## 2.30 Strict Legal Action in violation of Data Protection and Mobile Security

Enforcement of strict legal action is necessary against an entity of the Mobile Service Ecosystem violating the Digital Personal Data Protection Act, Mobile Security Standards and related Guidelines Issued by the Authorities from time to time.

In the digital world it is impossible for an entity of the Mobile service ecosystem to escape or get away if it has committed any malicious activity violating the rules. It requires collection, storage, maintenance and monitoring of security logs by the respective entities for traceability and proof of digital evidence. AI techniques are being used for it. Timely Legal action is equally necessary. Ancient Indian tradition of timely rewarding the disciplined entities and timely punishing the culprits or adversaries in the Mobile Service Ecosystem is to be cultivated.

## 2.31 AI Tools - Use Cases in Mobile Security

AI Tools are useful to identify threats in mobile security such as detecting malware, vulnerabilities, data leaks, and unusual behaviours. These AI Tools combine machine learning, anomaly detection, behavioural analysis, neural networks, fuzzy logic, deep learning and natural language processing to provide comprehensive protection against evolving threats. By utilizing these tools, organizations and individuals can enhance their ability to detect, respond to, and mitigate mobile security risks. The challenge is to choose the right mix of AI-powered tools based on the specific security needs.

Some AI tools and techniques useful for identification of mobile security threats are (i) Machine Learning based Threat Detection Tools as Cortex XDR by Palo Alto Networks, Zimperium for mobile malware and zero-day attacks, Lookout for identification of phishing attacks, malware, and data leakage, (ii) Anomaly Detection of irregular behaviour with AI Tools as Sift for fraudulent behaviour or abnormal app usage on mobile devices, IBM QRadar Tool for security information and event management (SIEM) solution to indicate mobile security threats, (iii) Behavioural Analysis Tools to monitor how mobile apps or devices behave over time such as SentinelOne Tool for behavioural analysis to detect threats based on how mobile apps interact with system resources and detect unknown malware based on behaviour and CrowdStrike Falcon Tool for behavioural monitoring to detect suspicious mobile device activity and potential breaches, (iv) Automated Mobile Malware Detection Tools to automatically analyse mobile apps and detect malicious code, unauthorized data access, or unusual app behaviour that is typically associated with malware such as Deep Instinct using deep learning to detect threats, including mobile malware, based on file and code behaviour patterns and AppScan by HCL to identify security flaws in mobile apps, including those that could be exploited by malicious actors, with machine learning-based scanning capabilities, (v) Phishing Detection Tools to identify phishing attempts on mobile platforms by fake websites, malicious links, or social engineering scams as Proofpoint Tool for detecting phishing attempts in real time on mobile devices, including spear-phishing

and URL-based attacks and Symantec Mobile Security Tool offering phishing protection and identifying harmful URLs, malicious links, and spoofed websites on mobile devices, (vi) Mobile Device Management (MDM) Tools for enterprises incorporating AI to detect anomalous device usage, enforce security policies, and protect against data leakage such as VMware Workspace ONE for security management for mobile devices, detecting unauthorized access, app vulnerabilities, and threat patterns and Microsoft Intune Tool to identify security risks on mobile devices and respond proactively, (vii) Mobile Vulnerability Scanner Tools for Scanning mobile apps and devices for vulnerabilities, outdated software, configuration flaws that could be exploited by attackers such as Veracode Tool for identifying vulnerabilities within mobile applications and provides recommendations for remediation and OWASP Dependency-Check Tool for scanning and evaluating mobile apps for security vulnerabilities in third-party libraries and frameworks, (viii) Network Traffic Analysis Tools using AI to analyse network traffic patterns from mobile devices to detect potential threats like data exfiltration or suspicious communication with malicious servers such as Darktrace Tool to detect suspicious network traffic patterns that could indicate mobile threats and unauthorized communication with an attacker's server and ExtraHop Tool for real-time threat detection and network traffic analysis for mobile and IoT devices, (ix) Natural Language Processing (NLP) Tools for Threat Intelligence mining various sources such as social media, forums, or technical reports to identify emerging mobile threats such as Recorded Future Tool to analyse large sets of data, including unstructured data sources, to gather insights on mobile security threats and attack trends and Anomali Tool to provide early detection of new mobile security threats, (x) Privacy Protection Tools assisting in monitoring and protecting users' privacy by identifying any sensitive information that might be at risk or exposed by mobile apps such as Pradeo Mobile Security Tool to detect privacy violations, including improper handling of sensitive user data by mobile apps, (xi) Hybrid AI Tools of all aspects of Mobile App behaviour, anomaly detection, data breaches, privacy, anti-virus tasks, MDM etc. of enterprise's such as Protectt.ai Tool for atmanirbhar Business to Business (B2B) solution of mobile application security.

## 2.32 Process Automation, Risk Monitoring and Dashboards

Process automation, risk monitoring, and dashboards are essential for strategic management of robust mobile security. They help in managing complexity, ensure real-time response, and enhance decision-making, particularly in an environment where mobile devices are constantly being targeted by cyber threats. They improve Efficiency, Speed, Scalability, Error Reduction and repetitive tasks such as monitoring device activity, scanning for malware, and applying patches. Process automation streamlines these tasks, reducing the manual effort required and ensuring tasks are completed consistently and accurately.

Process automation, risk monitoring, and dashboards play critical roles in ensuring the effectiveness of a mobile security strategy. By automating repetitive tasks, organizations can react faster to emerging threats, improving operational efficiency and reducing human error. Risk monitoring offers continuous vigilance, ensuring that mobile security remains proactive rather than reactive. Dashboards provide the essential insights and visibility needed for informed decision-making, enabling security teams to respond to and mitigate threats effectively. In the digital era where mobile devices are the target of cyberattacks, they are useful to protecting data, maintaining compliance, monitoring and ensuring the safety of mobile ecosystem.

Process Automation is useful in (i) automatically scanning mobile apps and files for malware whenever new mobile apps are installed or updates are made, (ii) automatic deployment of Security patches on mobile devices whenever vulnerabilities are discovered, thereby reducing the time devices are exposed to attacks, (iii) isolating the mobile device, block malicious apps, or alert security teams for immediate action, if an abnormal activity or threat is automatically detected on a mobile device such as  unusual data usage or unauthorized access.

Risk Monitoring is useful in (i) Real-Time, Continuous and Proactive  Threat Detection by continuously analysing mobile  device behaviour, app permissions, network traffic, and user activity for signs of suspicious behaviour, (ii) Device Health Monitoring for signs of compromised operating systems, jailbreaking, or rooting to identify potential mobile security risks before they are exploited, (iii) Network Traffic Analysis and compliance by monitoring data traffic from mobile devices to identify any anomalous activity such as unusual data transfers, connections to untrusted networks, or unauthorized communications with external servers.

