Unit 2:-

Security Models, Attacks and Counter-measures

★. Web Application :-

A web Application is an application program that is usually stored on a remote server, and users can access it through the use of softwares known as web Application.

Web Applications include online forms, shopping carts, word processors, spreadsheets, social media platforms etc.

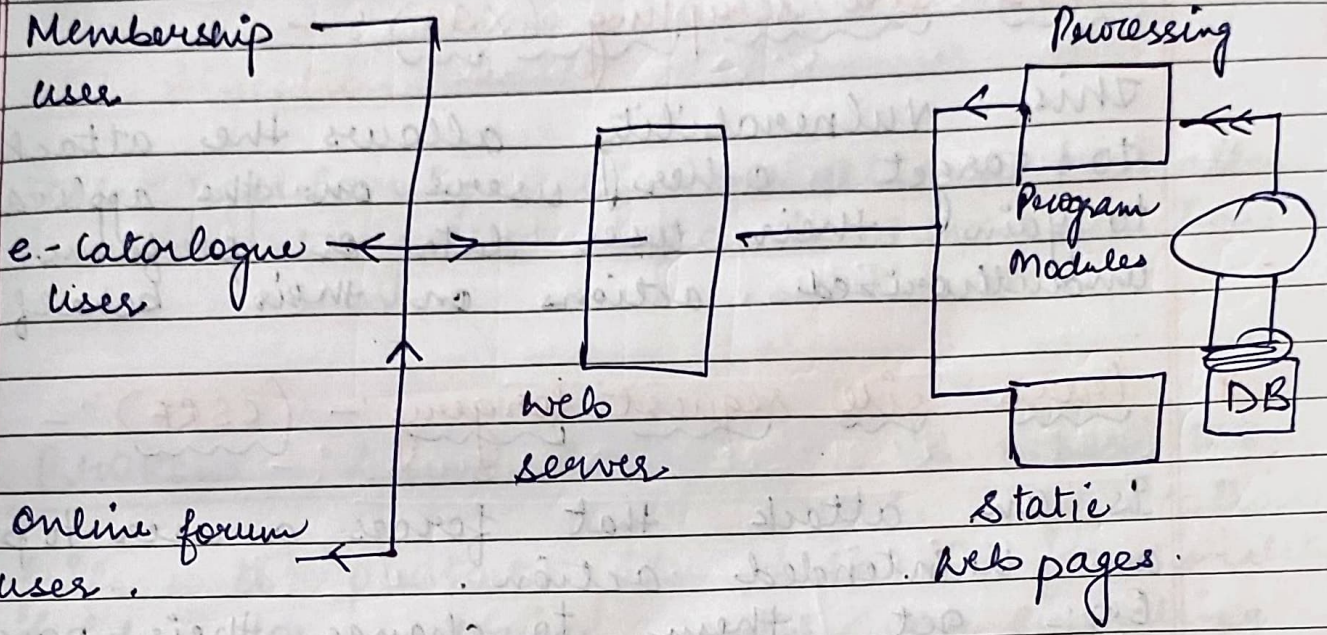
How does web-Application Work:-

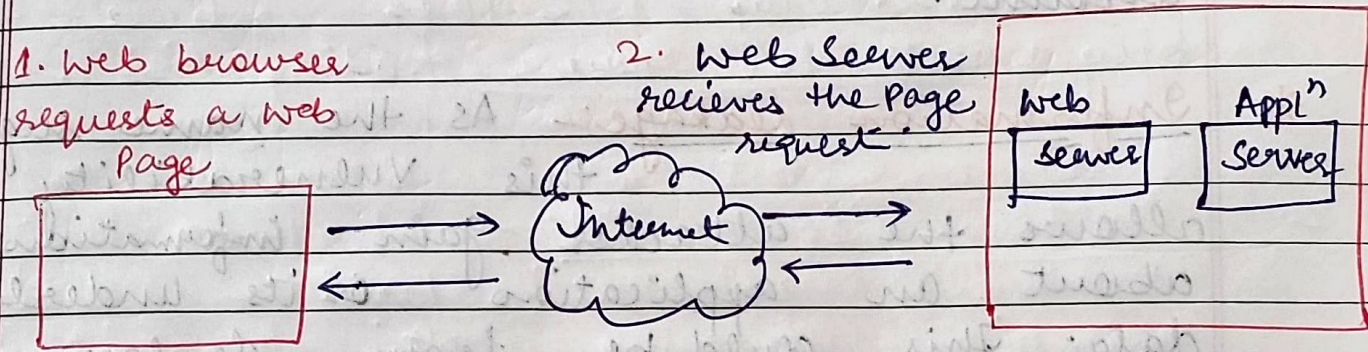
★. A web Application are generally coded using the languages supported by almost every web-browsers. such as HTML, javascript because these are the languages.

