# CAIIB Elective Subject – Information Technology – Subject Updates

## *Internet of Things (IoT)*

If you own a Smartphone and wear a Fitbit, then the Internet of Things (IoT) phenomenon is already impacting your daily life, and probably more than you think. In today's world, the Internet of Things, or IoT as it is also called, has grown beyond simply laptops, smartphones and tablets and includes everything from fitness trackers to even fritz, air conditioning unit at your home or office.

The IoT has a significant ability to impact the future of mankind. We are entering a world where everything has the potential to be connected. In fact, there is an estimate that by 2020, the installed base for the IoT will be as high as 212 billion, including 30 billion "connected things." This is a large market and will have a great impact on the daily life of the average person. There is already talk of connected and self-driving cars, "smart" homes and even connected healthcare is in the works, indicating the huge potential impact of the Internet of Things.

The Internet of Things has a financial impact as well, with the projected value expected to be close to $30 billion by 2020. This is going to become a major factor in the global economy as connectivity becomes the norm in the next few years. IoT is in fact termed by some as 'bigger than industrial revolution' in the world economy. One of the most important challenges associated with IoT is security, which needs to be addressed with priority as IoT is evolving with tremendous speed.

## *Initiatives by Government of India for Propagating e-Banking*

For growth and development and to promote e-banking in India the Indian government and RBI have been taken several initiatives.

- The Government of India enacted the IT Act, 2000 with effect from October 17, 2000 which provided legal recognition to electronic transactions and other means of electronic commerce.
- The Reserve Bank monitors and reviews the legal requirements of e-banking on a continuous basis to ensure that challenges related to e-banking may not pose any threat to financial stability of the nation
- Dr. K.C. Chakrabarty Committee including members from IIM, IDRBT, IIT and Reserve Bank prepared the IT Vision Document- 2011-17, which provides an indicative road map i.e. guidelines to enhance the usage of IT in the banking sector.
- The Reserve Bank is striving to make the payment systems more secure and efficient. It has advised banks and other stakeholders to strengthen the security aspects in internet banking by adopting certain security measures in a timely manner. RBI believes that the growing popularity of these alternate channels of payments (such as: Internet Banking, Mobile Banking, ATM etc.) brings an additional responsibility on banks to ensure safe and secure transactions through these channels.
- National Payments Corporation of India (NPCI) was permitted by the RBI to enhance the number of mobile banking services and widen the IMPS (Immediate Payment Service)

channels like ATMs, internet, mobile etc. Along with this, NPCI is also working to bring more mobile network operators which can provide mobile banking services through a common platform.

There has been a dramatic surge in the volume and value of mobile transactions in the recent past. MoM increase in no. of transactions from Dec14 to Dec 15 was 135% and Dec 15 to Dec 16 was 182%. MoM increase in value of transactions from Dec 14 to Dec 15 was 330% and Dec 15 to Dec 16 was 178%.

***The future:***

In the backdrop of demonetization- a colloquial term for the withdrawal of 86 percent of the value of India's currency in circulation by the Government of India since 8th November 2016 followed by digital push for 'less cash' economy, a dramatic multi-fold rise in e-banking transactions and especially mobile banking transactions, is expected in the near future.

***Interactive Technology for Banks***

With the launch of sbiINTOUCH on 1st July, 2014, State Bank of India was the first Bank in India to introduce the concept of "Digital Banking". State of the art technology like Debit Card Printing Kiosks, Interactive Smart Tables, Interactive Digital Screens, Remote Experts through video call etc were introduced to providing a completely different experience through online self-service mode.
The key feature of these branches is that one can open one's savings bank account - Account Opening Kiosk (AOK) within 15 minutes. Besides that you can have access to a vast array of Banking related activities and products.

India's first banking robot Lakshmi made her debut in November 2016 by City Union Bank, the artificial intelligence powered robot will be the first on-site bank helper. Lakshmi, which took more than six months to develop, can answer intelligently on more than 125 subjects. Top private lender HDFC Bank, which is also experimenting with robots to answer customer queries, is testing its humanoid at its innovation lab.

***Types of cloud computing***

Cloud computing is typically classified in two ways:

1. Location of the cloud computing
2. Type of services offered

**1. Location of the cloud**

Cloud computing is typically classified in the following three ways:

***Public cloud:*** In Public cloud the computing infrastructure is hosted by the cloud vendor at the vendor's premises. The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations.

***Private cloud:*** The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Some experts consider that private clouds are not real examples of cloud computing. Private clouds are more expensive and more secure when compared to public clouds.

Private clouds are of two types: On-premise private clouds and externally hosted private clouds. Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than On-premise private clouds.

***Hybrid cloud***: Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud.

***Community cloud*** involves sharing of computing infrastructure in between organizations of the same community. For example all Government organizations within the state of California may share computing infrastructure on the cloud to manage data related to citizens residing in California.

**2. Classification based upon service provided**

Based upon the services offered, clouds are classified in the following ways:

***Infrastructure as a service (IaaS)*** involves offering hardware related services using the principles of cloud computing. These could include some kind of storage services (database or disk storage) or virtual servers. Leading vendors that provide Infrastructure as a service are Amazon EC2, Amazon S3, Rackspace Cloud Servers and Flexiscale.

***Platform as a Service (PaaS*)** involves offering a development platform on the cloud. Platforms provided by different vendors are typically not compatible. Typical players in PaaS are Google's Application Engine, Microsoft's Azure and Salesforce.com's force.com .

***Software as a service (SaaS)*** includes a complete software offering on the cloud. Users can access a software application hosted by the cloud vendor on pay-per-use basis. This is a well-established sector. The pioneer in this field has been Salesforce.com's offering in the online Customer Relationship Management (CRM) space. Other examples are online email providers like Googles gmail and Microsoft's hotmail, Google docs and Microsoft's online version of office called BPOS (Business Productivity Online Standard Suite).

**Challenges of cloud computing**

Cloud computing challenges have always been there. Companies are increasingly aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. Some of the most important challenges are as follows.

***Security and Privacy:*** The main challenge to cloud computing is how it addresses the security and privacy concerns of businesses thinking of adopting it. The fact that the valuable enterprise data

will reside outside the corporate firewall raises serious concerns. Hacking and various attacks to cloud infrastructure would affect multiple clients even if only one site is attacked. These risks can be mitigated by using security applications, encrypted file systems, data loss software, and buying security hardware to track unusual behavior across servers.

***Availability & Scalability:*** It is difficult to assess the costs involved due to the on-demand nature of the services. Budgeting and assessment of the cost will be very difficult unless the provider has some good and comparable benchmarks to offer. The service-level agreements (SLAs) of the provider are not adequate to guarantee the availability and scalability. Businesses will be reluctant to switch to cloud without a strong service quality guarantee.

***Interoperability and Portability:*** Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT.

***Reliability and Availability:*** Cloud providers still lack round-the-clock service; this results in frequent outages. It is important to monitor the service being provided using internal or third-party tools. It is vital to have plans to supervise usage, SLAs, performance, robustness, and business dependency of these services.

***Performance and Bandwidth Cost:*** Businesses can save money on hardware but they have to spend more for the bandwidth. This can be a low cost for smaller applications but can be significantly high for the data-intensive applications. Delivering intensive and complex data over the network requires sufficient bandwidth. Because of this, many businesses are waiting for a reduced cost before switching to the cloud.

*All these challenges should not be considered as road blocks in the pursuit of cloud computing. It is rather important to give serious consideration to these issues and the possible ways out before adopting the technology.*

**Future of cloud technology in India**

In February 2017, US tech giant Oracle predicted that as enterprise cloud is expected to become the most secure place for IT processing with nearly 60 per cent IT organisations to move their systems management to the cloud in 2017, India will be among top beneficiaries from cloud computing.

Increased government spending on digital technologies, coupled with heightened demand from the private sector, continues to be a great boost for the cloud industry. Not only the large firms, cloud will empower small business innovation in 2017 and Artificial Intelligence (AI) will become a reality, Oracle said. Gartner has predicted that in India alone, the cloud market will reach over $3 billion by 2017—an almost five-fold increase from 2012.

India Inc has pledged R4.5 lakh crore for Digital India, which can create employment for some 18 lakh people. A good number of them will be in cloud computing. With the launch of 100 Smart Cities, 500 rejuvenated cities and numerous projects to create industrial hubs, a strong virtual backbone, which is possible with cloud technology, is a critical necessity to take the development process to the next level.

**Latest Trends in Virtualilzation**

**Network and Storage Virtualization**

The virtualization of storage and virtual storage area networks (VSANs) is another trend that's gaining ground. Like server virtualization, VSANs offer greater ease of use, security, flexibility and scalability, since businesses do not need to buy more hardware or invest in updating it while scaling up. This also reduces hardware redundancy, in addition to investment costs.

**Updated Physical Resources**

The computing and storage equipment that IT departments use, as well as physical network parts like routers and switches, have undergone a sea change in recent times. Newer kinds of hardware available today are designed to run and configure VLANs (virtual LANs) as well as support virtual network design and implementation, and companies are investing in these to avoid virtualization issues. We shall discuss VLANs in more detail in the chapter on 'Networking Systems'.

**New Players in Virtualization**

While VMware has been the main player in virtualization technology so far, there are many new ones joining the race. Some of these deal with specific solutions and activities like VMware monitoring while others like Citrix, IBM and HP are gaining ground with alternative software and systems, especially targeting companies who have faced VMware problems in the past.

***Mobile phone operating systems***

There are also mobile phone operating systems that have gained tremendous importance recently. In the mobile world mostly it is the operating system that rules the mobile phone market. Some of the most popular mobile operating systems are Android, iOS (iPhones), Blackberry and Windows. Each mobile OS has numerous versions. Android OS is the unquestioned king of mobile market followed far behind by iOS as of date.

***Microsoft Windows operating systems***

Microsoft Windows is a family of proprietary operating systems designed by Microsoft Corporation and primarily targeted to Intel architecture based computers, with an estimated 89 percent total usage share on Web connected computers. In 2011, Windows 7 overtook Windows XP as most common version in use. The latest version is Windows 10.

Microsoft Windows was first released in 1985, as an operating environment running on top of MS-DOS, which was the standard operating system shipped on most Intel architecture personal computers at the time. In 1995, Windows 95 was released which only used MS-DOS as a bootstrap. Later to 2000 all versions have been based on the Windows NT kernel. Windows NT (New Technology) is an operating system that supports preemptive multitasking. There are actually two versions of Windows NT: Windows NT Server, designed to act as a server in networks, and Windows NT Workstation for stand-alone or client workstations.

Server editions of Windows are widely used. In recent years, Microsoft has expended significant capital in an effort to promote the use of Windows as a server operating system. However, Windows' usage on servers is not as widespread as on personal computers as Windows competes

against Linux and BSD for server market share. The share of Windows server operating systems may range between 20-30%, whereas the Unix and Unix-like OS cuts the major chunk.

As per the latest statistics, in very high-end systems like super computers, the share of Windows OS is reduced to almost nil whereas the Unix and Unix-like operating systems are used in more than 99% of systems.

***Unix and Unix-like operating systems***

Unix was originally written in assembly language. Ken Thompson wrote B, mainly based on BCPL, based on his experience in the MULTICS project. B was replaced by C, and Unix, rewritten in C, developed into a large, complex family of inter-related operating systems which have been influential in every modern operating system.

The Unix-like family is a diverse group of operating systems, with several major sub-categories including System V, BSD, and Linux. The name "UNIX" is a trademark of The Open Group which licenses it for use with any operating system that has been shown to conform to their definitions. "UNIX-like" is commonly used to refer to the large set of operating systems which resemble the original UNIX.

Unix-like systems run on a wide variety of computer architectures. They are used heavily for servers in business, as well as workstations in academic and engineering environments. Free UNIX variants, such as Linux and BSD, are popular in these areas.

Four operating systems are certified by The Open Group (holder of the Unix trademark) as Unix. HP's HP-UX and IBM's AIX are both descendants of the original System V Unix and are designed to run only on their respective vendor's hardware. In contrast, Sun Microsystems's Solaris can run on multiple types of hardware, including x86 and Sparc servers, and PCs.

Apple's macOS, a replacement for Apple's earlier (non-Unix) Mac OS, is a hybrid kernel-based BSD variant.

***Fourth Generation programming languages:***

Fourth generation languages are also known as very high level languages. They are non-procedural languages, so named because they allow programmers and users to specify what the computer is supposed to do without having to specify how the computer is supposed to do it. Consequently, fourth generation languages need approximately one tenth the number of statements that a high level languages needs to achieve the same results.

A fourth-generation programming language (4GL) is a computer programming language envisioned as a refinement of the style of languages classified as third-generation programming language (3GL). Languages claimed to be 4GL may include support for database management, report generation, mathematical optimization, GUI development, or web development. Depending on the language, the sophistication of fourth generation languages varies widely. These languages are usually used in conjunction with a database and its data dictionary.

Basic types of language tools fall into the fourth generation language category are Query languages, Report generators, Applications generators and Decision support systems and financial planning languages.

Examples: Oracle Forms, Oracle Designer, PL/SQL, Clipper, Power Builder, SAS, SPSS, SQL

***Fifth Generation programming languages:***

While 4GL are designed to build specific programs, 5GL are designed to make the computer solve a given problem without the programmer. This way, the programmer only needs to worry about what problems need to be solved and what conditions need to be met, without worrying about how to implement a routine or algorithm to solve them.

Natural Languages represent the next step in the development of programming languages, i-e fifth generation languages. The text of a natural language statement very closely resembles human speech. In fact, one could word a statement in several ways perhaps even misspelling some words or changing the order of the words and get the same result. These languages are also designed to make the computer "smarter". Natural languages already available for microcomputers include Clout, Q&A, and Savvy Retriever (for use with databases) and HAL (Human Access Language). Other examples of 5GL are Prolog, OPS5 and Mercury.

The use of natural language touches on expert systems, computerized collection of the knowledge of many human experts in a given field, and artificial intelligence, independently smart computer systems.

***Widely used open-source software***: Open source software projects are built and maintained by a network of volunteer programmers and are widely used in free as well as commercial products. Prime examples of open-source products are the Apache HTTP Server, the e-commerce platform osCommerce, internet browsers Mozilla Firefox and Chromium (the project where the vast majority of development of the freeware Google Chrome is done) and the full office suite LibreOffice. One of the most successful open-source products is the GNU/Linux operating system, an open-source Unix-like operating system, and its derivative Android, an operating system for mobile devices. In some industries, open source software is the norm.

**WEB BROSWERS**

A web browser is a software application that lets us visit web pages on the Internet. Although browsers are primarily intended to use the World Wide Web, they can also be used to access information provided by web servers in private networks or files in file systems. Web browsers consist of a user interface, layout engine, rendering engine, JavaScript interpreter, UI backend, networking component and data persistence component. These components achieve different functionalities of a web browser and together provide all capabilities of a web browser.

The most popular web browsers that are used today are Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Apple Safari and the Opera browser. Internet Explorer was deprecated in Windows 10, with Microsoft Edge replacing it as the default web browser. As per

the statistics available in 2017, Google Chrome has a market share of 64% followed by Mozilla Firefox and Internet Explorer with 15% and 10% respectively.

***Operating System Compatibility:*** Both Firefox and Opera have compatible versions for all kinds of operating systems covering Windows, macOS, Linux, BSD, Android, iOS and Other Unix based operating systems. Google Chrome too supports all these operating systems except BSD & other UNIX based OS. Safari supports only macOS and iOS and IE only Windows as of date.

**Functioning of a Web browser**

The primary purpose of a web browser is to bring information resources to the user ("retrieval" or "fetching"), allowing them to view the information ("display", "rendering"), and then access other information ("navigation", "following links").

This process begins when the user inputs a Uniform Resource Locator (URL), for example http://en.wikipedia.org/, into the browser. The prefix of the URL, the Uniform Resource Identifier or URI, determines how the URL will be interpreted. The most commonly used kind of URI starts with http: and identifies a resource to be retrieved over the Hypertext Transfer Protocol (HTTP). Many browsers also support a variety of other prefixes, such as https: for HTTPS, ftp: for the File Transfer Protocol, and file: for local files. Prefixes that the web browser cannot directly handle are often handed off to another application entirely. For example, mailto: URIs are usually passed to the user's default e-mail application, and news: URIs are passed to the user's default newsgroup reader.

In the case of http, https, file, and others, once the resource has been retrieved the web browser will display it. HTML and associated content (image files, formatting information such as CSS, etc.) is passed to the browser's layout engine to be transformed from markup to an interactive document, a process known as "rendering". Aside from HTML, web browsers can generally display any kind of content that can be part of a web page. Most browsers can display images, audio, video, and XML files, and often have plug-ins to support Flash applications and Java applets. Upon encountering a file of an unsupported type or a file that is set up to be downloaded rather than displayed, the browser prompts the user to save the file to disk.

Information resources may contain hyperlinks to other information resources. Each link contains the URI of a resource to go to. When a link is clicked, the browser navigates to the resource indicated by the link's target URI, and the process of bringing content to the user begins again.

**Replacement of Dial-up by broadband**

Broadband internet access via cable, digital subscriber line, satellite and FTTx has been replacing dial-up access in many parts of the world. Broadband connections typically offer speeds of 700 kbit/s or higher for two-thirds more than the price of dial-up on average. In addition broadband connections are always on, thus avoiding the need to connect and disconnect at the start and end of each session. Finally, unlike dial-up, broadband does not require exclusive use of a phone line and so one can access the Internet and at the same time make and receive voice phone calls without having a second phone line.

Dial-up Internet access has undergone a precipitous fall in usage, and potentially approaches extinction as modern users turn towards broadband. In contrast to the year 2000 when about 34% of Internet users used dial-up, this dropped to 1% in 2016.

**Extranet**

The term Extranet is linked with Intranet. Extranet is an external of computer network that allows the outside users to access the Intranet of organization. On the other hand, Internet is a global network system and is available to all while Intranet and Extranet are available to the inside users and users of selectively linked outside organization respectively. For instance, whereas your organization's LAN or WAN network represents an Intranet, the external trusted networks such as RBI, NPCI and IDRBT, which are connected to your Intranet for limited access or flow of data may be called Extranet networks with respect to your WAN, i.e., your Intranet. Generally Extranets are connected to Intranet through Routers as well as network security devices such as Firewalls for securing Intranet from the users of Extranet.

***Network Switches and Routers***

There are three main devices that work to connect one computer to another computer. A network hub, switch, and router can all perform this function. It can sometimes be confusing when trying to figure out what device is currently being used on a computer network, without knowing what each device does. Routers and switches are both computer networking devices that allow one or more computers to be connected to other computers, networked devices, or to other networks. The functions of a router, switch and hub and are all different, even if at times they are integrated into a single device.

