Networking Notes – 3:

While talking to someone in our day-to-day life we always follow some rules and regulations how to talk with that person depending on who he or she is. In front of a teacher, you would be very polite and civil, in front of our parents we are very innocent and in front of our friends we forget all rules and regulations.

Similarly in a network there are set of rules that computers in the network have to follow to communicate to other computers. These rules are known as Protocols (Protocols are a general term and you would find them used everywhere, but their meaning remains the same).

Definition: Protocol refers to the set of rules and regulations applicable for a network. The protocol defines standardized format for the data packet to be transmitted through the network, techniques for detecting the errors whenever they arise and methods to correct these errors and so on.

(We would go through only the Definitions of the protocols for now, these have a lot of internal details and you would get to know about them in higher classes.)

1. **TCP/IP (Transmission Control Protocol/Internet Protocol):** TCP/IP comprises two protocols: TCP and IP. The Internet Protocol (IP) governs the transmission of information packets across networks, employing a packet addressing system enabling any Internet-connected computer to forward a packet to a destination that brings it closer to its intended recipient. Meanwhile, the Transmission Control Protocol (TCP) guarantees the dependable transmission of data across interconnected Internet networks. TCP conducts error checks on packets and initiates retransmission requests upon detecting errors.
2. **FTP (File Transfer Protocol):** FTP is designed to transfer files from one system to another. Using FTP, different people locating in different geographical locations can cooperate and work on a common project. FTP is designed to promote sharing of files and to encourage the indirect use of remote computers. Using FTP, any type of file can be transferred from one computer to another. Though for transferring files, we have to specify whether the file is in ASCII format or in binary format.
3. **PPP (Point to point Protocol):** The PPP is used with dial-up Internet connections including ISDN. It is a layered protocol, which is used for transmitting the data over usual telephone lines. It can provide connection authentication, transmission, encryption and compression.

4. **Remote Login(Telnet):** Telnet is a protocol enabling connections to remote computers, referred to as hosts, across a TCP/IP network like the internet. Utilizing telnet client software, your computer establishes a connection to a telnet server, essentially the remote host. This protocol enables a user, operating from one computer, to engage with a program situated on another computer through a remote login facility. The remote login service on the internet is termed TELNET. Accessing this service involves invoking a local application program and specifying the remote machine.

Wireless Communication Technologies:

1. **GSM (Global System for Mobile Computing) :** GSM is developed to describe protocols for second generation (2G) digital cellular networks used by mobile phones. It is developed by the European Telecommunications Standards Institute (ETSI) for the replacement of first generation (1G) analog cellular networks and originally described a digital circuit switched network optimized for full duplex voice telephony. Full duplex means receives and sends the data at a time. 'GSM' is a trademark owned by the GSM Association.
2. **CDMA (Code Division Multiple Access):** CDMA stands for Code Division Multiple Access. It is a digital cellular technology that uses spread spectrum techniques. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time and it is the common platform on which 3G technologies are built. CDMA is a military technology first used during world war II by english allies to foil german attempts at jamming transmission.
3. **WLL(Wireless Local Loop):** Wireless Local Loop (WLL) refers to an application delivering telephone service to remote rural areas, connecting subscribers to the nearest exchange through a radio link instead of traditional copper wires. Also known as Radio In The Loop (RITL) or Fixed-Radio Access (FRA), WLL offers advantages over satellite broadband due to its reduced transmission delay. Utilizing a full-duplex radio network with high data access capacity, WLL systems boast comparable installation costs to copper cables, contingent on factors like subscriber line length and local conditions. A commercialized PHS-WLL system is set for implementation in multiple countries, highlighting the technology's increasing deployment for widespread commercial service.

4. **GSM and GPRS:**
   GSM, short for Global Systems for Mobile, represents a cellular standard crucial for mobile phone communication, focusing on data delivery and mobile services through digital modulation, particularly impacting society through SMS. As the cornerstone of 2G technology, GSM operates as a circuit-switched network, heavily reliant on connection duration for billing. Not directly linked to the internet, GSM's hallmark feature is the widely embraced Short Messaging Service (SMS). This standard enjoys extensive global coverage, accessible in nearly all countries, offering its services to a vast user base.

