BANGLADESH METEOROLOGICAL DEPARTMENT

LOCAL TRAINING

MODULE 6: ADVANCED - ICT

Project:

Strengthening Meteorological Information Services and Early Warning Systems (Component-A)

PREPARED BY:
GRANT THORNTON CONSULTING BANGLADESH LTD.

THE WORLD BANK

Grant Thornton
An instinct for growth™

PURPOSE:

The purpose of this module is to acquaint the participants with the Advance concepts of information and communication technology. The demands of the digital age have created a need for ground-breaking, innovative solutions within the fields of environment, healthcare, economics and welfare. The Information and Communication Technology Area of Advance (ICT) is engaged in research that enables increased functionality of different systems, including intelligence and autonomy, fast and reliable communication, advanced data analysis and solutions to key questions regarding safety, security, integrity and sustainability.

Delivery and Description:

Methodology:

This module is designed in such a way that the participants get explicit idea regarding the Advance ICT terms and concepts. Besides, we also wish that the participants will be able to incorporate the facilities of ICT in their everyday life to enhance their official works. To achieve this objective, we have made the sessions based on the most important topics of Advance ICT. We have included sufficient practical exercises to ensure that the participants not only learn how to use ICT, but they can also implement them.

Key learning outcomes:

After attending the training, the participants will have explicit idea on the concepts of the Network Management & security, Data Centre management and Security (CDCP), Data archiving & retrieval Management. Cyber security, and Database Management & Security.

Disclaimer

This Module on Advanced ICT is intended solely for Bangladesh Meteorological Department (BMD) and respective stakeholders and should not be used for any other purpose or distributed to third parties or quoted or referred to in any other document without our express written consent, as the matters contained herein may be misunderstood if not placed in the proper context of our engagement.

Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more-member firms, as the context requires.

Grant Thornton Consulting is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms.

GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate one another and are not liable for one another's acts or omissions.
www.gti.org

TABLE OF CONTENTS

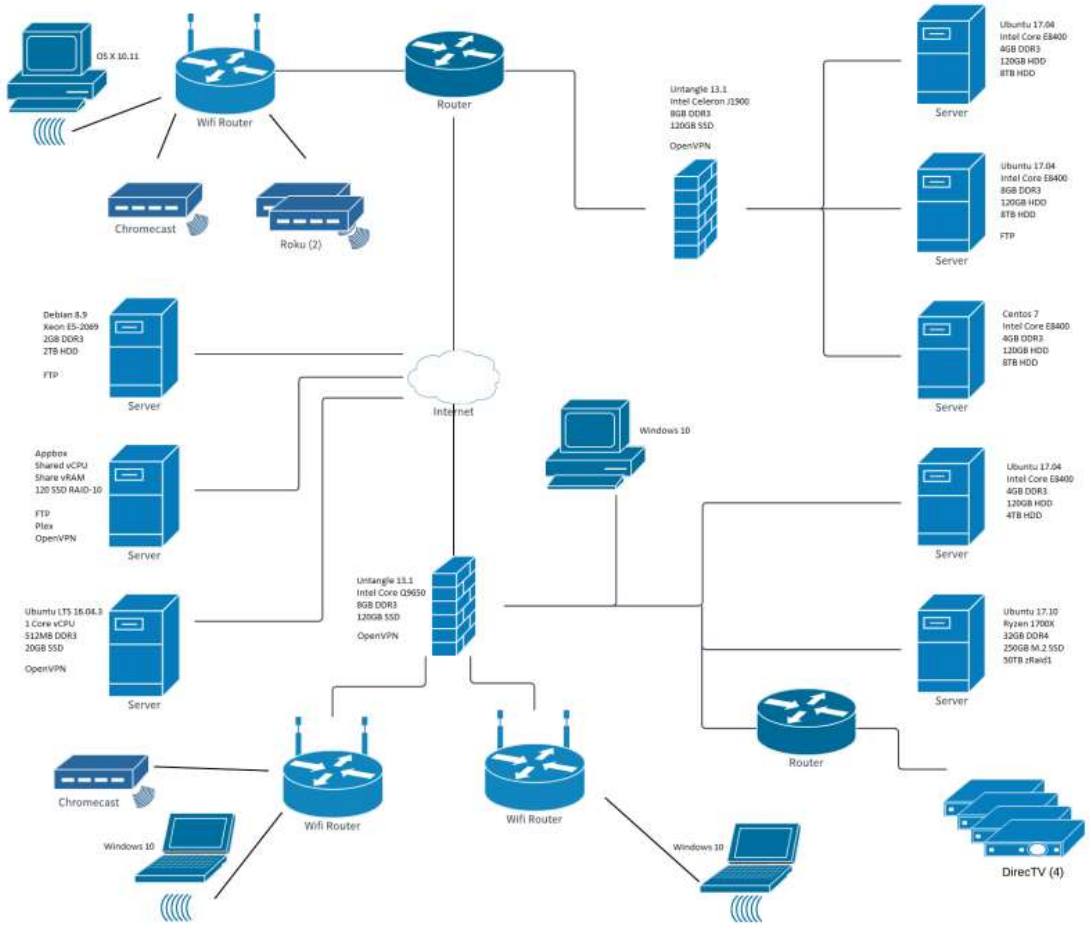
1. NETWORK MANAGEMENT AND SECURITY

1.1 Introduction of Network Management

1.1.1 Computer Networking

A computer network is a set of one or more computers connected to share data and resources, like access to the Internet, file servers, printers, and many other types of information. This connection gives authorized users the ability to access information stored on other computers on the network.

In general, a computer network refers to two or more connected computers that can share resources such as data, a printer, an Internet connection, applications, or a combination of these resources. It is the interconnection of multiple devices, generally termed as Hosts connected using multiple paths for sending/receiving data or media. There are also multiple devices or mediums which helps in the communication between two different devices which are known as Network devices. Ex: Computers, Router, Switch, Hub, Bridge. Computer networking enables devices and endpoints to be connected to each other on a local area network (LAN) or to a larger network, such as the internet or a private wide area network (WAN).



1.1.2 Types of Computer Networks

Computer networks keep changing the way we live and do things in the 21st century. This is because virtually every computing activity or information sharing, we do today depend on one form of network or another. The Internet is a very good example of a computer network that allows users to get information from any part of the world, using an internet-enabled device. There are many types of computer networks, the common types of area networks including:

i. Personal Area Network (PAN)
ii. Local Area Network (LAN)
iii. Wireless Local Area Network (WLAN)
iv. Campus Area Network (CAN)
v. Metropolitan Area Network (MAN)
vi. Wide Area Network (WAN)
vii. Storage-Area Network (SAN)
viii. System-Area Network (also known as SAN)
ix. Passive Optical Local Area Network (POLAN)
x. Enterprise Private Network (EPN)
xi. Virtual Private Network (VPN)

i. Personal Area Network (PAN)

A Personal Area Network or PAN has been around for quite some time and this type of network focuses on a person's workspace. A Personal Area Network handles data transmission within devices such as tablets, personal digital assistants, smartphones, and computers. Note that single users in most cases basically use this type of network. People make use of these types of networks commonly in situations where they need to connect wearable or mobile devices.

ii. Local Area Network (LAN)

This network covers small fixed areas such as a room, a building, an office or in a school. Can go up to 1 KM radius. A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment.

iii. Wireless Local Area Network (WLAN)

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using wireless communication within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet. Most modern

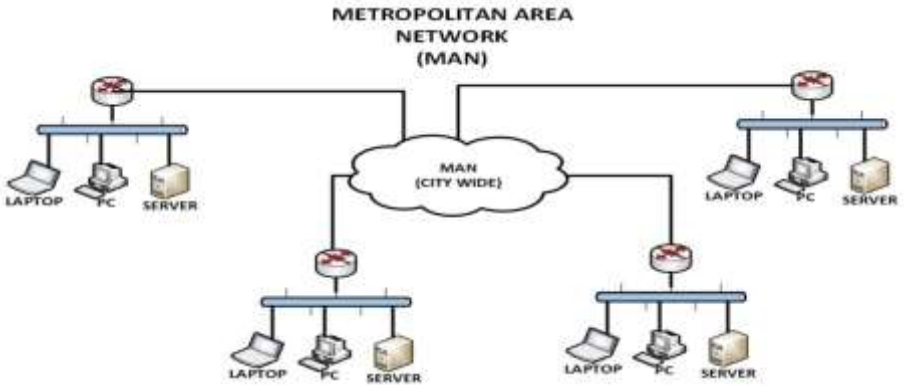
WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

iv. Campus Area Network (CAN)

Campus Area Networks are basically made up of several Local Area Networks, which are often within a campus area. Campus Area Networks are used in places such as hospitals, schools, universities or any organization that has multiple LANs and buildings that need to connect to each other to share resources. Somewhere CAN (Campus Area Network) is also known as a corporate area network (CAN).

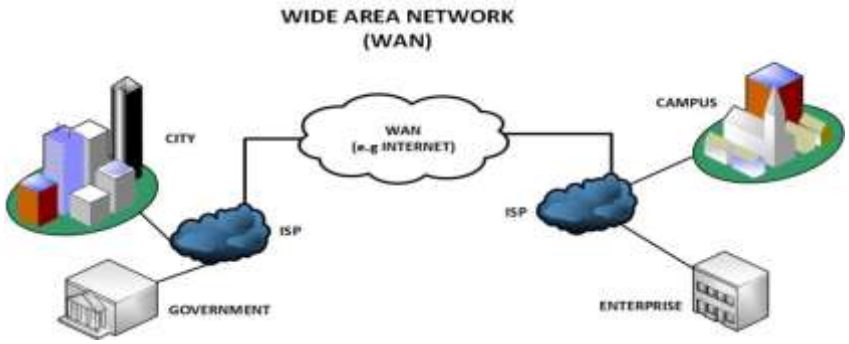
v. Metropolitan Area Network (MAN)

It is far larger than a LAN and smaller than a WAN. It covers a larger geographical area such as a university, an entire city, a valley, a district, a zone or a whole country. This type of network is prepared by connecting several LANs in different locations. To form a MAN, several LANs are connected through a telephone line, optical fiber cable or wireless communication media. The MAN network usually exists to provide connectivity to local ISPs, cable tv, or large corporations.



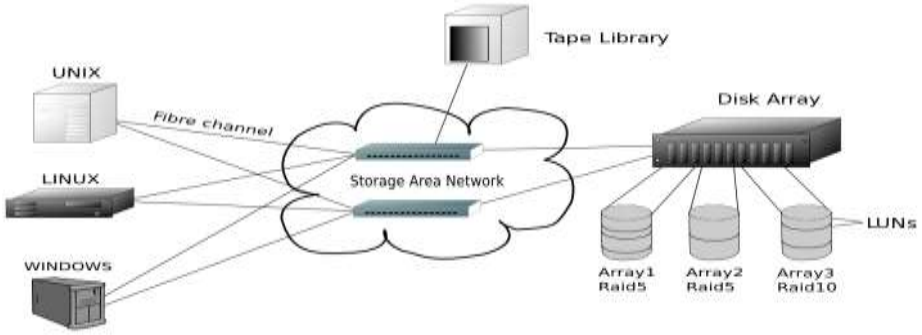
vi. Wide Area Network (WAN)

A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LANs) and metro area networks (MANs). This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.



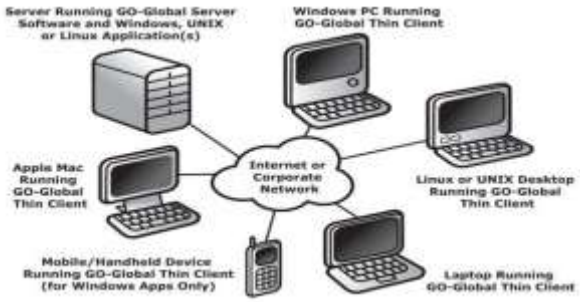
vii. Storage-Area Network (SAN)

SAN (Storage Area Network) is a type of high-speed dedicated network or subnetwork which interconnects and presenting sharing pools of storage devices to multiple servers. It moves storage resources to the user network and reorganizes them into independent, high-performance network.



viii. System-Area Network (also known as SAN)

System Area Network is basically designed for high-speed interconnection in cluster environments (server to server, multiprocessing system (processor to processor) and storage area networks (SANs). A SAN uses internet protocol (IP) address connection that assigned by TCP/IP. A System Area Network is a network that is designed to work in parallel computing environments; it connects computers that are in a High-Performance Computing setting. These are often used where high processing is needed. Computer clusters make use of System Area Networks to achieve connectivity. The major difference here is the distance in between the computers on the network, which is often a short distance



Network Topology

Network topology is the way a network is arranged, including the physical or logical description of how the links and nodes are set up to relate to each other. There are numerous ways a network can be arranged, all with different pros and cons, and some are more useful in certain circumstances than others.

The way a network is arranged can make or break network functionality, connectivity, and protection from downtime. The question of, "What is network topology?" can be answered with an explanation of the two categories that exist in the network topology.

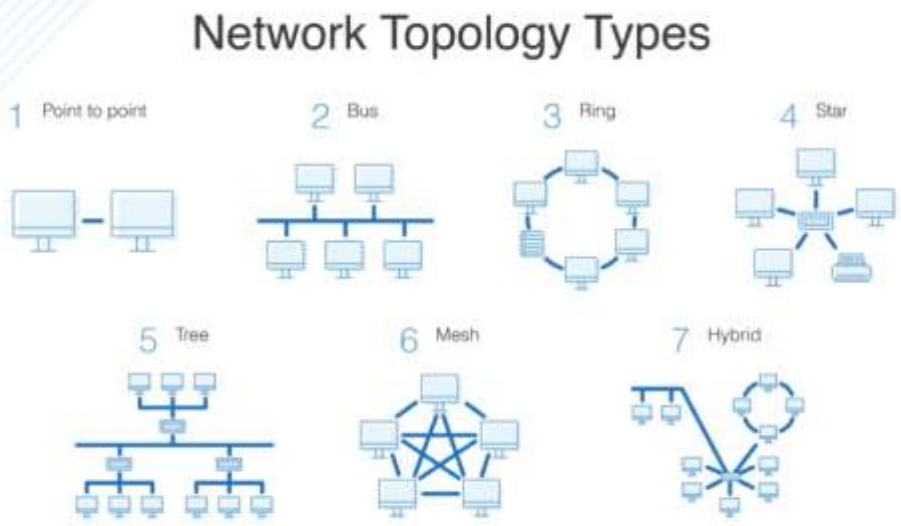
1. Physical – The physical network topology refers to the actual connections (wires, cables, etc.) of how the network is arranged. Clearly, setup, maintenance, and provisioning tasks require insight into the physical network.

2. Logical – The logical network topology is a higher-level *idea* of how the network is set up, including which nodes connect to each other and in which ways, as well as how data is transmitted through the network. Logical network topology includes any virtual and cloud resources.

Effective network management and monitoring require a strong grasp of both the physical and logical topology of a network to ensure our network is efficient and healthy.

Most Common Type of Network Topology

Building a local area network (LAN) topology can be make-or-break for a business, as we want to set up a resilient, secure, and easy-to-maintain topology. There are several different types of network topology and all are suitable for different purposes, depending on the overall network size and our objectives.



1.1.3 Network Protocols and Communication

A network protocol is a set of rules followed by the network. Network protocols are formal standards and policies made up of rules, procedures and formats that defines communication between two or more devices over a network. Network protocols conducts the action, policies, and affairs of the end-to-end process of timely, secured and managed data or network communication. They define rules and conventions for communication.

The OSI Model

The Open Systems Interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. In plain English, the OSI provides a standard for different computer systems to be able to communicate with each other. The OSI model can be seen as a universal language for computer networking. It's

based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last. Each layer of the OSI model handles a specific job and communicates with the layers above and below itself. DDoS attacks target specific layers of a network connection; application layer attacks target layer 7 and protocol layer attacks target layers 3 and 4.

The seven layers of the OSI model

The seven abstraction layers of the OSI model can be defined as follows, from top to bottom:

7. The Application Layer
6. The Presentation Layer
5. The Session Layer
4. The Transport Layer
3. The Network Layer
2. The Data Link Layer
1. The Physical Layer

TCP/IP Model

The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows:

TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.

Some Important Protocols with ports

TCP which stands for "Transmission Control Protocol", is a suite of communication protocols used to interconnect network devices on a local network or a public network like the internet. TCP is known as "connection-oriented" protocols as it ensures each data packet is delivered as requested. Therefore, TCP is used for transferring most types of data such as webpages and files over the Internet.

UDP which stands for "User Datagram Protocol" is part of the TCP/IP suite of protocols used for data transferring. UDP is a known as a "connectionless-oriented" protocol, meaning it doesn't acknowledge that the packets being sent have been received. For this reason, the UDP protocol is typically used for streaming media. While you might see skips in video or hear some fuzz in audio clips, UDP transmission prevents the playback from stopping completely.

Furthermore, TCP also includes built-in error checking means TCP has more overhead and is therefore slower than UDP, it ensures accurate delivery of data between systems. Therefore, TCP is used for transferring most types of data such as webpages and files over the local network or Internet. UDP is ideal for media streaming which does not require all packets to be delivered.

Port Numbers: They are the unique identifiers given to all protocol numbers so they can be accessed easily.

1.1.4 *Introduction to various Networking devices*

HUB

Hub is one of the basic icons of networking devices which works at physical layer and hence connect networking devices physically together. Hubs are fundamentally used in networks that use twisted pair cabling to connect devices. They are designed to transmit the packets to the other appended devices without altering any of the transmitted packets received. They act as pathways to direct electrical signals to travel along. They transmit the information regardless of the fact if data packet is destined for the device connected or not.

Hub falls in two categories:

Active Hub: They are smarter than the passive hubs. They not only provide the path for the data signals in fact they regenerate, concentrate and strengthen the signals before sending them to their destinations. Active hubs are also termed as 'repeaters.

Passive Hub: They are more like point contact for the wires to build in the physical network. They have nothing to do with modifying the signals.