**Switches** are used to connect multiple devices on the same network within a building or campus. For example, a switch can connect your computers, printers, and servers, creating a network of shared resources. The switch, one aspect of your networking basics, would serve as a controller, allowing the various devices to share information and talk to each other. Through information sharing and resource allocation, switches save you money and increase productivity.

There are two basic types of switches to choose from as part of your networking basics: managed and unmanaged. An unmanaged switch works out of the box and does not allow you to make changes. Home networking equipment typically includes unmanaged switches. A managed switch can be accessed and programmed. This capability provides greater network flexibility because the switch can be monitored and adjusted locally or remotely. With a managed switch, you have control over network traffic and network access.

**Routers,** the second valuable component of your networking basics, are used to connect multiple networks together. For example, you would use a router to connect your networked computers to the Internet and thereby share an Internet connection among many users. The router will act as a dispatcher, choosing the best route for your information to travel so that you receive it quickly. Routers analyze the data being sent over a network, change how it is packaged, and send it to another network or to a different type of network. They connect your business to the outside world,

protect your information from security threats, and can even decide which computers get priority over others. Depending on your business and your networking plans, you can choose from routers that include different capabilities. These can include networking basics such as:

- ***Firewall:*** Specialized software that examines incoming data and protects your business network against attacks.
- ***Virtual private network (VPN):*** A way to allow remote employees to safely access your network.
- ***IP phone network:*** Combines your company's computer and telephone network, using voice and conferencing technology, to simplify and unify your communications.

***Patch Panel vs Switch:*** A patch panel performs no other function except for acting as a connector. A network switch connects clients within a network to enable them to access the internet, share data and perform other functions.

***Network Security Equipment - Firewalls, NIDS, HIDS, IPS***

**Firewalls:**

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer based application upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are different types of firewalls which serve nearly same purpose but for different audiences. The two most common types are:

1) ***Network level firewalls***: These are standalone boxes & are much more sophisticated with loads of features. To mention a few, SPI[Stateful Packet Inspection],Deep Packet Inspection, Logging Capabilities etc. They usually run on proprietary Operating system such as the Cisco series, they run on the Cisco IOS[Internetwork Operating System.

2) ***Application level firewalls***: Software firewalls, application level proxies come under this category. Apart from the regular huff & puff they offer a few nifty features such as content filtering, blocking unwanted hosts.

Generally, firewalls are configured to protect against unauthenticated interactive logins from the outside world. This helps prevent hackers from logging into machines on your network. More sophisticated firewalls block traffic from the outside to the inside, but permit users on the inside to communicate a little more freely with the outside.

**NIDS (Network Intrusion Detection System) & HIDS (Host Intrusion Detection System):**

An intrusion detection system (IDS) is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. IDS is considered to be a passive-monitoring system, since the main function of an IDS product is to warn you of suspicious activity taking place − not prevent them. An IDS essentially reviews your network traffic and data and will identify probes, attacks, exploits and other vulnerabilities. IDSs can respond to the suspicious event in one of several ways, which includes displaying an alert, logging the event or even paging an administrator. In some cases the IDS may be prompted to reconfigure the network to reduce the effects of the suspicious intrusion.

An IDS specifically looks for suspicious activity and events that might be the result of a virus, worm or hacker. This is done by looking for known intrusion signatures or attack signatures that characterize different worms or viruses and by tracking general variances which differ from regular system activity. The IDS is able to provide notification of only known attacks.

***Network-based vs. Host-based IDS:***

Intrusion detection systems are network or host based solutions. Network-based IDS systems (NIDS) are often standalone hardware appliances that include network intrusion detection capabilities. It will usually consist of hardware sensors located at various points along the network or software that is installed to system computers connected to your network, which analyzes data packets entering and leaving the network.

Host-based IDS systems (HIDS) do not offer true real-time detection, but if configured correctly are close to true real-time. Host-based IDS systems consist of software agents installed on individual computers within the system. HIDS analyze the traffic to and from the specific computer on which the intrusion detection software is installed on. HIDS systems often provide features you can't get with network-based IDS. For example, HIDS are able to monitor activities that only an administrator should be able to implement. It is also able to monitor changes to key system files and any attempt to overwrite these files. Attempts to install Trojans or backdoors can also be monitored by a HIDS and stopped. These specific intrusion events are not always seen by a NIDS.

While it depends on the size of the network and the number of individual computers which require intrusion detection system, NIDS are usually a cheaper solution to implement and it requires less administration and training − but it is not as versatile as a HID.

**IPS (Intrusion Prevention System):**

IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) both increase the security level of networks, monitoring traffic and inspecting and scanning packets for suspicious data. Detection in both systems is mainly based on signatures already detected and recognized.

The main difference between one system and the other is the action they take when an attack is detected in its initial phases (network scanning and port scanning).

a) The Intrusion Detection System (IDS) provides the network with a level of detective and alertive security against any suspicious activity. The IDS achieves this objective

through early warnings aimed at systems administrators. However, unlike IPS, it is not designed to block attacks.

b) An Intrusion Prevention System (IPS) is a device that controls access to IT networks in order to protect systems from attack and abuse. It is designed to inspect attack data and take the corresponding action, blocking it as it is developing and before it succeeds.

While many in the security industry believe IPS is the way of the future and that IPS will take over IDS, it is somewhat of an apples and oranges comparison. The two solutions are different in that one is a passive detection monitoring system and the other is an active prevention system.

***False Positive and Negatives:***

The term *false positive* itself refers to security systems incorrectly seeing legitimate requests as spam or security breaches. Basically, the IDS will detect something it is not supposed to. Alternatively, IDS is prone to *false negatives* where the system fails to detect something it should. Both of these problems are associated with IDS and even IPS, It is a topic worth consideration when looking at different IDS solutions. Pre-implementation configuration of an IDS or IPS plays a great role in reducing false positives/false negatives to negligible levels.

***Emerging Trends in VSAT Technology***

Advances in technology have dramatically improved the price–performance ratio of fixed satellite service (FSS) over the past five years. New VSAT systems are coming online using Ka band technology that promise higher data rates for lower costs.

FSS systems currently in orbit have a huge capacity with a relatively low price structure. FSS systems provide various applications for subscribers, including: telephony, fax, television, high-speed data communication services, Internet access, satellite news gathering (SNG), Digital Audio Broadcasting (DAB) and others. These systems provide high-quality service because they create efficient communication systems for both residential and business users. Modern VSAT systems are a prime example of convergence, and hence require skills from both the RF (Radio Frequency) and IP (Internet Protocol) domains.

**MPLS**

**What is a computer networking protocol?**

The term ‘protocol’ is used extensively in computer networking language. Also for understanding the concept of MPLS, we need to have a fair idea about what a ‘protocol’ means.

In simple terms, protocols are a set of rules that govern a computer network. Protocols enable communication between two devices or even two different networks. A protocol is a kind of communication that is universally accepted to be used within a framework of pre-defined set of rules.

Network protocols are formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network. Network protocols govern the end-to-end processes of timely, secure and managed data or network communication.

There are several broad types of networking protocols, including:

a) Network communication protocols: These are basic data communication protocols such as TCP/IP and HTTP;
b) Network security protocols: Implement security over network communications and include HTTPS, SSL and SFTP and ;
c) Network management protocols: Provide network governance and maintenance and include SNMP and ICMP.

Now coming back to MPLS, Multiprotocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

The most prominent advantage of MPLS cloud technology is its better **resilience** with respect to the erstwhile point-to-point (P2P) leased line connectivity. Mainly for this reason, most of the Banks and other major financial institutions in India have switched to MPLS cloud technology for connecting their domestic as well as overseas establishments as of date.

**India Post,** which is a mammoth organization with respect to its widely distributed outlets across the country, is now transforming them to service centers while retaining the post and logistics. They plan to foray into Banking, Insurance & enabler for E-governance. They are now partnering with Sify for their backbone MPLS networking

**VLAN (Virtual LAN)**

Computer networks can be segmented into local area networks (LAN) and wide area networks (WAN). Network devices such as switches, hubs, bridges, workstations and servers connected to each other in the same network at a specific location are generally known as LANs. An LAN is also considered a broadcast domain.

A VLAN (virtual LAN) as the name indicates, allows several networks to work virtually as one LAN. One of the most beneficial elements of a VLAN is that it removes latency (reduction in speed) in the network, which saves network resources and increases network efficiency. In addition, VLANs are created to provide segmentation and assist in issues like security, network management and scalability. Traffic patterns can also easily be controlled by using VLANs. VLANs can quickly adapt to change in network requirements and relocation of workstations and server nodes.

Key benefits of implementing VLANs include:

- ✓ Allowing network administrators to apply additional security to network communication
- ✓ Making expansion and relocation of a network or a network device easier
- ✓ Providing flexibility because administrators are able to configure in a centralized environment while the devices might be located in different geographical locations
- ✓ Decreasing the latency and traffic load on the network and the network devices, offering increased performance

VLANs also have some disadvantages and limitations as listed below:

- High risk of virus issues because one infected system may spread a virus through the whole logical network
- More effective at controlling latency than a WAN but less efficient than a LAN

**Wireless Networks**

A wireless local-area network (LAN) uses radio waves to connect devices such as laptops to the Internet and to the business network and its applications. When one connects a laptop to a WiFi hotspot at a cafe, hotel, airport lounge, or other public place, one is connecting to that business's wireless network. On the contrary, a wired network connects devices to the Internet or other network using cables.

In the past, some believed wired networks were faster and more secure than wireless networks. But continual enhancements to wireless networking standards and technologies have eroded those speed and security differences.

Many network routers today act as wireless networking access points. They let anyone connect multiple computers to a single wireless network. And they connect the local network to the Internet.

One can extend wireless networking throughout one's office, store, or campus by placing additional wireless access points in various locations. The additional access points extend the wireless signal's range and strength over a wider geographical area, so that it's available in more places, such as conference rooms.

The signal generated from each wireless access point or router extends up to approximately 300 feet. Walls, metal (such as in elevator shafts) and floors can negatively affect range. And the wireless signal's strength weakens the longer it has to travel. For best results, we need to space out the access points and position them in central areas. Access points can provide stronger signals when installed on or near ceilings.

For best results, better not share any single wireless access point with more than 20 users. Typically, the more users sharing an access point, the slower the wireless network can become. If the business network supports a voice over Internet Protocol (VoIP) or Unified Communications system, we need to limit each access point to 8-12 users. This will prevent potential degradation in voice quality.

Security is vital to wireless networking. Some security methods to consider for the network include:

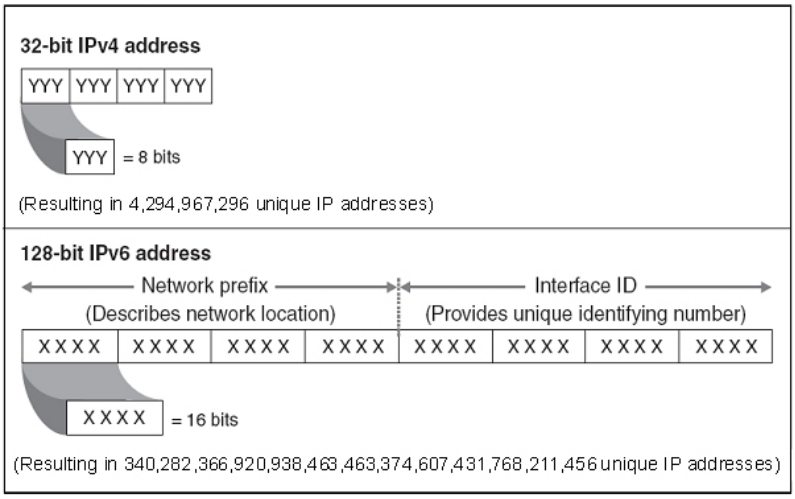
- Data encryption, so only authorized users can access information over the wireless network
- User authentication, which identifies computers trying to access the network
- Secure access for visitors and guests
- Control systems, which protect the laptops and other devices that use the network.

A **radio frequency (RF)** signal refers to a wireless electromagnetic signal used as a form of communication, if one is discussing wireless electronics. Radio waves are a form of electromagnetic radiation with identified radio frequencies that range from 3Hz to 300 GHz.

Apart from RF, **wireless 3G** connectivity under GSM technology is also being actively considered by many organizations for their network designs owing their low cost and questionably higher reliability. Security is one of the most important considerations in these solutions of wireless connectivity, which needs to addressed, mostly by way of strong encryption of data under transmission, before implementation.

### *IPv6 addresses*

The rapid exhaustion of IPv4 address space prompted the Internet Engineering Task Force (IETF) to explore new technologies to expand the addressing capability in the Internet. The permanent solution was deemed to be a redesign of the Internet Protocol itself. This new generation of the Internet Protocol was eventually named Internet Protocol Version 6 (IPv6) in 1995. The address size was increased from 32 to 128 bits (16 octets), thus providing up to 2128 (approximately 3.403×1038) addresses. This is deemed sufficient for the foreseeable future.




The intent of the new design was not to provide just a sufficient quantity of addresses, but also redesign routing in the Internet by more efficient aggregation of subnetwork routing prefixes. This resulted in slower growth of routing tables in routers. The smallest possible individual allocation is a subnet for 264 hosts, which is the square of the size of the entire IPv4 Internet. The following table depicts the major differences between IPv4 and IPv6 addressing schemes.

| IPv4 | IPv6 |
|---|---|
| The size of an address in IPv4 is 32 bits | The size of an address in IPv6 is 128 bits |
| Address Shortages:<br>IPv4 supports 4.3×109 (4.3 billion) addresses, which is inadequate to give one (or more if they possess more than one device) to every living person. | Larger address space:<br>IPv6 supports 3.4×1038 addresses, or 5×1028(50 octillion) for each of the roughly 6.5 billion people alive today.33(*) |
| IPv4 header has 20 bytes | IPv6 header is the double, it has 40 bytes |

| | |
|---|---|
| IPv4 header has many fields (13 fields) | IPv6 header has fewer fields, it has 8 fields. |
| IPv4 is subdivided into classes <A-E>. | IPv6 is classless.<br>IPv6 uses a prefix and an Identifier ID known as IPv4 network |
| IPv4 address uses a subnet mask. | IPv6 uses a prefix length. |
| IPv4 has no built-in security.<br>Encryption and authentication are optional | IPv6 has a built-in strong security<br>- Encryption<br>- Authentication |
| ISP have IPv4 connectivity or have both IPv4 and IPv6 | Many ISP don't have IPv6 connectivity |
| Non equal geographical distribution (>50% USA) | No geographic limitation |

The large number of IPv6 addresses allows large blocks to be assigned for specific purposes and, where appropriate, to be aggregated for efficient routing. With a large address space, there is no need to have complex address conservation methods as used in CIDR.

All modern desktop and enterprise server operating systems include native support for the IPv6 protocol, but it is not yet widely deployed in other devices, such as residential networking routers, voice over IP (VoIP) and multimedia equipment, and network peripherals.

***Bitcoin Crypto-currency & Block-chain Technology***

Now, most people have heard about Bitcoin, the cryptocurrency. The technology behind Bitcoin and what makes it so potentially disruptive at so many levels is called block-chain, or also a distributed ledger. Block-chain, thus; is essentially a distributed database. Many of the Banks, nationally and internationally, have started taking steps towards adopting block-chain technology for their cross-border payment systems, to start with.

Today, there are several banks pursuing individual block-chain strategies. These individual initiatives will be meaningful when they are used by all the banks. For instance, a payment system such as NEFT cannot be successful if it is adopted by only one bank. Block-chain, the technology behind cyber currency Bitcoin, follows the concept of a centralized registry that can be accessed by all members, and every event is registered as an unalterable 'block'. Being the largest bank in India, SBI has taken the lead in initiating block-chain. Other banks in the country are following suit gradually.

All the subsequent events related to the loan can be put on the “block” so that members can take informed decisions. Another business where block-chain can be used as a tool is in trade finance where there's a risk of fraud with the merchant going to multiple banks with the same invoice to get the bill discounted. If documents are put on the block-chain, everyone will know which invoices have been discounted by Bank X and this could prevent multiple discounting frauds.

### *Tiers of Redundancy of a Data centre*

A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. Some examples of SPOFs are database and application servers, network, power and storage systems. SPOFs are undesirable and redundancy needs to be maintained for all SPOFs in a DC. A Tier III data center is concurrently maintainable, allowing for any planned maintenance activity of power and cooling systems to take place without disrupting the operation of computer hardware located in the data center. In terms of redundancy, Tier III offers N+1 availability. Any unplanned activity such as operational errors or spontaneous failures of infrastructure components can still cause an outage. In other words, Tier III isn't completely fault tolerant. A Tier 4 data center is fault-tolerant, allowing for the occurrence of any unplanned activity while still maintaining operations. Tier 4 facilities have no single points of failure. Because of heavy cost constraints, most of the banks in India have adopted Tier III level redundancy. As the criticality has been increasing on account of 24x7 banking services being extended, the Indian banks have gradually started moving towards Tier-IV Data Centres.

### *Disaster Recovery Site (DRS) for Data Centre*

As the entire data of a bank resides at one place, viz. the Data Centre (DC), there is a concentration risk. In the event of something happening at the DC, or it getting isolated, the entire working of a bank will come to a stand-still. Therefore, another similar DC called the Disaster Recovery site (DR site) is setup in different seismic zone. The branches are linked to both DC & DR through a web of communication lines. Redundancy is provided at every stage in the form of a dial-up ISDN lines as a backup for a leased lines, the city Network Aggregation Point (NAP) being connected to both DC & DR. The idea is to ensure that in the event of failure of one; the other can take over, thus ensuring continuity of business and services.

While designing DCs for banks, redundancy needs to be maintained for all SPOFs (single point of failures) in a Data Centre. Even a replica of DC, which is called DRS (disaster recovery site) is established in a different seismic zone for business continuity purposes in case of any eventuality.

### Acquisition projects

Acquisition projects are similar to development projects because management approves project requests, defines functional, security, and system requirements, and appropriately tests and implements products. Organizations often employ structured acquisition methodologies similar to the SDLC when acquiring significant hardware and software products. However, organizations replace the SDLC design and development phases with a bid solicitation process that involves developing detailed lists of functional, security, and system requirements and distributing them to third parties.

Acquisition standards should also ensure managers complete appropriate vendor, contract, and licensing reviews and acquire products compatible with existing systems. Key tools in managing acquisition projects include invitations-to-tender and request-for-proposals. Invitations-to-tender involve soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software. Request-for-proposals involve soliciting bids when acquiring off-the-shelf or third-party developed software. However, the terms are sometimes used interchangeably.