★ Some of the web Applications are entirely static due to which they are not required any processing on the server at all, while, on the other hand, some web applications are dynamic and require server side processing.

Date
Page

* To operate a web-Application, we usually required a web-server to manage the client's upcoming requests and required an application server.





Date
Page

* Hacking Web Applications :-

→ Some of the most common forms of attacks.

* Cross-site scripting (XSS) :-

This vulnerability allows the attacker to target other users on the application to gain their user data or perform unauthorized actions on their behalf.

* Cross site request forgery :- (CSRF) :-

Is an attack that forces a user to perform an unintended action.
E.g :- get them to change their password or transfer funds to the attackers account.

* Information Leakage :- As the name suggests this vulnerability allows the attacker gain information about an application or its underlying data. This could be from developers leaving comments in the source code or through poor error handling.

Authentication

* **Broken access controls :-**

this include vulnerabilities that allow users to set weak passwords, have weak or easily guessable recovery password questions.

* **SQL injection :-**

The popularity of this attack has fallen in recent years due to new functions

Broken - Access control :- Is where the web application fails to protect its data or functionality held for admin users on enabling an attacker to acces data.

Browser Extension :-

A browser extension is a small unit of software (referred to as a 'plug-in' when the software executes code) that performs various filters & controls to change the way a user might visit a web page or view information emanating the web server. (Ex:- Gmail)

* Browser extensions are usually tasked with adding for additional features & functionalities to a website.

Best Browser Extensions :-

1. Readability — chrome, Firefox, Safari

→ Readability is a read-later app so you can save any web page article or blog post to your reading list.

2. Awesome Screenshot - chrome, Firefox Safari :-

It gives you the option to capture an entire web page. You can crop the image and even annotate with circles, arrows and text.

Browser Extension :-

A browser extension is a small unit of software (referred to as a 'plug-in' when the software executes code) that performs various filters & controls to change the way a user might visit a web page or view information emanating the web server. (Ex:- Gmail)

* Browser extensions are usually tasked with adding for additional features & functionalities to a website.

Best Browser Extensions :-

1. Readability — chrome, Firefox, Safari

→ Readability is a read-later app so you can save any web page article or blog post to your reading list.

2. Awesome Screenshot - chrome, Firefox

Safari :-

It gives you the option to capture an entire web page. You can crop the image and even annotate with circles, arrows and text.

3. Stay Focused :- Stay Focused allows you to set time limits for yourself on distracting websites and then blocks your access to these sites when time is up.

4. Gmail offline → chrome :-

Read & respond to emails, archive messages and more - even if you're working without an internet connection. As soon as it detects that you're back online, the Gmail offline web app will automatically carry out any actions.

5. Add to Wunderlist - chrome, firefox, Safari

Mobile Malware

Mobile Malware :-

* Mobile malware is malicious software specifically designed to target mobile devices, such as smartphones and tablets with the goal of gaining access to private data.

* Although mobile malware is not current as pervasive as malware

Different Types of Mobile Malware :-

1. Spyware and Madware :-

* Madware, short for mobile adware, usually finds its way onto a mobile phone through the installation of a script or program and often without the consent of the user.

*. Most madware variants usually include an element of spyware, which collects information about your internet usage and sends it to a third party.

* Drive - by Downloads :-

If you open the wrong email or visit a malicious website, you could became the victim of a form of mobile malware known as the drive - by - download.

Mobile Phishing :- Phishing is a hacking technique that makes a user believe that he is interacting with the interface of a trusted third party (eg... bank) in order to exfiltrate personal information such as password, credit card numbers, social security no. etc.

Browser Exploits :-

How to Protect Against Mobile Malwares :-

Keep Applications updated :-

Install mobile security software.

Use screen lock protection.

only download apps from official stores.