Dashboards are customized displays which provide Centralized Visibility, unified view and real-time monitoring of mobile security incidents of the entire mobile security landscape to the authorized personnel of the security teams or Mobile User. They consolidate security alerts, risk levels, and performance metrics into an easy-to-read format, enabling quicker decision-making and action, and provide features to drill down to specific needs and events. They show snapshot of current threats as well as allow teams to analyse trends over time, which helps in identifying recurring patterns of attacks, common vulnerabilities, or common risk factors that need to be addressed in the mobile security strategy. Dashboards can track key performance indicators (KPIs), such as the number of devices with updated security patches, the number of detected threats, or the percentage of devices that have passed security compliance checks. Security teams can use dashboards to prioritize threats and allocate resources efficiently such as if there are high number of threats in a particular region or business unit, teams can prioritize mitigation efforts in those areas.

Dashboard are useful to display (i) all security incidents, including detected threats, breaches, and vulnerabilities, and their resolution status. This allows security teams or Mobile Users to track ongoing incidents and their impact, (ii) highlight compliance metrics for mobile devices, such as whether devices meet regulatory requirements or security policies, (iii) health status of mobile devices across an organization, highlighting devices that are non-compliant or at risk such as  rooted devices, outdated OS, unpatched vulnerabilities, (iv) threat intelligence feeds, showing which threats are currently targeting mobile devices, providing context such as attack vectors, affected regions, and active threat campaigns.

### 2.33 Social Media Platforms, Applications and Threats

Social Media Platforms based various Mobile Apps such as WhatsApp, Facebook and Twitter are being highly used by Mobile Users of all levels and age groups.  Attackers may lure the users by asking to click on malicious links which are communicated to the users over various channels such as SMS, email or the social media platforms by pretending to be from a popular bank or someone whom the user may know or trust. Once the user clicks on these malicious links, it would be possible for the attackers to hack into the user's mobile devices, inject malware and steal sensitive user data. So, one should strictly avoid clicking on any suspicious links appearing in text, image or video icons or received over SMS, email or any social media platforms or mobile apps.

Organization-specific security requirements define the policies, regulations and guidance that an organization must follow to ensure the security posture of the organization. Examples include banning social media apps from installation on the organization's mobile devices and restricting installation of the security posture of mobile apps.

While using Social Media applications, users should protect their personal information safely by avoiding to click on malicious/suspicious links or attachments, using strong and secure passwords, keeping one's identity safe & secure, backup the data at regular intervals, keep the Anti-Virus solutions up to date, keep all operating system and applications up to date, verify the security of the website used.

### 2.34 Compliance to Digital Personal Data Protection Act of India

As per Digital Personal Data Protection (DPDP) Act-2023 and corresponding rules, (i) Mobile Users digital privacy and personal data, identity, location, path travelled, communication channels used etc. are to be protected, (ii) Mobile user consent mechanism and grievance redressal for tackling issues related to data privacy are to be followed, (iii) Protection of data on the mobile cloud from any attack is to be ensured. If the Cloud service providers are providing the mobile services worldwide then for Mobile Users in India, they need  to establish the cloud service mobile user data in servers that are located within India for data privacy and security including Database Security Management.

### 2.35 Mobile based Sensor and IoT Threats

Mobile Phone has various sensors in it such as GPS, accelerometer, microphone, camera, temperature, which if misused may pose threats to the mobile user. As these sensors may be permission based or permission less, it is important for a Mobile User to check, how the inbuild sensors are used by various mobile apps installed and stop access if any threat is observed.  Mobile phone acts as an IoT Device and also as IoT gateway for the connected devices as WiFi, Bluetooth, BLE, NFC devices, and access points, ear pods, speakers, mike, wearables etc. Sensor and IoT security are critical for mobile users because many mobile devices, apps, and services now rely on sensors and Internet of Things (IoT) devices for enhanced functionality and convenience. Insecure IoT devices connected with a mobile phone can compromise user privacy, safety, critical data of health and authentication credentials and data security. These devices gather data which is often deeply personal and sensitive, interact with each other, and communicate over the internet, but if they are not properly secured, they can present serious risks to user privacy, safety, and data security. IoT devices are often used in botnet attacks, where thousands of compromised devices are controlled remotely to overwhelm networks or servers. A hacked home security system could allow burglars to disable alarms or surveillance cameras. If a mobile user's IoT devices are part of a botnet, their personal devices could unknowingly participate in these attacks, damaging their reputation or leading to legal or financial consequences. Some IoT devices, when compromised, may send large amounts of data to mobile devices, which can overwhelm system resources as CPU, memory, network bandwidth and lead to device slowdowns or battery drain. This can degrade the user experience and, in extreme cases, lead to device crashes or data loss. Without strong encryption and proper authentication protocols, the communication between IoT devices and mobile phones is vulnerable to compromise. These challenges are to be taken into account and be resolved.

## 2.36 Mobile as a Remote, Command and Control Device

Mobile phone is used as a remote control for a range of devices such as smart homes, smart TV, lights, thermostats, security cameras, door locks, and appliances, health devices, cars, surveillance cameras etc. Some Home automation apps such as Google Home, Amazon Alexa, Apple HomeKit etc. enable users to manage and monitor their smart home ecosystem from their mobile phones like heating system, lock or unlock doors, or even turn off appliances remotely when away from home. Smart TV apps such as Samsung SmartThings or LG ThinQ enable users to control their TV, sound system, or other smart home devices directly from their mobile phone.

If one such connected device to Mobile Phone is compromised, it can affect linked devices or the entire network and lead to have cascading effects, jeopardizing not only the mobile device but also the services and data associated with it. Mobile phones act as command-and-control (C&C) devices for a variety of functions, leveraging their built-in sensors, connectivity, and processing power. This functionality if used for malicious purposes such as cyberattacks or hacking then it could be a disaster to the mobile user. Mobile phones can act as command-and-control devices for remote desktop software like TeamViewer or Chrome Remote Desktop. A user can use their mobile phone to connect to their work computer, check email, or troubleshoot issues even if they're not physically at the office. Through apps like Infrared IR blasters, Bluetooth, or Wi-Fi, mobile phones can be used to control a wide range of devices, including TVs, air conditioners, projectors, and other household electronics.

Mobile phones serve as powerful remote control and command-and-control devices across a wide range of legitimate applications, from managing home automation systems to controlling vehicles or drones. Car apps such as Tesla, BMW, KIA Connected allow users to lock/unlock the car, start the engine, adjust the temperature, or even track the car's location. A mobile phone can control the movement, camera, and even the flight path of a drone equipped with an app, which are often seen in Indian Functions and Music Concerts. A hacker could control a mobile phone in a botnet that has infected hundreds of IoT devices (smart cameras, routers, etc.) and instruct them to flood a website with traffic in a DDoS attack. An attacker may install a Remote Access Trojans (RAT) on a mobile phone, and then, from a remote location, control the phone to access sensitive information, track the user's movements, or listen in on private conversations. They can also access data, take pictures, record conversations, or even use the phone's microphone and camera for surveillance. Smishing (SMS phishing) and phishing attacks often involve the mobile phone as a C&C device for delivering malware or obtaining sensitive user information.

However, their role as command-and-control devices also makes them attractive targets for cybercriminals, who exploit vulnerabilities to compromise devices and launch attacks like botnets or remote access to private information. As mobile phone use continues to expand, both security measures and user awareness are essential to prevent malicious exploitation and ensure safe usage of these devices in the connected world.