The risks associated with using general business purpose, off-the-shelf software, such as a word processing application, are typically lower than those associated with using financial applications. Therefore, the acquisition of general business purpose, off-the-shelf software typically requires less stringent evaluation procedures than acquiring hardware or software specifically designed for financial purposes.

**CASE Tools & SDLC**

Computer-aided software engineering (CASE) is the domain of software tools used to design and implement applications. CASE tools are similar to and were partly inspired by computer-aided design (CAD) tools used for designing hardware products. The scope of CASE and CASE tools goes throughout SDLC. We shall discuss various types of CASE tools as follows.

***CASE Tools***

CASE tools are set of software application programs, which are used to automate SDLC activities. CASE tools are used by software project managers, analysts and engineers to develop software system. There are number of CASE tools available to simplify various stages of Software Development Life Cycle such as Analysis tools, Design tools, Project management tools, Database Management tools, Documentation tools are to name a few. Use of CASE tools accelerates the development of project to produce desired result and helps to uncover flaws before moving ahead with next stage in software development.

***Components of CASE Tools***

CASE tools can be broadly divided into the following parts based on their use at a particular SDLC stage: Central Repository - CASE tools require a central repository, which can serve as a source of common, integrated and consistent information. Central repository is a central place of storage where product specifications, requirement documents, related reports and diagrams, other useful information regarding management is stored. Central repository also serves as data dictionary.

1. Upper Case Tools - Upper CASE tools are used in planning, analysis and design stages of SDLC.
2. Lower Case Tools - Lower CASE tools are used in implementation, testing and maintenance.
3. Integrated Case Tools - Integrated CASE tools are helpful in all the stages of SDLC, from Requirement gathering to Testing and documentation.

CASE tools can be grouped together if they have similar functionality, process activities and capability of getting integrated with other tools.

We now briefly go through various CASE tools and their applications:

***Diagram tools*** - These tools are used to represent system components, data and control flow among various software components and system structure in a graphical form. For example, Flow Chart Maker tool for creating state-of-the-art flowcharts.

***Process Modeling Tools -*** Process modeling is method to create software process model, which is used to develop the software. Process modeling tools help the managers to choose a process model or modify it as per the requirement of software product. For example, EPF Composer

***Project Management Tools*** **-** These tools are used for project planning, cost and effort estimation, project scheduling and resource planning. Managers have to strictly comply project execution with every mentioned step in software project management. Project management tools help in storing and sharing project information in real-time throughout the organization. For example, Creative Pro Office, Trac Project, Basecamp.

***Documentation Tools*** **-** Documentation in a software project starts prior to the software process, goes throughout all phases of SDLC and after the completion of the project. Documentation tools generate documents for technical users and end users. Technical users are mostly in-house professionals of the development team who refer to system manual, reference manual, training manual, installation manuals etc. The end user documents describe the functioning and how-to of the system such as user manual. For example, Doxygen, DrExplain, Adobe RoboHelp for documentation.

***Analysis Tools*** - These tools help to gather requirements, automatically check for any inconsistency, inaccuracy in the diagrams, data redundancies or erroneous omissions. For example, Accept 360, Accompa, CaseComplete for requirement analysis, Visible Analyst for total analysis.

***Design Tools*** **-** These tools help software designers to design the block structure of the software, which may further be broken down in smaller modules using refinement techniques. These tools provides detailing of each module and interconnections among modules. For example, Animated Software Design

Configuration Management Tools - An instance of software is released under one version. Configuration Management tools deal with –

1. Version and revision management
2. Baseline configuration management
3. Change control management

CASE tools help in this by automatic tracking, version management and release management. For example, Fossil, Git, Accu REV.

***Change Control Tools*** - These tools are considered as a part of configuration management tools. They deal with changes made to the software after its baseline is fixed or when the software is first released. CASE tools automate change tracking, file management, code management and more. It also helps in enforcing change policy of the organization.

***Programming Tools*** - These tools consist of programming environments like IDE (Integrated Development Environment), in-built modules library and simulation tools. These tools provide comprehensive aid in building software product and include features for simulation and testing. For example, Cscope to search code in C, Eclipse.

***Prototyping Tools*** - Software prototype is simulated version of the intended software product. Prototype provides initial look and feel of the product and simulates few aspect of actual product.

Prototyping CASE tools essentially come with graphical libraries. They can create hardware independent user interfaces and design. These tools help us to build rapid prototypes based on existing information. In addition, they provide simulation of software prototype. For example, Serena prototype composer, Mockup Builder.

***Web Development Tools*** **-** These tools assist in designing web pages with all allied elements like forms, text, and script, graphic and so on. Web tools also provide live preview of what is being

developed and how will it look after completion. For example, Fontello, Adobe Edge Inspect, Foundation 3, Brackets.

***Quality Assurance Tools*** - Quality assurance in a software organization is monitoring the engineering process and methods adopted to develop the software product in order to ensure conformance of quality as per organization standards. QA tools consist of configuration and change control tools and software testing tools. For example, SoapTest, AppsWatch, JMeter.

***Maintenance Tools*** - Software maintenance includes modifications in the software product after it is delivered. Automatic logging and error reporting techniques, automatic error ticket generation and root cause Analysis are few CASE tools, which help software organization in maintenance phase of SDLC. For example, Bugzilla for defect tracking, HP Quality Center.

**DBMS vs Relational DBMS**

Relational software uses the concept of database normalization and the constraints of primary and foreign keys to establish relationships between rows of data in different database tables. That eliminates the need to redundantly store related data in multiple tables, which reduces data storage requirements, streamlines database maintenance and enables faster querying of databases. Normalization is a concept that applies to relational databases only.

Another notable difference between DBMS and RDBMS architectures, leaving the latter category out of the broad DBMS classification, is relational technology's support for referential integrity and other integrity checks designed to help keep data accurate and prevent inconsistent information from being entered in database tables. That's part of an adherence to the ACID properties -- atomicity, consistency, isolation and durability -- for ensuring that database transactions are processed in a reliable way. That isn't necessarily the case with other DBMS types -- for example, many NoSQL databases guarantee a more limited form of ACID compliance, called eventual consistency.

While these RDBMS concepts and features provide reliable, stable and relatively robust processing of structured transaction data, relational technology does have some limitations -- in particular, its requirement that databases include a rigid schema that's difficult for DBAs to modify on the fly. That has helped create an opening for NoSQL software and, to a greater extent, file-based Hadoop clusters in big data environments, although relational databases are still at the center of most IT architectures.

**ACID properties (Atomicity, Consistency, Isolation & Durability)**

***Atomicity:*** Atomicity requires that each transaction be "all or nothing": if one part of the transaction fails, then the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

***Consistency:*** The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules including constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted

(that is the responsibility of application-level code), but merely that any programming errors cannot result in the violation of any defined rules.

***Isolation:*** The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed sequentially, i.e., one after the other. Providing isolation is the main goal of concurrency control. Depending on the concurrency control method (i.e., if it uses strict - as opposed to relaxed - serializability), the effects of an incomplete transaction might not even be visible to another transaction.

***Durability:*** The durability property ensures that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL statements execute, the results need to be stored permanently (even if the database crashes immediately thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile memory.

## NORMALIZATION OF A DATABASE

Normalization is a process of organizing the data in database to avoid data redundancy, insertion anomaly, update anomaly & deletion anomaly. Normalization divides larger tables to smaller tables and link them using relationships.

Let's discuss anomalies first then we will discuss normal forms with examples.

### Anomalies in DBMS

There are three types of anomalies that occur when the database is not normalized. These are – Insertion, update and deletion anomaly. Let's take an example to understand this.

Example: Suppose a manufacturing company stores the employee details in a table named employee that has four attributes: emp_id for storing employee's id, emp_name for storing employee's name, emp_address for storing employee's address and emp_dept for storing the department details in which the employee works. At some point of time the table looks like this:

| emp_id | emp_name | emp_address | emp_dept |
|---|---|---|---|
| 101 | Krish | Delhi | D001 |
| 101 | Krish | Delhi | D002 |
| 123 | Malini | Agra | D890 |
| 166 | Navin | Chennai | D900 |
| 166 | Navin | Chennai | D004 |

The above table is not normalized. We will see the problems that we face when a table is not normalized.

***Update anomaly***: In the above table we have two rows for employee Krish as he belongs to two departments of the company. If we want to update the address of Krish then we have to update the same in two rows or the data will become inconsistent. If somehow, the correct address gets

updated in one department but not in other then as per the database, Krish would be having two different addresses, which is not correct and would lead to inconsistent data.

***Insert anomaly:*** Suppose a new employee joins the company, who is under training and currently not assigned to any department then we would not be able to insert the data into the table if *emp_dept* field doesn't allow nulls.

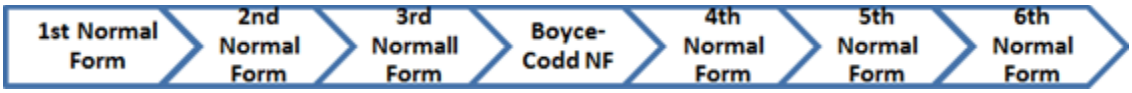
***Delete anomaly:*** Suppose, if at a point of time the company closes the department D890 then deleting the rows that are having *emp_dept* as D890 would also delete the information of employee Malini since she is assigned only to this department.

To overcome these anomalies we need to normalize the data. In the next section we will discuss normalization.

**Normalization**

The inventor of the relational model Edgar Codd proposed the theory of normalization with the introduction of First Normal Form and he continued to extend theory with Second and Third Normal Form. Later he joined with Raymond F. Boyce to develop the theory of Boyce-Codd Normal Form (BCNF).

Theory of Data Normalization in SQL is still being developed further. For example there are discussions even on 6th Normal Form. **But in most practical applications normalization achieves its best in 3rd Normal Form (3NF)**. The evolution of Normalization theories is illustrated below-




We need to understand the basic concepts of primary key, foreign key, candidate key and super key in a relational database, before we proceed further to understand the evolution of normal forms.

***Super, Candidate, Primary & Foreign keys***

A Super Key is the combination of fields by which the row is uniquely identified and the Candidate Key is the minimal Super Key. Basically, a Candidate Key is a Super Key from which no more Attribute can be pruned. A Super Key identifies uniquely rows/tuples in a table/relation of a database.

A Primary Key uniquely identify a record in the table. A Foreign Key is a field in the table that is Primary Key in another table. By default, Primary Key is clustered index and data in the database table is physically organized in the sequence of clustered index. We can have only one Primary Key in a table.

As discussed above, a Candidate Key can be any column or a combination of columns that can qualify as unique key in a database. There can be multiple Candidate Keys in one table. On the other hand, a Primary Key is a column or a combination of columns that uniquely identify a record. Thus each Candidate Key can qualify as Primary Key. However, as there may be multiple Candidate Keys in a table, a Primary Key can be only one for a given table.

The above terms are freely used in the following discussion on normal forms. You may notice that as the normalization process upgrades from 1NF to 2NF and then to 3NF and so on, the number of tables and reference keys keep increasing.

## A DATA WAREHOUSE ARCHITECTURE

Different data warehousing systems have different structures. Some may have an ODS (operational data store), while some may have multiple data marts. In general a Data Warehouse is used on an enterprise level, while ***Data Mart*** is used on a business division/department level. Some may have a small number of data sources, while some may have dozens of data sources. In view of this, it is far more reasonable to present the different layers of a data warehouse architecture rather than discussing the specifics of any one system.

### Layers in a Data Warehouse

In general, all data warehouse systems have the following layers:

- Data Source Layer
- Data Extraction Layer
- Staging Area
- ETL Layer
- Data Storage Layer
- Data Logic Layer
- Data Presentation Layer
- Metadata Layer
- System Operations Layer
-

The picture below shows the relationships among the different components of the data warehouse architecture:

<table>
<tr><td colspan="7">Metadata Layer</td></tr>
<tr><td rowspan="2">Data Source Layer</td><td>Data Extraction Layer</td><td>Staging Area</td><td>ETL Layer</td><td>Data Storage Layer</td><td>Data Logic Layer</td><td>Data Presentation Layer</td></tr>
<tr><td colspan="6">System Operations Layer</td></tr>
</table>

Each component is discussed individually below:

***Data Source Layer***

This represents the different data sources that feed data into the data warehouse. The data source can be of any format -- plain text file, relational database, other types of database, Excel file, etc., can all act as a data source.

Many different types of data can be a data source:

- Operations -- such as sales data, HR data, product data, inventory data, marketing data, systems data.
- Web server logs with user browsing data.
- Internal market research data.
- Third-party data, such as census data, demographics data, or survey data.

All these data sources together form the Data Source Layer.

Clearly, the goal of data warehousing is to free the information that is locked up in the operational databases and to mix it with information from other, often external, sources of data. Increasingly, large organizations are acquiring additional data from outside databases. This information includes demographic, econometric, competitive and purchasing trends.

***Data Extraction Layer***
Data gets pulled from the data source into the data warehouse system. There is likely some minimal data cleansing, but there is unlikely any major data transformation.

***Staging Area:*** This is where data sits prior to being scrubbed and transformed into a data warehouse / data mart. Having one common area makes it easier for subsequent data processing / integration.

***ETL Layer***
ETL stands for "Extract, Transform and Load". This is where data gains its "intelligence", as logic is applied to transform the data from a transactional nature to an analytical nature. This layer is also where data cleansing happens. The ETL design phase is often the most time-consuming phase in a data warehousing project, and an ETL tool is often used in this layer.

***Data Storage Layer***
This is where the transformed and cleansed data sit. Based on scope and functionality, 3 types of entities can be found here: data warehouse, data mart, and operational data store (ODS). In any given system, you may have just one of the three, two of the three, or all three types.

***Data Logic Layer***
This is where business rules are stored. Business rules stored here do not affect the underlying data transformation rules, but do affect what the report looks like.

***Data Presentation Layer***
This refers to the information that reaches the users. This can be in a form of a tabular / graphical report in a browser, an emailed report that gets automatically generated and sent every day, or an alert that warns users of exceptions, among others. Usually an OLAP tool and/or a reporting tool is used in this layer.

***Metadata Layer***

This is where information about the data stored in the data warehouse system is stored. *Metadata is data about data.* A logical data model would be an example of something that's in the metadata layer. A metadata tool is often used to manage metadata. Data warehouse contains huge amount of data. The metadata component contains the information like: (1) description of data warehouse; (2) rules to map, translate and transform data sources to warehouse elements; (3) the navigation paths and rules for browsing in the data warehouse; (4) the data dictionary; (5) the list of pre-designed and built-in queries available to the users etc. Record descriptions in a COBOL program DIMENSION statements in a FORTRAN program, or SQL Create statement fields are examples of metadata.

In order to have a fully functional warehouse, it is necessary to have a variety of meta-data available, data about the end-user views of data and data about the operational databases. Ideally, end-users should be able to access data from the data warehouse (or from the operational databases) without having to know where that data resides or the form in which it is stored.

***System Operations Layer***

This layer includes information on how the data warehouse system operates, such as ETL job status, system performance, and user access history.

## BUSINESS INTELLIGENCE–EXPERT SYSTEMS & ARTIFICIAL NEURAL NETWORKS

### Business intelligence (BI)

Business Intelligence includes several types of applications and technologies for acquiring, storing, analyzing, and providing access to information to help users make more sound business decisions. BI applications include decision support systems (DSS), query and reporting, online analytical processing (OLAP), statistical analysis, and data mining. We have discussed in detail the concepts off DSS, Group DSS in the foregoing Chapter 5.

Often BI applications use data gathered from a data warehouse (DW) or from a data mart, and the concepts of BI and DW sometimes combine as "BI/DW" or as "BIDW". A data warehouse contains a copy of analytical data that facilitates decision support.

### Artificial Neural Networks & Expert Systems

Artificial neural networks (ANNs) are inspired by the information processing model of the mind/brain. The human brain consists of billions of neurons that link with one another in an intricate pattern. Every neuron receives information from many other neurons, processes it, gets excited or not, and passes its state information to other neurons.

Just like the brain is a multipurpose system, so also the ANNs are very versatile systems. They can be used for many kinds of pattern recognition and prediction.

In artificial intelligence, an Expert System (ES) is a computer system that emulates the decision-making ability of a human expert. Expert systems are designed to solve complex problems by reasoning about knowledge, represented mainly as if–then rules rather than through conventional procedural code. An expert system is divided into two subsystems: the inference engine and the knowledge base. The knowledge base represents facts and rules. The inference engine applies

the rules to the known facts to deduce new facts. Inference engines can also include explanation and debugging abilities
An expert system is made up of three parts: A user interface - This is the system that allows a non-expert user to query (question) the expert system, and to receive advice. The user-interface is designed to be a simple to use as possible. A knowledge base - This is a collection of facts and rules. A rule-based system is a set of "if-then" statements that uses a set of assertions, to which rules on how to act upon those assertions are created. In software development, rule-based systems can be used to create software that will provide an answer to a problem in place of a human expert.

***Applications of ANN***
Artificial Neural Networks or ANN has a multitude of real world applications in the business domain which have been classified as follows:
Accounting · Identifying tax fraud · Enhancing auditing by finding irregularities Finance · Signature and bank note verification · Mortgage underwriting · Foreign exchange rate forecasting · Country risk rating · Predicting stock initial public offerings · Bankruptcy prediction · Customer credit scoring · Credit card approval and fraud detection · Stock and commodity selection and trading 3 · Forecasting economic turning points · Bond rating and trading · Loan approvals · Economic and financial forecasting · Risk management Human resources ·Predicting employee's performance and behaviour · Determining personnel resource requirements Marketing ·Classification of consumer spending patterns · New product analysis · Identification of customer characteristics · Sale forecasts · Targeted marketing.

**Artificial Intelligence (AI),** which is gaining popularity at a great pace today, is a much superior cousin of Artificial Neural Network (ANN) which has been discussed in the previous section. Artificial intelligence (AI) involves the study of cognitive phenomena in machines. One of the practical goals of AI is to implement aspects of human intelligence in computers. Computers are also widely used as a tool with which to study cognitive phenomena. Cognitive computing (CC) describes technology platforms that are based on the scientific disciplines of artificial intelligence (AI) and signal processing. These platforms encompass machine learning, reasoning, natural language processing, speech recognition and vision (object recognition), human–computer interaction, dialog and narrative generation, among other technologies.
The intelligence emerges from a business point of view when machines – based on information – are able to make decisions, which maximizes the chances of success in a given topic. By the use of Machine Learning, Artificial Intelligence is able to use learning from a data set to solve problems and give relevant recommendations. For example, we can use the learning about the correlation between weather, local events and sales numbers to create a fully automated system that decides upon the daily supply shipped to a given store.