Android Security Model :-

* Android platform uses the linux user-based permissions model to isolate applications resources.

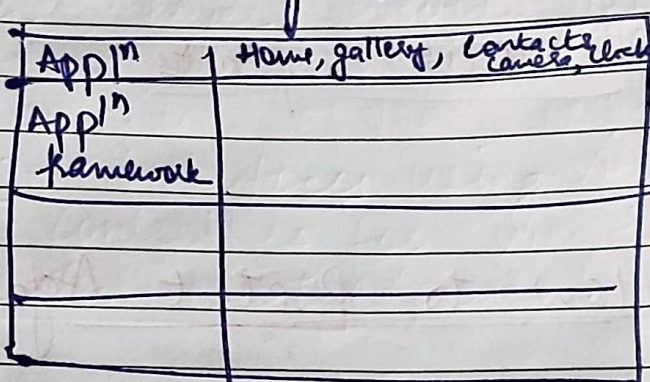
* This process is called application sandbox.

→ The main aim of sandboxing is to prevent malicious external programs from interacting with the protected app.

Three Security layers :-

The security model is based on the consent of the following parties :-

* Operating System
* Application
* End-user.



Sandboxing :-

Android platform uses the linux user-based permissions to isolate application resources. This process is called appl^n sandbox.

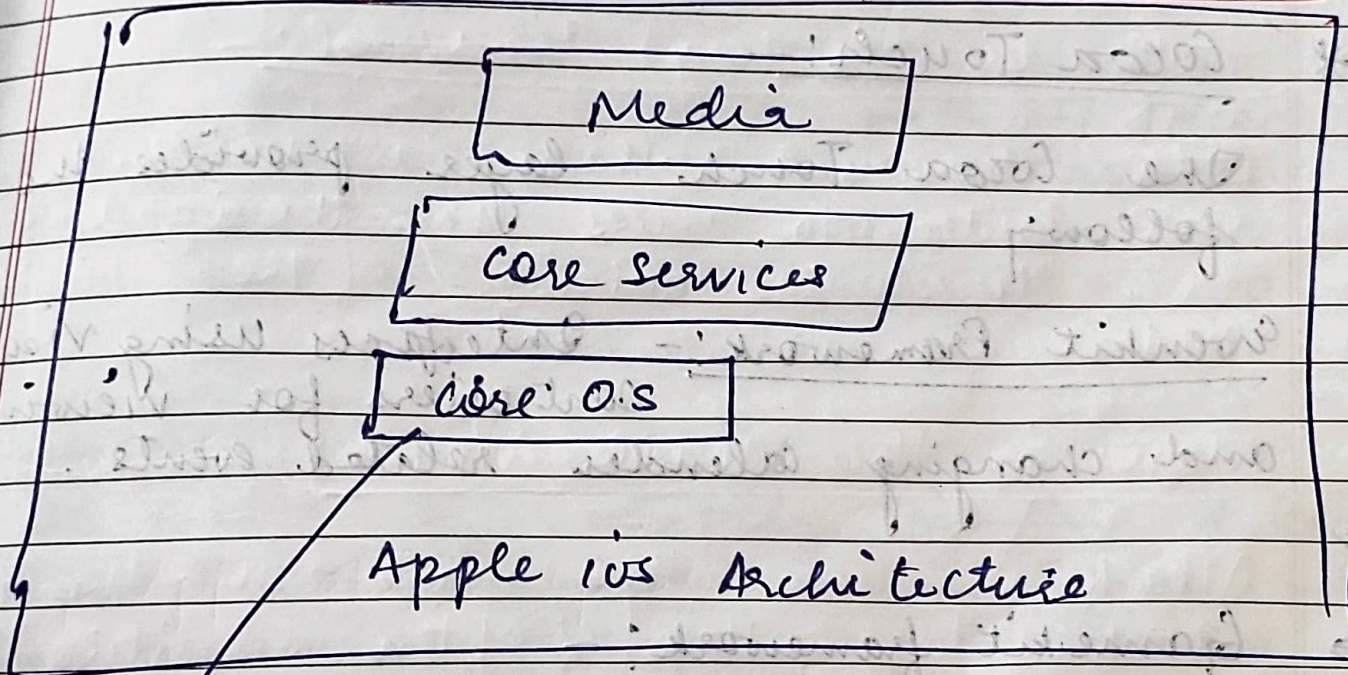
* The aim of sandboxing is to prevent malicious external programs from interacting with the protected app.