## 2.37 Ethical Hackers Group for National Defense of Mobile Users

An ethical hacker group (EHG) is a white hat hacker group of cyber and mobile security professionals who use their hacking skills for legal, constructive, and ethical purposes. The main goal of the group is to help organizations or mobile users to identify vulnerabilities and weaknesses in their digital systems before malicious hackers (black hats) can exploit them. Ethical hacker group plays vital role in protecting organizations from cyber threats and improve overall mobile security.

The EHG mainly focuses on (i) Penetration Testing by simulating  cyberattacks on a digital system or organization network to uncover potential vulnerabilities, (ii) Vulnerability Assessments by scanning and analysing IT systems to identify security flaws and weaknesses thereby  strengthening organizations defence preparedness, (iii) Security Audit of  software, digital systems or network systems for compliance with security standards, ensuring that there are no vulnerabilities that could be exploited, (iv) Participating in Bug Bounty Programs, where companies offer rewards to ethical hackers who discover and report security flaws. (v) conduct Training and Awareness workshops, seminars, and other educational activities to raise awareness about cybersecurity and ethical hacking practices.

Members of ethical hacker groups often follow a code of conduct, where they must have proper authorization before testing any system, and their actions must always aim to improve security rather than cause harm. Examples of such EHG are HackerOne community and Open Web Application Security Project (OWASP).

## 2.38 Security Drills for strengthening Mobile Ecosystem Entities

Security drills for mobile service ecosystem entities are simulated activities designed to prepare organizations within the mobile industry to handle potential security incidents effectively. These drills involve various scenarios where mobile service providers, app developers, and other stakeholders must respond to cybersecurity threats or breaches in a coordinated and efficient manner. The goal is to enhance the organization's preparedness and ensure that proper security protocols are followed when real incidents occur. Security drills are essential in maintaining robust defences and ensuring that entities within the mobile service ecosystem can handle cybersecurity incidents effectively. Regular drills help organizations and mobile users adapt to evolving threats and improve their overall security posture, making them more resilient in the face of future attacks.

Main Objectives of Security Drills for Mobile Service Ecosystem Entities are (i) Preparedness: To ensure that personnel of the security team or mobile users are prepared to detect, respond to, and recover from a variety of mobile and cybersecurity incidents, (ii) Coordination: To ensure that coordination between technical teams, legal teams, customer service, and communication teams to handle mobile security incidents are effective, (iii) Compliance: To ensure the adherence to industry standards, legal requirements, and best practices in mobile security, (iv) Resilience: To Improve the resilience of mobile services and infrastructure to prevent or minimize damage from attacks and (v) Continuous Improvement: To identify gaps and weaknesses in security posture, incident response protocols, and overall system security.

Mobile Security drills include (i) Incident Response to evaluate how quickly and effectively the team detects and responds to the incident, including containment, mitigation, and communication, (ii) Phishing and Social Engineering Attacks to test the awareness and readiness of users and staff against social engineering tactics as phishing emails or SMS or links, (iii) Denial-of-Service (DoS) Attack Simulation to evaluate how well the mobile infrastructure can handle traffic overloads or service disruptions, (iv) Mobile Application Security Drills to Assess how quickly the team identifies and fixes vulnerabilities in mobile apps, as well as how they communicate with affected users, (v) SIM Swap or Mobile Account Takeover Simulation to Prepare teams to respond to account takeovers and protect user authentication processes, (vi) Data Encryption and Privacy Breach Drill to evaluate how well encryption, access controls, and privacy policies are enforced, and how the organization responds to potential leaks of sensitive information. (vii) Ransomware Attack Simulation to test the ability to detect, contain, and recover from ransomware incidents, (viii) Compliance and Regulatory Drills to ensure mobile service providers and other entities comply with industry best practices, industry standards, regulations and latest guidelines. (ix) Third-Party and Vendor Risk Management Drills to assess the ability to evaluate and secure third-party relationships and vendor risk management strategies, (x) Mobile Device Security Drills to ensure proper security controls are in place for mobile devices accessing enterprise networks and services.

## 2.39 Handling International Issues of Mobile based Cyber Crimes

Handling international issues related to mobile-based cybercrimes is a complex task that requires collaboration across borders, legal frameworks, technological advancements, and strategic coordination among governments, law enforcement, private sectors, and international organizations. Mobile cybercrimes often involve cross-border activities, making them difficult to address within the boundaries of a single nation. Addressing international mobile-based cybercrimes requires a multi-faceted approach that includes international cooperation, robust legal frameworks, advanced technology, and public awareness. By combining efforts across countries, industries, and organizations, we can create a unified global response to the increasingly sophisticated and cross-border nature of mobile cybercrimes.

Some strategies to resolve international mobile-based cybercrimes are (i) International Collaboration and Cooperation to share threat intelligence reports of Cross-Border Cybercrimes and Mobile-based cybercrimes such as data breaches, identity theft, fraud, cyberbullying, and malware attacks with the involvement of Interpol, Europol, Global Action on Cybercrime (GAC), CCA, Bilateral and Multilateral Treaties in G20, WEF etc., (ii) Strengthening National Legal Frameworks, Cyber Laws and Legal Gaps by harmonizing around cybersecurity and mobile data protection. For this Organizations like the United Nations (UN), Organization for Economic Co-operation and Development (OECD), G20 and IFSMS can help create international standards for mobile cybersecurity to Adopt International Agreements and Digital Evidence Handling Data, (iv) Cybercrime Reporting and Accountability.

## 2.40 Block Chain based Mobile Frauds

Blockchain-based mobile frauds involve malicious activities or fraudulent schemes that exploit blockchain technologies in the context of mobile devices. Blockchain as decentralized system is designed to provide transparency, non-repudiation and security of transactions, but cybercriminals have found ways to manipulate or use these technologies for anynomous illicit purposes by exploiting vulnerabilities in user behaviour, app security, and smart contract flaws. Cybercriminals use these vulnerabilities to trick users into losing cryptocurrency, personal data, or other valuable assets. By being vigilant, adopting secure practices, and verifying sources, mobile users can better protect themselves against blockchain-based mobile frauds and from getting lured.

Some key types of blockchain-based mobile frauds are (i) Cryptocurrency Fraud where fraudsters exploit mobile users in various ways as Phishing, Ponzy Schemes, Fake Wallets or mobile apps, or mule accounts to steal cryptocurrencies or trick them into making fraudulent transactions, (ii) Smart Contract Exploits by Exploiting Bugs in Code to reroute funds, manipulate transaction outcomes, or cause a loss of value, (iii) Fake Initial Coin Offerings (ICOs) or Token Sales, Pump and Dump Schemes by falsely promoting it through mobile platforms. Once the price is artificially inflated, they sell off their holdings (pump), and the price crashes (dump), leaving other investors with worthless tokens, (iv) Blockchain Mining

Malware where malware is installed on the mobile device to secretly mine cryptocurrency without the user's consent or knowledge, (v) Blockchain Phishing and Social Engineering where fraudsters use social engineering tactics to trick mobile users into disclosing their private keys, wallet credentials, or sensitive information related to their blockchain-based assets, (vi) Blockchain-based Identity Theft where fraudsters exploit blockchain's decentralized nature to steal or manipulate identity data, leading to identity theft or fraud, (vii) Cross-Border Blockchain Fraud and Money Laundering which facilitates cross-border financial transactions without the oversight of traditional financial institutions. Criminals use mobile platforms to launder money or move illicit funds across borders with a degree of anonymity.