**Machine learning** is a field of computer science that uses statistical techniques to give computer systems the ability to learn, i.e., progressively improve performance on a specific task, with data, without being explicitly programmed. Machine Learning is algorithms that learn from data and create foresights based on this data. A simple example of how it can be used: Building a model, that can predict customer demand by understanding the correlation between sales numbers from a store correlated with historical weather data and local events happening in the area.

Machine learning is employed in a range of computing tasks where designing and programming explicit algorithms with good performance is difficult or infeasible; example applications include email filtering, detection of network intruders or malicious insiders working towards a data breach, optical character recognition (OCR), learning to rank, and computer vision.

**Cognitive analytics** is a cognitive computing technology platform typically specialize in the processing and analysis of large, unstructured datasets. Generally, word processing documents, emails, videos, images, audio files, presentations, webpages, social media and many other data formats often need to be manually tagged with metadata before they can be fed to a computer for analysis and insight generation. The principal benefit of utilizing cognitive analytics over traditional big data analytics is that such datasets do not need to be pre-tagged.

Cognitive analytics systems can use machine learning to adapt to different contexts with minimal human supervision. Cognitive analytics systems can be equipped with a chatbot or search assistant that understands queries, explains data insights and interacts with humans in natural language.

## Core Banking Solution (CBS)

Core Banking Solution (CBS) is networking of bank branches, which allows customers to manage their accounts, and use various banking facilities from any part of the world. In simple terms, there is no need to visit your own branch to do banking transactions. You can do it from any location, any time. You can enjoy banking services from any branch of the bank which is on CBS network regardless of branch you have opened your account. For the bank which implements CBS, the customer becomes the bank's customer instead of customer of particular branch.

Execution of Core banking system across all branches helps to speed up most of the common transactions of bank and customer. In Core banking, the all branches access banking applications from centralized server which is hosted in secured Data Centre. Banking software/application performs basic operations like maintaining transactions, balance of withdrawal & payment, interest calculations on deposits & loans etc. This banking applications are deployed on centralized server & can be accessed using internet from any location.

### *Need for Core Banking Technology*

Nowadays, the use of Information Technology (IT) is must for the survival & growth of any organization and same applicable to banking industry also. By using IT in any industry, banks can minimize the operation cost; also banks can offer products & services to customers at competitive rates.

CBS is required;

- To meet the dynamically changing market & customer needs.
- To improve & simplify banking processes so that bank staff can focus on sales & marketing stuff.
- Convenience to customer as well as bank.
- To speed up the banking transactions.

- To expand presence in rural & remote areas.

Basic elements of CBS that helps customers are:

- Internet Banking
- Mobile Banking
- ATM
- POS & kiosk systems
- Fund Transfers – NEFT, RTGS, IMPS etc.

**Benefits of Core banking –**

Core banking solutions are beneficial to both banks as well as customers.

**A. Benefits for Customers**

- Quicker services at the bank counters for routine transactions like cash deposits, withdrawal, passbooks, statement of accounts, demand drafts etc.
- Anywhere banking by eliminating branch banking.
- Provision of banking services 24 X 7.
- Fast payment processing through Internet banking, mobile banking.
- Anytime anywhere banking through ATMs.
- All branches access applications from central servers/datacentre, so deposits made in any branch reflects immediately and customer can withdraw money from any other branch throughout the world.
- CBS is very helpful to people living in rural areas. The farmers can receive e-payments towards subsidy etc. in his account directly. Transfer of funds from the cities to the villages and vice versa will be done easily.

**B. Benefits for Banks**

- Process standardization within bank & branches.
- Retention of customers through better customer service.
- Accuracy in transactions & minimization of errors.
- Improved management of documentation & records – having centralized databases results in quick gathering of data & MIS reports.
- Ease in submission of various reports to the Government & Regulatory boards like RBI.
- Convenience in opening accounts, processing cash, servicing loans, calculating interest, implementing change in policies like changing interest rates etc.

To cope up with the growing needs of customers; RRBs and Co-operative banks were needed to implement core banking solutions. To face the challenges of dynamic market, UCBs needed to take help of IT their operations. Considering the importance of the matter, the Reserve Bank of India (RBI) mandated a deadline for Urban Co-operative Banks (UCBs) and advised to implement the core banking solutions (CBS) by December 31, 2013, which has been met by all RRBs and UCBs.

**Web Server**

A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients. Dedicated computers and appliances may be referred to as Web servers as well.

The process is an example of the client/server model. All computers that host Web sites must have Web server programs. Leading Web servers include Apache (the most widely-installed Web server), Microsoft's Internet Information Server (IIS) and nginx (pronounced *engine X*) from NGNIX.

***a) Apache Web Server***

Apache is the most popular web server in the world developed by the Apache Software Foundation. Apache is an open source software and can be installed on almost all operating systems including Linux, Unix, Windows, FreeBSD, Mac OS X and more. About 60% of machines run on Apache Web Server.

An Apache server can be customized easily as it contains a modular structure. It is also an open source which means that you can add your own modules to the server when to require and make modifications that suit your specific needs. It is more stable than any other web servers and is easier to solve administrative issues. It can be install on multiple platforms successfully. Recent Apache releases provide you the feasibility of handling more requests when you compare to its earlier versions.

***b) IIS Web Server***

IIS is a Microsoft product. IIS server has all the features just like Apache. But it is not an open source and more over personal modules cannot be added easily and modification becomes a little difficult job. Microsoft developed, maintains it, and thus it works with all the Windows operating system platforms. Also, they had good customer support if it had any issues.

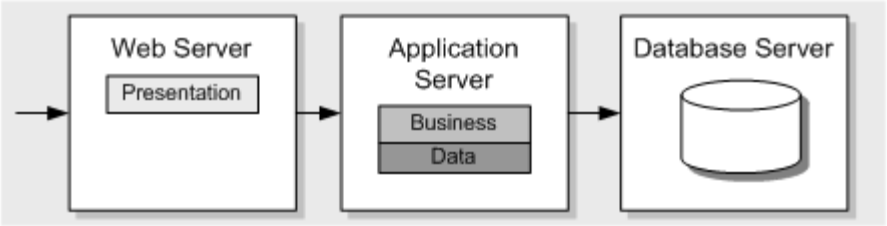
***c) Nginx Web Server***

Nginx is another free open source web server, it includes IMAP/POP3 proxy server. Nginx is known for its high performance, stability, simple configuration and low resource usage. This web server doesn't use threads to handle requests rather a much more scalable event-driven architecture which uses small and predictable amounts of memory under load. It is getting popular in the recent times and it is hosting about 7.5% of all domains worldwide.

Most of the web hosting companies select web server based on clients requirement, the number of clients on a single server, the applications/software clients use and the amount of traffic they generate that could handle by a web server. Web servers often come as part of a larger package of Internet- and intranet-related programs for serving email, downloading requests for File Transfer Protocol (FTP) files, and building and publishing Web pages. Considerations in choosing a Web server include how well it works with the operating system and other servers, its ability to handle server-side programming, security characteristics, and the particular publishing, search engine and site building tools that come with it.

**Application Server**

The application server is the middleman between browser-based front-ends and back-end databases and legacy systems.




This is the server on which the organization's created applications which are utilizing our database, web service, etc. This application server will host business layer (wrapped with web services), scheduled jobs, windows services, etc. This is a middle-tier business logic application or set of applications, possibly on a local area network or intranet server. Also called an app server, an application server is a program that handles all application operations between users and an organization's backend business applications or databases.

An application server is typically used for complex transaction-based applications. To support high-end needs, an application server has to have built-in redundancy, monitor for high-availability, high-performance distributed application services and support for complex database access. In many usages, the application server combines or works with a Web (Hypertext Transfer Protocol) server and is called a *Web application server*. The Web browser supports an easy-to-create HTML-based front-end for the user.

The Web server provides several different ways to forward a request to an application server and to forward back a modified or new Web page to the user. These approaches include the Common Gateway Interface (CGI), FastCGI, Microsoft's Active Server Page, and the Java Server Page. In some cases, the Web application servers also support request "brokering" interfaces such as CORBA Internet Inter-ORB Protocol (IIOP).

Example of Application Servers are:

- **JBoss:** Open-source server from JBoss community.
- **Sun Glassfish:** Provided by Sun Microsystem. Now acquired by Oracle.
- **Oracle Weblogic:** Provided by Oracle. It more secured.
- **IBM Websphere:** Provided by IBM.

**Database Server**

Legacy application databases and transaction management applications are part of the back end or third tier. See figure 9.3. The database is generally installed on a different server which is called a Database server. A third-tier, back-end, database and transaction server, sometimes on a mainframe or large server. Database server will have your one or more database hosted such as Oracle, SQL Server, MySql, etc.

***Network Domain***

A domain, in the context of networking, refers to a group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains

are defined by the *IP address*. All devices sharing a common part of the IP address are said to be in the same domain. There are also many types of subdomains.

A domain has a domain controller that governs all basic domain functions and manages network security. Thus, a domain is used to manage all user functions, including username/password and shared system resource authentication and access. A domain is also used to assign specific resource privileges, such as user accounts.

In a simple network domain, many computers and/or workgroups are directly connected. A domain is comprised of combined systems, servers and workgroups. Multiple server types may exist in one domain - such as Web, database and print - and depend on network requirements.

On the other hand, domain names are used to identify one or more IP addresses. For example, the domain name microsoft.com represents about a dozen IP addresses. Domain names are used in URLs to identify particular Web pages

***Windows Domain***

A Windows domain is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered with a central database located on one or more clusters of central computers known as domain controllers. Authentication takes place on domain controllers. Each person who uses computers within a domain receives a unique user account that can then be assigned access to resources within the domain. Starting with Windows 2000, Active Directory is the Windows component in charge of maintaining that central database. The concept of Windows domain is in contrast with that of a workgroup in which each computer maintains its own database of security principals.

Computers can connect to a domain via LAN, WAN or using a VPN connection. Users of a domain are able to use enhanced security for their VPN connection due to the support for a certification authority which is gained when a domain is added to a network, and as a result smart cards and digital certificates can be used to confirm identities and protect stored information.

In a Windows domain, the directory resides on computers that are configured as "domain controllers." A domain controller is a Windows or Samba server that manages all security-related aspects between user and domain interactions, centralizing security and administration. A domain controller is generally suited for businesses and/or organizations when more than 10 PCs are in use. A domain does not refer to a single location or specific type of network configuration. The computers in a domain can share physical proximity on a small LAN or they can be located in different parts of the world. As long as they can communicate, their physical position is irrelevant.

Where PCs running a Windows operating system must be integrated into a domain that includes non-Windows PCs, the free open source package Samba is a suitable alternative. Whichever package is used to control it, the database contains the user accounts and security information for the resources in that domain.

**Data Storage Devices**

Alternatively referred to as digital storage, storage, storage media, or storage medium, a storage device is any hardware capable of holding information either temporarily or permanently.
There are two types of storage devices used with computers: a primary storage device, such as RAM, and a secondary storage device, like a hard drive. Secondary storage can be removable, internal, external or network storage. Some examples of data storage devices are discussed as below:

***Magnetic storage devices***

Today, magnetic storage is one of the most common types of storage used with computers and is the technology that many computer hard drives use. Examples are Floppy diskette, Hard drive, Magnetic strip, SuperDisk, Tape cassette and Zip diskette.

***Optical storage devices***

Another common storage is optical storage, which uses lasers and lights as its method of reading and writing data. Examples are Blu-ray disc, CD-ROM disc, CD-R and CD-RW disc, DVD-R, DVD+R, DVD-RW and DVD+RW disc.

***Flash memory devices***

Flash memory has started to replace magnetic media as it becomes cheaper as it is the more efficient and reliable solution. e.g., Jump drive or flash drive, Memory card, Memory stick, and SSD (Solid State Drive).

***Online and cloud***

Storing data online and in cloud storage is becoming popular as people need to access their data from more than one device. Examples are Cloud storage and Network media such as NAS (Network Attached Storage) & SAN (Storage Area Network).

***Paper storage***

Early computers had no method of using any of the above technologies for storing information and had to rely on paper. Today, these forms of storage are rarely used or found. In the picture to the right is an example of a woman entering data to a punch card using a punch card machine. Examples are OMR and Punch Card.
Most of the storage device examples mentioned are no longer used with today's computers which primarily use a hard disk drive or SSD to store information and have the options for USB flash drives and access to cloud storage. Desktop computers with disc drives typically use a disc drive that is capable of reading CD's and DVD's and writing CD-R and other recordable discs.
For most computers, the largest storage device is the hard drive or SSD. However, networked computers may also have access to even larger storage with large tape drives, cloud computing, NAS or SAN storage devices. Below is a list of storage devices from the smallest capacity to the largest capacity.

**Desired Features of Mobile Banking**

Apps are fast becoming the primary way to interact with consumers - When banks first launched apps, they were convenient tools to check your balance and keep on top of your spending. However, consumers are expecting - and banks are delivering - ever more functionality. Particularly with younger consumers, apps are becoming critical to attracting and retaining consumers. The benchmarks for ranking a mobile banking are;

- range of touchpoints,
- enrollment and login,
- account information,
- transactional functionality,
- service features,
- cross channel guidance, and
- marketing and sales.

Some of the important desired features in a mobile banking app across the world and India are as follows:

**Download apps for a range of smartphone operating systems**. This is one of the greatest challenges -to make the app work across operating systems with various versions of each. Downloadable smartphone apps let digital banking teams use device-specific features to create a smoother and more intuitive experience for mobile banking customers. Although some operating systems are more important in some countries than others, the major four operating systems are - Android, BlackBerry OS, iOS, and Windows Phone.

**Easily complete banking tasks via a mobile website**. Many customers use the browser on their mobile device to access their bank account information, pay bills on the run, or make other mobile transactions — and today they expect to perform these tasks without the hassle of pinching and zooming their way through a mobile-unfriendly web experience.

**Interact with the bank via SMS**. Most banks report falling use of SMS text messaging relative to other mobile banking touchpoints. Yet some consumers — especially those who do not have a smartphone — continue to use text banking.

**Enroll in mobile banking directly from their smartphone**. As younger generations start opening their first bank accounts, the proportion of customers who are mobile-first and mobile-only will rise. Digital banking teams need to enable customers to register for digital banking directly from their mobile devices — rather than forcing them to sign up for online banking first.

**Understand how to use mobile banking**. As content and functionality become more extensive, with leading banks offering regular mobile updates, it's important that digital banking teams communicate these improvements and guide new users through how to use mobile banking.

**Easily access security and privacy content**. Many customers who are just starting to use mobile banking worry about privacy and security, while others might want to be reassured in specific situations. This area still remains a weak spot for many retail banks.

**Get valuable content and account information pre-login**. Digital banking teams have recognized that customers don't need to be logged in for every banking task and that many like the convenience of accessing simple information without needing to enter a password. Log in

easily. Banks must make the mobile banking login process as painless as possible, without compromising security. Leading banks do this by using multifactor authentication the first time customers use the app, then letting them use a simplified login subsequently. Many banks offer convenient features, such as a "remember this device" option and the ability to save user names, and they let users opt into an abbreviated login process using a simple PIN code rather than entering a full alphanumeric password.

**Log in easily**. Banks must make the mobile banking login process as painless as possible, without compromising security. Leading banks do this by using multifactor authentication the first time customers use the app, then letting them use a simplified login subsequently. Many banks offer convenient features, such as a "remember this device" option and the ability to save user names, and they let users opt into an abbreviated login process using a simple PIN code rather than entering a full alphanumeric password.

**Quickly work out how to achieve their mobile banking goals**. The mobile screen customers land on immediately after logging in is a crucial part of their mobile banking experience. Digital banking teams must design screens that make it easy for customers to complete the tasks they logged into mobile banking to do. Most leading banks display prominent one-click links to the most common tasks directly on the home screen.

**Quickly and conveniently find transactions.** Different customers will search their transaction history with different search tools, according to personal preferences: Many banks are expanding the transaction history tools available via mobile. See an accurate forecast for their spending. A growing number of banks provide customers with a "future view" of their upcoming payments and transfers. And some are even using predictive tools to include transactions the customer hasn't yet set up.

**Better understand their financial lives with embedded money management tools**. Digital money management will ultimately be embedded at the heart of digital banking. Not all money management features make sense for mobile touchpoints, but digital teams should offer simple, integrated, and contextual tools that help customers quickly and easily get the information they want or take the action they need.

**Move money without hassles**. Overall, the banks offer strong and easy mobile money movement functionality such as account-to-account and P2P money transfers.

**Send money to other people without sensitive personal details**- This is one of the important desired features in most of the countries.

**Buy items in stores without plastic**. It is observed that digital wallets integrating offers, coupons, point-of-sale (POS) payments, and loyalty rewards are poised to transform the way consumers shop and make payments.

**Solve account issues within the mobile app**. Self-service features let a customer initiate or complete a request without having to interact with a bank employee. Functionality that lets a customer dispute a card transaction, report fraud, or order a new debit card is not widely available on banks' mobile banking apps.

**Set up, receive, and manage alerts**. Alerts continue to offer great value to customers. Just a few years ago, customers were content to set up and manage alerts via the bank's secure website and receive the alerts via SMS or email. But behavior is changing with the mobile mind shift, and an

increasing number of banks are differentiating themselves by offering alerts delivery and management within the mobile banking app.

**Find branches and ATMs**. Most of the banks evaluated make it easy for customers to find nearby branches and ATMs, including key information such as hours of operation and providing step-by-step directions.

**Easily apply for a new product, account, or service**. Application abandonment has been an issue for digital sales teams at banks for years, and the physical limitations of mobile devices can amplify the problem. Someone trying to open a new account is more likely to give up if he or she needs to pinch and zoom through the task flow while also entering information into dozens of data entry fields. So cross-selling effectively means making buying as easy and quick as possible for a customer. For example, mBank has developed simplified product applications with two-step task flows and embedded them within mobile banking.

## INTERNET SERVICE PROVIDERS / HOSTING / BANDWIDTH / DATA DOWNLOAD & UPLOAD

In a typical world scenario, we come across Internet Service Providers (ISPs) advertising about "high speed internet". But when we look at our own internet connections, the download speeds seems to be far below compared to what has been advertised. So what did your ISP actually mean by "Connection Speed"? Is "Connection Speed" totally different from "Download Speed"?

### Connection Speeds and Download Speeds

People often confuse connection speed with downloading speed. Though both of these terms refer fairly to the same thing, their interpretation is slightly different from one another.