Switches

Switches are the linkage points of an Ethernet network. Just as in hub, devices in switches are connected to them through twisted pair cabling. But the difference shows up in the manner both the devices; hub and a switch treat the data they receive. Hub works by sending the data to all the ports on the device whereas a switch transfers it only to that port which is connected to the destination device. Switches operate in full-duplex mode where devices can send and receive data from the switch at the simultaneously unlike in half-duplex mode. The transmission speed in switches is double than in Ethernet hub transferring a 20Mbps connection into 30Mbps and a 200Mbps connection to become 300Mbps.

Bridges

A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them. It connects two local-area networks; two physical LANs into larger logical LAN or two *segments* of the same LAN that use the same protocol.

Routers

Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. They process *logical* addressing information in the Network header of a packet such as IP Addresses. Router is used to create larger complex networks by complex traffic routing. It has the ability to connect dissimilar LANs on the same protocol. It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware device or a system of the computer which has more than one network interface and routing software.

Functionality:

When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its routing table to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router.

Routing tables play a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be *updated* and *complete*. The two ways through which a router can receive information are:

- Static Routing: In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well. The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place. Thus, static routing is feasible for tinniest environments with minimum of one or two routers.
- Dynamic Routing: For larger environment dynamic routing proves to be the practical solution. The process involves use of peculiar routing protocols to hold communication. The purpose of these protocols is to enable the other routers to transfer information about to other routers, so that the other routers can build their own routing tables.

Gateways

Gateway is a device which is used to connect multiple networks and passes packets from one packet to the other network. Acting as the 'gateway' between different networking systems or computer programs, a gateway is a device which forms a link between them. It allows the computer programs, either on the same computer or on different computers to share information across the network through protocols. A router is also a gateway, since it interprets data from one network protocol to another.

Network card

Network cards also known as Network Interface Cards (NICs) are hardware devices that connect a computer with the network. They are installed on the mother board. They are responsible for developing a physical connection between the network and the computer. Computer data is translated into electrical signals send to the network via Network Interface Cards.

Media Specific: - LAN card is used according to the media type. Different types of the NICs are used to connect the different types of media. To connect a specific media type, we must have to use a NIC which is particularly made for that type of media.

Network Design Specific: - A specific network design needs a specific LAN card. For example, FDDI, Token Ring and Ethernet have their own distinctive type of NIC cards. They cannot use other types of NIC cards.

ISDN (Integrated Services Digital Network)

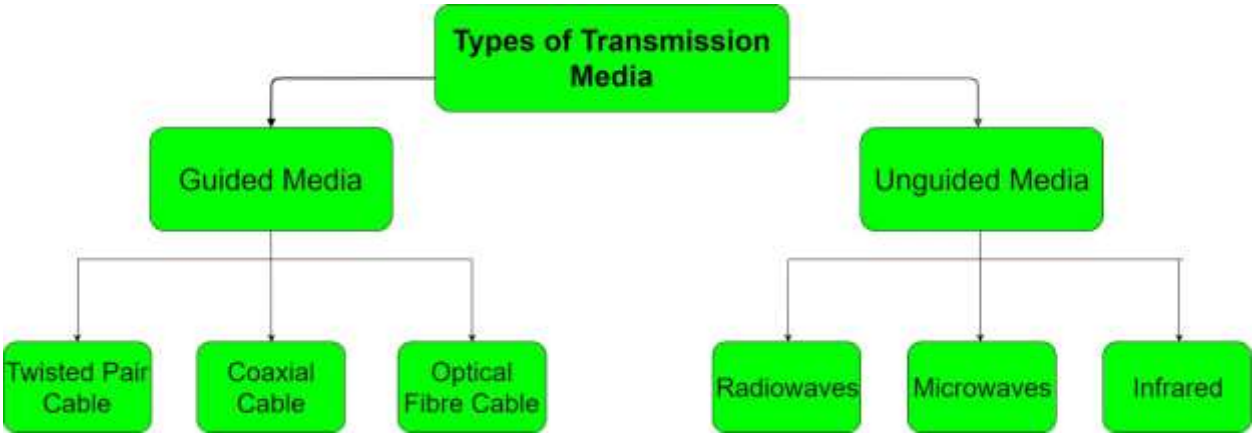
ISDN are used to send over graphic or audio data files. It is a WAN technology that can be used in place of a dial up link. The accessibility of ISDN depends upon the provision of the service by the service provider, the quality of the line set up to your area. It surely provides higher speed than a modem and has the capability to pick up the line and drop it considerably at a faster rate.

ISDN can create numerous communication routes on a single line. Nowadays, even faster and cheaper technologies that ISDN have found their way in the realm of technology.

Network media

Network media is the actual path over which an electrical signal travels as it moves from one component to another. Network media refers to the communication channels used to interconnect nodes on a computer network. Typical examples of network media include copper coaxial cable, copper twisted pair cables and optical fiber cables used in wired networks, and radio waves used in wireless data communications networks.

In data communication and networking terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



Types of Wireless Communication Technologies

Satellite

Satellite communication is one of the wireless technologies, which is widely spread all over the world allowing users to stay connected virtually anywhere on the Earth. The Satellites used in this mode of communication, communicate directly with the orbiting satellites via radio signals. Portable satellite phones and modems have more powerful broadcasting abilities than the cellular devices as they have high range, apart from being more expensive in terms of cost, than their counterparts.

Wireless Networking

Wireless Networking technologies connect multiple computers, systems and devices together without requiring wires or cables: a wireless local area network or WLAN comes under Wi-Fi.

WiMAX

There are wireless broadband systems that offer fast Web surfing without being getting connected through cable or DSL (Example of wireless broadband is WiMAX). Although WiMAX can potentially deliver data rates of more than 30 Megabits per second, yet the providers offer average 0 data rates of 6 Mbps and often deliver less, making the service significantly slower than the hard-wired broadband. The actual cost of the data available using WiMAX widely varies with the distance from the transmitter. WiMAX is also one of the versions of 4G wireless available in phones as Sprint's 4G technology.

Wireless Networking

Wi-Fi

Wi-Fi is a form of low-power wireless communication used by many electronic devices such as laptops, systems, smart phones, etc. In a Wi-Fi setup, a wireless router serves as the communication hub. These networks are extremely limited in range due to low power of transmissions allowing users to connect only within close proximity to a router or signal repeater. Wi-Fi is common in-home networking applications which provides portability without any need of cables. Wi-Fi networks need to be secured with passwords for security purposes in order not to be accessed by others.

Bluetooth Technology

Bluetooth technology allows you to connect a variety of different electronic devices wirelessly to a system for the transfer and sharing of data and this is the main function of Bluetooth. Cell phones are connected to hands-free earpieces, wireless keyboard, mouse and mike to laptops with the help of Bluetooth as it transmits information from one device to other device. Bluetooth technology has many functions, and it is used most commonly in wireless communications' market.

1.2 CISCO Packet Tracer

Network simulators are one of the key ingredients of training for the CCNA. There are few network simulators as widely used as Cisco Packet Tracer. Packet Tracer has been a staple tool of CCNA students ever since it was released. With Packet Tracer, you can imitative a live networking environment. Cisco Packet Tracer is one of the best simulators for the beginners to learn cisco device configuration. All basic configurations features are available in cisco packet tracer.

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

Packet Tracer does not require physical equipment. It creates a virtual network with an almost unlimited number of devices, encouraging practice, design scenarios testing and troubleshooting.

Creating/Making a simple topology using CPT:

Now let's Make a topology using Cisco Packet tracer: So we are going to make a topology like the below one.

In this lab, we use switches, DHCP server, DNS server, HTTP server, and PC.

1. Switch: - Switch is a networking device that is used for connecting many systems or PCs with each other on the same network. In other words, we can say that a Network Switch is a Computer Networking device which is used for connects devices together with each other on the same network. Switch Provides a platform to us through which we can easily send and receive data between two systems.

2. DHCP Server: - The DHCP (Dynamic Host Configuration Protocol) is a network protocol used to assign IP automatically to the systems with the help of a machine called DHCP server. A DHCP Server allows computers to request an IP address and networking parameters automatically. If you do not have a DHCP Server to configure IP addresses automatically to the PCs, then you need to assign a static or manual IP address on the Computers. So, in simple words, we can say that DHCP Server is only used for assigning the IP addresses to the Systems automatically.

3.DNS Server: - DNS (Domain Name Server) is a Server which is used to assign names to the domain IP'S. It is really hard to remember the IP of any site, so DNS server converts that number into a name, and we have to type just only the name of the site to search it on the

internet. So, in simple words, we can say that DNS Server allows us to do a search on the Internet using a specific name instead of its IP address. So, we can easily remember it for future use and reach it without having difficulties.

4.HTTP Server: - A HTTP (Hypertext Transfer Text Protocol) Server AKA web server is the Server that shows web pages on the request of clients. Its main function is to store web pages. In simple words, we can say that HTTP Server is a platform which provides a medium to make communication in between Server and Clients. Generally, HTTP Server delivered HTML Documents, Stylesheets, Scripts and images, etc.

Configuring DHCP, DNS & HTTP Server

Now to understand this lab we take a lab in Cisco Packet Tracer. In which we take Switches, DNS Server, PCs, DHCP Server, HTTP Server, and Connecting Wires. So, let's start here how to configure Servers along with Switches.

Step 1: – Now, first, we configure DHCP Server so we can assign the automatic IP address on all other systems. To do so go to DHCP server and open it. Now in the desktop menu go to IP configuration and assign IP statically to the server and also gives the DNS Server address as 1.0.0.2.

Step 2: – Now to make this Server as DHCP Server we need to enable DHCP service on this Server. To do so go to its services menu and select DHCP in which fill the entries as your requirement and turn on the DHCP server by choosing the ON option from it. The figure is shown below

Now the work on the DHCP server is completed and DHCP Service is configured successfully. Now this Server is able to provide an IP address to the systems which are connected to this network.

Step 3: – Now in next step we configure DNS Server so we can provide a medium in between HTTP Server and clients. To do so, first of all, select the DNS server after that in the desktop menu click on the IP configuration option and then change the IP Configuration method from Static to DHCP. Now you can observe that it will request for an IP address from DHCP Server and an IP address is given automatically to the DNS server. The figure is shown below

Step 4: – Now we configure DNS Services on this Server so we can provide a platform to make communication between Serves and clients. To do so go to services and select DNS then give the name and IP address of the HTTP Server as given below and click on add button to add these entries in DNS Server. After that turn ON DNS Services on this Server.

Step 5: – Now to configure HTTP server on the next machine similarly as DNS server and DHCP Server. First of all, assign an IP address to it by using DHCP server as given in step 4 and then go to HTTP in services menu and create a page or edit a page which will be shown on the browser.

Step 6: – Now all the servers are configured. So, now we assign the IP address to the PCs using DHCP Server as given above. Now in a browser type the name of our page google.com and as a result, our page will appear there on the screen. This is done because the clients request first of all goes to the DNS server where it directs it to the HTTP server and then webpage loads from HTTP server to our computer using the name instead of IP address.

1.3 Introduction of Network Security, Network Scanning and Information Gathering

1.3.1 Brief Overview of Network Security

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on a network. Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies.

What is network security attack?

A *network attack* can be defined as any method, process, or means used to maliciously attempt to compromise network security. Network security is the process of preventing network attacks across a given network infrastructure, but the techniques and methods used by the attacker further distinguish whether the attack is an active cyber-attack, a passive type attack, or some combination of the two.

Let's consider a simple network attack example to understand the difference between active and passive attack.

Active Attacks

An active attack is a network exploit in which attacker attempts to make changes to data on the target or data en route to the target.

Passive Attacks

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities but does not affect system resources.

Types of network security

There are many components to a network security system that work together to improve security posture. The most common network security components are discussed below:

Access Control

To keep out potential attackers, you should be able to block unauthorized users and devices from accessing your network. Users that are permitted network access should only be able to work with the set of resources for which they've been authorized.

Application Security

Application security includes the hardware, software, and processes that can be used to track and lock down application vulnerabilities that attackers can use to infiltrate your network.

Firewalls

A firewall is a device or service that acts as a gatekeeper, deciding what enters and exits the network. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both.

Virtual Private Networks (VPN)

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. This way it authenticates the communication between a device and a secure network, creating a secure, encrypted "tunnel" across the open internet.

Behavioral Analytics

We should know what normal network behavior looks like so that you can spot anomalies or network breaches as they happen. Behavioral analytics tools automatically identify activities that deviate from the norm.

Wireless Security

Wireless networks are not as secure as wired ones. Cybercriminals are increasingly targeting mobile devices and apps. So, you need to control which devices can access your network.

Intrusion Prevention System

These systems scan network traffic to identify and block attacks, often by correlating network activity signatures with databases of known attack techniques.

Data loss prevention

Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

Email security

Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email

security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

Network segmentation

Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

Web security

A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps we take to protect our own website.

Different types of Threats & Vulnerabilities in Networks

Network security is significantly more challenging than it was several years ago. Today's IT teams struggle against a cybersecurity talent shortage, an increasing number of endpoints in their network, and the ever-changing cybercrime threat vector. Most experts agree that 2019 will bring a higher sophistication of malicious hacking. More of these network security threats and attacks will be high profile and reinforce the importance of cybersecurity plan. Hackers will target well-known brands, looking for notoriety as well as money. As a result, the security response of the business community must rise to the occasion.

Any network with a connection to the Internet is potentially vulnerable. The number one thing we can do to protect our systems is to establish a backup strategy for our data, now.

Missing patches

All it takes for an attacker, or a rogue insider, is a missing patch on a server that permits an unauthenticated command prompt or other backdoor path into the web environment. Sure, we have to be careful when applying patches to servers but to not apply patches at all just makes it too easy.

Solution: Follow network security best practices by updating your operating system and any other software running on it with the latest security patches. Too many incidents occur because criminal hackers take advantage and exploit un-patched systems.

Weak or default passwords

Passwords shouldn't even be part of a network security vulnerability discussion knowing what we now know. However, many web applications, content management systems, and even database servers are still configured with weak or default

passwords. Who needs file inclusion or SQL injection when the file system or database can be accessed directly?

Solution: Change and test for weak passwords regularly and consider using a password management tool. Implement intruder lockout after a defined number of failed login attempts.

Misconfigured firewall rulebases

One of the biggest, most dangerous, assumptions is that everything is well in the firewall because it's been working fine. Digging into a firewall rule base that has never been analyzed will inevitably turn up serious configuration weaknesses that allow for unauthorized access into the web environment. Sometimes it's direct access while other times it's indirect from other network segments including Wi-Fi – parts of the network that may have been long forgotten.

Solution: Start with organization's security policy; one that reflects the current situation and foreseeable business requirements. After all, our firewall rulebase is the technical implementation of this security policy. Review it regularly and keep it relevant. OWASP provides some good guidance on building operational security guides.

Mobile devices

Phones, tablets, and unencrypted laptops pose some of the greatest risks to web security. Think about all the VPN connections, cached passwords in web browsers, and emails containing sensitive login information that us – and likely everyone else responsible for managing our web environment – have stored on mobile devices. The use of unsecured (and rogue) Wi-Fi via mobile devices is the proverbial icing on the cake.

Solution: Install clear data management rules for all employees and make mandatory data encryption part of our security policy. This is becoming even more important with employees connecting their personal devices to the corporate network.

USB Flash Drives

The dangers of these innocent-looking portable devices have been known for long enough. But still, all that Edward Snowden reportedly needed to walk away from the National Security Agency building with a cache of national secrets was a USB flash drive. USB drives are also one of the most common ways a network can get infected from inside a firewall.

Solution: Have clear security policies regarding personal storage devices including who can use them and in what places. Restrict the computers that can read USB flash drives and help prevent unauthorized access by encrypting the data as soon as it hits the device.

Wireless access points

Wireless APs provide immediate connectivity to any user within proximity of the network. Wireless attacks by wardrivers (people in vehicles searching for unsecured Wi-Fi networks) are common and have caused significant damage in the past. TJ Stores, owners of Marshalls and TJMaxx, was attacked using this method, and intruders penetrated the company's computer systems that process and store customer transactions including credit card, debit card, check and merchandise return transactions. It's been reported that this intrusion has cost TJ Stores more than $500 million dollars to date. Wireless APs are naturally insecure, regardless if encryption is used or not. Protocols such as wireless encryption protocol contain known vulnerabilities that are easily compromised with attack frameworks, such as Aircrack. More robust protocols such as wireless protected access (WPA) and WPA2 are still prone to dictionary attacks if strong keys are not used.

Solution: WPA2 Enterprise using RADIUS is recommended along with an AP that is capable of performing authentication and enforcing security measures. Strong, mixed passwords should be used and changed on a fairly frequent basis. Generally, wireless APs are connected for convenience, so it is usually not necessary to have them connected to a working environment.

E-mail:

E-mail is frequently used within businesses to send and receive data; however, it's often misused. Messages with confidential information can easily be forwarded to any external target. In addition, the e-mails themselves can carry nasty viruses. One targeted e-mail could phish for access credentials from an employee. These stolen credentials would then be leveraged in a second-stage attack.

Solution: With e-mail security, source identification is key. Identify the sender using technology such as PGP, or a simple array of questions before sending sensitive information. Access control to broad alias-based e-mail addresses should be enforced. And policy and reminders should be sent out to employees.

Foot-printing Techniques

Foot printing is the process of accumulating data regarding a specific network environment for revealing system vulnerabilities. It is the very first step in information gathering which provides a blueprint of the target system or a network. So basically, foot-printing is all about gathering as much information as possible about a website available over the internet.

If an organization wants to protect their systems from attacks, they must take measures to thwart potential attacks. They must conduct their own foot-printing to find ways to intrude into their environment. Going through the process of foot-printing can reveal system vulnerabilities and help put in measures and processes to minimize or eliminate their exploitation.

Foot-printing uses various security techniques such as DNS queries, network enumeration, network queries, operating system identification, organizational queries, ping sweeps, point of contact queries, port scanning, and registrar queries (WHOIS queries) to collect their information.

Gathered Information

User and Group ids', system banners, routing tables, SNMP information, system architecture, passwords, policies. email addresses, domain names, network blocks, IP addresses of reachable systems, private websites, TCP and UDP services running, VPN points, ACLs, IDSes running, analog or digital telephone numbers, authentication mechanisms, etc are gathered by footprinting.