   GPRS, or General Packet Radio Service, stands as an advancement over GSM, enhancing its capabilities significantly. This upgrade offers users faster data speeds and seamless, wireless access to packet data networks, surpassing the conventional GSM technology. As a pioneer of 2.5G technology, GPRS operates as a packet-switched network, where billing hinges on the total data transferred rather than connection duration. Enabling direct internet connections, GPRS boasts the popular Multimedia Messaging Service (MMS) among its offerings. However, GPRS services are limited to developed regions with robust network infrastructure, restricting its availability to select countries.

Mobile Telecommunications:

We use mobile phones in our day to day life and they are the most common and most used example of wireless communication. Mobile communication technologies are divided into several generations. With each generation new technologies, features etc are introduced into the mobile communication market. Some of these are:

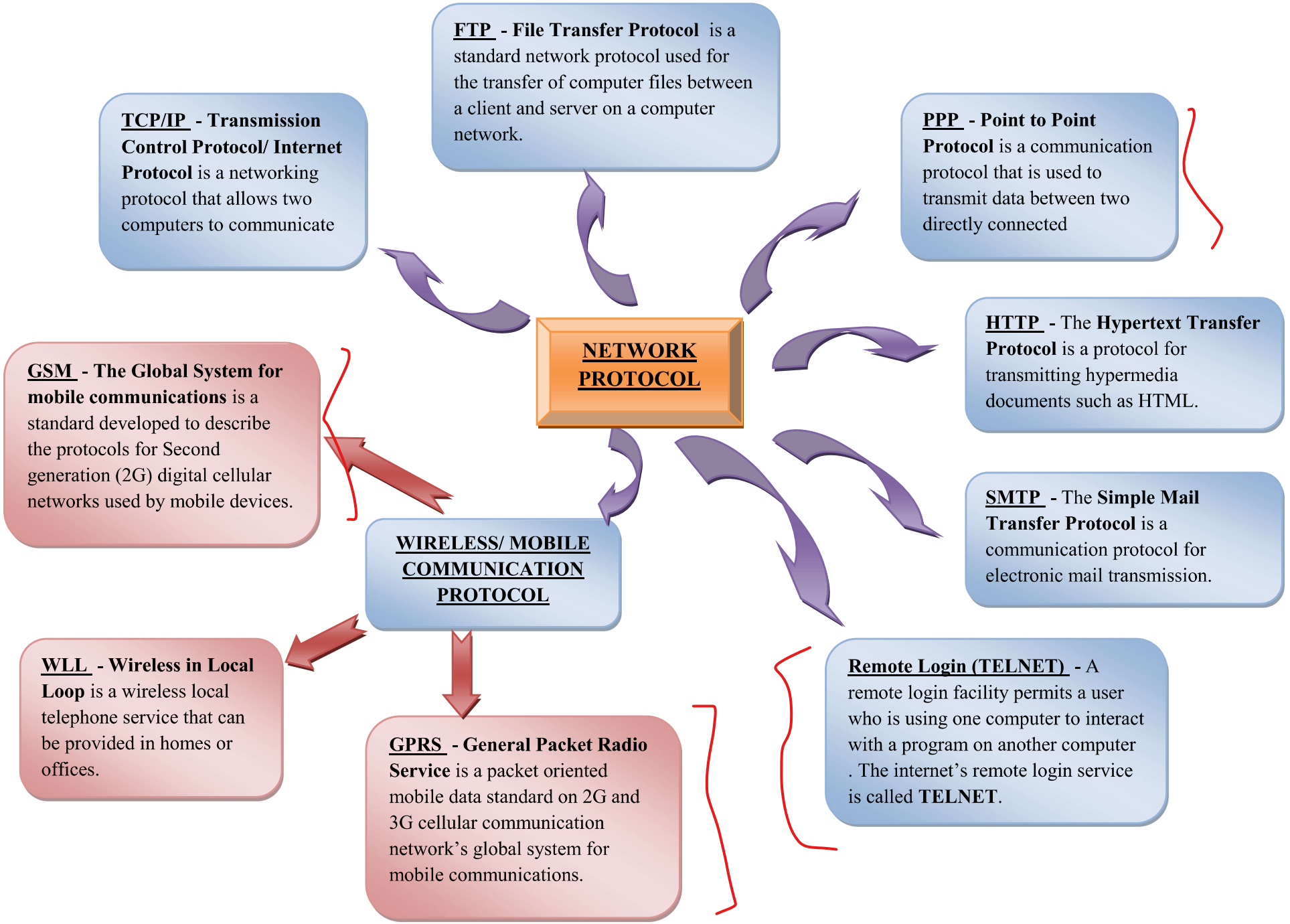
1. 1G(1st Generation) : The first generation 1G came around 1982. In this network system, users can do voice calls only. It was using an only analog signal that was carrying out the voice from the caller to the server.