***Connection speed*** (or Internet Bandwidth) refers to the raw data transfer rate of the connection provided by your ISP. This is the property that is usually advertised and can vary largely among different providers and data plans. Nowadays, this figure is usually expressed in terms of Kbps (Kilobit per Second) or Mbps (Megabit per Second).

On the other hand, when we download files from the internet, the same data transfer rate is interpreted as Download Speed. Download speed is usually measured in KBps (Kilobyte per second).

### *A Typical Scenario*

Say you have a 1 Mbps Internet connection. With such a connection speed, you might expect to download files at a rate of around 1 MB per second, but when you actually download a file, the download speed only reaches up to 100 – 120 KB per second.

Where's the catch? If connection speed and download speed are fairly one and the same, as we mentioned earlier, then we should be ideally getting the same speed for connection and download. So what's missing here?

Actually, connection and download speeds are measured in two different units, so even though these measurements refer to the same thing, their interpreted values turn out to be quite different.

Connection v/s Download (Units)

***Unit used for Connection Speed*:** Kbps (Kilobit per Second), Mbps (Megabit per Second), Gbps (Gigabit per Second) and so on…

***Unit used for Download Speed*:** KBps (Kilobyte per Second), MBps (Megabyte per Second) and so on.

**Relation between bit and byte**

1 byte = 8 bit1 kilobyte (KB) = 8 kilobit (Kb)

Why different units are used for measuring connection and download speed?

A Bit is the most fundamental unit of representing data. That is why it was adopted as a standard for measuring the raw data transfer rate, which refers to the connection speed. Hence, connection speeds are measured in Megabit per second (Mbps).

But a bit in itself is quite meaningless. The data in your computer is stored in the form of 8 bit blocks, known as a byte. So when you download any file from the internet, it is generally represented in Byte. Hence, download speed is usually measured in Kilobyte per second (KBps).

The noteworthy point here is the difference between bit and byte as used in the two units. Connection speed is represented with a (small) **'b'** for **bit** while download speed takes a (capital) **'B'** for **Byte**. Let us have a deeper look at the two units.

1 Megabyte (MB) = 8 Megabit (Mb)

1 Megabyte (MB) = 1024 Kilobyte (KB)

8 Megabit (Mb) = 1024 Kilobyte (KB)

Therefore,1 Megabit (Mb)= [1024/8 =] 128 Kilobyte (KB)

So, in a 1 Mbps connection, your maximum download speed would be 128 KBps (=1Mbps). And this convention kind of suits the ISPs too, as it helps them to lure consumers into visually greater figures.

***Factors affecting Download Speeds***

So, we should get a maximum download speed of 128 KBps on a 1 Mbps connection. But practically, we would only be able to download files at 80 KBps – 120 KBps on average. The fall in the download rate can be attributed to several external and internal factors.

**External factors affecting download speeds**

Your downloading speed is affected by several server-side factors:

***Packet delivery method:*** The data that you download from the internet are received by your device in the form of packets. Each of these packets contain additional information, like sender and receiver address, etc. These information, referred to as message headers, make up a considerable

part of the data that is downloaded; but is discarded once it reaches the client. The size of each packet and the size of the header information it contains, varies among different hosts.

***Server capacity:*** File downloading speed also depends on the host's network speed. The server you are downloading from should be able to serve the file at a greater speed than your own connection speed. Otherwise, your download speed will be limited to the maximum speed at which the server can serve.

***Server load:*** Capacity is not the only factor affecting the server's serving speed. Sometimes, a server which is serving too many parallel requests might throttle connections and regulate the bandwidth utilized by each connection. In that case, the server limits the maximum bandwidth available for you to download a particular file. More the load on the server, more would be the number of parallel requests it is processing, hence less will be the maximum bandwidth available for you to download.

***Routing:*** A download request can reach the destination server in multiple ways. Generally, the shortest possible route is selected. But the maximum available download bandwidth will be fairly dependent on the distance between the server's location and the client's location. If you are downloading from a server near you, more bandwidth will be available for downloading. But if the server is far from your location, available bandwidth would be reduced as some of it is consumed by the routing process.

Internal factors affecting download speeds

Download speed may also depend on several internal / device factors:

***Network Interface Controller (NIC):*** Network adapters vary in specifications from manufacturer to manufacturer. If the network adapter in your device cannot fully utilize the connection speed, you won't be able to achieve the maximum download speed provided by your ISP.

***Operating System (OS):*** Your device's operating system runs a few background services that is used to establish and maintain the connection related activities. These OS level services consume some bandwidth to run their operations. However, the amount of bandwidth consumed by these services vary from OS to OS.

***Disk Read/Write Speed*****:** This is not usually a crucial factor unless you're on a very high speed internet connection or using a hard drive with very low R/W speed. But if your device is not able to write the data to the disk fast enough, a faster connection won't be useful. In other words, the connection speed should be less than you disk speed.

### *Bandwidth limitation in file hosting sites*

A lot of file hosting websites and services (for ex. RapidShare) offer file downloads at two different schemes. A free regular download, where your download speed, bandwidth, number of parallel connection, auto resume capability, etc. are limited, and some paid Premium plans which remove these limitations. The same server may be capable of handling both types of requests. Here, the server controls the speed and bandwidth for individual connections.

If the connections are from paid users, speed / bandwidth caps are lifted and they get to utilize full server resources. Other users, however, only get to use a small portion of these resources for a

limited amount of time. Sometimes, parallel connections from the same IP is also restricted. In that case, even your download manager won't be able to download any faster than your regular speed.

Premium plans in these kind of file hosting services allow you to utilize their full bandwidth. However, it does not mean that you will get more speed and bandwidth than your local ISP can provide. So, even though a particular server allows you to download, say at 2000 KBps; on a 2Mbps connection, you can only utilize up to 256 KBps.

### *Downloading via Download Managers*

Regular downloaders that are integrated with web browsers download files through a single connection. To enhance downloading speeds, third party ***download manager*** applications (For example; IDM, DAP, Orbit Downloader, etc.) are available which are able to set up multiple connections in parallel to download a file. Of course, this feature can be primarily controlled by server restrictions. However, if allowed, download managers can simultaneously download several parts of the file and hence improve the overall downloading speed.

### *Downloading from Torrents*

Torrent downloads work in a different way than regular downloads. Instead of the conventional client-server model, this technology is based on a peer-to-peer model (P2P). In this model, data can flow universally among number of connected users, known as peers. A file being shared on P2P is distributed across the entire network.

There are two types of ***Peer –Seeder*** and ***Leecher.*** Seeders are users uploading data in the network, and leechers are those who are downloading it. In a torrent network, if there are more number of leechers than seeders, downloading speed might decrease as there are more nodes downloading the data than those who are uploading. On the other hand, if there are more number of seeders, downloading speed might be higher.

Torrent downloads can, in fact, be faster than regular downloads, since there are numerous active parallel connections to download parts of the data. Nodes can connect to a torrent network via BitTorrent clients. Once peers complete download, they can also seed it for other leechers to download from.

You can find out your own connection speed by performing an online test. Speedtest.net is a good web application to rate your connection in terms of Download and Upload speed.

Connection speed and download speed are fairly the same thing, only measured in different units. So, to get download speed (in KBps) from connection speed (in Mbps), first multiply the connection speed by 1024 to convert from Megabit (Mb) to Kilobit (Kb), and then divide by 8 to convert it from Kilobit (Kb) to Kilobyte (KB).

**Cheque Truncation System (CTS)** or Image-based Clearing System (ICS), in India, is a project of the Reserve Bank of India (RBI), commencing in 2010, for faster clearing of cheques. CTS is based on a cheque truncation or online image-based cheque clearing system where cheque images and magnetic ink character recognition (MICR) data are captured at the collecting bank branch and transmitted electronically.

Cheque truncation means stopping the flow of the physical cheques issued by a drawer to the drawee branch. The physical instrument is truncated at some point en-route to the drawee branch and an electronic image of the cheque is sent to the drawee branch along with the relevant information like the MICR fields, date of presentation, presenting banks etc. This would eliminate the need to move the physical instruments across branches, except in exceptional circumstances, resulting in an effective reduction in the time required for payment of cheques, the associated cost of transit and delays in processing, etc., thus speeding up the process of collection or realization of cheques.

CTS has been implemented in New Delhi, Chennai and Mumbai with effect from February 1, 2008, September 24, 2011 and April 27, 2013 respectively. After migration of the entire cheque volume from MICR system to CTS, the traditional MICR-based cheque processing has been discontinued across the country. The CTS-2010 compliant cheques are both image friendly and have enhanced security features. All banks providing cheque facility to their customers have been advised to issue only 'CTS-2010' standard cheques. Cheques not complying with CTS-2010 standards would be cleared at less frequent intervals i.e. weekly once from November 1, 2014 onwards.

Banks derive multiple benefits through the implementation of CTS, like a faster clearing cycle meaning technically possible realization of proceeds of a cheque within the same day. It offers better reconciliation/ verification, better customer service and enhanced customer window. Operational efficiency provides a direct boost to bottom lines of banks as clearing of local cheques is a high cost low revenue activity. Besides, it reduces operational risk by securing the transmission route. Centralized image archival systems ensure that data storage and retrieval is easy. Reduction of manual tasks leads to reduction of errors. Real-time tracking and visibility of the cheques, less frauds with secured transfer of images to the RBI are other benefits that banks derive from this solution.

**NG RTGS-Next Generation RTGS**

NG-RTGS has been introduced in India since October 2013. With its advanced liquidity and queue management features, the new RTGS system is expected to significantly improve the efficiency of financial markets. He hoped the new RTGS system would be such a driver for India‘s financial system.

Reportedly the first in the world to be built on ***ISO 20022*** messaging standards, the new RTGS system is highly scalable and will have several new functionalities. These include advance liquidity features, including gridlock resolution mechanism and hybrid settlement facility, facility to accept future value dated transactions, options to process multi-currency transactions, etc. These functionalities, as and when made available for use, will be notified to the participants.

The new ISO 20022 compliant RTGS system provides three access options to participants thick-client, Web-API (through INFINET or any other approved network) and Payment Originator module. The participants can decide the mode of participation in the system based on the volume of transactions and the cost of setting up the infrastructure.

The RTGS infrastructure in India is critical in facilitating the orderly settlement of payment obligations. The role of central banks as operators of large-value payment systems is important in the context of the broader role of the central bank in a nation’s financial system insofar as it offers safety net attributes by providing final settlement in central bank money.

RTGS is a critical Financial market Infrastructure (FMI) operated by the Reserve Bank of India and it will be assessed against the Committee on Payment and Settlement Systems and the International Organisation of Securities Commissions (CPSS-IOSCO) Principles for Financial Market Infrastructures applicable to FMIs.

With implementation of the new RTGS system, the existing RTGS system will cease to be operational. Further, the RTGS System Regulations 2013would replace the RTGS (Membership) Business Operating Guidelines, 2004 and RTGS (Membership) Regulations, 2004.

**National Electronic Fund Transfer (NEFT)**

National Electronic Funds Transfer (NEFT) is a nation-wide payment system maintained by Reserve Bank of India (RBI), facilitating one-to-one funds transfer. Under this Scheme, individuals, firms and corporates can electronically transfer funds from any bank branch to any individual, firm or corporate having an account with any other bank branch in the country participating in the Scheme. Against the principle of RTGS which is a Real-Time as well as Gross Settlement system, NEFT settlement happens in batches.

For being part of the NEFT funds transfer network, a bank branch has to be NEFT- enabled. The list of bank-wise branches which are participating in NEFT is provided in the website of Reserve Bank of India.

Individuals, firms or corporates maintaining accounts with a bank branch can transfer funds using NEFT. Even such individuals who do not have a bank account (walk-in customers) can also deposit cash at the NEFT-enabled branches with instructions to transfer funds using NEFT. However, such cash remittances will be restricted to a maximum of Rs.50,000/- per transaction. Such customers have to furnish full details including complete address, telephone number, etc. NEFT, thus, facilitates originators or remitters to initiate funds transfer transactions even without having a bank account.

Individuals, firms or corporates maintaining accounts with a bank branch can receive funds through the NEFT system. It is, therefore, necessary for the beneficiary to have an account with the NEFT enabled destination bank branch in the country.

The NEFT system also facilitates one-way cross-border transfer of funds from India to Nepal. This is known as the Indo-Nepal Remittance Facility Scheme. A remitter can transfer funds from any of the NEFT-enabled branches in to Nepal, irrespective of whether the beneficiary in Nepal maintains an account with a bank branch in Nepal or not. The beneficiary would receive funds in Nepalese Rupees.

**Limit on the amount that could be transferred using NEFT –** No**.** There is no limit – either minimum or maximum – on the amount of funds that could be transferred using NEFT. However, maximum amount per transaction is limited to Rs.50,000/- for cash-based remittances within India and also for remittances to Nepal under the Indo-Nepal Remittance Facility Scheme.

**Operating hours of NEFT -** Unlike Real-time gross settlement (RTGS), fund transfers through the NEFT system do not occur in real-time basis. NEFT settles fund transfers in half-hourly

batches with 23 settlements occurring between 8:00 AM and 7:00 PM on week days. Transfers initiated outside this time period are settled at the next available window. No settlements are made on the second and fourth Saturday of the month or on Sundays.

**Process of NEFT system -** An individual / firm / corporate intending to originate transfer of funds through NEFT has to fill an application form providing details of the beneficiary (like name of the beneficiary, name of the bank branch where the beneficiary has an account, IFSC of the beneficiary bank branch, account type and account number) and the amount to be remitted. Customers enjoying net banking facility offered by their bankers can also initiate the funds transfer request online. Some banks offer the NEFT facility even through the ATMs.

The originating bank branch prepares a message and sends the message to its pooling centre (also called the NEFT Service Centre). The pooling centre forwards the message to the NEFT Clearing Centre (operated by National Clearing Cell, Reserve Bank of India, Mumbai) to be included for the next available batch.

The Clearing Centre sorts the funds transfer transactions destination bank-wise and prepares accounting entries to receive funds from the originating banks (debit) and give the funds to the destination banks (credit). Thereafter, bank-wise remittance messages are forwarded to the destination banks through their pooling centre (NEFT Service Centre).

Finally, the destination banks receive the inward remittance messages from the Clearing Centre and pass on the credit to the beneficiary customers' accounts.

**IFSC-** IFSC or Indian Financial System Code is an alpha-numeric code that uniquely identifies a bank-branch participating in the NEFT system. This is an 11 digit code with the first 4 alpha characters representing the bank, and the last 6 characters representing the branch. The 5th character is 0 (zero). IFSC is used by the NEFT system to identify the originating / destination banks / branches and also to route the messages appropriately to the concerned banks / branches.

**Acknowledgement by SMS** - In case of successful credit to the beneficiary's account, the bank which had originated the transaction is expected to send a confirmation to the originating customer (through SMS or e-mail) advising of the credit as also mentioning the date and time of credit. For the purpose, remitters need to provide their mobile number / e-mail-id to the branch at the time of originating the transaction.

**Tracking an NEFT transaction** - The remitter can track the NEFT transaction through the originating bank branch or its CFC using the unique transaction reference number provided at the time of initiating the funds transfer. It is possible for the originating bank branch to keep track and be aware of the status of the NEFT transaction at all times.

***Benefits of using NEFT:***

NEFT offers many advantages over the other modes of funds transfer:

- The remitter need not send the physical cheque or Demand Draft to the beneficiary.

- The beneficiary need not visit his / her bank for depositing the paper instruments.
- The beneficiary need not be apprehensive of loss / theft of physical instruments or the likelihood of fraudulent encashment thereof.
- Cost effective.
- Credit confirmation of the remittances sent by SMS or email.
- Remitter can initiate the remittances from his home / place of work using the internet banking also.
- Near real time transfer of the funds to the beneficiary account in a secure manner.

NEFT has gained popularity due to its saving on time and the ease with which the transactions can be concluded. Introduction of Immediate Payment Services (IMPS) by National Payments Corporation of India (NPCI), which is gaining popularity reduces the burden on NEFT systems at RBI.

**National Payments Corporation of India (NPCI) – Its Products & Services**

**National Payments Corporation of India** (NPCI), is the umbrella organisation for all retail payment systems in India, which aims to allow all Indian citizens to have unrestricted access to e-payment services.

Founded in 2008, NPCI is a not-for-profit organisation registered under section 8 of the Companies Act 2013. The organisation is owned by a consortium of major banks,[3] and has been promoted by the country's central bank, the Reserve Bank of India. Its recent work of developing Unified Payments Interface aims to move India to a cashless society with only digital transactions.

It has successfully completed the development of a domestic card payment network called RuPay, reducing the dependency on international card schemes. The RuPay card is now accepted at all the ATMs, Point-of-Sale terminals and most of the online merchants in the country. More than 300 cooperative banks and the Regional Rural Banks (RRBs) in the country have also issued RuPay ATM cards.

More than 250 million cards have been issued by various banks, and it is growing at a rate of about 3 million per month. A variant of the card called 'Kisan Card' is now being issued by all the Public Sector Banks in addition to the mainstream debit card which has been issued by 43 banks. RuPay cards are also issued under the Jan Dhan Yojana scheme.

NPCI has taken over NFS (National Financial Switch) operations from 14 December 2009 from IDRBT. Membership regulations and rules are being framed for enrolling all banks in the country as members so that when the nationwide payment systems are launched, all would get included on a standardized platform.

***The key products of NPCI are:***

National Financial Switch (NFS) which connects 1, 98, 953 ATMs of 449 banks (91 Member Banks, 358 Sub- Member). Immediate Payment Service (IMPS) provided to 84 member banks, with more than 8.49 crore MMID (Mobile Money Identifier) issued, and crossed 10 million transactions.

National Automated Clearing House (NACH) - has close to 400 banks on board. Aadhaar Payments Bridge System (APBS) has more than 358 banks. Cheque Truncation System (CTS)

has fully migrated in 3 grids - southern, western & northern grids from MICR centres. Aadhaar-enabled payment system (AEPS) - has 36 member banks. RuPay – Domestic Card Scheme- has issued over 20 crore cards and enabled 10, 70, 000 PoS terminals in the country. The newest and most advanced addition to the NPCI revolution is the Unified Payments Interface (UPI) which has been launched on 11 April 2016.

*RuPay PaySecure* - Over 20 banks now offer this authentication mechanism to their RuPay cardholders. The new transaction flow of Card + OTP has infused more simplicity to cardholders. More than 70,000 merchants accept Rupay cards online. RuPay PaySecure is live on 10 acquiring banks which includes Union Bank of India, Kotak Mahindra Bank, Citi Bank, ICICI Bank, HDFC Bank, State Bank of India, IDBI Bank, IndusInd Bank, Bank of Baroda and Bank of India.