Ways to Protect Against Blockchain-Based Mobile Frauds (i) Enable Two-Factor Authentication (2FA): Always enable 2FA on mobile wallets, exchanges, and blockchain applications. This adds an extra layer of protection, (ii) Download Apps from Trusted Sources: Only download cryptocurrency apps and blockchain-related apps from official app stores and avoid third-party or untrusted sources, (iii) Verify Initial Company Offerings (ICO) and Token Sales: Do research and verify any ICOs or token sales before investing. Look for red flags like lack of transparency, unrealistic promises, or no verifiable team, (iv) Be Cautious with Links and Phishing Attacks: Avoid clicking on suspicious links or downloading unknown apps. Always verify URLs and check for the legitimacy of communications before providing sensitive information, (v) Use Antivirus and Anti-Malware Software: Install reliable security software on mobile devices to detect and prevent malware, including cryptojacking apps, (vi) Avoid Unnecessary Transactions: Be wary of offers or promotions that seem too good to be true, such as unsolicited token giveaways or fake cryptocurrency prizes.

## 2.41 Recommender System for Mobile Security

Recommender systems play significant role in enhancing mobile security by offering personalized security-related recommendations and improving overall user experience and guiding developers for developing foolproof security for mobile services.

Some Use cases of Recommender System for Mobile Security are (i) App Permissions and Privacy Settings where mobile apps installed on a mobile device are analysed and changes are recommended on app permissions based on the user's behavior and security preferences. For example, if an app is accessing unnecessary sensitive data (like contacts or location), the system might suggest limiting its permissions or even uninstalling the app or change .privacy settings that would minimize the risk of data breaches or unauthorized access, (ii) Personalized Security Alerts to mobile users by warning them about potential threats or unsafe activities on their devices or alerting when in a vulnerable location or when the phone has been exposed to potentially harmful public Wi-Fi or Bluetooth networks, (iii) Malware and Risk Assessment by analyzing app behavior, file downloads, or browsing activity and suggest scans or specific antivirus tools that would improve the security posture or recommend specialized tools or apps that protect against malware, phishing, or identity theft based on a user's specific activities and risk profile, (iv) Behavioral Authentication by recommending to strengthen authentication or to switch from basic PINs

to biometric authentication of fingerprint or facial recognition based on usage patterns or security risks or user's behavior, such as login location, time, and device history, (v) Network Security Threat Detection when a mobile device connects to a potentially insecure network then it suggests  immediate security measures like using VPN or disabling certain data-sharing features or automatic connection to secure networks or prompt the user to enable encryption for added security, (vi) Personalized Incident Response of a security incident like a breach or lost device then suggesting the most effective steps based on the severity, such as locking the device, enabling remote wipe, changing passwords, or contacting customer support, (vii)  Access Control Recommendations where suggesting specific access control features such as limiting access to sensitive apps or files, to protect personal or business data from unauthorized access.

## 2.42 Checklist on Mobile Security for Stakeholders

Security checklist for each category of entities of the mobile service ecosystem is important to (i) ensure  that all aspects of security are considered, made available and informed systematically, (ii) serve as a comprehensive guide to safeguard the mobile ecosystem, protect users' data, and maintain overall system integrity, (iii) promote standardized security practices across different stakeholders thereby reducing the chances of overlooked vulnerabilities or inconsistent security measures and help in consistent approach to security, (iv) ensures that common risks such as data breaches, unauthorized access, insecure data storage, and communication weaknesses are addressed proactively, (v) create awareness about security regulations and their compliance requirements, (vi) protect from cybercrimes and cyber-attacks, (vii) for developers to know the Secure Application Development and security by design approaches, (vii) for effective incident response in case of security breaches, ensuring that entities are prepared to quickly contain, mitigate, and recover from security incidents., (viii)  maintain operational resilience of mobile services by regularly testing IT systems, networks, and devices, ecosystem entities can detect weaknesses early, preventing downtime or significant security breaches that could harm users or the business.

A security checklist is vital for ensuring that all stakeholders in the mobile service ecosystem take the necessary steps to secure mobile services, data, and devices. It provides a structured approach to identify, mitigate, and manage security risks across the ecosystem. It should be prepared by the organization's security teams, led by the CISO, with input from legal, compliance, and third-party experts. Once finalized, the checklist should be released and implemented by all relevant parties in the mobile ecosystem, ensuring consistent security practices that protect users and maintain trust.

Mobile Security Checklists are published and maintained by (i) the Security and IT teams within an organization, particularly those responsible for cybersecurity as Chief Information Security Officer (CISO), (ii) Mobile Service Ecosystem Collaborators as  mobile device manufacturers, app developers, cloud service providers, and telecom companies must all collaborate to ensure that their devices, applications, and networks are secure and adhere to the checklist, (iii) Compliance and Legal Teams for legal and regulatory compliance. (iv) Security Standards Bodies and Industry Groups as OWASP, NIST, ISO/IEC 27001, BIS, MEITY, DoT, TRAI, TSDSI, RBI, IDRBT and sectoral regulators provide valuable input into the creation of security checklists, ensuring alignment with established security standards, (v) External Auditors and Security Consultants and Professionals do independent reviews based on the checklist and suggest improvements in the checklist with respect to the new and emerging threats.

## 2.43 Policy on Recycling of E-Waste of Mobile Equipment and Digital Infrastructure

E-waste management is an important requirement for personal and organization's sustainable growth. Policy on e-Waste disposal of outdated gadgets, digital devices, mobile phones, cables etc. and recycling in a secure manner need to be adopted to meet regulatory standards and compliance requirements. It is important to see that before disposal data on the device is taken proper backup by the Mobile user.

# 3

# Case Study of Mobile Financial Services

Here we consider the Case Study of Mobile Financial Services in India to show how the various risks and mobile security challenges are faced, how mobile ecosystem entities co-ordinate to provide end-to-end secure mobile payment transactions, how the security by design is adopted to achieve mobile security goals for seamless mobile payment transaction and the various remedial measures taken to handle the emerging mobile security threats and mobile based crimes. It will be useful as a way forward for securing various sectoral services and mobile governance services to mobile users.

Mobile Phone Users get mobile services of various sectors such as Education, Communication, Travel, Transport, Healthcare, Finance, Entertainment, Industry, Business, Sports and Games etc. Here, we focus on Financial Sector which covers banking, insurance, pension fund, foreign exchange, investment, loans, wealth management, stock markets, financial markets and, related Fintechs and Financial Institutions. Digital Payments is common to BFSI and central to the financial sector. Banks handle digital payments through their multiple delivery channels, such as Banking Branch Automation (1984-1987), ATM (1987), shared ATM Network - Swadhan by IBA in 1997, Payment Cards as Credit Cards (1987) and Debit Cards (1998), PoS Devices (1990), Internet Banking (1990), Total Branch Automation (TBA-2000), Centralized Core Banking System (CBS, 1990-2005), Cash Dispensing Machines (CDM) and Cash Collecting Machines (CCM in 2000), Coin Vending Machines (CVM in 2004), Banking kiosks (2006) and fund transfer through NFS (2004) set up by IDRBT, RTGS (2004) set up by RBI and NEFT (2005) set up by IDRBT, Mobile Payments though IMPS (2010) and using messaging standards as ISO 8583 (1987), SWIFT (1987), PCI-DSS (2004) and SFMS (2009) by RBI through the Closed User Group INFINET (1999) platform set up by IDRBT. These messaging standards specify the classes of financial services and the indexing pattern followed for seamless integration across all entities involved in a financial transaction. Security of these messages is an add on feature for end to end security of transactions.