✓ Finding companies external and internal URLs:

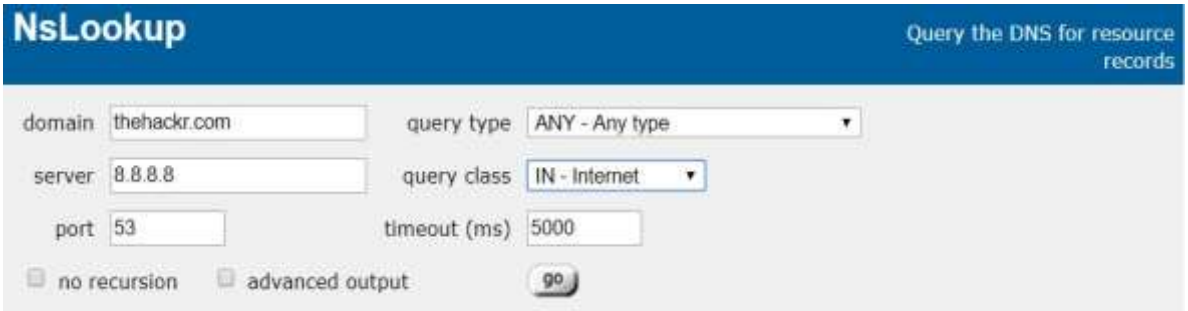
An attacker can find a company's URL using various types of tools, such as Google search engine, various types of news groups, blogs for sensitive data, etc. Internal URLs provide an insight into different departments and business units in an organization. You can also use trial and error methods.

✓ Performing WHOIS lookup:

The attacker can use whois queries to determine the IP address ranges associated with clients. A whois query can be run on most UNIX environments. In a Windows environment, the tools such as WsPingPro and Sam Spade can be used to perform whois queries. Whois queries can also be executed over the Web from www.arin.net and www.networksolutions.com.

✓ Extracting DNS information:

The Domain Name System (DNS) is a hierarchical distributed naming system connected to the Internet or a private network. It translates domain names meaningful to humans into the numerical identifiers associated.



✓ Mirroring the entire Website:

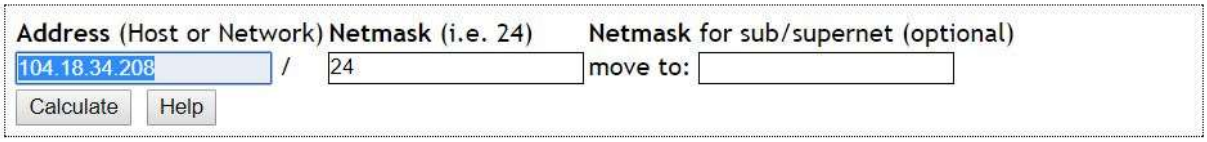
Website mirroring is a type of information gathering attack in which an attacker downloads a copy of an entire Website to the local hard disk for foot printing.

✓ Searching in Google for personal information of employees:

The attacker/penetration tester can use Google, Yahoo people search, Yahoo finance, Google finance, Anacubis.com, people-search-america.com, bestpeoplesearch.com, etc.

✓ Locating the network range:

In this type of footprinting attack, the attacker finds the range of IP addresses and discerns the subnet mask.




```
Address:   104.18.34.208          01101000.00010010.00100010 .11010000
Netmask:   255.255.255.0 = 24     11111111.11111111.11111111 .00000000
Wildcard:  0.0.0.255              00000000.00000000.00000000 .11111111
=>
Network:   104.18.34.0/24         01101000.00010010.00100010 .00000000 (Class A)
```

✓ Analysing companies' infrastructure details from job postings:

In this type of foot-printing attack, the hacker/penetration tester can gather company's infrastructure details from job postings. Job posting sites can be helpful in determining job requirements, employee profile, hardware information, software information, etc.

✓ Tracking email:

E-mail tracking is a method for monitoring the e-mail delivery to the intended recipient.

DNS Foot-printing

DNS is a naming system for computers that converts human-readable domain names into computer readable IP-addresses and vice versa. DNS uses UDP port 53 to serve its requests. A zone subsequently stores all information, or resource records,

associated with a particular domain into a zone file; Resource records responded by the name servers should have the following fields:

- Domain Name — Identifying the domain name or owner of the records
- Record Types — Specifying the type of data in the resource record
- Record Class — Identifying a class of network or protocol family in use
- Time to Live (TTL) — Specifying the amount of time a record can be stored in cache before discarded.
- Record Data — Providing the type and class dependent data to describe the resources.

A (address)—Maps a hostname to an IP address
SOA (Start of Authority)—Identifies the DNS server responsible for the domain information
CNAME (canonical name)—Provides additional names or aliases for the address record
MX (mail exchange)—Identifies the mail server for the domain
SRV (service)—Identifies services such as directory services
PTR (pointer)—Maps IP addresses to hostnames
NS (name server)—Identifies other name servers for the domain
HINFO = Host Information Records
DNS servers perform zone transfers to keep themselves up to date with the latest information. A zone transfer of a target domain gives a list of all public hosts, their respective IP addresses, and the record type.
Foot-printing through Social Engineering:
Social media like Twitter, Facebook are searched to collect information like personal details, user credentials, other sensitive information using various social engineering techniques. Some of the techniques include

- Eavesdropping: It is the process of intercepting unauthorized communication to gather information
- Shoulder surfing: Secretly observing the target to gather sensitive information like passwords, personal identification information, account information etc.
- Dumpster Diving: This is a process of collecting sensitive information by looking into the trash bin. Many of the documents are not shredded before disposing them into the trash bin. Retrieving these documents from trash bin may reveal sensitive information regarding contact information, financial information, tender information etc.

Foot printing countermeasures:

- Creating awareness among the employees and users about the dangers of social engineering
- Limiting the sensitive information
- encrypting sensitive information
- using privacy services on whois lookup database

- Disable directory listings in the web servers
- Enforcing security policies

Scanning Techniques

Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports and various services within a network. Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization (target organization: means the group of people or organization which falls in the prey of the Hacker). Vulnerability scanning is performed by pen-testers to detect the possibility of network security attacks. This technique led hackers to identify vulnerabilities such as missing patches, unnecessary services, weak authentication or weak encryption algorithm. So, a pen-tester and/or ethical hacker list down all such vulnerabilities found in an organization's network. Scanning is of three types:

- Network Scanning
- Port Scanning
- Vulnerability Scanning

Major Objectives of Scanning

1. To discover live hosts/computer, IP address and open ports of the victim
2. To discover services that are running on a host computer
3. To discover the Operating System and system architecture of the target
4. To discover and deal with vulnerabilities in Live hosts

Scanning Methodologies

1. Hackers and Pen-testers check for Live systems
2. Check for open ports (The technique is called Port Scanning, which will be discussed below)
3. Scanning beyond IDS (Intrusion Detection System)
4. Banner Grabbing: is the method for obtaining information regarding the targeted system on a network and services running on its open ports. Telnet and ID Serve are the tools used mainly to perform Banner-grabbing attack. This information may be used by intruders/hackers to portray the lists of applicable exploits.
5. Scan for vulnerability
6. Prepare Proxies

Port Scanning

It is a conventional technique used by penetration testers and hackers to search for open doors from where hackers can get access to any organization's system. During this scan hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system and topology of the targeted

organization. Once the hacker fetches the IP address of the victim organization by scanning TCP and UDP ports, the hacker maps the network of this organization under his/her grab. NMAP is a tool to perform port scanning.

Vulnerability Scanning

It is the proactive identification of vulnerabilities of the system within a network in an automated manner, to determine whether the system can be exploited or threatened. I this case, the computer should have to be connected to the internet.

Tools and Steps Used

If a hacker wants to perform ICMP (Internet Control Message Protocol) scanning, it can be done manually. The steps are:

- Open Windows OS
- Press Win+R (Run) buttons in combination
- In the Run, type- cmd
- Type the command: ping IP Address or type: ping DomainName

Tools that are used to scan networks and ports are:

- Nmap: to extract information such as live hosts on the network, services, type of packet filters/firewalls, operating systems and OS versions.
- Angry IP Scanner: scans for systems available in a given input range.
- Hping2/Hping3: are command-line packet crafting and network scanning tools used for TCP/IP protocols.
- Superscan: is another powerful tool developed by Mcafee, which is a TCP port scanner, also used for pinging.
- ZenMap: is another very powerful Graphical user interface (GUI) tool to detect the type of OS, OS version, ping sweep, port scanning, etc.
- Net Scan Tool Suite Pack: is a collection of different types of tools which can perform a port scan, flooding, webrippers, mass emailers, and This tool is trial version, but paid versions are also available.
- Wireshark and Omnipeak are two powerful and famous tools which listen to network traffic and acts as a network analyzer.
- Names of other famous tools for PCs are Advanced Port Scanner, Net Tools, MegaPing, CurrPorts, PRTG Network Monitor, SoftPerfect Network Scanner, Network Inventory Explorer, etc.
- There are various other scanners available free and inbuilt in Kali Linux OS.
- Tools and software that are used in mobiles as scanners include the names such as Umit Network Scanner, Fing, IP network Scanner, PortDroid network Analysis, Panm IP Scanner, Nessus Vulnerability Scanner, Shadow Sec Scanner, etc.

Countermeasures against Scanning

1. Configure firewalls and IDS to detect and block probes.
2. Use custom rules to lock down the network and block unwanted ports.
3. Run port Scanning tools to determine whether the firewall accurately detects the port scanning activities.
4. Security Experts should ensure the proper configuration of anti-scanners and anti-spoofing rules.
5. Security experts of an organization must also ensure that the IDS, routers, and firewall firmware are updated to their latest releases.

1.4 Networks Security Tools and Techniques

Firewall

As hacking and cyber-criminals become more sophisticated and defenses become stronger, you might assume that a firewall is obsolete. And while a firewall is arguably the most core of security tools, it remains one of the most important. Its job is to block any unauthorized access to your system. A firewall monitors network traffic as well as connection attempts, deciding on whether or not these should be able to pass freely onto your network or computer. Of course, while they are useful, they do have limitations. Skilled hackers have learned how to create data and programs that trick firewalls into believing that they are trusted – this means that the program can pass through the firewall without any problems. Despite these limitations, firewalls are still very effective in detecting the large majority of less sophisticated malicious attacks on your business.

Types of Firewalls

Proxy firewall

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

Stateful inspection firewall

Now thought of as a "traditional" firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

Unified threat management (UTM) firewall

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

Next-generation firewall (NGFW)

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.

According to Gartner, Inc.'s definition, a next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

While these capabilities are increasingly becoming the standard for most companies, NGFWs can do more.

Antivirus Software

It is necessary to have both a strong firewall and up-to-date antivirus software in place to keep your system secure. In 2018, both remain vital components of cybersecurity. Antivirus software will alert users to virus and malware infections and many will also provide additional services such as scanning emails to ensure they are free from malicious attachments or web links. Modern antivirus programs perform useful protective measures, such as quarantining potential threats and removing them. There is a huge range of antivirus software, and you can easily find a package that is suited to the needs of your business.

Penetration Testing

Penetration testing is an important way to test your business' security systems. During a penetration test, cybersecurity professionals will use the same techniques utilized by criminal hackers to check for potential vulnerabilities and areas of weakness. A pen test attempts to simulate the kind of attack a business might face from criminal hackers, including everything from password cracking and code injection to phishing.

Once the test has taken place, the testers will present you with their findings and can even help by recommending potential changes to your system.

Staff Training

Someone might not think of staff training as a 'tool' but ultimately, having knowledgeable employees who understand their role in cybersecurity is one of the strongest forms of defense against attacks. There are many training tools that you can invest in to educate staff about best cyber security practices.

INTRUSION DETECTION AND PREVENTION SYSTEMS

IDS and IPS tools help IT staff identify and protect their wired and wireless networks against several security threat types. These technologies, like several other categories of network security tools, are being deployed with greater frequency as networks grow in size and complexity. Annual IPS revenues are expected to more than double between 2012 and 2017

(from $1.21 billion to $2.44 billion) according to estimates from the research and analysis firm Frost & Sullivan. Both IDS and IPS solutions detect threat activity in the form of malware, spyware, viruses, worms and other attack types, as well as threats posed by policy violations. IDS tools passively monitor and detect suspicious activity; IPS tools perform active, in-line monitoring and can prevent attacks by known and unknown sources. Both tool types can identify and classify attack types.

ANTI-MALWARE

Anti-malware network tools help administrators identify, block and remove malware. They enable the IT department to tailor its anti-malware policies to identify known and unknown malware sources, for example, or surveil specific users and groups. Malware is always on the lookout for network vulnerabilities — in security defenses, operating systems, browsers, applications and popular targets such as Adobe Flash, Acrobat and Reader — that they can exploit to fully access a victim's network. Best practices call for a multipronged defense that might also include IP blacklisting, data loss prevention (DLP) tools, anti-virus and anti-spyware software, web browsing policies, egress filtering, and outbound-traffic proxies.

MOBILE DEVICE MANAGEMENT

MDM software bolsters network security through remote monitoring and control of security configurations, policy enforcement and patch pushes to mobile devices. Further, these systems can remotely lock lost, stolen or compromised mobile devices and, if needed, wipe all stored data.

NETWORK ACCESS CONTROL

NAC products enforce security policy by granting only security policy–compliant devices access to network assets. They handle access authentication and authorization functions and can even control the data that specific user's access, based on their ability to recognize users, their devices and their network roles.

AUTHENTICATION AND AUTHORIZATION

Traditional directory-based services, such as Active Directory, authenticate users and grant access based on authorization rules. Newer identity-based security technologies manage authentication and authorization through such methods as digital certificates and public key infrastructure solutions. Additional security is provided by the SNMP protocol itself. The most recent version, SNMPv3, provides authentication, authorization and encryption capabilities lacking in the previous two versions.

VPN

A virtual private network (VPN) is programming that creates a safe, encrypted connection over a less secure network, such as the public internet. A VPN uses tunneling protocols to encrypt data at the sending end and decrypt it at the receiving end. To provide additional security, the originating and receiving network addresses are also encrypted. VPNs are used to provide remote corporate employees, gig economy freelance workers and business travelers with access to software applications hosted on proprietary networks. To gain access to a restricted

resource through a VPN, the user must be authorized to use the VPN app and provide one or more authentication factors, such as a password, security token or biometric data. VPN apps are often used by individuals who want to protect data transmissions on their mobile devices or visit web sites that are geographically restricted. Secure access to an isolated network or website through a mobile VPN should not be confused with private browsing, however. Private browsing does not involve encryption; it is simply an optional browser setting that prevents identifiable user data, such as cookies, from being collected and forwarded to a third-party server.

At its most basic level, VPN tunneling creates a point-to-point connection that cannot be accessed by unauthorized users. To actually create the VPN tunnel, the endpoint device needs to be running a VPN client (software application) locally or in the cloud. The VPN client runs in the background and is not noticeable to the end user unless there are performance issues. The performance of a VPN can be affected by a variety of factors, among them the speed of users' internet connections, the types of protocols an internet service provider may use and the type of encryption the VPN uses. In the enterprise, performance can also be affected by poor quality of service (QoS) outside the control of an organization's information technology (IT) department.

Honeypot

A honeypot is a computer or computer system intended to mimic likely targets of cyberattacks. It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how cybercriminals operate. The principle behind them is simple: Don't go looking for attackers. Prepare something that would attract their interest — the honeypot — and then wait for the attackers to show up. Like mice to cheese-baited mousetraps, cybercriminals are attracted to honeypots — not because they're honeypots. The bad guys think the honeypot is a legitimate target, something worthy of their time. That's because the bait includes applications and data that simulate a real computer system.

Honeypot is an Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored. Most honeypots are installed inside firewalls so that they can better be controlled, though it is possible to install them outside of firewalls. A firewall in a honeypot works in the opposite way that a normal firewall works instead of restricting what comes into a system from the Internet, the honeypot firewall allows all traffic to come in from the Internet and restricts what the system sends back out. By luring a hacker into a system, a honeypot serves several purposes:

- The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.
- The hacker can be caught and stopped while trying to obtain root access to the system.

- By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.
- A network of honeypots is often called a honeynet.

2.1. Data Centre Standards and Best Practices

Brief Introduction to Data Centre

A data center (or datacenter) is a facility composed of networked computers and storage that businesses or other organizations use to organize, process, store and disseminate large amounts of data. A business typically relies heavily upon the applications, services and data contained within a data center, making it a focal point and critical asset for everyday operations. A data center is a repository that houses computing facilities like servers, routers, switches and firewalls, as well as supporting components like backup equipment, fire suppression facilities and air conditioning. A data center may be complex (dedicated building) or simple (an area or room that houses only a few servers). Additionally, a data center may be private or shared. A data center is also known as a datacenter or data centre. The data center centrally houses computer systems and storage devices with data on them enabling them to operate securely.

Data centers are simply centralized locations where computing and networking equipment is concentrated for collecting, storing, processing, distributing or allowing access to large amounts of data. They have existed in one form or another since the advent of computers.

In the days of the room-sized behemoths that were our early computers, a data center might have had one supercomputer. As equipment got smaller and cheaper, and data processing needs began to increase, and they have increased exponentially -- we started networking multiple servers (the industrial counterparts to our home computers) together to increase processing power. We connect them to communication networks so that people can access them, or the information on them, remotely. Large numbers of these clustered servers and related equipment can be housed in a room, an entire building or groups of buildings. Today's data center is likely to have thousands of very powerful and very small servers running 24/7. Because of their high concentrations of servers, often stacked in racks that are placed in rows, data centers are sometimes referred to a server farm. They provide important services such as data storage, backup and recovery, data management and networking. These centers can store and serve up Web sites, run e-mail and instant messaging (IM) services, provide cloud storage and applications, enable e-commerce transactions, power online gaming communities and do a host of other things that require the wholesale crunching of zeroes and ones.

Just about every business and government entity either needs its own data center or needs access to someone else's. Some build and maintain them in-house, some rent servers at co-location facilities (also called colos) and some use public cloud-based services at hosts like Amazon, Microsoft, Sony and Google.

The colos and the other huge data centers began to spring up in the late 1990s and early 2000s, sometime after Internet usage went mainstream. The data centers of some large companies are spaced all over the planet to serve the constant need for access to massive amounts of information. There are reportedly more than 3 million data centers of various shapes and sizes in the world today [source: Glanz].