2. 2G (2nd Generation): The second generation of mobile network system was developed in 1991. This network system was using the digital signal for data transmission. The more features were added in 2G as more people can communicate simultaneously and improved the security with signal encryption. In this technology SMS and MMS were introduced.

3. 3G (3rd Generation): The 3G was developed during the late 90s, but it was introduced around 2001. It provided both voice and data services. In fact, 3G network system has increased the use of the internet as it was used in mobiles. It provides internet access via the same radio towers which are providing network signal to mobile phones.

4. 4G(4th Generation): 4G has changed the entire world and smart phones came into the picture. In India, Reliance Jio has launched the 4G first with free of cost and rapidly changed the market of smart phones and internet. 4G provides better speed and given the access to wireless devices with interactive multimedia, voice, radio, internet and broadband service.

NETWORK PROTOCOL



MOBILE TELECOMMUNICATION TECHNOLOGIES

COMPARISON BETWEEN 1G, 2G, 3G, 4G AND 5G

Technology / Features	*1G*	*2/2.5G*	*3G*	*4G*	*5G*
Start/ Deployment	1970/ 1984	1980/ 1999	1990/ 2002	2000/ 2010	2010/ 2015
Data Bandwidth	2 kbps	14.4-64 kbps	2 Mbps	200 Mbps to 1 Gbps for low mobility	1 Gbps and higher
Standards	AMPS	2G: TDMA, CDMA, GSM 2.5G: GPRS, EDGE,1xRTT	WCDMA, CDMA-2000	Single unified standard	Single unified standard
Technology	Analog cellular technology	Digital cellular technology	Broad bandwidth CDMA, IP technology	Unified IP and seamless combination of broadband, LAN/WAN/	Unified IP and seamless combination of broadband,

VoIP – Voice Over Internet Protocol

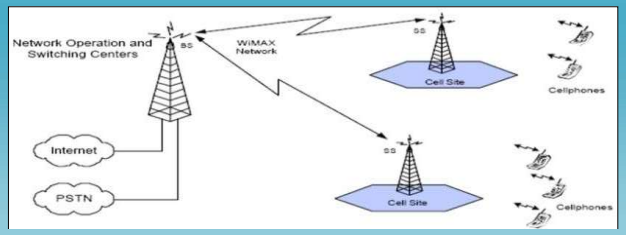
It is a technology that allows you to make voice calls using a broadband internet connection instead of a regular phone line.

WiFi – Wireless Fidelity

Wifi is a universal wireless networking technology that utilizes radio frequencies to transfer data.

WiMax –

WiMax stand for **Worldwide Interoperability for Microwave Access (AXess)**, and it is a technology for point to multipoint wireless networking. It provides high speed data over a wide area.



NETWORK SECURITY CONCEPTS

VIRUS

- A **computer virus** is malware attached to another program (such as a document), which can replicate and spread after an initial execution on a target system where human interaction is required.

WORMS

- A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers.

TROJAN HORSE

- A **Trojan horse**, or **Trojan**, is a type of malicious code or software that looks legitimate but can take control of your computer. A **Trojan** is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network. A **Trojan** acts like a bona fide application or file to trick you

SPAM

- **Spam** is digital junk mail: unsolicited communications sent in bulk over the internet or through any electronic messaging system