IOS Security Model :-

The IOS architecture is layered, It contains an intermediate layer between the applications and the hardware so they do not communicate directly.

* The lower layers in ios provide the basic services and the higher layers provide the user interface and sophisticated graphics.

The Layered architecture of IOS.



Technologies Core Bluetooth Framework, & External Accessory Framework.

Core Services

cloudkit framework.

The data can be moved b/w the app the icloud using.

core foundation framework

This provides the data management and services features for the IOS apps.

* Cocoa Touch:-

The Cocoa Touch layer provides the following

↳ Eventkit Framework:- Interfaces using View controllers for viewing and changing calender related events.

↳ Gamekit framework:-

↳ Mapkit framework:-

Media :-

This provides support for designing images and animating the views content.

* Web Security Attacks :-

* Malware Attack :-

* cross-site scripting (XSS) :-

* Injection Attacks :-

The injection attack methods target the website and the server's database directly.

* fuzzing :-

It works by initially inputting a large amount of random data (fuzz) into an application to get it to crash.

→ The best way to combat a fuzzing attack is by keeping os, your security, and other apps updated.

* Zero - Day Attack

There are two scenario of how malicious hackers can benefit from the zero-day attack.

↳ The first case is if the attackers can get information about an upcoming security update, they can learn where the loopholes are before the update goes live.

↳ The cyber criminals get the patch info and target users who don't haven't yet updated their systems.

* Path (or Directory) Traversal :-

Path traversal attacks target the web root folder to access unauthorized files or directories outside of the targeted folder.

* Man in the Middle Attack :-

Attackers use the man-in-the middle attack to gather (often sensitive) information. The criminal intercepts the data as it is being transferred b/w two parties.

Brute Force Attack :-

It is very straight forward method for accessing the login information of a web applⁿ.

* The attacker tries to guess the username and password combination to access the user's account.

Phishing :-

PHP & ASP.NET

* PHP is compatible with all major OS including windows, linux & mac os.

* PHP:- Pros and Cons:-

Pros:-
* free & open-source
* easy to learn & use
* server-side
* Good for small & medium size projects.
* Good for database functioning & communication.

Cons:-

* Not suitable for every project
* Error handling is poor.
* Run a bit slow
* Some debugging issues

Difference b/w PHP & ASP.NET

PHP	ASP.NET
* PHP is a server side coding / Programming language.	* ASP.NET is a web application framework.
* Its base language is C language.	* Its base language is Visual basic syntax language.
* It is supported by community and technology.	* It is supported by microsoft.
* PHP is focused on UI and client side.	* ASP.NET is focused on functionality & security.
* It works in accordance with HTML.	* It is highly flexible with OOPS concept.
* Freely available all over the web.	* License cost attached
* It provides decent speed & fast enough for desktop appln.	* It is not suitable & slower desktop app
* It is Platform independent	* ASP.NET only supports the windows platform