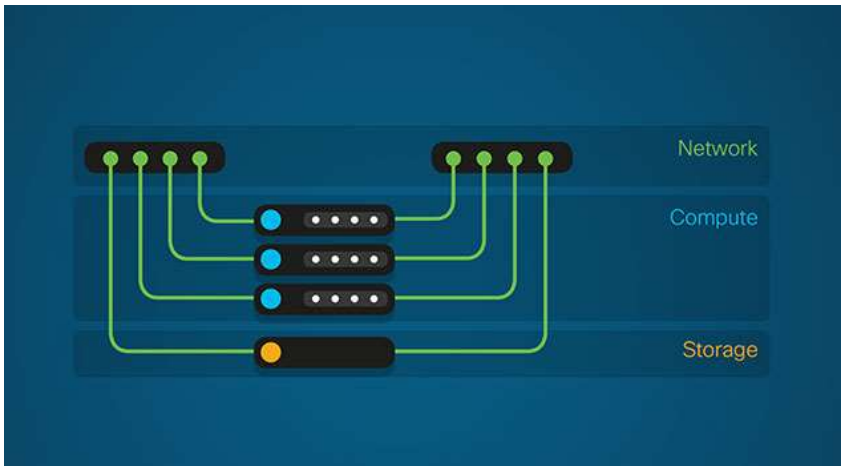
Types of Data Centers

There are a number of ways to classify data centers according to how they are set up and used. These factors include:

1. Whether they are owned or used by one or multiple organizations
2. Whether and how they fit into a topology of other data centers
3. Which technologies and management approaches they use for computing, storage, cooling, power, and operations
4. How green they are, which has become more important and visible in recent years

Data centers can be loosely classified into three types according to who owns them and who uses them. Exclusive Data Centers are facilities wholly built, maintained, operated and managed by the business for the optimal operation of its IT equipment. Some of these centers are well-known companies such as Facebook, Google, or Microsoft, while others are less public-facing big telecoms, insurance companies, or other service providers.

Managed Hosting Providers are data centers managed by a third party on behalf of a business. The business does not own data center or space within it. Rather, the business rents IT equipment and infrastructure it needs instead of investing in the outright purchase of what it needs. Colocation Data Centers are usually large facilities built to accommodate multiple businesses within the center. The business rents its own space within the data center and subsequently fills the space with its IT equipment, or possibly uses equipment provided by the data center operator.



The Big Three

The three major data center design and infrastructure standards developed for the industry include:

1. Uptime Institute's Tier Standard

This standard develops a performance-based methodology for the data center during the design, construction, and commissioning phases to determine the resiliency of the facility with respect to four Tiers or levels of redundancy/reliability. The Tiers are compared in the table below and can be found in greater definition in UI's white paper TUI3026E. The origins of the Uptime Institute as a data center users group established it as the first group to measure and compare a data center's reliability. It is a for-profit entity that will certify a facility to its standard, for which the standard is often criticized.

Tier Rating	Tier 1	Tier 2	Tier 3	Tier 4
Active Capacity Components	N	N+1	N+1	N after Failure
Distribution Paths	1	1	1 Active + 1 Alternate	2 Active
Concurrently Maintainable	No	No	Yes	Yes
Fault Tolerant	No	No	No	Yes
Compartmentalization	No	No	No	Yes

ANSI/BICSI 002-2014

Data Center Design and Implementation Best Practices: This standard covers the major aspects of planning, design, construction, and commissioning of the MEP building trades, as well as fire protection, IT, and maintenance. It is arranged as a guide for data center design, construction, and operation. Ratings/Reliability is defined by Class 0 to 4 and certified by BICSI-trained and certified professionals.

ANSI/TIA 942-A 2014

Telecommunication Infrastructure Standard for Data Centers: This standard is more IT cable and network oriented and has various infrastructure redundancy and reliability concepts based on the Uptime Institute's Tier Standard. In 2013, UI requested that TIA stop using the Tier system to describe reliability levels, and TIA switched to using the word "Rated" in lieu of "Tiers," defined as Rated 1-4. TIA uses tables within the standard to easily identify the ratings for telecommunications, architectural, electrical, and mechanical systems. Here's a sample from the 2005 standard (click the image to enlarge):

Table 10: Tiering reference guide (electrical)

	TIER 1	TIER 2	TIER 3	TIER 4
ELECTRICAL				
General				
Number of Delivery Paths	1	1	1 active and 1 passive	2 active
Utility Entrance	Single Feed	Single Feed	Dual Feed (600 volts or higher)	Dual Feed (600 volts or higher) from different utility substations
System allows concurrent maintenance	No	No	Yes	Yes
Computer & Telecommunications Equipment Power Cords	Single Cord Feed with 100% capacity	Dual Cord Feed with 100% capacity on each cord	Dual Cord Feed with 100% capacity on each cord	Dual Cord Feed with 100% capacity on each cord
All electrical system equipment labeled with certification from 3rd party test laboratory	Yes	Yes	Yes	Yes
Single Points of Failure	One or more single points of failure for distribution systems serving electrical equipment or mechanical systems	One or more single points of failure for distribution systems serving electrical equipment or mechanical systems	No single points of failure for distribution systems serving electrical equipment or mechanical systems	No single points of failure for distribution systems serving electrical equipment or mechanical systems
Critical Load System Transfer	Automatic Transfer Switch (ATS) with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs	Automatic Transfer Switch (ATS) with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs	Automatic Transfer Switch (ATS) with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs	Automatic Transfer Switch (ATS) with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs
Site Switchgear	None	None	Fixed air circuit breakers or fixed molded case breakers. Mechanical interlocking of breakers. Any switchgear in distribution system can be shutdown for maintenance with by-passes without dropping the critical load	Drawout air circuit breakers or drawout molded case breakers. Mechanical interlocking of breakers. Any switchgear in distribution system can be shutdown for maintenance with by-passes without dropping the critical load
Generators correctly sized according to installed capacity of UPS	Yes	Yes	Yes	Yes
Generator Fuel Capacity (at full load)	8 hrs (no generator required if UPS has 8 minutes of backup time)	24 hrs	72 hrs	96 hrs

TIA has a certification system in place with dedicated vendors that can be retained to provide facility certification.

EN 50600: an International Standard

An international series of data center standards in continuous development is the EN 50600 series. Many aspects of this standard reflect the UI, TIA, and BCSI standards. Facility ratings are based on Availability Classes, from 1 to 4. The standard breaks down as follows:

- EN 50600-1 General concepts
- EN 50600-2-1 Building construction
- EN 50600-2-2 Power distribution
- EN 50600-2-3 Environmental control
- EN 50600-2-4 Telecommunications cabling infrastructure
- EN 50600-2-5 Security systems
- EN 50600-2-6 Management and operational information systems

2. Regulatory Standards

Government regulations for data centers will depend on the nature of the business and can include HIPPA (Health Insurance Portability and Accountability Act), SOX (Sarbanes Oxley) 2002, SAS 70 Type I or II, GLBA (Gramm-Leach Bliley Act), as well as new regulations that may be implemented depending on the nature of our business and the present security situation.

3. Operational Standards

There are also many operational standards to choose from. These are standards that guide day-to-day processes and procedures once the data center is built:

- Uptime Institute: Operational Sustainability (with and without Tier certification)
- ISO 9000 - Quality System
- ISO 14000 - Environmental Management System
- ISO 27001 - Information Security
- PCI – Payment Card Industry Security Standard
- SOC, SAS70 & ISAE 3402 or SSAE16, FFIEC (USA) - Assurance Controls
- AMS-IX – Amsterdam Internet Exchange - Data Centre Business Continuity Standard

- EN50600-2-6 Management and Operational Information

These standards will also vary based on the nature of the business and include guidelines associated with detailed operations and maintenance procedures for all of the equipment in the data center.

Data Centre Existing Standards

- Color coding

All Electrical and Data cabling has a color standard depending on use. Color Coded Power Leads – The A feed Primary PDU connection must use a black power cable. The B Feed secondary PDU connection must use a white cable.

- Data Cabling Types

All ISD racks are provided with an amount of Cat6a, Multi-Mode and Single Mode Fibre connectivity to a network distribution rack.

- Patch leads:
  - Cat6a Copper cables are to be Low Smoke Zero Halogen (LSZH)
  - Copper computer Data cabling must be shielded and CommScope branded and can be provided from Data Centre Services stock. Example product.
  - All data centers have Multimode and Single Mode fibre with LC type connectors
  - Network ports will be allocated by ISD's Data Centre Services team and network port labels are to be used to identify the equipment connected
  - Diverse routes are available within TP3. Please review Data Cabling Schematics for more information.
- Off-Site Cross Connects

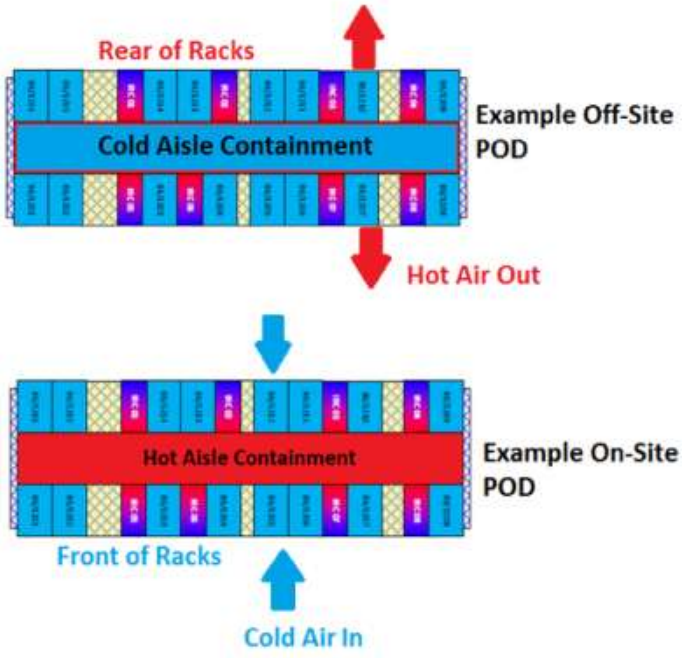
The installation and maintenance of data cabling between racks and areas outside of the UCL data hall and/or racks must always be undertaken by the off-site data centre engineers or nominated sub-contractors.

- Cable Management
  - All racks have vertical and horizontal cable management systems, and these should be utilised.
  - All cables must be labelled either-end following the same naming standard – (Cable Identifying character and sequential 5-digit number) E.g. A12345 or C65401
  - We must use cables of the appropriate length.
  - Velcro cable ties must be used.
  - Cable management arms can be used at our discretion.
  - All cabling must be neat and tidy.
- Racking

Equipment should be racked from the bottom of the cabinet up and one must use a mechanical lifter to assist with higher level racking. All equipment must have a physical identification label, visible both front and rear. Rail kits must be used. The ISD Data Centre Services team will provide standard rack nuts and bolts.

- Airflow

Airflow is cold at the front, hot at the back with no exceptions to this rule.



- UPS

Customer UPS equipment must not be installed. We must discuss any UPS requirement with the ISD Data Centre Services team.

- Security

All access in and out of the on-site data center and TP3 racks are managed by authorized access cards. All access into the off-site data center is only possible with an access card that has been provided by the off-site security team, after induction or as an approved guest. Access Cards must be worn visibly at all times by authorized staff or guests.

- Power

PDU power outlets will be allocated by Data Centre Services team, appropriate to the installation. All equipment should be fitted with at least two separate power supply units if the equipment model allows for redundancy. Otherwise, single feed devices must be identified with an orange power cables. All PDUs installed are Intelligent PDUs with vertical orientation. Various levels of power and phases are available at each data centre facility, Data Centre Services team will assist to verify requirements.

- Power and Cooling Design Specification

Due to power and cooling availability, it will be necessary for Data Centre Services to verify and monitor all installations. It may be necessary to re-balance, if the load exceeds the specification of the POD.

➢ Open DCIM Inventory and Monitoring

One should maintain an operational DCIM (data center Infrastructure management) tool, which includes equipment audit, rack plans and a rack power monitoring facility, which should also be available to all UCL data center clients.

Data Centre Services are responsible for completing a standardized set of mandatory fields from the installation point, including, server identification, location, contact details etc.

Compute and Cloud Platform will perform periodic audit to ensure data within the DCIM is accurate.

Use of the DCIM

OpenDCIM functions provided:

- Provide complete physical inventory (asset tracking) of the data centres
- Support for Multiple Rooms (data centre within a data centre)
- Management of key elements of capacity management – e.g. space and power
- Basic contact management
- Computation of Centre of Gravity for each cabinet
- Template management for devices, with ability to override per device
- Optional tracking of cable connections within each cabinet, and for each switch device
- Archival functions for equipment sent to salvage/disposal
- Integration with intelligent power strips and UPS. Easy to update with OIDs for other manufacturers.
- Aggregation of monitoring systems into a dashboard
- Open Architecture

2.2. Designing a Scalable Network Infrastructure

A. Importance of Structured Data Center Cabling

Data Center Cabling

Cabling process can be done in two ways: structured and unstructured.

Structured cabling

Structured cabling is a type of infrastructure that supports the performance of an organisation's cabling system or network. It is the glue that binds all PCs, phones and other devices used within the business together – providing a reliable and versatile solution to a wide range of communication requirements. The importance of organized cabling systems will vary from business to business, but for the majority, it can ensure a highly reliable and cost-effective network infrastructure that will stand the test of time. Below we explore in depth the benefits of structured network cabling and why our business could benefit from our specialist network and cabling service here at Leading Edge.

- Future Proof Investment
- Simplicity
- Cost Effective
- Enhanced Flexibility

- Reduced Risk of Downtime
- Works with the Internet of Things
- Safety
- Aesthetically Pleasing
- Easily Scalable

B. Planning considerations

The data center is home to the computational power, storage, and applications necessary to support an enterprise business. The data center infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered.

C. Copper and Fiber cable technology and standards

Deciding to build a data center architecture using fiber, copper or the selective use of both depend on a variety of criteria including:

- Bandwidth and performance of computing equipment required per data center area
- Immunity to Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI)
- Need for density and space saving connectivity
- Flexibility and speed of reconfiguration
- Device media interface considerations
- Standardization
- Future vision and tolerance for recabling
- Cost of electronics.

D. ANSI/TIA-942 Cabling hierarchy and recommendations

THE PURPOSE OF ANSI/TIA/EIA-942

TIA/EIA 942 is the telecommunications infrastructure standard for data centers. The list below shows its purpose:

1. The purpose of this standard is to provide requirements and guidelines for the design and installation of a data center or computer room.
2. It is intended for designers who need a comprehensive understanding of the data center design including the facility planning, the cabling system, and the network design.
3. It facilitates the planning for data centers to occur earlier in the building development process (architectural, facilities, and IT).

Data centers support a wide range of transmission protocols. Some of these protocols impose distance restrictions that are shorter than those imposed by this standard. When applying specific transmission protocols, consult standards, regulations, equipment vendors, and system service suppliers for applicability, limitations, and ancillary requirements. Consider consolidating standardized and proprietary cabling into a single structured cabling system.
The ANSI/TIA/EIA-942 standard specifies:

1. *Cabling Design*

2. *Network Design*
3. *Facilities Design*
4. *Informative annexes containing "best practices" and availability requirements*
5. *Spaces*
6. *Pathways*
7. *Racks/cabinets*

DATA CENTER CABLING INFRASTRUCTURE

The basic elements of the data center cabling system structure are the following:

- Horizontal Cabling
- Backbone Cabling
- Cross-connect in the entrance room or main distribution area
- Main Cross-Connect (MC) in the main distribution area
- Horizontal Cross-Connect (HC) in the telecommunication room, horizontal distribution area or main distribution area
- Zone outlet or consolidation point in the zone distribution area
- Outlet in the equipment distribution area

E. SAN storage cabling

A SAN (storage area network) is a network of data storage devices. By taking storage devices and storage traffic off the Local Area Network (LAN), another network is created specifically for Storage Data. SAN storage solutions can range from a few servers accessing a central pool of storage devices to thousands of servers accessing TBs or more of storage. In a SAN, data is presented from storage devices to a host so that the storage looks like it is locally attached. This is achieved through various types of data virtualization. SAN storage, then, is a high-speed network that provides network access to Storage. In some cases, SANs can be so large that they span multiple sites, as well as internal data centers and the cloud.

F. Network redundancy

The underlying concept of redundant networks is simple. Without any backup systems in place, all it takes is one point of failure in a network to disrupt or bring down an entire system. Network redundancy is the process of adding additional instances of network devices and lines of communication to help ensure network availability and decrease the risk of failure along the critical data path.

There are two forms of redundancy that data centers use to ensure systems will stay up and running:

- Fault Tolerance: A fault-tolerant redundant system provides full hardware redundancy, mirroring applications across two or more identical systems that run in tandem. Should anything go wrong with the primary system, the mirrored backup system will take over with no loss of service. Ideal for any operations in which any

amount of downtime is unacceptable (such as industrial or healthcare applications), fault-tolerance redundant systems are complex and often expensive to implement.

- High Availability: A software-based redundant system, high-availability uses clusters of servers that monitor one another and have failover protocols in place. If something goes wrong with one server, the backup servers take over and restart applications that were running on the failed server. This approach to network redundancy is less infrastructure intensive, but it does tolerate a certain amount of downtime in that there is a brief loss of service while the backup servers boot up applications.

G. Building-to-Building connectivity

Wireless may not be the best solution

Too often, when a team is contemplating how to connect two buildings, someone will offer a wireless solution. Yes, there are wireless solutions that will connect two buildings, and antenna boosting equipment for better service. However, a hard-line connection is more reliable if installed in conduit correctly. Here's a general rule of thumb: "Use a hard-line connection unless you can't."

Site-to-site connections using wireless connections are frequently disrupted by an obstruction, weather (in some technologies and applications), or interference. Also, wireless technologies have a shorter lifespan, as replacement technologies are rapidly developing for this market space.