Although Mobile Payments initiative has started by couple of leading Banks in India in 2001 linking with specific Telecom Operators but their scope, scale and reach was very limited. With initial background research work done by IDRBT, it was inferred that unlike other digital delivery channels of Banks, Mobile Payment Channel requires active and responsible participation of all entities of the mobile ecosystem. Although Banks have reasonably good control on various delivery channels offered to customers but on Mobile phones of mobile users, they hardly have any control so it was initially felt highly risky to offer mobile payment services in large scale.

Prof.Ashok Jhunjhunwala (IIT-Madras) as Member of the then Governing Council of IDRBT and Prof.V N Sastry (IDRBT) have initiated a brain storming workshop at IIT-Madras in 2006 and concluded to set up the Mobile Payment Forum which in a later meeting was decided to be named as the Mobile Payment Forum of India (MPFI) in the first meeting of MPFI was held at IDRBT on Ganesh Chaturthi day in August 2007, MPFI was launched. MPFI had an active Executive Committee with members representing all stakeholders and driving the Technical Committee, Regulatory Committee and Business Committee with respective experts representing all stakeholders of mobile service ecosystem such as Banks, Telecom Operators, Regulators as RBI and TRAI, Mobile Device manufacturers as Samsung and Ericsson, Govt. Bodies as DoT and NIC, Tech Companies as Microsoft, TCS and Infosys, FinTechs, Research Organizations as IDRBT, IIT-Madras and IIT-Bombay and Mobile Users. MPFI was officially registered in Hyderabad as a non-profit society in 2009 with its office at IDRBT Staff Quarters initially and later moved to another venue in Hyderabad.

Regulatory Guidelines for Mobile Payments prepared by MPFI was published by RBI in 2008. This gave confidence and push to Banks to launch Mobile Payment Services and later Mobile Banking Services. The Interoperability Standard for Mobile Payments published by MPFI in 2009 has laid the basic foundation for Mobile Payments in India with successful pilot involving few Banks, Telcom Operators and Tech companies. The experience gained through the pilot and user acceptance testing has helped to revise and publish the amended version of Interoperability Standard for Mobile Payments in India which included the UML design diagrams, messaging formats and APIs to pay, collect, split and failure scenarios of end-to-end transactions. The Interoperability of mobile payment solution was very clearly defined in terms of it being agnostic to or independent of (i) mobile device (mobile OS platform, make and model), (ii) Mobile Telecom Operator (any SIM) and (iii) Bank (Any Bank with any CBS). This Interoperability Standard for Mobile Payments is a ground breaking contribution to the Nation, which has given solid foundation for development of all Mobile Payment Solutions in India.

In order to pay from one mobile user (Payer) to another mobile user (Beneficiary) of different mobile operator and of different bank using just the mobile number of the beneficiary, it was felt necessary to have a trusted centralized entity which would create a mapper database of users mobile phones linked with banks, route the transaction and enable settlement of funds for retail payments. Since there was no such centralized entity ready at that time, so this condition was relaxed and the concept of MMID for Mobile Payments was introduced as an additional number. MMID is a 7-digit number with first 4 digits linked with a Bank for its identification, 2 digits are linked with customers bank account and 1 digit is for check sum. The check sum introduced is a security measure for auto check of correctness or integrity of the data sent, for example, whether the mobile number and the MMID of the beneficiary are both correctly entered or not by the payer and if there is any mistake occurred in entering either or both of them, then it would show as mismatch and failed transaction. This is a simple example of Security by Design of Data Integrity.

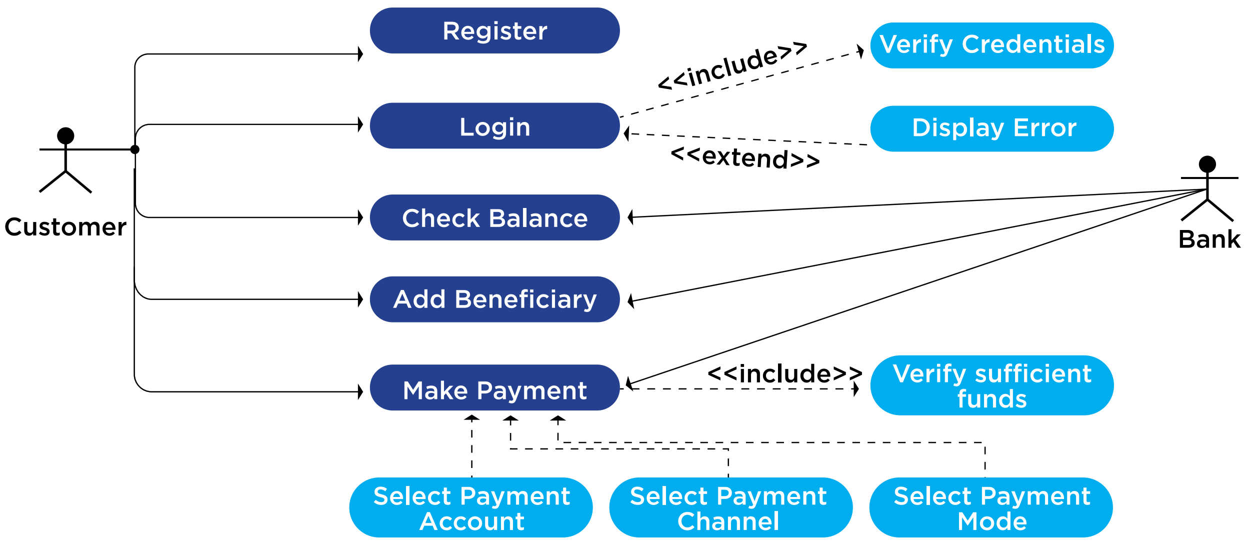
NPCI was set up in 2009 to rollout retail payments with its initial office and operational set up at IDRBT Campus and later moved its operations and office to BKC, Mumbai.  Inter Bank Mobile Payment Service – IMPS using mobile phone number and MMID of the beneficiary, was publicly launched on November 22, 2010, by Smt. Shyamala Gopinath, DG RBI, in Mumbai and it was later renamed as Immediate Payment Service (IMPS), once it has become interoperable on any device including ATM, Internet Banking Computer and PoS Device. Subsequently RuPay (2012), Direct Benefit Transfer (DBT-2013), PMJDY (2014), AEPS(2016), UPI(2016), BHIM (2016), Bharat QR (2016), BBPS (2016), NIPL (2020), e-RUPI (2021) and UPI Light (2022)  were launched.