Date
Page

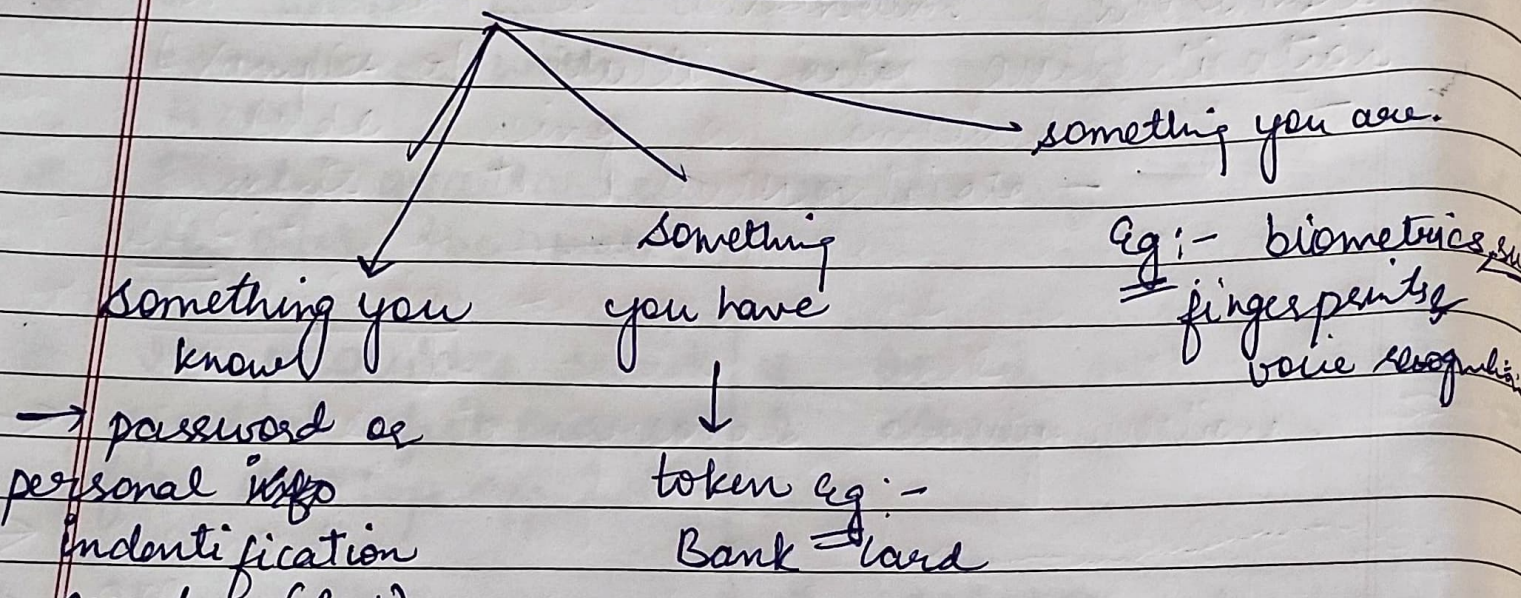
Authentication :-

* Authentication is the process of determining whether someone or something is, infact, ...

* Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users.

Eg :- Username and password combination is the most popular authentication mechanism, and it is also known as password authentication.

3 Authentication Methods :-



2FA :- 2-factor authentication

It is a security process.

→ First Layer → Password

2nd Layer → finger / biometric

→ Now whether you are.

1 → * Two-factor authentication verifies your identity and referred to as 'two-step verification or dual-factor authentication.

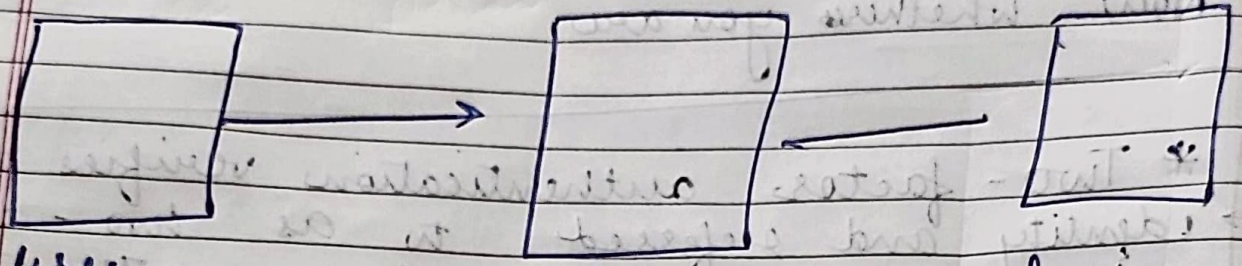
2. It is a security process in which users provide two different authentication factors to verify themselves.

→ 2FA is implemented to better protect both a user's credentials and the resources the user can access.

Multi-factor authentication

★ Multifactor authentication is a authentication that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account or a VPN.

Step 1:- User



User name & password | Pin from phone | finger print.

A layered approach to securing data & applications where a system requires a user to present a combination of two or more credentials to verify a user's identity to login

Examples of Multi-factor authentication include using a combination of these elements to authenticate:-

★ Knowledge:-

→ Answers to personal security questions.

→ Password.