***NPCI service portfolio now and in the near future include:***

- National Financial Switch (NFS) - network of shared automated teller machines in India.
- Unified Payment Interface (UPI) - Single mobile application for accessing different bank accounts
- BHIM App - Smartphone app built using UPI interface.
- Immediate Payment Service (IMPS) - Real time payment with mobile number.
- *99# - mobile banking using USSD
- National Automated Clearing House (NACH)-
- Cheque Truncation System -online image-based cheque clearing system
- Aadhaar Payments Bridge System (APBS) -

RuPay - card scheme

- Bharat Bill Payment System (BBPS) - integrated bill payment system

**IMPS (Immediate Payment Services)**

**Immediate Payment Service (IMPS)** is an instant real-time inter-bank electronic funds transfer system in India. IMPS offers an inter-bank electronic fund transfer service through mobile phones. Unlike NEFT and RTGS, the service is available 24/7 throughout the year including bank holidays. When one initiates a fund transfer via IMPS, the initiator bank sends a message to IMPS, which debits the money and sends it to the receiving account. All this happens within 5-10 seconds.

IMPS is an innovative real time payment service that is available round the clock. This service is offered by National Payments Corporation of India (NPCI) that empowers customers to transfer money instantly through banks and RBI authorized Prepaid Payment Instrument Issuers (PPI) across India.

***Benefits of IMPS***

- Instant
- **Available 24 x7 (functional even on holidays)**
- Safe and secure, easily accessible and cost effective
- Channel Independent can be initiated from Mobile/ Internet / ATM channels

- **Debit & Credit Confirmation by SMS to both sender and receiver**

***National Unified USSD Platform (NUUP):***

NUUP (National Unified USSD Platform) is a USSD based mobile banking service from NPCI that brings together all the Banks and Telecom Service Providers. In NUUP, a customer can access banking services by just pressing *99# from his/her mobile phones. This service works across all GSM mobile handsets.

*IMPS transactions can be sent and received 24X7, (round the clock), including on holidays. Both sender & receiver get SMS confirmation.*

For using IMPS on mobile phones, a customer will have to register for mobile banking with his/her individual bank. However, for initiating IMPS using Bank branch, Internet banking and ATM channels, no prior Mobile banking registration is required. Both banked as well as un-banked customer can avail IMPS. However, unbanked customer can initiate IMPS transaction using the services of Pre-Paid Payments instrument issuer (PPI). MMID - Mobile Money Identifier is a 7 digit number, issued by banks. MMID is one of the input which when clubbed with mobile number facilitates fund transfer. Combination of Mobile no. & MMID is uniquely linked with an Account number and helps in identifying the beneficiary details. Different MMID's can be linked to same Mobile Number. (Please contact your bank for getting the MMID issued)

***Options available for a customer for doing IMPS transaction***

- Using Beneficiary Mobile no. and MMID
- Using Beneficiary Account no. and IFS Code
- Using Beneficiary Aadhaar Number

**Bharat Interface for Money (BHIM)**

Bharat Interface for Money (BHIM) is an app that lets you make simple, easy and quick payment transactions using Unified Payments Interface (UPI). You can make instant bank-to-bank payments and Pay and collect money using just Mobile number or Virtual Payment Address (VPA).

The following are the features of BHIM:

1. **Send Money:** User can send money using a Virtual Payment Address (VPA), Account Number & IFSC, Aadhaar Number or QR code.
2. **Request Money**: User can collect money by entering Virtual Payment Address (VPA). Additionally through BHIM App, one can also transfer money using Mobile No. (Mobile No should be registered with BHIM or *99# and account should be linked)
3. **Scan & Pay**: User can pay by scanning the QR code through Scan & Pay & generate your QR option is also present.
4. **Transactions**: User can check transaction history and also pending UPI collect requests (if any) and approve or reject. User can also raise complaint for the declined transactions by clicking on Report issue in transactions.

5. **Profile**: User can view the static QR code and Payment addresses created or also share the QR code through various messenger applications like WhatsApp, Email etc. available on phone and download the QR code.
6. **Bank Account**: User can see the bank account linked with his/her BHIM App and set/change the UPI PIN. User can also change the bank account linked with BHIM App by clicking Change account provided in Menu and can also check Balance of his/her linked Bank Account by clicking "REQUEST BALANCE"
7. **Language:** Up to 8 regional languages (Tamil, Telugu, Bengali, Malayalam, Oriya, Gujarati, Kannada ,Hindi) available on BHIM to improve user experience.
8. **Block User:** Block/Spam users who are sending you collect requests from illicit sources.
9. **Privacy:** Allow a user to disable and enable mobilenumber@upi in the profile if a secondary VPA is created (QR for the disabled VPA is also disabled).

****BHIM APP is available in play store (for android User) and App Store (for Apple User)****

**Bharat QR**

In a major push for seamless cashless transactions, Govt. of India has launched Bharat QR Code, which is world's first interoperable payment platform. National Payments Corporation of India (NPCI), which is the umbrella organisation for all digital and online retail payment systems in India, has developed this platform, which is expected to inspire and encourage more digital payments, without using debit or credit card.

***QR Codes*** are black and white two-dimensional machine readable code, which stores information about the merchant's bank accounts and URLs. With Bharat QR Code interface, merchants need to take a printout of their QR code (or have a soft copy) and show it to the consumer, who can simply scan the code using his or her smartphone, and the payment would be made. Instantly, seamlessly and without any hassles.

We had reported last year that Govt. is considering to create a common QR Code based payment mechanism, which has now been officially launched. The Retail industry is excited by its possibilities because QR code-based payments solves two major problems in a single go: a) less time consumed to make the payment, compared to debit/credit card b) no requirement to actually flash your credit/debit cards for making the payment.

Here are some interesting facts about Bharat QR Code payment system, which every debit/credit holder (who is also a bank account holder) should be aware of:

**Smart Cards**

The smartcards have increased data security, an active anti-fraud capabilities, multipurpose capabilities, flexibility in applications, and off-line validation. These functions are more or less inter-related but the most important of all is the high level of security provided by the smartcard compared to the other type of cards in operation. This makes it possible the use the smart cards in transactions dealing with money, property and personal data.

The Reserve Bank of India has set a target for banks to upgrade all ATMs by September 2017 with additional safety measures to process EMV chip and PIN cards in order to prevent skimming and cloning of debit and credit cards.

While the POS terminal infrastructure in the country has been enabled to accept and process EMV chip and PIN cards, the ATM infrastructure continues to process the card transactions based on data from the magnetic stripe. As a result, the ATM card transactions remain vulnerable to skimming, cloning, etc. frauds, even though the cards are EMV chip and PIN based.

It has become necessary to mandate EMV (Europay, MasterCard, Visa) chip and PIN card acceptance and processing at ATMs also. Contact chip processing of EMV chip and PIN cards at ATMs would not only enhance the safety and security of transactions at ATMs but also facilitate preparedness of the banks for the proposed "EMV Liability Shift" for ATM transactions, as and when it comes into effect.

Further, in order to ensure uniformity in card payments ecosystem, banks should also implement the new requirements at their micro-ATMs which are enabled to handle card-based payments.

**CVV OR CSC NUMBER**

The **CVV Number** ("**C**ard **V**erification **V**alue") on credit card or debit card is a 3 digit number on VISA, MasterCard and Discover branded credit and debit cards. On American Express branded credit or debit card it is a 4 digit numeric code.

The CVV number can be located by looking on credit or debit card, as illustrated in the image below:

Providing the CVV number to an online merchant proves that one actually has the physical credit or debit card - and helps to keep one safe while reducing fraud.

**CVV numbers** are NOT the card's secret **PIN** (**P**ersonal **I**dentification **N**umber).

One should never enter one's PIN number when asked to provide the **CVV**. (PIN numbers allow one to use one's credit or debit card at an ATM or when making an in-person purchase with debit card or a cash advance with any credit card.)

**CVV** numbers are also known as **CSC numbers** ("Card Security Code"), as well as **CVV2 numbers**, which are the same as CVV numbers, except that they have been generated by a 2nd generation process that makes them harder to "guess".

In 2016, a new e-commerce technology called ***Motioncode*** was introduced, designed to automatically refresh the CVV code to a new one every hour or so.

## ATM & POINT OF SALE (POS)

***ATM (Automated Teller Machine)*** A typical ATM could duplicate most of the services of a live teller; deposits, withdrawals, and money transfers between accounts all could be made with relative ease. More significantly, the terminals could be located outside the bank lobby, allowing 24 hour access and greater customer convenience. For the banks ATM's became mini-branches that extended their financial territory and customer base far beyond physical buildings. As a result, many ATMs rapidly found homes inside major retail outlets, convenience stores, gas stations, and other highly trafficked locations, a situation welcomed by businesses because it provided instant cash for customers.

*White label ATMs* are those ATMs which do not belong to any bank but managed by a non-banking entity, e.g., Indicash, India-1 ATM, Prism Payment Services.

However, ATM's would not be the final solution to the common electronic goal, because they still involved the use of paper money. Yet, in a second generation machine called a Point of Sale terminal (POS), the prospect of having a truly cashless society suddenly took a giant leap forward. The potential of POS for achieving a totally automated economy was enormous. It was logical to assume that if the capability existed for electronic banking to the extent of obtaining cash out of an account using a networked ATM system, then the technology also must be ripe for eliminating the need for physical money altogether. POS terminals were seen as a key ingredient in the transition to this goal.

***A point of sale terminal (POS terminal)*** is an electronic device used to process card payments at retail locations. . Point of sale terminals are a combination of software and hardware that allows retail locations to accept card payments without updating their cash registers to read cards directly. The costs of installing POS terminals vary with the size of the business and the terms from the supplier. Small merchants may have to pay rent for the terminal, as well as pay an additional per-transaction fee.

The trend is away from the traditional use of just magnetic stripe reader as more options open up for mobile payments.

A POS terminal generally does the following:

- Reads the information off a customer's credit or debit card
- Checks whether the funds in a customer's bank account are sufficient
- Transfers the funds from the customer's account to the seller's account (or at least, accounts for the transfer with the credit card network)
- Records the transaction and prints a receipt

Despite the more advanced technology of a POS system as compared to a simple cash register, the POS system is still as vulnerable to employee theft through the sale window. A dishonest cashier at a retail outlet can collude with a friend who pretends to be just another customer. During checkout the cashier can bypass scanning certain items or enter a lower quantity for some items thus profiting thereby from the "free" goods.

With the launch of mobile payment particularly Android Pay and Apple Pay both in 2015, it is expected that because of its greater convenience coupled with good security features, this would eventually eclipse other types of payment services - including the use of payment terminals. However, for mobile payment to go fully mainstream, mobile devices like smartphones that are NFC-enabled must first become universal. NFC (near field communication) is the technology that allows two devices—like your phone and a payments terminal—to talk to each other when they're close together. NFC is the technology that enables contactless payments.

Electronic funds transfer at point of sale (**EFTPOS)** is an electronic payment system involving electronic funds transfers based on the use of payment cards, such as debit or credit cards, at payment terminals located at points of sale. EFTPOS is highly popular in Australia and New Zealand, and being used in NZ for about 60% of all retail transactions.

**Latest Trends in eCommerce**

A key outcome of the technology revolution in India has been connectivity, which has fuelled unprecedented access to information. Millions of people who had little means to join the national discourse can now gain new insights into the world around them. Farmers know crop prices. Consumers understand global standards of product and service quality. Rural Indians recognise the differences between the opportunities available to them and those available to their urban counterparts. And citizens have a mass forum for expressing their political opinions. The upshot of this connectivity revolution has been empowerment of Indians.

An analysis of the demographic profile of internet users further testifies that eCommerce will rise rapidly in India in coming years. Around 75% of Indian internet users are in the age group of 15 to 34 years. This category shops more than the remaining population. Peer pressure, rising aspirations with career growth, fashion and trends encourage this segment to shop more than any other category and India, therefore, clearly enjoys a demographic dividend that favours the growth of eCommerce. In coming years, as internet presence increases in rural areas, rural India will yield more eCommerce business

***Mobile to be the most influential aspect of eCommerce*** -With mobile apps being developed by most eCommerce websites, smartphones are increasingly replacing PCs for online shopping. In 2013, only 10% of the mobile users used smartphones, and only 5% of the eCommerce transactions were made through a mobile device. This figure has more than doubled, and more than 13% of all eCommerce transactions today happen via mobile3. According to some industry players, over 50% of the orders are being placed through mobile apps, which is not only leading to substantial customer acquisition but also building customer loyalty for various brands. However, most mobile transactions so far are for entertainment, such as booking movie tickets and music downloads. This trend will change soon with more and more merchandise being ordered online.

***More business coming from smaller towns*** - eCommerce is increasingly attracting customers from Tier 2 and 3 cities, where people have limited access to brands but have high aspirations. According to eCommerce companies, these cities have seen a 30% to 50% rise in transactions.

***Enhanced shopping experience*** - Besides general online shopping, customers are also shopping online for weddings and festivals, thanks to wider range of products being offered and aggressive advertisements. The free and quick shipment and wider choice of products, along with the ease of

shopping online as compared to in-store shopping, is also helping eCommerce gather momentum. Further, eCommerce companies are doing rapid business due to sales.

***Exclusive partnerships with leading brands*** - Over the year or so, there has been a trend of exclusive tie-ups between eTailers and established boutiques, designers, and high-end lifestyle and fashion brands. For instance, Jabong added international fashion brands such as Dorothy Perkins, River Island, Blue saint and Miss Selfridge, along with local fashion brands through Jabong Boutiques. Similarly, Myntra benefited from exclusive tie-ups with brands such as Harvard Lifestyle, Desigual and WROGN from Virat Kohli.

***Expanding the product basket*** - There is a recent trend of relatively newer products such as grocery, hygiene, and healthcare products being purchased online. Similarly, lingerie and Indian jewellery has also been in great demand among customers outside India. Export comprises 95% of cross-border eCommerce, with the US, UK, Australia, Canada and Germany being the major markets.

**Innovation in online business models**

To get the maximum benefit from eCommerce business, a large number of companies such as Amazon, Alibaba etc. are adopting different innovative ideas and operating models including partnering with online marketplaces or setting up their own online stores. Some key operating models include the following:

- ***Marketplace and pick-up & drop*** is a model where sellers often partner with leading marketplaces to set up a dedicated online store on the latter's website. Here sellers play a key role of managing inventory and driving sales. They leverage on high traffic on the marketplaces' website and access their distribution network. However, the sellers have limited say on pricing and customer experience.
- ***Self-owned inventory*** is a model where the eCommerce player owns the inventory. The model provides better post-purchase customer experience and fulfilment. It provides smoother operations due to ready information on the inventory, location, supply chain and shipments, effectively leading to better control over inventory. On the flipside, however, there are risks of potential mark downs and working capital getting tied up in inventory.
- ***Private label*** reflects a business where an eCommerce company sets up its own brand goods, which it sells through its own website. This model offers a wide-ranging products and pricing to its customers and competes with branded labels. Here, margins are typically higher than third-party branded goods.
- ***White label*** involves the setting up of a branded online store managed by the eCommerce player or a third party. The brand takes the responsibility of generating website traffic and providing services by partnering with payment gateways. It helps build trust, customer affinity and loyalty and provides better control of brand and product experience.

## SMS BANKING & BANKING ALERTS

**SMS banking** is a form of mobile banking. It is a facility used by some banks or other financial institutions to send messages (also called notifications or alerts) to customers' mobile phones using SMS messaging, or a service provided by them which enables customers to perform some financial transactions using SMS.

SMS banking services may use either push and pull messages. Push messages are those that a bank sends out to a customer's mobile phone, without the customer initiating a request for the information. Typically, a push message could be a mobile marketing message or an alert of an event which happens in the customer's bank account, such as a large withdrawal of funds from an ATM or a large payment involving the customer's credit card, etc. It may also be an alert that some payment is due, or that an e-statement is ready to be downloaded.

Another type of push message is one-time password (OTPs). OTPs are the latest tool used by financial institutions to combat cyber fraud. Instead of relying on traditional memorized passwords, OTPs are sent to a customer's mobile phone via SMS, who are required to repeat the OTP to complete transactions using online or mobile banking. The OTP is valid for a relatively short period and expires once it has been used.

Bank customers can select the type of activities for which they wish to receive an alert. The selection can be done either using internet banking or by phone.

Pull messages are initiated by the customer, using a mobile phone, for obtaining information or performing a transaction in the bank account. Examples of pull messages include an account balance enquiry, or requests for current information like currency exchange rates and deposit interest rates, as published and updated by the bank. Depending on the selected extent of SMS banking transactions offered by the bank, a customer can be authorized to carry out either non-financial transactions, or both and financial and non-financial transactions. SMS banking solutions offer customers a range of functionality, classified by push and pull services as outlined below.

Typical push services would include:

- periodic account balance reporting (say at the end of month);
- reporting of salary and other credits to the bank account;
- successful or un-successful execution of a standing order;
- successful payment of a cheque issued on the account;
- insufficient funds;
- large value withdrawals on an account;
- large value withdrawals on the ATM or EFTPOS on a debit card;
- large value payment on a credit card or out of country activity on a credit card.
- one-time password and authentication
- an alert that some payment is due
- an alert that an e-statement is ready to be downloaded.

Typical pull services would include:

- Account balance enquiry;

- Mini statement request;
- Electronic bill payment;
- Transfers between customer's own accounts, like moving money from a savings account to a current account to fund a cheque;
- Stop payment instruction on a cheque;
- Requesting for an ATM card or credit card to be suspended;
- De-activating a credit or debit card when it is lost or the PIN is known to be compromised;
- Foreign currency exchange rates enquiry;
- Fixed deposit interest rates enquiry

**Security concerns in SMS Banking**

The lack of encryption on SMS messages is an area of concern that is often discussed. This concern sometimes arises within the group of the bank's technology personnel, due to their familiarity and past experience with encryption on the ATM and other payment channels. The lack of encryption is inherent to the SMS banking channel and several banks that use it have overcome their fears by introducing compensating controls and limiting the scope of the SMS banking application to where it offers an advantage over other channels.

Suppliers of SMS banking software solutions have found reliable means by which the security concerns can be addressed. Typically the methods employed are by pre-registration and using security tokens where the transaction risk is perceived to be high.

Most online banking platforms are owned and developed by the banks using them. There is only one open source online banking platform supporting mobile banking and SMS payments called Cyclos, which is developed to stimulate and empower local banks in development countries.