These along with several financial sector initiatives as SEBI (1992), NSE (1994), BSE Electronic Trading (1995), NSDL(1996), G-Sec Market (1999), MCX (2000), CCIL (2001), e-Tendering (2002), NCDEX (2003), e-filing of Tax (2006), Online Insurance Payments (2007), FASTag (2014) as Digital Financial Infrastructure (DFI) of the Digital Public Infrastructure (DPI) have helped in Financial Inclusion, migration to digital and mobile payments by everyone due to demonetization in 2016, Covid in 2020 and presently by FinTech innovations and Digital India Movement. The example of MPFI is a successful story of strong foundations and Make in India initiative in 2007 with the coordinated involvement of multiple stakeholders of the mobile financial services ecosystem. It has given the insight that to achieve the success of digital public services in large scale in India or elsewhere, the 3 most significant pillars are  (i) Technology : providing demanding technology service solutions, (ii) Regulations: corresponding regulatory policy frameworks and guidelines for the stakeholders and (iii) Business Model: proper  business model with the engagement of stakeholders and balanced win-win strategy are the most significant pillars.

Banks manage 3 broad categories of risks namely Credit Risk, Market Risk and Operational Risks, first two are well established business risks and the latter on operations management driven by people, process and technology is new, ever changing, complex and has higher external dependency. Adequate capital is required to be maintained with RBI by Banks as per its regulatory specifications of Risk Management for Banks based on Basel-III norms. Mobile Banking and Mobile Payment as Technology based Services fall under the operational risks category.

Mobile Payments using SMS, requires an SMS message from mobile phone to be sent to the destination Bank's short code or long code.  Mobile Payments using USSD requires making a  call from the mobile user's phone to the PAN India number  *99#  which is maintained by NPCI and a live session is established with the Bank server displaying the options to be chosen. The session duration of USSD is 3 minutes and earlier 1 rupee used to be charged, later 50 paise and now it is free to the mobile customer. Both SMS and USSD are categorized as un-encrypted channels by RBI. These are specifically beneficial to mobile users who still use feature phones which do not have capacity to support mobile app installation. Although most of the mobile users are smart phone users but Voice, SMS and USSD based Banking services are to be continued to support feature phone users as well to avoid digital divide. However, multi-lingual support to all mobile users to suit their customized requirement is to be further enhanced. Mobile broadband services by mobile telecom operators have facilitated Internet banking services through the mobile browser of the mobile user and using GRRS for mobile application based Mobile Payments and Mobile Banking. Banks had tough time to develop and provide mobile banking and mobile payment apps for all operating systems (around 10 a decade back and now only 2 for Android and iOS) and for all versions of an OS used by mobile users. Later RBI has facilitated non-bank entities such as technology company, mobile telecom operator and Fintechs to facilitate financial inclusion with an Escrow account in a Bank and to offer mobile payments using mobile wallet and mobile apps such as BHIM, Jiomoney, Airtel Money, Phone Pe, Google Pe, Paytm, etc. Further use of QR Code, OTP, Mobile PoS and BBPS set up by NPCI have revolutionized mobile payments adoption in a mass scale by every mobile user and every business person in India towards cashless transaction economy and now other countries are inspired to adopt the same for their population as well and UPI Payments solution is being extended to many countries by NIPL of NPCI.

Let us consider digital mobile payment where the entities involved in the Mobile Payment transaction are (i) Payer : A Registered Mobile User whose account is debited, say Payer-X, (ii) Payee : A Registered Mobile User who receives payment as Beneficiary, say, Payee-Y (iii) Payer's Bank: Bank of the Payer, where the account is debited or withdrawn, say Bank-A (iv) Payee's Bank: Bank of the Payee or Beneficiary, where the account is credited or deposited, say Bank-B, (v) Payer's PSP: Payment Service Provider who initiates Payers request through the Mobile Wallet or Mobile Payment App provided, say, PSP-1 (vi) Payee's PSP: Payment Service Provider who processes payment for receipt by the Beneficiary and confirms receipt to the Payee onto the Mobile Wallet or Mobile Payment App provided, say PSP-2, (vii) NPCI : Switching and Payment Gateway Organization, (ix) RBI : Settlement Bank (earlier CCIL) for Mobile Payments, (x) UIDAI : Central Biometric Authentication Agency for Mobile Users using AADHAR Number, (xi) Payer's Mobile Telecom Operator, say, MNO-1 (xii) Payees Mobile Telecom Operator, say, MNO-2. Here Payer may use a Banks Mobile Banking App or PSP's Wallet App such as BHIM, Phone Pe, Google Pay , PayTM, Jio Money, Airtel Money etc. A Mobile User can Directly Pay as a Payer or send request to Collect payment like a merchant Payee.



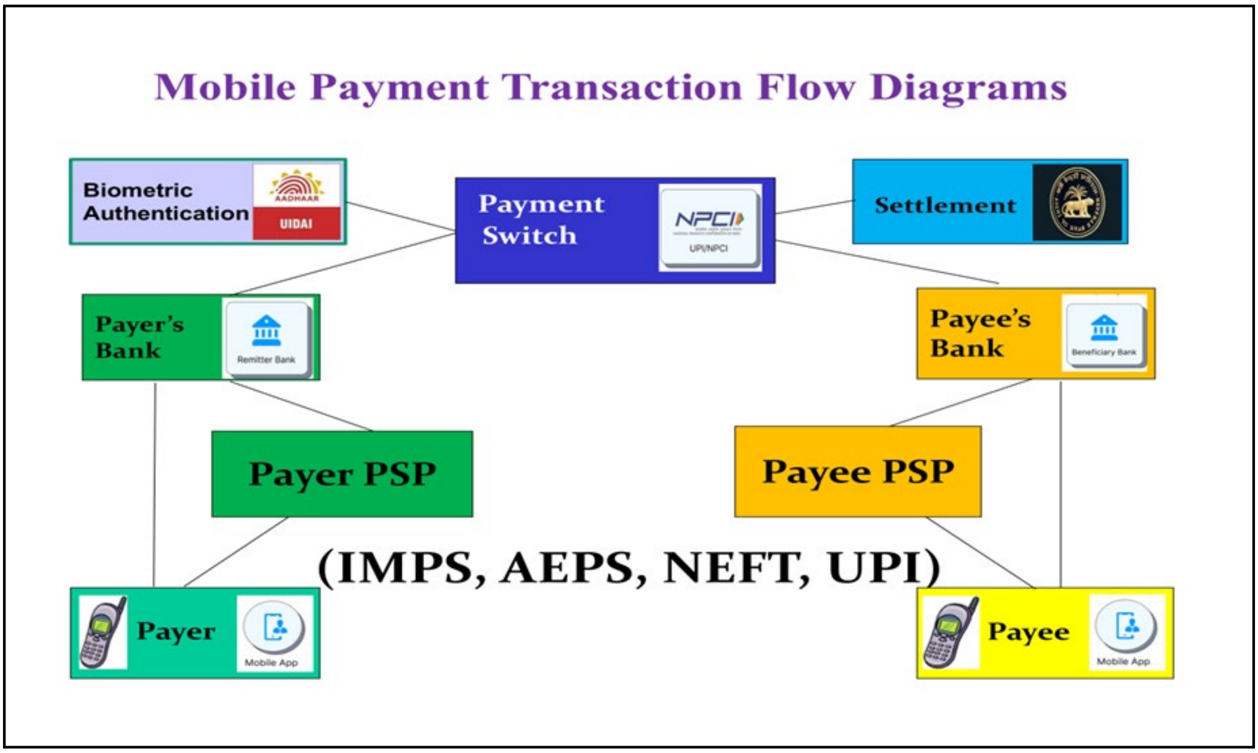
**Mobile Payment Transaction Steps**:

1. To start, Payer-X initiates payment transaction through PSP-1 Mobile application on own Mobile Device.
2. Payer-X provides authentication credentials on own Mobile Device.
3. The Payer-X Mobile Device initiates the Pay request with Payee-Y credentials to Payer PSP-1.
4. Payer PSP-1 checks the Payer-X credentials, validates and authenticates.
5. Payer PSP-1 forwards the pay request to NPCI.
6. NPCI resolves the Payee-Y Address (Account Held in Which Bank) in the following two ways

(a) If the Payee-Y Address has global identifiers (Mobile #, Aadhaar # or Account #) then the Payee-Y Address is resolved by NPCI central Mapper.

(b) If the Payee-Y Address has virtual address offered by Payee's PSP--2, then NPCI will send the request to Payee's PSP-2 for address translation.

7. In case of 6b, the Payee PSP-2 accepts or rejects the request based on the rules set at its end.
8. In case of 6b, on accepting the Pay request, Payee PSP-2 populates the Payee-Y details and responds to NPCI.
9. NPCI sends the debit request to the debit account provider Bank-A.
10. Account provider Bank-A authenticates the Payer-X based on the credential provided.
11. Account provider Bank-A debits the Payer-X account.
12. Account provider Bank-A sends Debit response to NPCI.
13. NPCI sends the Credit request to the credit account provider Bank-B.
14. Account provider Bank-B credits the beneficiary account based on the Payee-Y details
15. Account provider Bank-B sends Credit response to NPCI.
16. NPCI sends Pay response to Payee PSP-2.
17. Payee PSP-2 informs Payee-Y of Amount credited to the Account with Transaction Details.
18. NPCI sends pay response to Payer PSP-1.
19. Payer PSP-1 notifies the Payer-X immediately of the Amount Debited and confirmation of credit to Payee-Y with Transaction Details.
20. End of Transaction.



Mobile Payment Transaction Flow Diagrams

Biometric Authentication

AADHAAR

UIDAI

Payment Switch

NPCI

UPI/NPCI

Settlement

Payer's Bank

Remitter Bank

Payee's Bank

Beneficiary Bank

Payer PSP

Payee PSP

(IMPS, AEPS, NEFT, UPI)