When dealing with conduit, think big

Most building connections today will be a fiber connection in hard plastic conduit. This conduit is usually buried about two feet below the ground. When sizing out what type of conduit to use (even if you're working with a heavy equipment or installation professional), always think larger than you need.

Consider this example: You can fit the bare cable of fiber optic networking in just about any size conduit. However, if this project is a "one of a kind" type, you may have some price pressure to deliver the best solution for the technology need. When you size up the equipment and supplies, you may require a set of fibers cutting tools to end the line at each point. But the most cost-efficient solution may be simply ordering a to-length fiber optic cable that's pre-terminated. In this case, you may save a great deal on fiber tools, but you should go up to the next size (and test the entire fit) for pushing a termination through conduit. For a recent project I did, we pulled two SC connectors through 1-inch conduit.

Best practice

When pulling fiber through a conduit, be careful with the line. Take the following steps to make it easier on the pull:

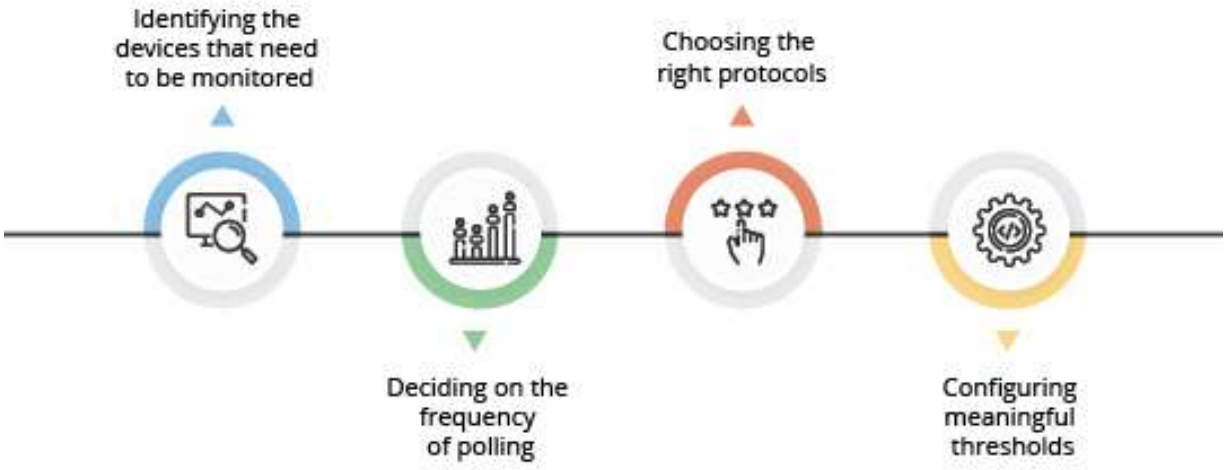
- Get the pull line to the end of the conduit the easy way: Make a small ball of tape, put it in a plastic bag (sandwich size), tape the pull line to it, and pull it through with a medium duty vacuum on the end side.
- Have conduit straightened out before pulling the fiber through.

- Insulate the header of the cable well with electrical tape. Any pressure will then be taken by the tape instead of the connector or cable.
- Have people on each side pulling at the end and feeding the cable into the beginning to minimize stress points.

H. Network monitoring system requirements

What is Network Monitoring?

In today's world, the term network monitoring is widespread throughout the IT industry. Network monitoring is a critical IT process where all networking components like routers, switches, firewalls, servers, and VMs are monitored for fault and performance and evaluated continuously to maintain and optimize their availability. One important aspect of network monitoring is that it should be proactive. Finding performance issues and bottlenecks proactively helps in identifying issues at the initial stage. Efficient proactive monitoring can prevent network downtime or failures.



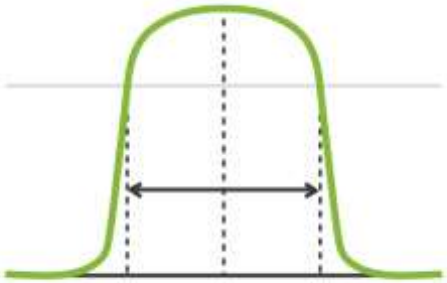
Important aspects of network monitoring:

- Monitoring the essentials
- Optimizing the monitoring interval
- Selecting the right protocol
- Setting thresholds

Tools for bandwidth measuring

Bandwidth: Valid for Linux and Windows (http://bandwidthd.sourceforge.net/)

Band Width Monitor NG. Beta. To measure network traffic and analyze protocols such as TCP, http, UPD, etc. (http://sourceforge.net/projects/bwmng/)



These two tools, correctly configured, give you the basics on your network's health and allow you to configure and trigger alarms, as well as record and measure network activity, but do not let you manage the network. For that you will need a platform you can configure to act when specific parameters are met, or thresholds passed. This is the next step for network management.

Advanced network monitoring

What to keep in mind when choosing network monitoring software

- Alert notifications.
- External server integration.
- Utility and proper representation of data on your panels.
- Flexibility to adapt to specific tools or software.
- Access to API from external systems.
- Automated device detection.
- Database integration.
- Multi-device.
- Scalability.
- Support for the greatest number of data acquisition protocols possible.
- Security.
- Virtual machine integration.
- Hardware integration.
- Remote control.
- Hardware and Software inventory.
- Geolocation.
- Cloud monitoring.

2.3. Data Centre Monitoring

Data center monitoring is the process of monitoring, managing and operating a data center to follow the operating and organizational requirements. It is the process of using manual and automated tools and techniques to ensure the best operating health of a data center. It ensures that the key functions and services of a data center are delivered without any interruptions or abnormalities. Data center monitoring is also known as data center management.

Data center monitoring is a broad process that focuses on monitoring the entire data center infrastructure. Typically, data center monitoring is performed through automated tools that provide statistical insights into data center performance/status. This data is used by data center administrators in identifying irregularities and in fixing them.
Data center monitoring usually incorporates:

- Monitoring data center servers and computers for performance, security uptime and more
- Monitoring and managing network operations and resolving network problems as they arise
- Providing end-to-end visibility across all data center components including computers, storage, network and software

In addition to monitoring IT-specific components, data center monitoring also focuses on monitoring supported elements such as:

- Power availability and consumption
- Data center temperature, and the heating and ventilation systems
- Physical data center security to restrict unauthorized personnel from entering the premises

How Does Data Center Monitoring Work?

Data center monitoring enables you to centrally manage all devices in your data centers. It allows you to connect to, collect data from, and configure your devices via SNMP, HTTPs, and other protocols for IP-based networks.

- Automatically collect real-time data from all your devices – down to the individual outlet level – through a single interface
- Set power and environmental thresholds on collected data and receive alerts so you'll be the first to know about potential issues before they become bigger problems
- Configure polling frequencies to your intervals that provide meaningful data while maintaining efficient network traffic
- Forward and filter traps to receive only the notifications that matter to you
- Analyze and trend collected data to uncover insights around your data center operations, including capacity forecasting

- Gain peace of mind about your data center security with door locks and card reader permissions that let authorized users in and keep intruders out
- Use protocols such as SNMP, HTTPS, Modbus, BACnet, Wiegand, RF, etc. to communicate with data center monitoring software

2.4. Operational Security and Safety Practices

Data Center Operations Best Practices

Data Center operations best practices call for a strategic approach to balancing IT service delivery and cost efficiency. With the growing complexity of data centers from the demand for new service offerings and the sheer amount of physical compute, network, and storage required to provide those services, Data Center Managers are quickly realizing that manual tools, such as excel spreadsheets and Visio diagrams, are no longer an effective way to manage their Data Centers. Instead, sophisticated data center infrastructure management (DCIM) tools that measure, monitor, and provide a best practices operations framework are needed. To become more efficient and to ensure that the demand for new services can be met by the capacity and the infrastructure, successful IT organizations have spent a lot of time creating a set of best practices surrounding an organization's tools, technologies and processes. It's about using these tools to provide a more functional, reliable, and energy efficient data center. Here are some of the best practices, centered around the use of DCIM tools, organizations like yourself have adopted:

- Know what you have – identify your current assets, their connections, and capacity information storing all such information in a single database repository system. Having all this information in a single place ensures accurate capacity planning and forecasting, faster provisioning, quicker troubleshooting and mean time to repair (MTTR).
- Benchmark your current performance – you can't measure what you don't monitor. Use meters and monitoring tools to identify current energy performance, hot spots, heat related equipment failure. Using this data later to compare trends data over time to baseline performance can help predict and avoid equipment failure, improving long-term reliability
- Optimize to maximize capacity and utilization. Develop an Energy Management Program to minimize ongoing energy costs. Continually measure and adjust energy usage, Power Usage Effectiveness (PUE), airflow, cooling, humidity, temperature, and power. Use this data to understand what draws energy in your facility, do more with less, find ways to save on energy usage and adjust to real-time operating conditions, including lowering/raising of temperature set points to maintain a safe environment for your IT equipment.
- Plan and change management throughout the entire lifecycle. Put processes in place to enable quick response, streamlining of activities and the ability to audit. Automate as many of the manually intensive processes to reduce errors and time to deploy.
- Review and analyze space, power, and energy performance to maintain an optimized data center. Use dashboard, performance and trending reports to predict future needs.

- Ensure IT and facilities management work together to understand the business objectives, develop plans for integrating services and infrastructure, as well as to share the cost burden.

Operational security (OPSEC)

Operational security (OPSEC), also known as procedural security, is a risk management process that encourages managers to view operations from the perspective of an adversary in order to protect sensitive information from falling into the wrong hands.

Though originally used by the military, OPSEC is becoming popular in the private sector as well. Things that fall under the OPSEC umbrella include monitoring behaviors and habits on social media sites as well as discouraging employees from sharing login credentials via email or text message.

5 focus areas for Data Center security

1. Physical Security of DC

Physical security of the data center building and its components is crucial for keeping the data within it safe. The data center building must be designed to weather all types of physical challenges, from terrorist attacks and industrial accidents to natural disasters. Enhancing physical security includes a variety of measures such as DC design with thicker walls and fewer windows and doors, enhancing CCTV monitoring, fire protection and investing in specialized security team.

2. Restricting Access

DC security team needs to keep a close watch on the people who enter the data center. From cleaning crew and internal IT staff to visitors, access to critical areas must be restricted and all movement must be tracked to ensure that unauthorized people are kept out of sensitive server rooms.

3. Securing your Data

All data center security is ultimately aimed at keeping the hosted data safe and private. This includes comprehensive measures such as complete data backup and recovery, using data encryption while transferring files, enforcing the latest data privacy regulations and comprehensive monitoring of traffic.

4. Network security

The first layer of network security is securing the perimeter by installing firewalls to clean up traffic right at the point of entry. This can be followed up by using the Zero trust model and inspecting and monitoring the internal traffic within the network, to detect and mitigate any threat that might have bypassed the perimeter firewall.

5. Server security

With virtualization, server security has become more complex and challenging. It is imperative to follow industry standards to ensure complete server security with 24×7 monitoring, intrusion

detection and intrusion prevention. Comprehensive security solutions need to protect all virtual and physical server environments and infrastructure as well as all web-based applications.

Data Center Security Standards

There is a trend in making data services safer and standardizing the security for data centers. In support of this, the Uptime Institute published the Tier Classification System for data centers. The classification system sets standards for data center's' controls that ensure availability. As security can affect the uptime of the system, it forms part of their Tier Classification Standard.

There are four 4 tiers defined by the system. Each tier maps to a business need that depends on what kind of data is being stored and managed.

Tiers 1 & 2

Seen as tactical services, Tier 1 and 2 will only have some of the security features listed in this article. They are low cost and used by companies who do not want real-time access to their data and who won't suffer financially due to a temporary system failure.

They are mainly used for offsite data storage.

Tiers 3 & 4

These tiers have higher levels of security. They have built-in redundancies that ensure uptime and access. Providing mission critical services for companies who know the cost of damage to a reputation a break in service creates.
These real-time data processing facilities provide the highest standards of security.

3. DATA ARCHIVING & RETRIEVAL MANAGEMENT

3.1 Data Archiving & Retrieval Management

3.1.1 What and Why Data Archiving

Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Archive data consists of older data that remains important to the organization or must be retained for future reference or regulatory compliance reasons. Data archives are indexed and have search capabilities, so files can be located and retrieved.

Archived data is stored on a lower-cost tier of storage, serving as a way to reduce primary storage consumption and related costs. An important aspect of a business's data archiving strategy is to inventory its data and identify what data is a candidate for archiving.

Some archive systems treat archive data as read-only to protect it from modification, while other data archiving products enable writes, as well as reads. For example, WORM (write once, read many) technology uses media that is not rewritable.

Data archiving is most suitable for data that must be retained due to operational or regulatory requirements, such as document files, email messages and possibly old database records.

3.1.2 Data archiving benefits

The greatest benefit of archiving data is it reduces the cost of primary storage. Primary storage is typically expensive, because a storage array must produce a sufficient level of IOPS to meet operational requirements for user read/write activity. In contrast, archive storage costs less, because it is typically based on a low-performance, high-capacity storage medium. Data archives can be stored on low-cost hard disk drives (HDDs), tape or optical storage that is generally slower than performance disk or flash drives.

Archive storage also reduces the volume of data that must be backed up. Removing infrequently accessed data from the backup data set improves backup and restore performance. Typically, data de-duplication is performed on data being moved to a lower storage tier, which reduces the overall storage footprint and lowers secondary storage costs.

3.1.3 Data archiving vs. backup

Data archives are not to be confused with data backups, which are copies of data. Although both are considered secondary storage and use a lower-performance, higher-capacity storage medium than primary storage, they serve different purposes. Archives fill a data retention purpose, whereas backups are used for data protection and disaster recovery.

Data archives can be thought of as a data repository for infrequently accessed, but still readily available data. Backups, on the other hand, are part of a data recovery mechanism that can be used to restore data in the event it is corrupted or destroyed. Backup data often consists of important information that must be restored quickly when lost or deleted.

3.2 Basic Principles of Data Archiving

As with all forms of digital technology, digital coding schemes are subject to ongoing development. As such, discussion around the most appropriate formats for preservation will also continue to evolve. Irrespective of the options available however, several principles can be applied in choosing target formats.

1. File-based formats offer greater data security and integrity monitoring capability than do carrier-based formats containing data streams such as DAT, audio CD or Digital Betacam.
2. When transferring digital carrier-based content (for example from DAT or DV cassette formats) the resultant file must, when deemed appropriate, retain the coding scheme of the original data stream. Where this is not appropriate, for example where a lossy and proprietary coding scheme has been used, a coding scheme should be chosen which preserves the integrity of the original.
3. An essential requirement of any archival file format is that coding schemes used for preservation purposes be openly defined, and not proprietary to a limited number of manufacturers.
4. Where there is little or no consensus throughout the archival community on the choice of target format for a given purpose, a repository must choose a format for which they can be at least relatively confident of their own ability to support it sustainably. This would require sufficient available resource including expertise, as well as ongoing wider industry support for the format.
5. A repository must ensure that a chosen target format will retain the minimum required combination of primary and secondary information.

The core actions in file-based archiving pertain to bit preservation, i.e., a set of actions that maintain the integrity of the digital data ("bitstreams") that are being managed by the responsible institution. Actions beyond bit preservation will ultimately be needed when the formatting of the content is obsolescent. The most common action will be format migration, although there may be contexts in which system emulation is required. While bit preservation decisions may be left to information technology specialists and appropriate software and hardware applications, the actions beyond bit preservation will benefit from the involvement of people with curatorial responsibilities.

Data management must observe the following core principles:

1. Files are generally placed in storage systems by copying. This process must produce duplicates that are verifiably identical to the originals. This process of data integrity checking can be achieved through the prior creation of a checksum, also known as a

hash or digest. The process of verification should take place immediately after the creation of the copy, ideally as an automated procedure.

2. The ongoing data integrity of file-based content must be checked at regular intervals to ensure that it can be read exactly as it was written, with no errors or changes.
3. Depending on the original file format however, it may be desirable to transcend to a new target format rather than simply copy from the original file. This process is known as format migration.
4. Digital content, whether file- or carrier-based, must be copied to a new physical carrier before uncorrectable errors occur. When the original and target formats are the same, this process is known as refreshment or media migration.
5. It is essential to keep at least two digital preservation copies, ideally more, and to use further dedicated copies for access as appropriate. The preservation copies should be kept in different geographic locations whenever possible. Additional security may also be provided by the use of different storage technologies for each set of preservation copies. When choosing which technologies to use, it should be borne in mind that a strategy will only be as strong as its weakest link.
6. Access copies should be made whenever possible. Unlike archival master files however, such access or distribution copies may be subjectively modified, depending on the requirements of users. Data reduction may also be employed when compatible with user requirements. As with the creation of archival masters, careful documentation of all parameters and procedures employed is essential.
7. Where possible, checks to ensure data integrity should be automated, as is possible with equipment within trusted digital repositories. If this is not possible, then manual checks will need to be undertaken, on a statistically significant basis.

3.3 Data Lifecycle Management

What is Data Lifecycle Management?

- Data life cycle management (DLM) is a policy-based approach to managing the flow of an information system's data throughout its life cycle: from creation and initial storage to the time when it becomes obsolete and is deleted. DLM products automate the processes involved, typically organizing data into separate tiers according to specified policies and automating data migration from one tier to another based on those criteria. As a rule, newer data, and data that must be accessed more frequently, is stored on faster, but more expensive storage media, while less critical data is stored on cheaper, but slower media.

- Data Lifecycle Management (DLM) is a process that helps organizations manage the flow of data throughout its lifecycle—from creation, to use, to sharing, archive and deletion. Tracking your data accurately throughout the information lifecycle is the foundation of a sensitive data protection strategy and helps you determine where to apply security controls.

A Brief History of Data Lifecycle Management

The 1980s brought the introduction of random-access storage (RAM) and with that enterprise businesses transitioned from sequential cardpunch and tape approaches to databases. This era heralded the rise of data management to solve the issues of the time. The duplication of sensitive customer data, for instance, was a major cause for concern.

On a parallel path, information lifecycle management (ILM) was also born. In fact, ILM solved an even older problem than contemporary data management initiatives. That's because ILM could be applied to all types of records from microfiche to film.