**SMS & Email Alerts in Banking**

This is a very useful facility that sends customer information on customer's banking transactions. The alerts are either event based or frequency based. When register for certain alerts they are sent to customer either via SMS or email, or both. Some alerts are made mandatory by regulator whereas for others they customer may choose as per his requirement. Some banks send email alerts for monthly account statements in encrypted pdf format which may be opened using a password only.

***RBI's has made SMS for clearing cheque transactions mandatory***- Expressing concern over the rise in cheque-related fraud cases, the Reserve Bank of India (RBI) has made SMS alerts mandatory for such transactions since November 2014. Banks now send SMS alerts to both payer and drawer in cheque transactions as soon as the instruments are received for clearing.

**Bharat Bill Payment System (BBPS)**

**Bharat Bill Payment System (BBPS)** is an integrated bill payment system in India offering interoperable and accessible bill payment service to customers online as well as through a network of agents, enabling multiple payment modes, and providing instant confirmation of payment.

National Payments Corporation of India (NPCI) will function as the authorised Bharat Bill Payment Central Unit (BBPCU), which will be responsible for setting business standards, rules and procedures for technical and business requirements for all the participants. NPCI, as the BBPCU, will also undertake clearing and settlement activities related to transactions routed through BBPS. Existing bill aggregators and banks are envisaged to work as Operating Units to provide an interoperable bill payment system irrespective of which unit has on-boarded a particular biller. Payments may be made through the BBPS using cash, transfer cheques, and electronic modes. To start with, the scope of BBPS will cover repetitive payments for everyday utility services such as electricity, water, gas, telephone and Direct-to-Home (DTH). Gradually, the scope would be expanded to include other types of repetitive payments, like school / university fees, municipal taxes etc.

**Computer Security which is also at times referred to as information security is concerned with three main areas:**

1. Confidentiality:- Only authorized users can access the data resources and information.
2. Integrity:- Only authorized users should be able to modify the data when needed.
3. Availability:- Data should be available to users when needed.

Each of the above three areas is critical for computer security. Confidentiality deals with prevention of data theft such as bank account information, credit card information, passwords etc. Integrity refers to prevention of unauthorized data creation, modification or deletion. Last but not the least is availability, which ensures that the users are able to access data whenever needed.

**What Are ISO 27000 series standards?**

The ISO 27000 series of standards are a compilation of international standards all related to information security. Every standard from the ISO 27000 series is designed with a certain focus – if you want to build the foundations of information security in your organization, and devise its framework, you should use ISO 27001; if you want to implement controls, you should use ISO 27002, if you want to carry out risk assessment and risk treatment, you should use ISO 27005 etc.

ISO 27001 establishes requirements - if an organization wants to certify its Information Security Management System (ISMS) it needs to comply with all requirements in ISO 27001. On the other hand, ISO 27002 are best practices that are not mandatory. That means that an organization does not need to comply with ISO 27002 but can use it as inspiration to implement requirements in ISO 27001. ISO 27002 was formerly known as ISO 17799, having been renamed in 2007. ISO 27002 is more complex and difficult to comply with but it is not mandatory because depending on the context and the business of the organization it could implement the control in another way. ISO 27001 establishes what you have to do but not how. ISO 27002 describes how.

**Logical Security**

Generally, passwords must be at least 8 characters long and include upper and lower case characters and at least one numeric character and one special character. It is amazing to note that a ‘brute force’ tool which may crack a 4 character password in just 4 seconds, takes about 10 years to crack an 8 character password.

**Privileged identity management (PIM**) is a recent concept involving a domain within identity management focused on the special requirements of powerful accounts within the IT infrastructure of an enterprise. It is frequently used as an information security and governance tool to help companies in meeting compliance regulations and to prevent internal data breaches through the use of privileged accounts, like system or database administrator. PIM, privileged identity management; PUM, privileged user management; and PAM, privileged account management OR privileged access management; all three of these acronyms revolve around the same simple concept: who can get to a server, how they can get to a server and what they can do when they get there.

***Denial-of-service (DoS) attacks:*** Where the intruder attempts to crash a service (or the machine), overload network links, overloaded the CPU, or fill up the disk. The intruder is not trying to gain information, but to simply act as a vandal to prevent from making use of machine.

***Distributed Denial of Service (DDoS) attacks:*** In most respects it is similar to a DoS attack but the results are much, much different. Instead of one computer and one internet connection the DDoS attack utilises many computers and many connections. The computers behind such an attack may be often distributed around the whole world and will be part of what is known as a botnet. The main difference between a DDoS attack vs a DoS attack, therefore, is that the target server will be overload by hundreds or even thousands of requests in the case of the former as opposed to just one attacker in the case of the latter. Therefore it is much, much harder for a server to withstand a DDoS attack as opposed to the simpler DoS incursion.

***An Intrusion Detection System (IDS*)** is a system for detecting such intrusions. IDS can be broken down into the following categories:

***An Intrusion Prevention System (IPS)*** sits between the firewall and the rest of the network. That way, if an attack is detected, the IPS can stop the malicious traffic before it makes it to the rest of the network. In contrast, an IDS simply sits on top of the network rather than in front of it. Unlike IDS, IPS actively takes steps to prevent or block intrusions that are detected. These preventing steps include activities like dropping malicious packets and resetting or blocking traffic coming from malicious IP addresses. IPS can be seen as an extension of IDS, which has the additional capabilities to prevent intrusions while detecting them.

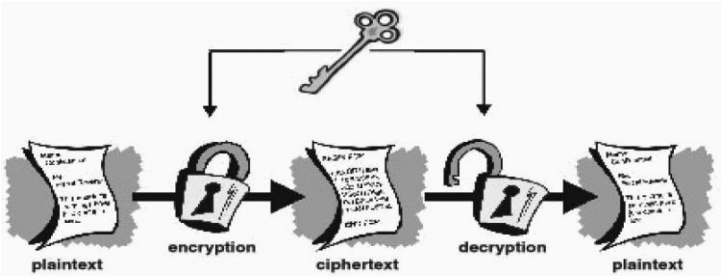
IPS is a system that actively takes steps to prevent an intrusion or an attack when it identifies one. IPS are divided in to four categories. First one is the Network-based Intrusion Prevention (NIPS), which monitors the entire network for suspicious activity. The second type is the Network Behavior Analysis (NBA) systems that examine the traffic flow to detect unusual traffic flows which could be results of attack such as distributed denial of service (DDoS). The third kind is the Wireless Intrusion Prevention Systems (WIPS), which analyzes wireless networks for suspicious traffic. The fourth type is the Host-based Intrusion Prevention Systems (HIPS), where a software package is installed to monitor activities of a single host.

## CRYPTOGRAPHY

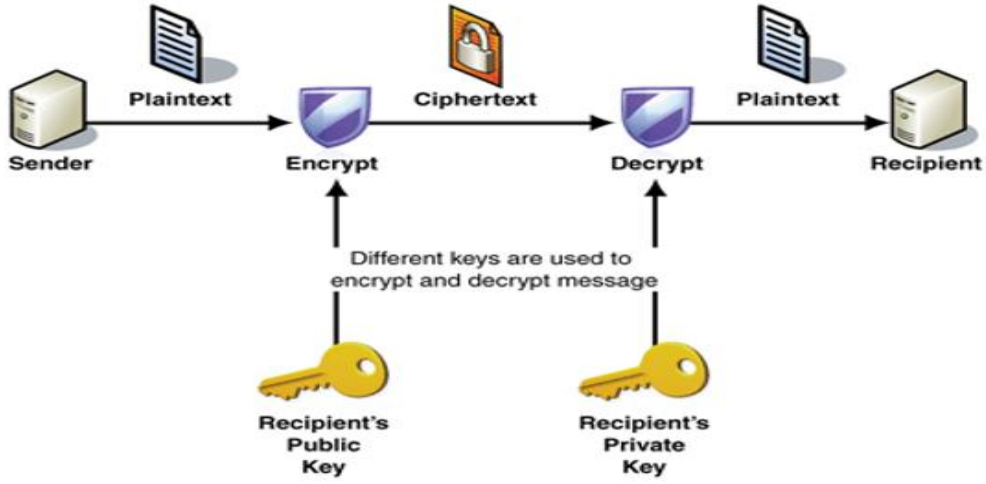
***There are two basic types of Encryption algorithms:***

(i) Symmetric encryption
(ii) Asymmetric Encryption

***Symmetric Encryption***: In this encryption technique the sender and receiver encrypts and decrypts the message with the same key. Examples are Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Kuznyechik, RC4, 3DES, Skipjack etc.




***Asymmetric encryption***: In this encryption technique the sender encrypts the message with the receiver's public key and the receiver decrypts the information with recipient's private key. Hence this technique is called public key encryption. Examples are: Diffie-Hellman, RSA, ECC, ElGamal, DSA etc.



| S.N. | Attributes | Symmetric Cryptosystem | Asymmetric Cryptosystem |
|---|---|---|---|
| 1 | Key | One key is shared between two or more entities | On entity has a public key and another entity has a private key |
| 2 | Key exchange | Out of band | Public key is encrypted and set with message, and thus the key is distributed by inbound means. |
| 3 | Speed | Algorithm is less complex and faster | Algorithm is more complex and slower |
| 4 | Key length | Fixed key length | Variable key length |
| 5 | Applications | Bulk encryption like files | Key encryption and distribution key e.g. PIN of ATM |
| 6 | Security Level | Confidentiality and Integrity | Confidentiality, Integrity, Authentication and non-repudiation |

Among the various models of symmetric cipher analyzed the Rijndael is the best. Actually it is the role model of DES and AES. This model is adopted by different information security agencies like NSA, NIST and FIPS.
Among the various asymmetric ciphers, RSA is a moderate and most useful cipher for small data encryption like digital signature, ATM Pin etc.
But as discussed above, RSA (asymmetric technique) is much slower than Rijndael (symmetric technique) and other symmetric cipher techniques. But the scalability of asymmetric cryptosystem is far higher than the symmetric cryptosystem. Thus where the number of users is huge and required keys are very high, asymmetric cryptosystem proves to be superior.

It is scientifically predicted that the symmetric cipher like Rijndael is supposed to be secure against mathematical attacks until 2090. Thus they are very suitable for hardware level security in communicating devices.

***Advanced Encryption Standard (AES):*** is the successor of DES (Data Encryption Standard) as standard symmetric encryption algorithm for US federal organizations. AES uses keys of 128, 192 or 256 bits, although, 128 bit keys provide sufficient strength today. It uses 128 bit blocks, and is efficient in both software and hardware implementations. It was selected through an open competition involving hundreds of cryptographers during several years.

### *Safe Key Length*

128-bit encryption is a data/file encryption technique that uses a 128-bit key to encrypt and decrypt data or files. In today's parlance, it is considered one of the most secure encryption methods and used in most modern encryption algorithms and technologies. 128-bit encryption is considered to be logically unbreakable as of date. However, it is to be remembered that breakability is only relative considering the technology available at that time. Keeping this in view, it is also recommended by many that the cipher AES-256 be used among other places in SSL/TLS across the Internet. It's considered among the top ciphers. In theory it's not crackable since the combinations of keys is massive.

### Digital Signature

In technical terms, a digital signature is the sequence of bits that is created by running an electronic message through a one-way hash function (a program). The resulting message is called Message Digest (MD). Some of the popular MD algorithms are MD5, SHA1 and SHA256. It has been shown that MD5 is less reliable with problems relating to collision (where 2 keys for different data

are the same). Besides MD5, SHA and CRC32 are other message digest algorithms. The SHA (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. SHA-256algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back.

**Emerging Trends in Public Key Infrastructure:**

With the long-term success of PKI, it's no surprise that it has been popping up in an increasing number of situations – from the Web to identity documents to mobile devices to today's "smart" appliances, remote-controlled home systems and the entire Internet of Things (IOT). PKI's ability to combine strong protection with cost-effective management and user-friendliness is now at the core of its success. And it is expected to increase sharply as mobile devices proliferate, with more and more "smart" applications and uses.

***The Growth of Mobile***

PKI will continue to play a key role in the growth of mobile for trust anchoring, device identity and authentication. As more and more organizations use certificates for secure mobile connection to Wi-Fi and VPN networks, PKI meets the increased demand for safe, secure transmission of all kinds of data.
This includes a wide range of mobile apps, mobile payments, cloud services and access to physical and logical assets. Mobile certificates are also essential in identifying and securing corporate-issued devices and the growing number of Bring-Your-Own-Devices. (BYODs)

***Internet of things (IOT)***

Widely predicted to be a major factor in future IT infrastructure and identity, the Internet of Things will rely on PKI to play an essential role in a vast number of interconnected applications and devices. These network-connected things already include ATMs and financial accounts, lighting systems and thermostats, home surveillance equipment, medical devices, smart meters of all varieties, electronic doggie doors, TV's, home electronics – even planes, trains and automobiles. All of these require a transparent, consistent form of certificate-based identity authentication. And having dealt with network connected devices for decades, PKI is the ideal solution to deliver and manage large numbers of certificates at high speed. Even though mobility and IoT are relatively new market drivers, their requirements are essentially the same as those of earlier network connected devices. Given the remarkable strength of PKI and its flexibility in adapting to new applications, one can expect the technology to continue for quite some time, because it does what it does really well.

***In India***

In India, a number of nationally important e-Governance initiatives have already been embarked upon by the Government. Large-scale adoption of Digital Signatures will be one of the key success factors in these initiatives, as they will rely on Digital Signatures for their authentication requirements. Several Training programs for different user segments have been conducted nation-wide.
Below listed are few examples of usage of digital signatures in India.

***Use of PKI in Aadhaar Data Encryption****:* Aadhaar enrolment data packets (individual electronic file containing resident demographics and biometrics) are strongly encrypted by the Enrolment Page 2 of 16 Client software at the time of enrolment even before saving any data to any hard disk. Encryption uses highest available public key cryptography encryption (PKI-2048 and AES-256) with each data record having a built-in mechanism to detect any tampering. Even if someone attempts to decrypt, due to the use of strongest available encryption (2048-bit asymmetric encryption), even with millions of computers, it will take billions of years to break such encryption.
***Income Tax e-filing:*** A Digital Signature Certificate lets you file your Tax Returns easier and more secure. According to revised provisions under section 44AB of IT Act "E-Filing is mandatory for all the individuals/professionals having an annual gross receipt of INR 25 Lakhs and above, and for business houses with annual turnover of INR 1 Crore and above.
***Ministry of Corporate Affairs (MCA):*** A Digital Signature Certificate helps make light work of various transactions related to the Ministry of Corporate Affairs, or Registrar of Companies. In addition to saving time, a Digital Signature Certificate also helps secure data.
***eProcurement*** is an online tender processing system for the state government departments. More than 1000 tenders published so far. The Digital Signatures are being used both by the vendors and government officials for tender submission and processing. The vendors/traders are using it for applying tenders online, while the government officials are using it at time of opening the tenders and during finalizing of the tenders.
***Voters List Preparation*** – The State Election Commission has issued a GO that the field data along with the photo ID will be digitized and the same will be digitally signed assuring the correctness of data.
The DSC (Digital Signature Certificate) will be used to counter verify the digitized data of voters list and the photo ID. This can be used by other applications such as eDistrict for online verification of citizen details.
***Online Counseling*** for admission to more than 1 lakh seats of Engineering, Medical, Polytechnic & B.Ed. courses. The Digital Signatures are being used by the Counseling In-charge for document verification, fee submission, registration & for choice locking opted by the candidates which are finally locked by the invigilators using DSC.
***IRCTC:*** IRCTC has facilitated online ticketing for RTSA agents and IATA approved agents. With this new technology, using Digital Signature Certificates, agents registered with IRCTC will be able to issue Railway tickets from the comfort of their homes. This will ensure speedy and secure business giving it a 24X7 dimension.
***DGFT:*** Export and Import Organizations (EXIM organizations) can apply for licenses online which means that they can also file accompanying documents electronically on the DGFT website. Since a Digital Signature Certificate ensures authenticity of the document, DGFT has mandated use of Digital Signature Certificates with all electronic documents uploaded on the DGFT site.
Since a Digital Signature Certificate is recognized by the legal system, all documents submitted using a Digital Signature Certificate is considered on par with physically signed documents, and also attract benefits endowed upon them through the Indian Information Technology Act 2000.

### *The Future is PKI*

Looking back to the early days of public-key technology, the inherent simplicity of the most popular schemes was a concern to many. How we could we place our faith in the long-term security of such simple mathematical operations is the question. While some narrow loopholes have been discovered in some of the basic schemes, the technology itself has withstood close scrutiny by

countless experts over the past forty years. In many ways, user confidence in the effectiveness of PKI is stronger than ever – and it remains the most practical and cost-effective solution to our ever-growing security challenges.

**Types of Disaster Recovery Strategies and Disaster Recovery Sites**

There are basically three levels of Disaster Recovery Strategies -

***Cold Site Replication*** - This is basically an entry level solution where the recovery time may be as much as 10 days but for a medium sized bank are typically between 5-7 days.

- Recovery in Days
- Lowest Cost Solution
- Restore data from Tape
- Hardware is Optional
- No Data Replicated via Communication Line

***Warm Site Replication*** - This is a good initial level solution for a medium sized branch where the recovery time generally is between one hour and 8 hours extending sometimes to 24 hours. Systems are synchronized via a secure network connection from the primary production system to the secondary system located elsewhere. Data is periodically synchronized via a network using a choice of industry leading data synchronization and replication software.

- Recovery in Hours
- Medium Cost Solution
- Faster Restoration
- Hardware needs to be purchased or leased
- Data Synchronization Over Communication Line

***Hot Site Replication*** - This is a high end solution for businesses which cannot even stop for seconds. Systems are synchronized via a secure network connection from the primary production system to the secondary system located elsewhere. Data is frequently synchronized via a network using a choice of industry leading data synchronization and replication software. Recovery times can be as low as a minute extending to 10 minutes.

- Recovery in Seconds/Minutes
- Higher Cost Solution
- Almost immediate Restoration
- Hardware needs to be purchased or leased
- Fully Redundant & Mirrored Environment

**Data Mirroring and Disk Arrays**: RAID 5 is the most common secure RAID level. It requires at least 3 drives. A RAID 5 array can withstand a single drive failure without losing data or access to data. If a drive fails, you still have access to all data, even while the failed drive is being replaced and the storage controller rebuilds the data on the new drive.

**BCP & DRP**

Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP) are used together so often that people often begin to forget that there is a difference between the two. A BCP is a plan that allows a business to plan in advance what it needs to do to ensure that its key products and services continue to be delivered (technicality: at a predefined level) in case of a disaster, while a DRP allows a business to plan what needs to be done immediately after a disaster to recover from the event. So, a BCP tells your business the steps to be taken to continue its key product and services, while a DRP tells your business the steps to be taken to recover post an incident. Some experts also opine that DRP takes care of technology side of BCP.

