**FACULTY OF EGINEERING & TECHNOLOGY**

MOBILE SECURITY

LECTURE -14

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

## OUTLINE

- **Protecting Android databases and data in transit**

- **User data protection**

- **App data protection**

- **Data Storage on Android**

- **MCQ**

- **References**

## Protecting Android Databases And Data In Transit

The amount of personal info kept on mobile devices these days is absolutely mind-boggling. From the exact location and favorite places, to bank accounts and passwords — our smart phones have become a true gold mine of information that many would like to get their filthy hands on. In light of this, the issue of data protection has never been so urgent as for both users and developers alike. We already explained how to protect data in iOS, so today we'll be addressing the key security points to consider when building Android applications.
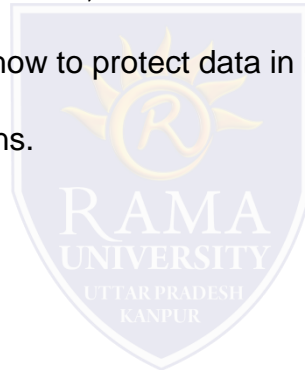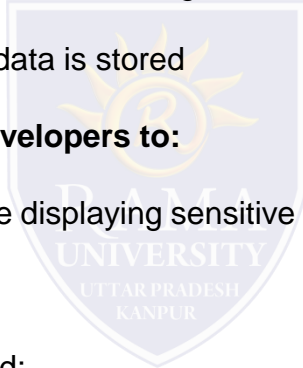
## User data protection

**These are the standard means of storing user data in Android:**

❑ Shared Preferences, a tool that keeps small amounts of data, e.g. app settings

❑ Account Manager, a tool that keeps user account data, i.e. logins, emails, passwords

❑ SQLite, the database where the rest of the app data is stored

**The standard means of data protection allow developers to:**

❑ set a mandatory lock password to request before displaying sensitive information;

❑ disable in-app screenshotting;

❑ disable screenshotting the app in the background;

❑ set a mandatory password to enter before important actions.

## App data protection

❑ Android applications are distributed as .apk files. Normally, users download them from official places like Google Play or Amazon.

❑ However, the same and many other applications are also available on third-party websites. And since the .apk format can be easily decompiled into pure Java code, attackers can gain access to various user data, e.g. authentication credentials, mechanisms of data transmission and protection, keys etc.

❑ To prevent that, developers use ProGuard, a tool that allows for compressing data, removing unused parts of libraries, as well as renaming methods and variables.
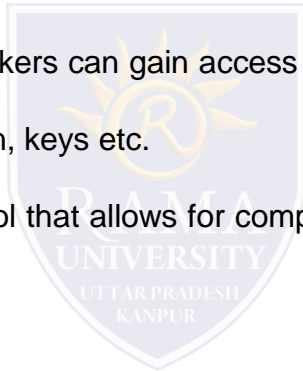
## Data Storage on Android

❑ Protecting authentication tokens, private information, and other sensitive data is key to mobile security. In this chapter, you will learn about the APIs Android offers for local data storage and best practices for using them.

❑ Storing data is essential for many mobile apps. For example, some apps use data storage to keep track of user settings or user-provided data. Data can be stored persistently in several ways. The following list of storage techniques are widely used on the Android platform:

- ❑ Shared Preferences

- ❑ SQLite Databases

- ❑ Realm Databases

- ❑ Internal Storage

- ❑ External Storage
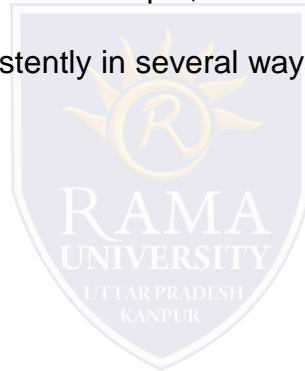
# MCQ

1. _____ is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction.
a) Network Security
b) Database Security
c) Information Security
d) Physical Security

2. From the options below, which of them is not a threat to information security?
a) Disaster
b) Eavesdropping
c) Information leakage
d) Unchanged default password

3. From the options below, which of them is not a vulnerability to information security?
a) flood
b) without deleting data, disposal of storage media
c) unchanged default password
d) latest patches and updates not done

4. _____ platforms are used for safety and protection of information in the cloud.
a) Cloud workload protection platforms
b) Cloud security protocols
c) AWS
d) One Drive

5. Which of the following information security technology is used for avoiding browser-based hacking?
a) Anti-malware in browsers
b) Remote browser access
c) Adware remover in browsers
d) Incognito mode in a browser

# REFERENCES

❑https://mobile-security.gitbook.io/mobile-security-testing-guide/android-testing-guide/0x05d-testing-data-storage