COOKIES

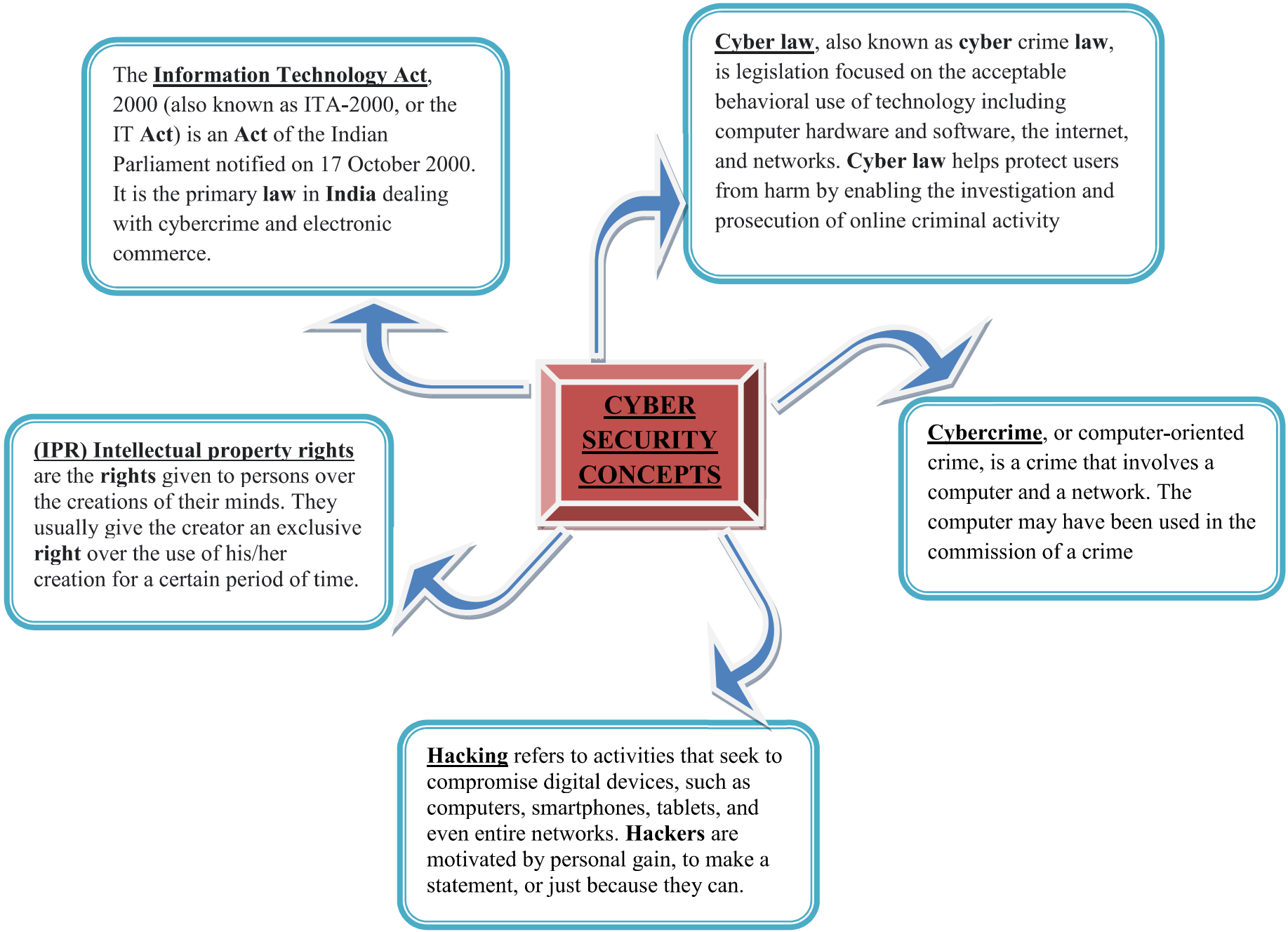
- **Cookies** are text files with small pieces of data — like a username and password — that are used to identify your **computer** as you use a **computer** network. Specific **cookies** known as HTTP **cookies** are used to identify specific users and improve your web browsing experience.

FIREWALL

- A **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A **firewall** typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

HTTPS

- Hypertext Transfer Protocol Secure (**HTTPS**) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.


CYBER SECURITY CONCEPTS
The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.
Cyber law, also known as cyber crime law, is legislation focused on the acceptable behavioral use of technology including computer hardware and software, the internet, and networks. Cyber law helps protect users from harm by enabling the investigation and prosecution of online criminal activity
(IPR) Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time.
Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime
Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks. Hackers are motivated by personal gain, to make a statement, or just because they can.