Your impact analysis, your business continuity strategy and business continuity plans are a part of BCP. Your incident response, emergency response, damage assessment, evacuation plans, etc. are all a part of DRP. It makes sense to divide your planning into two parts

- Planning to continue your business operations (BCP) and
- Planning to recover from disaster situations (DRP).

As part of the business continuity process an organisation will normally develop a series of DRPs. These are more technical plans that are developed for specific groups within an organisation to allow them to recover a particular business application. The most well-known example of a DRP is the Information Technology (IT) DRP. The typical test for a DR Plan for IT would be; "if we lost our IT services how would recover them?"

It is pertinent to note that BCP and DRP have similarities in banking industry since information processing application and business application have thin line of distinction and look like one and the same. All banking business operations and the concerned data processing operations are inseparable.

**A few more kinds of attacks**

***Phishing:*** Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Phishing has become rampant now a days and entities worldwide have lost their sensitive data and money.

***Spoofing:*** In the context of computer security, a spoofing attack is a situation in which one person or program successfully pretending as another by falsifying data, thereby gaining an illegitimate advantage. Spoofing is of two types. (1) Email spoofing is the creation of email messages with a forged sender address. Because the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such spoofing to mislead the recipient about the origin of the message. (2) Network spoofing-in computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system.

***Sniffing:*** Sniffing is the act of intercepting and inspecting data packets using sniffers (software or hardware devices) over the network. On the other hand, Spoofing is the act of identity

impersonation. Packet sniffing allows individuals to capture data as it is transmitted over a network and is used by network professionals to diagnose network issues, and by malicious users to capture unencrypted data, like passwords and usernames.

***Spamming:*** Electronic spamming is the use of electronic messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same site. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media too. Spam can also be used to spread computer viruses, Trojan or other malicious software. The objective may be identity theft, or worse (e.g., advance fee fraud). Some spam attempts to capitalize on human greed, while some attempts to take advantage of the victims' inexperience with computer technology to trick them (e.g., phishing).

***Ransomware***: Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse. More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. The ransomware may also encrypt the computer's Master File Table (MFT) or the entire hard drive. Thus, ransomware is a denial-of-access attack that prevents computer users from accessing files since it is intractable to decrypt the files without the decryption key.

Some examples of ransomware are Reveton, Cryptolocker, Cryptowall, Fusob and WannaCry. Wide-ranging attacks involving encryption-based ransomware began to increase through Trojans such as CryptoLocker, which had procured an estimated US$3 million before it was taken down by authorities, and CryptoWall, which was estimated by the US Federal Bureau of Investigation (FBI) to have accrued over $18m as ransom money by the attackers by June 2015.

In May 2017, the WannaCry ransomware attack spread through the Internet, using an exploit vector that Microsoft had issued a "Critical" patch for (MS17-010) two months before on March 14, 2017. The ransomware attack infected lakhs of users in over 150 countries, using 20 different languages to demand money from users.

**Measures against attacks**

Against Phishing attacks, obviously there cannot be an antivirus tool for checking. Only appropriate user education and generating awareness can prevent or reduce phishing menace.

Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message

To protect against sniffing, we need to encrypt all important data we send or receive, scan our networks for any issues or dangers and use only trusted Wi-Fi networks.

To prevent spamming, most of the email services, viz., Gmail, Yahoo, Hotmail etc. provide filtering facilities and also enable users to categorize certain messages as spam.

Best measures for protection against ransomware are taking regular backups of data, applying OS patches regularly and using latest anti-malware solution.

***Types of Computer Frauds***

1. Sending hoax emails to scare people
2. Illegally using someone else's computer or "posing" as someone else on the internet
3. Using spyware to gather information about people
4. Emails requesting money in return for "small deposits"
5. Pyramid schemes or investment schemes via computer with the intent to take and use someone else's money
6. Emails attempting to gather personal information used to access and use credit cards or social security numbers
7. Using the computer to solicit minors into sexual alliances
8. Violating copyright laws by coping information with the intent to sell it
9. Hacking into computer systems to gather large amounts of information for illegal purposes
10. Hacking into or illegally using a computer to change information such as grades, work, reports, etc.
11. Sending computer viruses or worms with the internet to destroy or ruin someone else's computer

***Precautions***

Refrain from opening e-mail and e-mail attachments from individuals you do not know. Have ALL external storage devices scanned by virus-scanning software before inserted on your PC. Secure your Internet Web browsing.

Make sure you have a regular backup, in case you need to restore data. If you have high-speed (broadband) Internet access in your office, think about getting either a hardware or software firewall to protect your computer system. If you run a "Wireless Network" you must take time to secure it and understand how it works.

Individuals should not pay attention to get rich quick schemes. If they seem too good to be true, they absolutely are. Children should be taught about safe communication on the Internet to protect them from predators. Avoid communication with strangers and never tell strangers your location.

**Traps by ATM fraudsters at ATM**

1. ***Hidden camera***: Tiny, pinhole cameras may be placed on the machine or even the roof at strategic positions to capture your PIN.
2. ***Card skimmer***: These devices are installed on the card reader slot to either copy the information from the magnetic strip of your card or steal the card itself.
3. ***Bulky slot:*** If the slot feels slightly bulky or misaligned, in all probability an additional card reader slot has been placed on top of the actual one. Loose slot: If the slot is wobbly or loose, it indicates the presence of a 'Lebanese loop', which is a small plastic device with a barb that holds your card back in the machine. You may think the machine has swallowed your card or it has been stuck.

4. ***Shoulder surfers***: These are people lurking in the ATM room or outside. They will either peer over your shoulder to read your PIN or offer help if your card is stuck.
5. ***False front:*** It may be a little difficult to detect as the fake front completely covers the original machine because it is installed on top of it. This allows fraudsters to take your PIN as well as money.
6. ***Fake keypad:*** This is placed on top of the actual keypad. If the keypad feels spongy to touch or loose, don't enter your PIN.

***Frauds in Online transactions***

The ease of e-shopping or online bill payment is matched by the felicity with which identity theft can be carried out on computer or smartphone. This can then be used for unauthorised transactions ***Pharming***: In this technique, fraudsters reroute you to a fake website that seems similar to the original. So even as you conduct transactions and make payment via credit or debit card, the card details can be stolen.

***Keystroke logging***: Here, you unintentionally download a software, which allows the fraudster to trace your key strokes and steal passwords or credit card and net banking details.

***Public Wi-Fi***: If you are used to carrying out transactions on your smartphone, public Wi-Fi makes for a good hacking opportunity for thieves to steal your card details.

***Malware:*** This is a malicious software that can damage computer systems at ATMs or bank servers and allows fraudsters to access confidential card data.

***Merchant or point-of-sale theft:*** This is perhaps the simplest and most effective form of stealth, wherein your card is taken by the salesperson for swiping and the information from the magnetic strip is copied to be used later for illegal transactions.

P***hishing & vishing***: While phishing involves identity theft through spam mails which seem to be from a genuine source, vishing is essentially the same through a mobile phone using messages or SMS. These trick you into revealing your password, PIN or account number.

***SIM swipe fraud***: Here the fraudster contacts your mobile operator with fake identity proof and gets a duplicate SIM card. The operator deactivates your original SIM and the thief generates one-time password (OTP) on the phone to conduct online transactions.

***Unsafe apps:*** Mobile apps other than those from established stores can gain access to information on your phone like passwords, etc., and use it for unauthorised transactions.

***Lost or stolen cards, interception***: This is the oldest form of theft, wherein transactions are carried out using stolen cards, those intercepted from mail before they reach the owner from the card issuer, or by fishing out information like PINs and passwords from trash bins.

***Cards using other documents:*** This is also an easy form of identity theft, where new cards are made by the fraudster using personal information that is stolen from application forms or other lost or discarded documents.

***How to prevent card related frauds?***

Some basic, preventive steps can ensure that you do not fall prey to credit or debit card fraud. Here's how:

**ATM safeguards**

***Check machine:*** Do not use ATMs with unusual signage, such as a command to enter your PIN twice to complete the transaction. Also watch out for machines that appear to have been altered, if the front looks crooked, loose or damaged. It could be a sign that someone has attached a skimming device.

***Cover keypad:*** Make sure to cover the keypad with your hand while entering the PIN to escape any cameras attached nearby.

***Don't take help:*** It is advisable to use only your own bank ATMs, particularly those attached to a bank branch and those that have security guards. Also, avoid taking the help of any person loitering outside the ATM or volunteering to assist you if you get stuck.

**Online precautions**

***Use safe sites***: Go only to well-known, established sites for e-shopping. Remember to confirm the site's legitimacy before using it and shop only on those that are Secure Sockets Layer (SSL)-certified. These can be identified through the lock symbol next to the browser's URL box. Also make sure that the website uses the 'https' protocol instead of 'http', where 's' stands for 'secure'. Additionally, make sure not to click on the option that asks for saving your card details on any site.

***Anti-virus software***: While banks deploy ATM network security measures, on an individual level you can safeguard transactions by installing anti-virus software on your computer and smartphone to keep out malware. You can also install identity theft detection apps on your phone from an official app store. Besides, have software on your smartphone that enables you to wipe out the data remotely in case the mobile gets stolen.

***Debit card***: Make sure that you do not use your debit card for e-commerce transactions. This is because if your card is compromised, the entire cash in your bank account can be wiped out instantly. The credit card, on the other hand, offers a month's grace period before the cash leaves your account, during which the investigation can possibly nail the fraud.

***Hide CVV:*** When you enter the CVV on the site, it should be masked by asterisks. This is especially important while shopping on foreign websites where the CVV is the only point of verification. Also use a virtual keyboard to avoid keystroke logging.

***Public Wi-Fi:*** "Customers must avoid using unsecured W-Fi networks or public Wi-Fi as these are easy targets for identity theft cases in online transactions.

***Register for alerts***: This is a very important step since the bank will alert you to any online card transaction or ATM withdrawals the moment these take place. Also remember to update your mobile contact number in case of a change.

***Log out:*** Always log out from social media sites and other online accounts to ensure data security and avoid storing confidential passwords on your mobile phones as these can be used by fraudsters.

***Change passwords:*** Keep changing your passwords from time to time to reduce the probability of identity theft.

***Virtual cards:*** You can use this prepaid card if you are not a frequent shopper. It is a limited debit card that does not provide the primary card information to the merchant and expires after a day or 48 hours.

**Offline preventive measures**

Here are some additional precautions you can take to ensure your card is safe.

***Don't disclose details***: Never reveal your PIN, CVV or password to anyone. Make sure not to respond to e-mails or SMSes that ask for crucial personal or card-related details. No bank or credit card firm is authorised to seek card details from customers on mail or through phone.

***Check statements:*** Regularly go through your bank or credit card statements so that you can detect any unauthorised transaction through identity theft and alert the bank immediately.

***Merchants & POS***: At shops or petrol pumps, make sure that the card is not taken by the salesperson to a remote location where you cannot see it as the card information can be easily copied and stolen. Also, try shopping with retailers that use chip-enabled card readers. Though not every merchant has such readers, this provision can help bring down the risk of fraudulent card activity significantly.

***RBI mandate on security of card transactions***

The Reserve Bank of India has asked banks to upgrade all ATMs by September 2017 with additional safety measures to process EMV chip and PIN cards in order to prevent skimming and cloning of debit and credit cards.

While the POS terminal infrastructure in the country has been enabled to accept and process EMV chip and PIN cards, the ATM infrastructure continues to process the card transactions based on data from the magnetic stripe. As a result, the ATM card transactions remain vulnerable to skimming, cloning, etc. frauds, even though the cards are EMV chip and PIN based. It has become necessary to mandate EMV (Europay, Mastercard, Visa) chip and PIN card acceptance and processing at ATMs also, RBI said. Contact chip processing of EMV chip and PIN cards at ATMs would not only enhance the safety and security of transactions at ATMs but also facilitate preparedness of the banks for the proposed "EMV Liability Shift" for ATM transactions, as and when it comes into effect.

***Computer Aided Audit Tools and Techniques (CAATTs)*** can refer to any computer program utilized to improve the audit process. Generally, however, it is used to refer to any data extraction and analysis software. This would include programs such as data analysis and extraction tools, spreadsheets (e.g. Excel), databases (e.g. Access), statistical analysis (e.g. SAS), general audit software (e.g. ACL, Arbutus, EAS, business intelligence (e.g. Crystal Reports and Business Objects), etc.

An IT auditor uses some general tools, technical guides and other resources recommended by ISACA or any other accredited body. This is why many audit organizations will encourage their

employees to obtain relevant certifications such as CISA (Certified Information Systems Auditor) which is awarded by ISACA.

**Emerging Trends in IS Audit**

There are also new audits being imposed by various standard boards which are required to be performed, depending upon the audited organization, which will affect IT and ensure that IT departments are performing certain functions and controls appropriately to be considered compliant. Examples of such audits are SSAE 16, ISAE 3402, PCI DSS and ISO27001:2013.

ISAE 3402 and SSAE 16 audits deal with internal control over financial reporting and compliance controls of an organization respectively.

A Report on Compliance (ROC) is a form that has to be filled by all Visa and MasterCard merchants undergoing a PCI DSS (Payment Card Industry Data Security Standard) audit. The ROC form is used to verify that the merchant being audited is compliant with the PCI DSS standard. Currently both Visa and MasterCard require merchants and service providers to be validated according to the PCI DSS.

ISO/IEC 27001:2013 is an information security standard that was published in September 2013. It supersedes ISO/IEC 27001:2005, and is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee. It is a specification for an information security management system (ISMS). Organizations which meet the standard may be certified compliant by an independent and accredited certification body on successful completion of a formal compliance audit.

**Amendment to IT Act in 2008**

A major amendment to IT Act 2000 was made in 2008. It introduced the Section 66A which penalised sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced penalties for child porn, cyber terrorism and voyeurism. However, on 24 March 2015, the Supreme Court of India, gave the verdict that Section 66A is unconstitutional in entirety. The court said that Section 66A of IT Act 2000 is "arbitrarily, excessively and disproportionately invades the right of free speech" provided under Article 19(1) of the Constitution of India.

**Change Management**

A well-defined change management procedure is a critical security measure to protect the production IT environment from any unwanted/unintended disruptions on account application of system and application patches and hardware changes. The vendor should be bound through SLA to strictly follow the laid down change management processes.

Changes in the system may be divided into two types, (a) scheduled changes and (b) emergency changes. As a rule a change cannot happen without undergoing the change management process, however, in case of emergency changes, though the change is implemented in urgency, the entire change management process should invariably be followed post implementation of change.

The change management process should be documented, and include approving and testing changes to ensure that they do not compromise security controls, performing changes and signing them off to ensure they are made correctly and securely, reviewing completed changes to ensure that no unauthorized changes have been made.

Some of the sound Change Management processes include;

1. Following a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.
2. Putting in place systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/Databases/Applications/ Middleware, etc.
3. Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes, configuration baseline that ensure integrity of any changes thereto.
4. Having clearly defined roll-back methodology in place if any applied change fails in production environment.
5. As a threat mitigation strategy, identifying the root cause of any incident and apply necessary patches to plug the vulnerabilities.

### 18.7.2 System Resiliency, SPOF & Clustering

In the previous modules, we have discussed the concepts of Single Point of Failure (SPOF) and its mitigations to a certain extent. Clustering is one of the popular solutions to ensure system resiliency and to reduce the existence of SPOF.

**System Resiliency**: System resiliency is a planned part of a facility's architecture and is usually associated with other disaster planning and data center disaster-recovery considerations such as data protection. The adjective resilient means "having the ability to spring back."

Resiliency may also at times be called as ***fault tolerance***. Fault-tolerant technology is the capability of a computer system, electronic system or network to deliver uninterrupted service, despite one or more of its components failing. Fault tolerance also resolves potential service interruptions related to software or logic errors. The purpose is to prevent catastrophic failure that could result from a single point of failure.

Data center resiliency is often achieved through the use of redundant components, subsystems, systems or facilities. When one element fails or experiences a disruption, the redundant element takes over seamlessly and continues to support computing services to the user base. Ideally, users of a resilient system never know that a disruption has even occurred.

**SPOF and clustering*:*** In a data center or other information technology (IT) environment, a single point of failure (SPOF) can compromise the availability of workloads – or the entire data center – depending on the location and interdependencies involved in the failure.

Consider a data center where a single server runs a single application. The underlying server hardware would present a single point of failure for the application's availability. If the server

failed, the application would become unstable or crash entirely; preventing users from accessing the application, and possibly even resulting in some measure of data loss. In this situation, the use of server clustering technology would allow a duplicate copy of the application to run on a second physical server. If the first server failed, the second would take over to preserve access to the application and avoid the SPOF.

Consider another example where an array of servers is networked through a single network switch. The switch would present a single point of failure. If the switch failed (or simply disconnected from its power source), all of the servers connected to that switch would become inaccessible from the remainder of the network. For a large switch, this could render dozens of servers and their workloads inaccessible. Redundant switches and network connections can provide alternative network paths for interconnected servers if the original switch should fail, avoiding the SPOF.

It is the responsibility of the data center architect to identify and correct single points of failure that appear in the infrastructure's design. However, it's important to remember that the resiliency needed to overcome single points of failure carries a cost (e.g. the price of additional servers within a cluster or additional switches, network interfaces and cabling). Architects must weigh the need for each workload against the additional costs incurred to avoid each SPOF. In some cases, designers may determine that the cost to correct a SPOF is costlier than the benefits of the workloads at risk.

Much as a chain is only as strong as its weakest link, the effectiveness of a high availability cluster is limited by any single point of failures (SPOF) which exist within its deployment. To ensure the absolute highest levels of availability, SPOFs must be removed. There is a straightforward method for ridding the cluster of these weak links.

First, we must identify any SPOFs which exist with particular attention paid to servers, network connections and storage devices. Modern servers come with redundant and error correcting memory, data striping across hard disks and multiple CPUs which eliminates most hardware components as a SPOF.

But even configured with multi-pathing, shared storage/SANs still represent single points of failure as does the physical data center where it is located. To provide further protection, off-site replication of critical data combined with cross-site clustering must be deployed. Combined with network redundancy between sites, this optimal solution removes all SPOFs. Real-time replication ensures that an up-to-date copy of business critical data is always available; doing this off-site to a backup data center or into a cloud service also protects against primary data center outages that can result from fire, power outages, etc.

The use of application-level monitoring and auto-recovery, multi-pathing for shared storage, and data replication for off-site protection each eliminate potential Single Points of Failure within our cluster architecture. Paying attention to these components during cluster architecture and deployment will ensure the greatest possible levels of uptime.