↳ OTPs (can be both Knowledge and Possession)

Possession *

1. OTPs generated by smartphone app.
2. OTP sent via text or email.
3. Access badges.

Inherence:

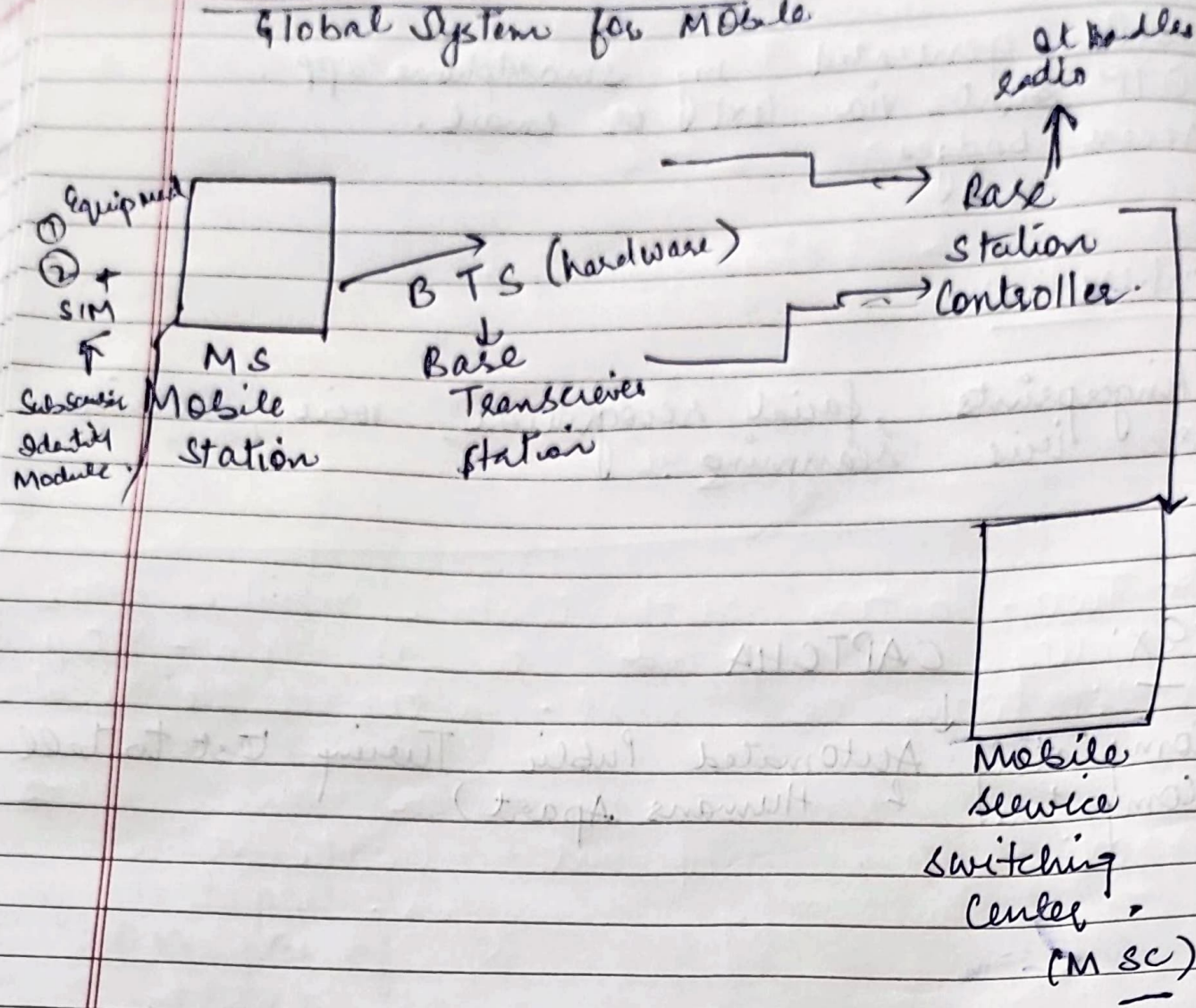
* Fingerprints, facial recognition, voice, retina or iris scanning.

Ex:- CAPTCHA

(Completely Automated Public Turing test to tell Computers & Humans Apart)

GSM Architecture

Global System for Mobile



BSC:- The manages the radio resources for one or more BTS. It handles radio channel setup, frequency hopping & handovers.

It is a connection b/w mobile & MSC.

MSC: The central component of the N/w sg subsystem is the MSC.

*. The MSC performs the switching of calls b/w the mobile and other fixed or mobile n/w users, as well as the managmt of mobile services.