However, this definition of ILM became too broad for the digital resources of today. In fact, in 2004, it was decided by the Storage Networking Industry Association (SNIA) that ILM's definition needed to be reevaluated. Now, ILM it refers to a policy, process and practice-driven approach to aligning the worth of business information with appropriate IT tools, systems and infrastructures for the useful life of a piece of data.

But what exactly does this mean and how is this process different from DLM?

Benefits of DLM for Enterprises

There are a number of reasons why an enterprise corporation would want to implement DLM processes. These are as follows:

a. Compliance and Governance: Each industry sector has its own stipulations for data retention and implementing a sound DLM strategy helps businesses remain compliant.
b. Data Protection: In the grand scheme of data protection, DLM and ILM have their own role. A good DLM strategy offers redundancy that can ensure data stays safe in the event of an emergency. It also helps to ensure that customer data is safeguarded from being duplicated in different parts of a data infrastructure, where security may be a concern.
c. ILM Strategy: At the foundation of ILM is DLM. For enterprises to fully actualize an ILM strategy that keeps data current and secure, they must first have a working DLM strategy that pulls data through the lifecycle.
d. Efficiency: At the crux of every IT solution is greater efficiency. When DLM and ILM are properly implemented in tandem, useful data is clean, accurate and readily available to users. Automation helps drive this process. All of this helps businesses achieve greater agility and efficiency.

3.4 Document Management System

Tracking and storing electronic documents and/or images of paper documents, keeping track of the different versions modified by different users, and archiving as needed. A document management system (DMS) is technology that provides a comprehensive solution for managing the creation, capture, indexing, storage, retrieval, and disposition of the records and information assets of an organization.

DMS Features

a. Create, Review and Approval

When a document is created, it may be sent to review and approval. After reviewing the document is reviewed either digital signature is used to approve it.

b. Searching Indexing of Documents

Quickly find documents with instant searches, advanced searches, and saved searches and Full-text indexing of file content, including scanned paper files, returns instant search results.

c. Version Control Management

Find the latest version, view and promote prior versions, and capture a record of every change.

d. File Types Management

Different type of file required type of action or operation.

e. Alerts/Notification Management

A change in document should be notified.

f. Backup/Recovery

All document should be Backed up periodically and recovered/restore when needed.

g. Reports/Analytics

Different type of Activity/Tracking report should be provided.

Document Management Best Practices

Document management systems are undoubtedly helpful in simplifying the creation, revision, and storage of official files. However, you should not expect these software solutions to automatically know how you want your documents to be organized. It is important that you put in some time to understand how to make these platforms work for you.

One thing you can do to make the most out of its features is through the use of document management best practices. With these, you can fine-tune your digital filing process while maximizing your new software.

Follow a Naming Convention. Document organization starts from the moment you name your files. With a disorganized naming system, it will be difficult to sort and archive your documents. This is why it is important that you follow a naming convention. As you build your naming scheme, consider how you would like to retrieve your files later on. You might want to start file names according to when they were created. In such case, you can add date stamps or version numbers to filenames to make them easier to track. You can also choose to organize documents based on their content category. Furthermore, you should try to set limitations on character counts and special characters for easier searching in the future.

Formulate a File Retention Policy. No matter how important a particular piece of document is to you now, there's a chance that you won't need the file after a few months or years. With

that said, you need to come up with a file retention policy. You can set maturity dates for certain files as well as create a guideline for determining when a particular file should be deleted. This allows you to keep your database free from any unnecessary files

Create an Indexing System. Just because your documents are now digital, and you can simply search the files you need doesn't mean you no longer require an indexing system. There will be times when you need to scan documents for a particular topic rather than search for specific files. By creating an index for your digital database, it is easier for you to handle this task.

What are the features of document management software?

What does document management software do? Getting to know its paramount features can help you understand what the software can do for your business. Get to know some of the examples below:

a. Document storage. Archive your files in a single vault for easy retrieval, storage, and sharing for future use. Centralizing this process ensures relevant information is immediately accessible when needed.
b. Security and access control. Avoid unauthorized access by implementing role-based permissions for file entry. Some software programs also restrict IP addresses. This ensures only the right people can open, view, and modify certain files.
c. Version control. Stay in control of your document's versions without having to maintain multiple copies of a single document. It lets you see all the versions made and alerts every member of the most up-to-date version.
d. Indexing and classification. Index files systematically for a quick, easy retrieval later on given its file key.
e. Bulk upload. In most cases, documents come in bulk. Uploading them one by one is time-consuming. With the software, you can upload everything in one go more efficiently.
f. PDF document editor. Applying adjustments and modifications to a PDF file is made simpler. Add text, textbox, date, and check bar for customizations. You can also make notes and eliminate typo errors with an online spell checker.
g. White labelling. Define your company's branding by setting up its color, theme, and logo to ensure it conveys your brand's look and feel effectively. Doing so makes your company appear more professional.
h. Mobile apps. Access your files even when you are using a tablet or mobile device. This also simplifies image capture of documents and quick uploads.
i. File synchronization. Sync online files with the copies of documents stored in your system. This is essential in updating your team with the latest documents.
j. Audit trail. Referring to a document's path in its lifecycle, this feature lets users pull detailed reports on the path that the file has followed. This contains the name of the user, date and time the file was accessed, the type of action performed, and keeps comments from the user.

What are the types of document management software?

How does document management software work? This is one of the first questions you must answer as this can determine what type of software you need. The factors you'll have to consider are how you want to use the system and how your IT network structure is designed. Here are two common types you must consider:

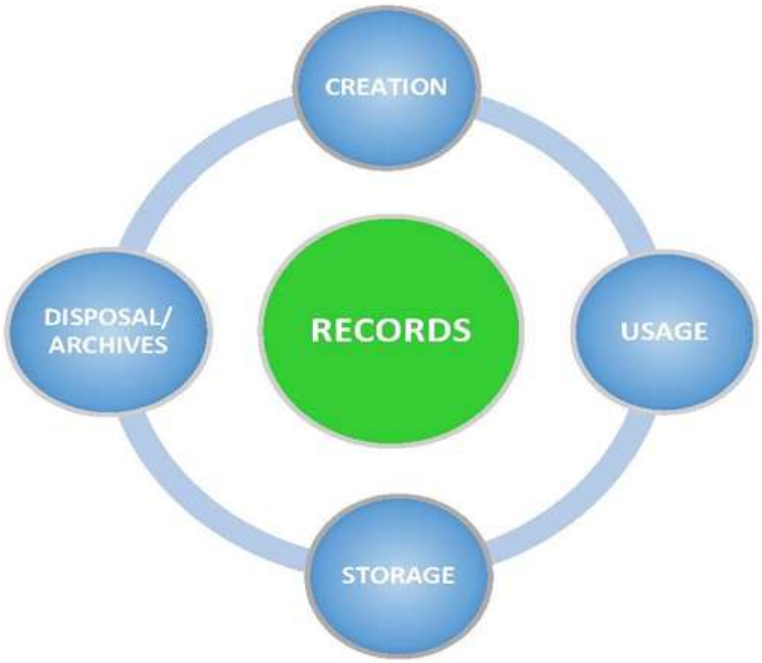
1. Cloud-based
2. Self-hosted

No type is better than the other. The key to choosing which one suits your business is understanding your requirements first and knowing which are your priorities and available resources.

3.5 Records Archiving System

Maintaining the records of an organization from the time they are created up to their eventual disposal; this may include classifying, storing, securing, archiving, and destroying records. Records management knows what you have, where you have it, how long you have to keep it and how secure it is.

a) Creation
b) Usage
c) Storage
d) Archiving Policy Management
e) Disposal and Approval



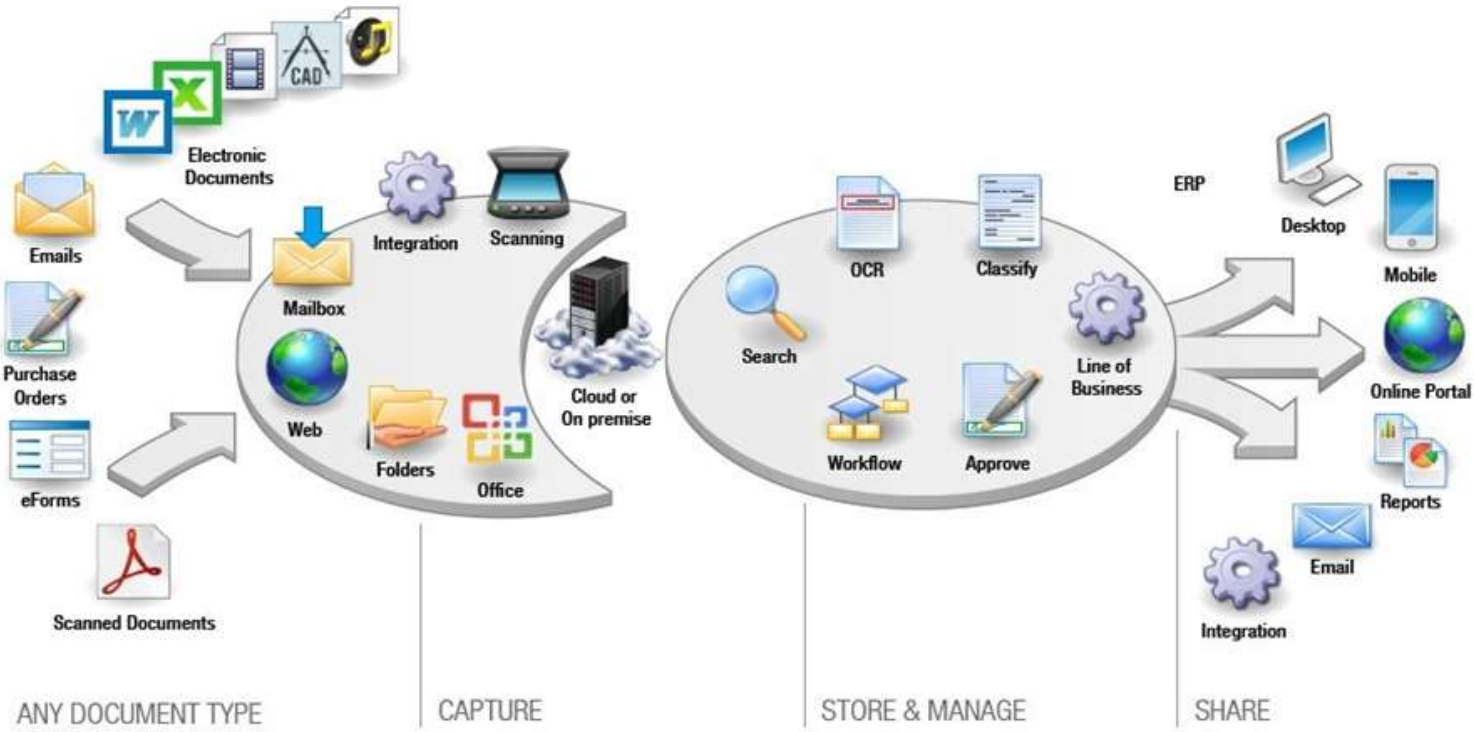
Three types of Records:

1. Record (Database): This is a unique data object structured in a table format. Excel is a well-known application that allows us to manage alphanumeric data in the form of tables, composed of cells - organized in rows and columns. If we take all data relating to a customer (code, name, address, activity ...) that sets fields that contain data that belong to the same entity (client) that is a record.
2. Record (metadata): The word metadata literally means "data that provides information about another data". For example, in a library, the system of records tells us that the book "The Odyssey" by Homer, is on the 2nd floor, shelves VIII shelf D3. Data relating to the location of the book would be collected as a record in the library.
3. Record (file): is a set of documents that are produced and received in the same process in the logical sequence of resolution of the matter. The file itself, has a probative value, so in the management of records in paper support was established the requirement of paginating dossiers. The idea is that by consecutively numbering the document; no one can misrepresent the sequence or include document posteriori. The implementation of the

electronic file can take shape in different ways; all with the intention that the links between the documents are not lost and cannot be included later.

3.6 Process, Policies and Procedures

Process: The ideal information lifecycle management process provides an easy method for content to be reviewed, with the reusable content preserved and the other content archived on suitable media. For example, at the end of a project, all documents in the project team space are listed, the user checks boxes for the reusable ones, and then clicks on an archive button. The result is that the reusable documents are extracted from the team space and stored in the appropriate repository using the associated metadata, and all other documents are archived to a CD which is then stored in the specified archive library.



Policy: defines the policy for how the organization's business records are to be managed

Procedure: details the steps to follow in support of the records management policy's archiving rules

a. Records Inventory and Classification

The purpose of a records inventory is to identify and quantify all records created or maintained by your department or office. The records inventory is used to collect information about your records including type, date range, format, volume, storage location, and applicable records series information.

The inventory is not intended to be an individual folder or document-item list, but rather an examination of groups of similar or related records referred to as a records series. Staff familiar with the creation and maintenance of the records should complete the inventory form. The information gathered during the inventory process will assist in the identification of any records not currently covered by an existing retention schedule and provides a department or office with a comprehensive list of their records.

Before beginning an inventory, a department or office should identify all possible storage locations, including but not limited to:

- On-site: private offices, closets, and records storage rooms, desktop hard drives, and shared network drives
- Off-site: record centers, commercial warehouses, and vacant buildings on campus.

b. Retention Scheduling

The records manager will research state and federal requirements, professional best practices, and policies set by peer institutions to draft the new/updated schedule and/or records series.

The following individuals and departments may be offered opportunity to review and comment on the draft schedule:

- The appropriate office(s) or department(s) may review to identify incomplete or missing series and potential conflicts with business practice.
- The University archivist may review to identify records requiring transfer to the Archives.
- General Counsel may review to identify issues of regulatory compliance.
- The records manager maintains the approved schedule on the records management website.

c. Records Storage and Conversion

Records should be stored in conditions that are clean and secure, with low risk of damage from fire, water, dampness, mold, insects and rodents. They should also be kept away from direct sunlight and other sources of light and heat. The storage area should be well ventilated and ideally maintained at a stable temperature and humidity. Records in non-paper formats such as photographs, maps or computer disks require specialized storage conditions and handling process that take account of their specific physical and chemical properties. Irrespective of format, records of continuing value require higher quality storage and handling to preserve them for as long as that value exists.

An electronic conversion of paper records is more than just scanning documents with a multifunction printer. To successfully convert paper records to electronic documents, specialized knowledge and equipment, detailed processes, and special software are required. Professional scanning and imaging services use trained technicians to ensure quality throughout every step of the conversion. Scanning is just one part of the process; other key procedures include:

- File preparation
- Data entry
- Image output
- Media delivery
- Quality control

Most businesses' records inventories consist of more than just standard size paper records. Your company may have odd size files that can't be scanned with a desktop scanner. In specialized industries, it is common to have large format documents such as:

- Seismic sections
- Arial photos
- Maps
- Blueprints
- Posters
- Mylar and sepia prints
- Books and bound material

d. Vital Records Management Program

What are vital records?

Vital records are those records that are necessary for an organization to continue to operate in the event of a disaster. There are four key areas of risk: Flood; Fire; Security; Infestation/ environmental pollution etc.

How can I identify our vital records?

On average, less than 5% of records are identified as vital. Although losing most records will cause inconvenience, you can often work around or recreate records. Vital records are the ones required in order to operate.

There is no definitive list of vital records and what constitutes a vital record will vary from section to section across the organization. To identify your vital records, you should consider the following:

1) Identify the key functions, business processes and stakeholders of your department e.g. teaching and research, student registration and administration, handling accounts etc.
2) Identify the impact of not providing these key functions
3) Identify the records needed to support or document these functions and processes. The summary report of the information survey of your department may help with this.
4) Identify which of these records are vital i.e. Can the functions these records relate to be re-established in the event of the loss of these records? If so, the record is not vital. Also consider that records can be vital for varying lengths of time. e.g., a current student record of marks is vital as the information is needed to know whether a student can graduate whereas records of a student's marks 20 years ago are less important.
5) Identify how long you can carry out these key functions without the records

Identifying Vital Records: It can be difficult to divide records into vital and non-vital. Some records might not be strictly vital as the organization could function without them, but the effort in replacing them or their historical value might be such that they should be given the same level of protection as records essential to the business of the organization. You will need to perform a risk assessment to decide how vital the record is, considering how serious the impact will be if the record were lost, and how soon you would feel it.

The best approach is to divide records into the following four categories:
Vital: records without which the organization cannot function. These records are essential to the core business of the organization. *Important:* records important to the continued operation of the organization, they can be recreated from original sources but only at considerable time and expense

Useful: records which, if lost, would cause temporary inconvenience but are replaceable.
Non-essential: Records which have no value beyond the immediate purpose

How to Protect Electronic Vital Records

- Electronic vital records must be stored on central servers so that they are protected by appropriate back-up and disaster recovery.
- Do not store vital records on portable hardware, such as USBs, DVDs/CDs
- Do not store vital records on a laptop hard drive or on your personal hard drive
- For vital records that need to be retained for a long time, use a readable format such as PDF/PDFA or plain text or rich text format.

How to Protect Hard Copy Vital Records

Vital Records which are only available in paper format should be duplicated, in the same or original format depending on requirements, and the originals and copies stored in separate locations if possible. There are several ways of doing this:

- Scan and save electronically
- Off-site storage: Copies may be stored with our off-site storage provider who specialize in secure storage.
- Store in another Organization building: This offers the least protection due to the close proximity of the buildings, so it is important to weigh up the risk of losing the records against the cost of storing elsewhere.

e. Disaster Prevention and Recovery

Disaster Prevention and Recovery is a contingency plan put in place to retrieve electronic records in case they are lost, destroyed, or compromised in any way. Depending on the type of business, a disaster recovery plan may differ drastically.

For example, a smaller business with a handful of employees may have a simple disaster recovery plan of a sole backup of electronic information. Their computer software may have a built-in backup system, or they may use an external hard drive which they update every night.

f. Disposal Policy

Disposal a range of processes associated with implementing appraisal decisions. These include the retention, deletion or destruction of records in or from record keeping systems. They may also include the migration or transmission of records between record keeping systems, and the transfer of custody or ownership of records.