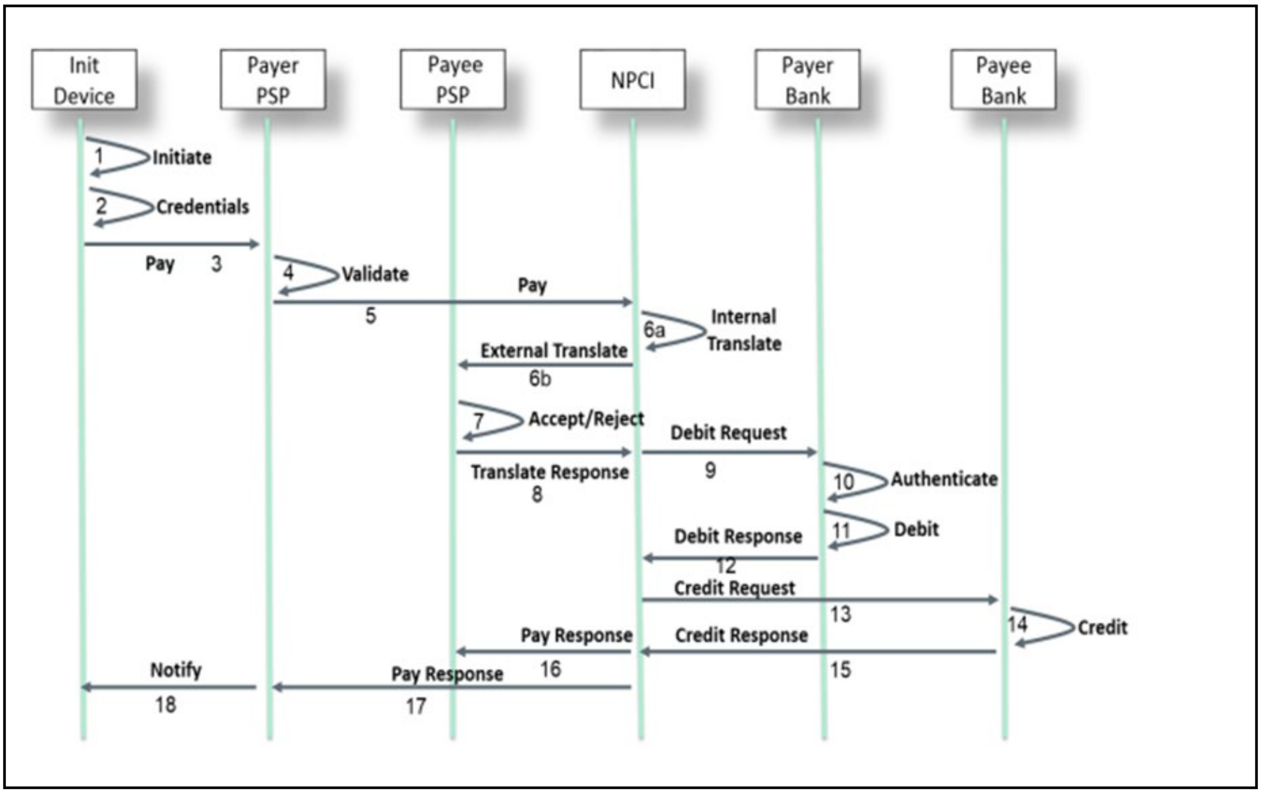
Payer

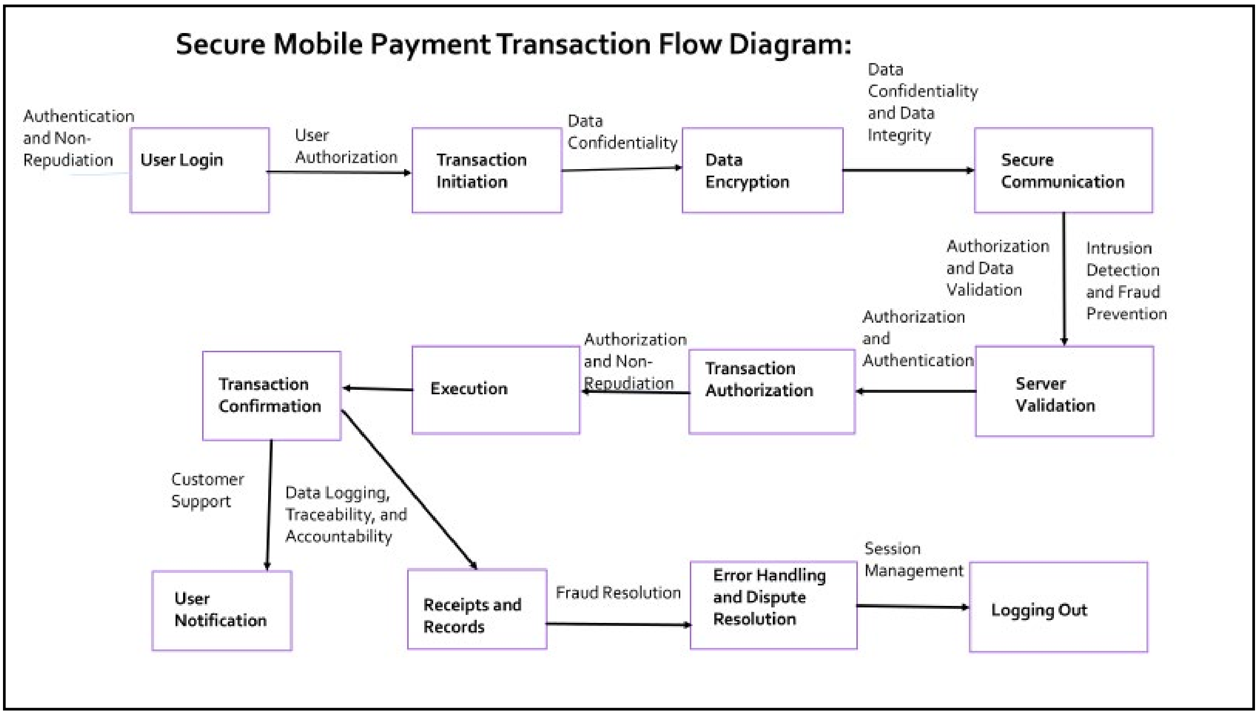
Mobile App

Payee

Mobile App

Sequence Diagram of Mobile Payment Transaction Flow




Secure Mobile Payment Transaction Flow Diagram:
Authentication and Non-Repudiation
User Login
User Authorization
Transaction Initiation
Data Confidentiality
Data Encryption
Data Confidentiality and Data Integrity
Secure Communication
Authorization and Data Validation
Intrusion Detection and Fraud Prevention
Authorization and Authentication
Server Validation
Transaction Authorization
Authorization and Non-Repudiation
Execution
Transaction Confirmation
Customer Support
Data Logging, Traceability, and Accountability
User Notification
Receipts and Records
Fraud Resolution
Error Handling and Dispute Resolution
Session Management
Logging Out

## Implementation of Mobile Payment Security Goals and Measures

| Mobile Security Goals | Entities Responsible | Achieved Through |
|---|---|---|
| Confidentiality | Payer’s Mobile Device, Bank, PSP, NPCI, MNO | Encryption/Decryption, Javax.crypto library |
| Integrity | Bank, PSP, NPCI, MNO | Encryption/Decryption, Check by Hash function, Checksum, digital signature library (Openssl). |
| Availability | Bank, PSP, NPCI, MNO | Server availability using server clusters and Services Availability by Testing for redundancy and scalability, Real time monitoring of DoS and DDOS attacks |
| Authentication | Payers Mobile Device, Bank, PSP, NPCI,MNO | Authentication of Mobile User, Mobile Device, Mobile App, Mobile Transaction Channel Used, Authentication APIs (Android fingerprint api, Touchid, etc.), IMEI, IMSI, MAC Address, Port Number |
| Authorization | Mobile Device, Bank, PSP, NPCI, MNO | Database or backend service to manage roles and permissions and enforce authorization checks in code, monitoring authenticated entities, mobile apps and APIs |
| Non-Repudiation | Mobile User, Bank, PSP, NPCI, MNO | e-Sign, PKI, Digital Signature, Cryptographic lib., Secure Element, Hardware Tokens, For digital signature and implement logging system to capture transaction time staming and location details. |

| | | |
|---|---|---|
| Access Control | Mobile Device, Bank, PSP, NPCI, MNO | Implementing access control logic in application code, use of access control lists (ACLs), RBAC, MAC, DAC, FGAC. |
| Traceability | Bank, PSP, NPCI, MNO | Log and event data files, data Use logging lib, Frameworks as Log4j to capture and store log data etc. |
| Accountability | Payers Mobile Device, Bank, PSP, MNO | Roles and Rules mapping, Mobile Banking Policy and Operative Guidelines, Associate actions with user accounts in application's database and log user activity. |
| Trust | Mobile User, Bank, PSP, NPCI, RBI, MNO | Metrics of measuring failures, established through HTTPs, secure boot process, and use of digital certificates (SSL/TLS) used by trusted Cas, User Awareness and Feedback |
| Reliability | Mobile User, Bank, PSP, NPCI, RBI, MNO | IT Scurity Policy, Services uptime maintaining to 99.9999 % , redundant hardware, error checking mechanisms and failover system, BCP/DR Policy, Security Drills |

### Remarks:

1. This case study is briefly explained to give broad understanding of meeting the emerging challenges of mobile service security for various verticals of mobile governance.

2. Banks have Operational Risk Management Policy, IT Policy, IT Security Policy, Digital Banking Policy, Mobile Banking Policy, Internet Banking Policy etc. along with Operative Guidelines specifying check lists for various security operations center teams to take appropriate and timely action, monitored by IT Strategy Committee, IT Security Committee and Integrated Risk Management Committees.

3. IDRBT (Institute for Development and Research in Banking Technology) has six research centers focused on areas relevant to the banking and financial sector, namely, AI & ML, Cyber Security, Emerging Networks, Open & Digital Banking, Quantum Computing, and Distributed Ledger & Innovation and collaboration with RBI, NIBM, NPCI, IFTAS, REBIT, IITs, NITs and Central University of Hyderabad and conducts Ph.D., M.Tech.(IT), PGDFT, PMPBF, EDPs, Workshops etc. ( https://www.idrbt.ac.in )

4. IDRBT conducts Security Drills, EDPs, IB-CART Threat Intelligence and CISO forum meetings, Training programs etc. to strengthen the Security Hygiene of the Banking Sector.

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

The National Centre of Excellence (NCoE) for Cybersecurity Technology Development has been conceptualized by the Ministry of Electronics & Information Technology (MeitY), Government of India, in collaboration with the Data Security Council of India (DSCI). Its primary objective is to catalyze and accelerate cybersecurity technology development and entrepreneurship within the country. NCoE plays a crucial role in scaling and advancing the cybersecurity ecosystem, with a focus on critical and emerging areas of security.

Equipped with state-of-the-art facilities, including advanced lab infrastructure and test beds, NCoE enables research, technology development, and solution validation for adoption across government and industrial sectors. By adopting a concerted strategy, NCoE aims to translate innovations and research into market-ready, deployable solutions—contributing to the evolution of an integrated technology stack comprising cutting-edge, homegrown security products and solutions.

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

## DATA SECURITY COUNCIL OF INDIA

☎ +91-120-4990253 | ncoe@dsci.in

https://www.n-coe.in/

4 Floor, NASSCOM Campus, Plot No.
7-10, Sector 126, Noida, UP -201303

Follow us on

@CoeNational
nationalcoe
nationalcoe
NationalCoE