3.7 Data Retrieval Management

Some of the key issues involved with retrieving data from archives, such as data security, indexing and searching, and data retention.

a. Meta Data Policy

- Overview of the various metadata captured by archivists and records managers.
- Overview of archival description techniques.
- Overview of Encoded Archival Description (EAD).
- Overview of ISO Records Management Metadata.
- Automated Metadata Extraction.
- Applying Records Management Models to Non-bureaucratic Environments.

Archivists and records managers have always been metadata experts. Archivists create finding aids, file lists, inventories, registers, catalog records, calendars of correspondence, published repository guides, and file plans. Records managers also capture metadata about their organization's records in their records systems and related tools.

All of these products of description contain recordkeeping metadata - descriptive information about the content, context and form of records.

This type of metadata has long been used by researchers to identify, locate and interpret records. Although archivists and record managers have always been in the business of metadata, only recently have they begun to work together to develop standards and tools that ensure the appropriate metadata is captured and maintained across time and domain.

The purpose of this installment is to provide an introduction to archival metadata and its potential in supporting the preservation and reuse of digital data and information. It will then explain some of the ways in which archival metadata may be able to support preservation requirements, highlight a number of key initiatives, and review prospects for the future.

b. Indexing for Searching

An archive can eventually contain hundreds of gigabytes or more spread out across hundreds of millions of unique files. Retrieving important data months or years later would be problematic at best, so powerful indexing and searching capabilities are an essential element of many archive platforms.

Indexing basically generates metadata details about each file and possibly the contents of the file, and then organizes those details into a database or repository of some sort with indices that can be efficiently searched at a later date. Metadata may include details like a filename, description, creator, creation date, key search words, and many other items that are often customized to meet the unique needs of each company. The index may be stored on the archive along with the data.

Search tools are actually used to locate the data for retrieval. Depending on the actual search tool, searches can utilize the metadata indexes or even "look inside" some files, such as documents or .PDF files, to perform deeper contextual searches of file content. For example, a healthcare provider might search for records based on patient name, provider ID and dates of service. Similarly, broader searches might be performed for all patients sharing the same illness/diagnosis or prescribed drugs. In many cases, search results are displayed by relevance in a Web browser-based display similar to Google.

c. Data Retrieval Approaches

As you design your archival system, remember that over time, the archives will probably grow to a monolithic size. So, you need an efficient way of retrieving data from the archives should the need arise.

It might be simple to dump your archive data to tape, for example, but how well are your tapes indexed? If you aren't sure, ask yourself how much work would be involved in locating and retrieving a file that was archived three years ago. If you don't even know where to begin, it's time to consider a different method for archiving your data. Many commercial archival products provide a Web interface that simplifies the task of searching the archives for data.

3.8 Data Archiving Security and Risk Management

Digital preservation is not simply about risks. It also creates opportunities and by protecting digital materials it means that new or extended value can be derived from them. It can be easy to become overwhelmed with risks, so It is worth being explicit early in the process about what opportunities are being protected or created. There are many things that put your digital resources at risk including changes to your organisation or technology. If not managed, these risks will have a significant impact on your ability to carry out your digital preservation activities, wider business functions, or comply with legislation.

To manage digital preservation, you must understand your organization's specific issues and risks. You can do this by undertaking a risk and opportunities assessment. The assessment will highlight specific risks to the continuity of your digital resources, and opportunities that can be realized from mitigating these risks.

Risk management

Experience shows that the risks facing digital resources are subtle and varied. They include, but are not limited to the following:

- Merger, closure, or transfer of functions between organizations.
- Changes in strategic direction or funding and the functions supported by an organization.
- Major changes in individual leaders or experts.
- Outsourcing with no consideration of future preservation needs.
- File format obsolescence meaning that it is expensive or impossible to process data.
- Media obsolescence making it expensive or impossible to recover data.
- Media degradation meaning that data is damaged or changed.
- Loss of contextual information resulting in loss of meaning.
- Breakdown of resource discovery data resulting in difficulty retrieving data.
- Loss of copyright or other legal information resulting in uncertainty over rights and obligations.
- Loss of provenance information or fixity about a document resulting in loss of authenticity.
- Breakdown of version control making it hard to identify authoritative instances of a document.
- Human error leading to accidental deletion.
- The degree of use. A dark archive is more at risk than one than is heavily used. If digital material is accessed infrequently the impact of failure is less immediately apparent.
- Natural Disasters affecting buildings or infrastructure.

Data loss is likely to have a variety of real-world consequences depending on context. In the context of a court case, for example, the authenticity of a document could become a significant legal issue; whereas for highly structured research data the chain of custody may matter less than access to explanatory context that enables the reproducibility of an experiment. In many contexts it may be technically possible to recover digital collections but where an organization simply doesn't have the wherewithal or skills necessary to restore a data set, then practical obsolescence and data loss can result. This is likely to become more of a reality as the number and complexity of digital collections expand.

The risks to digital content usually matter because of their consequences in the real world. Again, this depends on the context, but the following can occur:

- Loss of reputation.
- Inadequate resources for a critical task.
- Inability to support users in their activities.
- Failure to discharge legal or regulatory function.
- Inability to exploit and reuse data.
- Loss of identity and corporate memory.
- Cost of recreation and recovery.

Risks are typically prioritized by calculating a 'risk score' based on likelihood, impact and imminence: an imminent risk with a strong probability and a large negative impact needs prompt action. Depending on the nature of the risk this might include taking steps to reduce

the likelihood of a risk emerging, reducing the impact if a risk does occur, or buying time for mitigation steps to be implemented.

Risk assessment is an ongoing process that can be developed and expanded through time. It can help bring together different stakeholders and, because risk management is understood by senior management it can also help to make the case for investment. Even an elementary risk assessment will highlight priorities for anyone getting started in digital preservation.

Finally, it is worth noting that digital preservation is distinctive in being long-term and most risk methodologies are typically focused on the short-term. For digital preservation, you need to be aware that over the long-term improbable events will become more likely and special attention should be paid to those with significant consequences.

3.9 General Features in Data Archiving Automated Software

It is important to understand that data archiving is not the same as data backup. Data backups provide copies of data in the event of disasters or system failures and are meant to address short-term needs (less than 90 days). Data archiving, however, takes inactive data and moves it to a storage device for long-term retention, freeing up operational storage space and shortening backup windows. Data archiving software should streamline some of the biggest challenges:

Efficiency

Re-Moving infrequently used data from computer hard drives will help systems run faster and make current files easier to locate.

Costs

Automated archiving can help lower future backup and storage costs by reducing administrative overhead.

Flexibility

Must supports several operating systems and platforms such Mac OS X, Windows, VMware, Hyper-V and Windows Server. No matter a company's industry, archiving software is a helpful tool that can help safeguard against a myriad of data issues.

In addition to data archiving solution should have:

- Data backup
- Disaster recovery
- Security and antivirus
- Email protection
- Patch management
- Web protection
- Asset tracking
- Risk and vulnerability assessment

3.10 Cloud Storage Services

A cloud storage service is a business that maintains and manages its customers' data and makes that data accessible over a network, usually the internet.

Most of these types of services are based on a utility storage model. They tend to offer flexible, pay-as-you-go pricing and scalability. Cloud storage providers also provide for unlimited growth and the ability to increase and decrease storage capacity on demand.

[Utility storage is a service model in which a provider makes storage capacity available to an individual, an organization or a business unit on a pay-per-use basis. The utility model is sometimes called metered services or storage on demand.]

Leading use cases for a cloud storage service include backup, disaster recovery (DR), collaboration and file sharing, archiving, primary data storage and near-line storage.

Three types of cloud storage Model:
Public cloud storage
Private cloud storage
Hybrid Cloud Storage

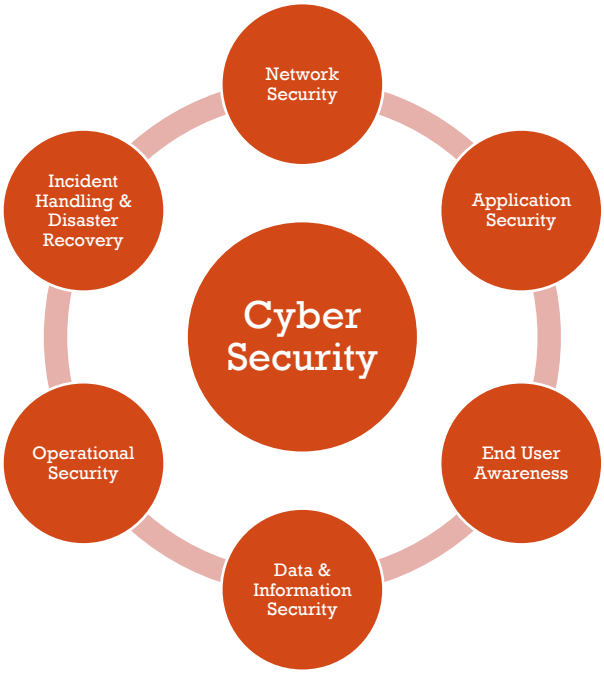
4. CYBER SECURITY

4.1 Introduction to Cyber Security

4.1.1 Defining Cyber Security

Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. Cyber security focuses on protecting computer systems – including hardware, software, data and digital infrastructure – from unauthorized access or being otherwise damaged or made inaccessible. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- Information security protects the integrity and privacy of data, both in storage and in transit.



- Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data.

Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

- End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

4.2 Difference between Information Security & Cyber Security

The terms Cyber Security and Information Security are often used interchangeably. As they both are responsible for security and protecting the computer system from threats and information breaches and often Cybersecurity and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously.

CYBER SECURITY	INFORMATION SECURITY
It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized user, access and data modification or removal to provide confidentiality, integrity, and availability.
It is about the ability to protect the use of cyberspace from cyber-attacks.	It deals with protection of data from any form of threat.
Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Cybersecurity deals with danger against cyberspace.	Information security deals with the protection of data from any form of threat.
Cybersecurity strikes against Cybercrimes, cyber frauds and law enforcement.	Information security strives against unauthorized access, disclosure modification and disruption.

4.3 Confidentiality, Integrity, and Availability (CIA triad)

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security. In this context, confidentiality is a set of rules that limits

access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

The CIA triad is becoming the standard model for conceptualizing challenges to information security in the 21st century. CIA stands for confidentiality, integrity and availability, which are said to be the three most important elements of reliable security. Every IT worker should have a thorough understanding of the triad and its intricacies, but every staff member who works around sensitive data should at least be made aware of the concept.

4.4 Common Cyber Security Terms

1) Adware
2) Botnet
3) Clickfraud
4) Cyber Espionage
5) Dark Web
6) Defense-in-Depth
7) Demilitarized Zone
8) Detection Deficit
9) Easter Egg
10) End-to-End Encryption
11) Evil Twin
12) Exploit Kits
13) Firewall
14) FTP
15) Gateway
16) Guessing Entropy
17) Hashing
18) Handshaking Procedures
19) Identity Theft
20) IDS
21) IP Spoofing
22) Keylogger
23) Macro Virus
24) Malware
25) Mobile Banking Trojans
26) One-Way Encryption
27) Open Wi-Fi
28) Password Sniffing
29) Pharming
30) Phishing
31) QAZ
32) Ransomware
33) Reverse Engineering
34) Rootkit
35) Script Kiddie
36) Social Engineering
37) Trojan Horse
38) Vishing
39) Zero-Day
40) Zombie Computer
41) Spam
42) Spyware
43) Hacker
44) Denial-of-Service Attack
45) Encryption
46) Exploit

4.5 Types of Hackers

There are many definitions for "hacker". In the early 1990s, the word "hacker" was used to describe a great programmer, someone who could build complex logics.

1) WHITE HAT HACKER

First up, we have the perfect type of hacker to break the stereotype. The white hat hacker is a good guy, as ironic as it may sound. White Hackers, white hat hackers or ethical hackers are

the people who test existing internet infrastructures to research loopholes in the system. They create algorithms and perform multiple methodologies to break into systems, only to strengthen them. Think of this as a lockpick, who would work his way around locks, only to inform the owners of how to make the locks work better.

2) BLACK HAT HACKER

Simply put, these are the bad guys. Black hat hackers are responsible for all that is wrong with hacking. These guys break into systems purely with negative intentions. From stealing credit card information, to altering public databases, a black hat hacker looks to gain fame or monetary benefits from exploiting the loopholes in internet frameworks. Famous black hat hackers have notoriously robbed banks and financial institutions of millions of dollars, and invaluable private data.

3) GREY HAT HACKER

A grey hat hacker usually has mixed intentions. As the color code implies, this hacker type does not have the good intentions of a white hat hacker, nor does he have the ill intentions of a black hacker. A grey hat would break into systems but never for his own benefit. Famous grey hat hackers have exploited systems only to make the information public, and to bring to limelight vast datasets of information that contains wrongdoings. This hacker type is the most commonly found type on the internet. The most common break-ins usually are of the back and grey hat type, but since there are no major personal gains with grey hats, black hats take the crown for being the real bad guys.

4.6 The Hacking Methodologies

Although there is no specific step-by-step methodology used by all hackers, a typical hacking process comprises of the following steps:

Step 1. Recon

Reconnaissance is the most important step of the process and can be broken down into two sub-phases, active and passive. During this phase, our primary goal is obtaining as much information about SillyVictim as possible. We are searching for vulnerabilities or weaknesses that we can use in later steps to gain access to the internal corporate network.

- Phase 1: Passive
    - Passive reconnaissance is what occurs when you don't interact with the target. This is done by viewing the webpage, searching google, looking at social media for information on employees. In short, you're looking for any information that can be used to leverage against your target. This is the only step that is not illegal. Anything past this step can be considered a crime.

- Phase 2: Active
    - Active reconnaissance is the step you use when you actively are probing your target. Let's hypothetically say that SillyVictim is hosting their own DNS server and that when we did our who is lookup, we discovered the IP address to that

server. So now we're going to take information from our passive recon and use that to feed into our active recon. Because we know the IP address of one server inside of our targets network, we could scan against it using nmap, zenmap or any other scanning tool you wish. Scanning this server will reveal open ports and services (server applications) that the server uses to communicate.

Step 2. Exploitation

Exploitation is defined as using a vulnerability identified during by our recon phase and using it to gain access to the intended machine. We have a TON of ports and services available. Each of these services are potential entry ways into our victim's network because they are open lines of communication to the outside world. A popular framework for exploitation is Metasploit. Metasploit is too large of a topic to cover here and will be covered in future lessons. Another method would be sending a phishing email to one of your targets identified during the recon phase that had a call back to a listener you had running on your attack box.

Step 3. Privilege Elevation

Great so we now have access through our box after searching for vulnerabilities and exploiting one of them to give us a shell. From here we could skip to data extraction and poke around on whatever user account our vulnerability has given us. But that's not the point, we want super user, we want the ability to do whatever we want in this environment. So, we figure out a way to elevate our privileges. This could include a wide variety of things; we could create new user accounts, or we could even do this during the exploitation phase by using an exploit that would drop us into the machine with elevated rights.

Step 4. Establish Persistence

At this point we would drop in a backdoor or Remote Access tool. This allows us persistence in the machine, or the ability for us to come and go as we please in the event we get disconnected from our victim. A common and easy to use backdoor can be created using NETCAT. Persistence also allows us something else. It allows us to tunnel our traffic through the machine deeper into the victim's network and serve as a lifeline to pass information through back to our attacker box. This way we can exploit the inherent trust that all machines on the same network share, while sending commands from our attack box.

Step 5. Extract Data

Now that we have established persistence let's get to the real stuff, data ex filtration. This is the point where you set up tunnel to your attack platform or to a dead drop on some server that you will be using as an intermediary. You pull off any data that you may consider important. Usually in a *nix system this will comprise of at LEAST the /etc./shadow and /etc./passwd files, in Windows it will be the SAM file and registry. E-mails are often good to go for as people send out lots of information such as passwords, phone numbers etc.

Step 6. Cover Your Tracks

The big one, how not to get caught. We could spend forever talking about covering your tracks and ways to do this but for this lesson it means system log and tool clean-up. You need to

restore the machine back to the way you found it. If you exploit a vulnerability in a machine you want that vulnerability to stay there so you may use it again later. If a savvy system admin finds presence of a breach, he/she is likely to go into panic mode and either pull the server offline or begin going through vulnerability remediation. As a hacker or penetration tester you do not want this to happen. It's important to note that the absence of logs is just a fishy as the presence of odd things in them. The trick is to adjust the logs so that normal events are listed, and your actions are not.

Wrap Up

We've gone over the high points of hacker methodology process. It's important to note that each phase of this methodology is much deeper than described here. The recon phase could take weeks or even months. Exploitation could require custom tools to be developed, or physical access to the system it requires DEEP knowledge of how computers and the internet works. Data extraction could take days get out the information that you want to trickle out. I've oversimplified this process to get your brain thinking logically and systematically.

4.7 The Threat and Vulnerability Landscape

4.7.1 Privacy, Anonymity and Pseudosymmetry

Privacy

In general, the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed. In specific, privacy may be divided into four categories (1) Physical: restriction on others to experience a person or situation through one or more of the human senses; (2) Informational: restriction on searching for or revealing facts that are unknown or unknowable to others; (3) Decisional: restriction on interfering in decisions that are exclusive to an entity; (4) Dispositional: restriction on attempts to know an individual's state of mind.

Information privacy

Information privacy is considered an important aspect of information sharing. With the advancement of the digital age, personal information vulnerabilities have increased. Information privacy may be applied in numerous ways, including encryption, authentication and data masking - each attempting to ensure that information is available only to those with authorized access. These protective measures are geared toward preventing data mining and the unauthorized use of personal information, which are illegal in many parts of the world.

Anonymity

Anonymity is derived from the Greek word ἀνωνυμία, anonymia, meaning "without a name" or "namelessness". In colloquial use, anonymity typically refers to the state of an individual's personal identity, or personally identifiable information, being publicly unknown. There are various situations in which a person might choose to withhold their identity.

4.8 Threat Modelling and Risk Assessment

Threat modeling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. In this context, a threat is a potential or actual adverse event that may be malicious (such as a denial-of-service attack) or incidental (such as the failure of a storage device), and that can compromise the assets of an enterprise. The key to threat modeling is to determine where the most effort should be applied to keep a system secure. This is a variable that changes as new factors develop and become known, applications are added, removed, or upgraded, and user requirements evolve. Threat modeling is an iterative process that consists of defining enterprise assets, identifying what each application does with respect to these assets, creating a security profile for each application, identifying potential threats, prioritizing potential threats, and documenting adverse events and the actions taken in each case. Threat modelling helps to achieve following:

- Defines security of application
- Identifies and investigates potential threats and vulnerabilities
- Results in finding architecture bugs earlier

4.9 Defense

Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack. This multi-layered approach with intentional redundancies increases the security of a system and addresses many different attack vectors. Defense in Depth is commonly referred to as the "castle approach" because it mirrors the layered defenses of a medieval castle. Before you can penetrate a castle, you are faced with the moat, ramparts, drawbridge, towers, and battlements and so on. The digital world has revolutionized how we live, work and play. However, it's a digital world that is constantly open to attack, and because there are so many potential attackers, we need to ensure we have the right security in place to prevent systems and networks being compromised. Unfortunately, there is no single method that can successfully protect against every single type of attack. This is where a defense in depth architecture comes into play.

4.10 The Zero Trust Model

Zero Trust, Zero Trust Network, or Zero Trust Architecture refer to security concepts and threat model that no longer assumes that actors, systems or services operating from within the security perimeter should be automatically trusted, and instead must verify anything and everything trying to connect to its systems before granting access. The term was coined by a security analyst at Forrester Research. The Zero Trust model is the response to the realization that the perimeter security approach isn't working because many data breaches happened because hackers, once they got past the corporate firewalls, were able to move through internal systems without much resistance. And because the perimeter itself is no longer clearly defined, because applications and data stores are on-premises and in the cloud, with users

accessing them from multiple devices and locations. Zero Trust is a general approach that calls for enterprises to leverage micro-segmentation and granular perimeter enforcement based on users, their locations and other data to determine whether to trust a user, machine or application seeking access to a part of the enterprise. Zero Trust draws on technologies such as multifactor authentication, IAM, orchestration, analytics, encryption, scoring and file system permissions. Zero Trust also calls for governance policies such as giving users the least amount of access they need to accomplish a specific task.

4.11 Trust and Backdoors

A backdoor refers to any method by which authorized and unauthorized users can get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application. A backdoor is a technique in which a system security mechanism is bypassed undetectably to access a computer or its data. The backdoor access method is sometimes written by the programmer who develops a program. Backdoor threats increase when multiuser and networking operating systems are used by many organizations. In a login system, a backdoor used for system access may be in the form of a hard-coded username and password. A network administrator (NA) may intentionally create or install a backdoor program for troubleshooting or other official use. Hackers use backdoors to install malicious software (malware) files or programs, modify code or detect files and gain system and/or data access. Even backdoors installed by network administrators pose security risks because they provide a mechanism by which the system can be exploited if discovered.

4.12 Censorship

According to Webster's Dictionary, to "censor" means "to examine to suppress or delete anything considered objectionable." The word "censor" originated in ancient Rome, where the government appointed officials to take the census and to supervise public morals. Censorship happens whenever some people succeed in imposing their political or moral values on others by suppressing words, images, or ideas that they find offensive.

Internet censorship puts restrictions on what information can be publicized or viewed on the Internet. Governments and other organizations commonly use internet censorship to block access to copyrighted information as well as to harmful or sensitive content. However, internet censorship can also be used as a propaganda method to promote specific religions and political agendas.

4.13 Encryption

Introduction to Encryption

In its most basic form, encryption is the process of encoding data, making it unintelligible and scrambled. In a lot of cases, encrypted data is also paired with an encryption key, and only those that possess the key will be able to open it. An encryption key is a collection of algorithms

designed to be totally unique. These can scramble and unscramble data, essentially unlocking the information and turning it back to readable data. Usually, the person that is encrypting the data will possess the key that locks the data and will make 'copies' and pass them on to relevant people that require access. This process is called public-key cryptography. Encryption is the process of helping protect personal data by using a "secret code" to scramble it so that it cannot be read by anyone who doesn't have the code key.

Why is encryption necessary?

Privacy:

Encryption ensures that no one can read communications or data at rest except the intended recipient or proper data owner. This prevents cyber criminals, ad networks, Internet service providers, and in some cases governments from intercepting and reading sensitive data.

Security:

Encryption helps data breaches, whether the data is in transit or at rest. If a corporate device is lost or stolen and its hard drive is properly encrypted, the data on that device will likely still be secure. Similarly, encrypted communications enable the communicating parties to exchange sensitive data without leaking the data. Encryption also helps prevent malicious behavior such as man-in-the-middle attacks.

Authentication:

Public key encryption, among other things, establishes that a website's origin server owns the private key and therefore was legitimately issued an SSL certificate (see What is public key encryption? to learn more).

Regulations:

For all these reasons, many industry and government regulations require companies that handle user data to keep that data encrypted. Examples of regulatory and compliance standards that require encryption include HIPAA, PCI-DSS, and the GDPR.

How does encryption work?

In practice, when we send a message using an encrypted messaging service (WhatsApp for example), the service wraps the message in code, scrambling it and creating an encryption key. It can then only be unlocked by the recipient of the message.

Unencrypted data, often referred to as plaintext, is encrypted using an encryption algorithm and an encryption key. This process generates ciphertext that can only be viewed in its original form if decrypted with the correct key. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied. Today's most widely used encryption algorithms fall into two categories: symmetric and asymmetric. Digital encryption is extremely complicated and that's why it is considered difficult to crack. To

bolster that protection, a new set of encryption algorithms is created each time two smartphones begin communicating with one another.

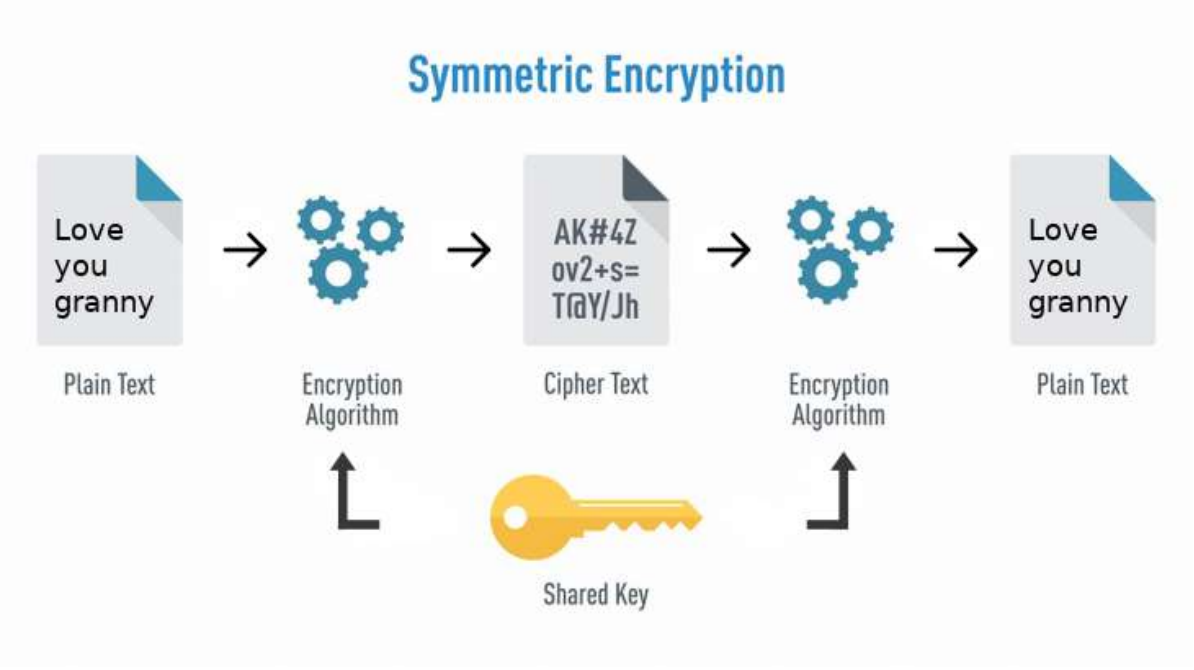
End-to-end encryption refers to the process of encoding and scrambling some information so only the sender and receiver can see it. As previously explained, encryption keys can work as a pair, one locking the information and multiple (which can be passed out) to unlock the encrypted information. With end-to-end encryption, however, only the sender and recipient are able to unlock and read the information. With WhatsApp, the messages are passed through a server, but it is not able to read the messages.

4.14 Symmetric/Asymmetric Encryption

Cryptography is the art of encoding and decoding secret messages. Cryptographic techniques have been used for thousands of years, well before the introduction of computers, and the techniques have evolved since.

Symmetric encryption

In symmetric encryption, you use the same key for both encryption and decryption of your data or message. Taking the example, I gave above, sending a secure message to your granny, both of you need to have the same key to encrypt and decrypt the messages that you may exchange with each other.



Asymmetric encryption

Asymmetric encryption is quite the opposite of the symmetric encryption as it uses not one key but a pair of keys: a private one and a public one. One might ask:

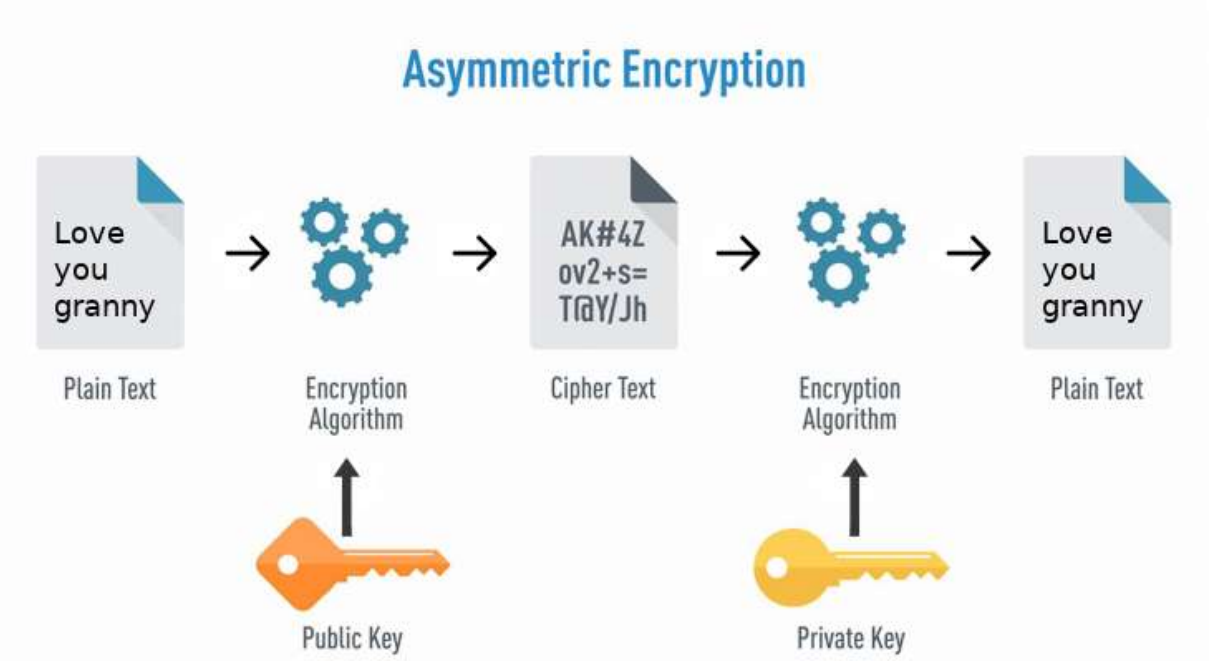
We use one to encrypt our data, which is called public key, and the other to decrypt the encrypted message, which is called the private key. When we encrypt our message using, let's say, your granny's public key, that same message can only be decrypted using her private key.

Private keys

Our private key, as the name states, is ours and it must be kept private, as it's the only key that can decrypt any messaged that was encrypted with your public key.

Public keys

Public keys as, yet again, the name states, are public and thus no security is required because of it should publicly available and can be passed over the internet. The public key is used to encrypt a message that can only be decrypted using, as written above, its private counterpart.



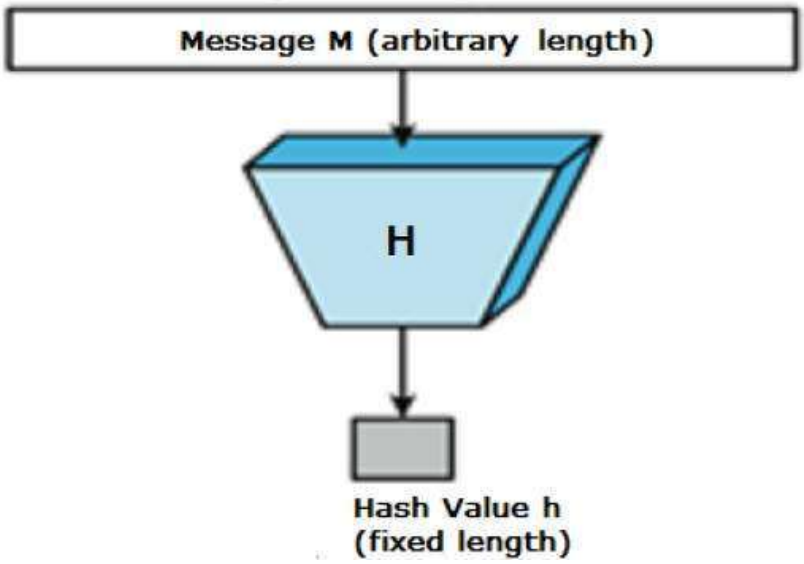
Hybrid systems

In many applications, symmetric and asymmetric encryption are used together. Typical examples of such hybrid systems are the Security Sockets Layer (SSL) and the Transport Layer Security (TLS) cryptographic protocols, which were designed to provide secure communication within the Internet. The SSL protocols are now considered insecure and its use should be discontinued. In contrast, the TLS protocols are deemed safe and have been extensively used by all major web browsers.

4.15 Hash Function

A hash function takes a group of characters (called a key) and maps it to a value of a certain length (called a hash value or hash). The hash value is representative of the original string of characters but is normally smaller than the original. Hashing is done for indexing and locating items in databases because it is easier to find the shorter hash value than the longer string. Hashing is also used in encryption. This term is also known as a hashing algorithm or message digest function.

Hash functions are extremely useful and appear in almost all information security applications. A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length. Values returned by a hash function are called message digest or simply hash values. The following picture illustrated hash function-



Popular Hash Functions

- ✓ Message Digest (MD)
- ✓ Secure Hash Function (SHA)
- ✓ RIPEMD
- ✓ Whirlpool

5. DATABASE MANAGEMENT

5.1 Introduction

Before we start let's understand -

- ✓ What is Data?
- ✓ What is a Database?
- ✓ What is a Database Management System (DBMS)?

What is Data?

In simple words data can be facts related to any object in consideration. For example, your name, age, height, weight, etc. are some data related to you. A picture, image, file, pdf etc. can also be considered data.

What is a Database?

Database is a systematic collection of data. Databases support storage and manipulation of data. Databases make data management easy. Let's discuss few examples. An online telephone directory would definitely use database to store data pertaining to people, phone numbers, other contact details, etc.

Your electricity service provider is obviously using a database to manage billing, client related issues, to handle fault data, etc. Let's also consider the Facebook. It needs to store, manipulate and present data related to members, their friends, member activities, messages, advertisements and lot more. We can provide countless number of examples for usage of databases.

What is a Database Management System (DBMS)?

Database Management System (DBMS) is a collection of programs which enables its users to access database, manipulate data, reporting / representation of data. It also helps to control access to the database. Database Management Systems are not a new concept and as such had been first implemented in 1960s. Charles Bachmen's Integrated Data Store (IDS) is said to be the first DBMS in history. With time database technologies evolved a lot while usage and expected functionalities of databases have been increased immensely.

Types of DBMS

Let's see how the DBMS family got evolved with the time. Following diagram shows the evolution of DBMS categories. There are 4 major types of DBMS. Let's look into them in detail.

Hierarchical - this type of DBMS employs the "parent-child" relationship of storing data. This type of DBMS is rarely used nowadays. Its structure is like a tree with nodes representing records and branches representing fields. The windows registry used in Windows XP is an

example of a hierarchical database. Configuration settings are stored as tree structures with nodes.
Network DBMS - this type of DBMS supports many-to many relations. This usually results in complex database structures. RDM Server is an example of a database management system that implements the network model.

Relational DBMS - this type of DBMS defines database relationships in form of tables, also known as relations. Unlike network DBMS, RDBMS does not support many to many relationships. Relational DBMS usually have pre-defined data types that they can support. This is the most popular DBMS type in the market. Examples of relational database management systems include MySQL, Oracle, and Microsoft SQL Server database.

Object Oriented Relation DBMS - this type supports storage of new data types. The data to be stored is in form of objects. The objects to be stored in the database have attributes (i.e. gender, ager) and methods that define what to do with the data. PostgreSQL is an example of an object-oriented relational DBMS.

What is SQL?

Structured Query language (SQL) pronounced as "S-Q-L" or sometimes as "See-Quel"is actually the standard language for dealing with Relational Databases. SQL programming can be effectively used to insert, search, update, delete database records.

That doesn't mean SQL cannot do things beyond that. In fact, it can do lot of things including, but not limited to, optimizing and maintenance of databases. Relational databases like MySQL Database, Oracle, Ms SQL server, Sybase, etc. uses SQL.

How to use SQL syntaxes?

SQL syntaxes used in these databases are almost similar, except the fact that some are using few different syntaxes and even proprietary SQL syntaxes. SQL Example:
SELECT * FROM Members WHERE Age > 30

What is NoSQL?

NoSQL is an upcoming category of Database Management Systems. Its main characteristic is its non-adherence to Relational Database Concepts. NOSQL means "Not only SQL".

Concept of NoSQL databases grew with internet giants such as Google, Facebook, Amazon etc. who deal with gigantic volumes of data. When you use relational database for massive volumes of data, the system starts getting slow in terms of response time. To overcome this, we could of course "scale up" our systems by upgrading our existing hardware. The alternative to the above problem would be to distribute our database load on multiple hosts as the load increases. This is known as "scaling out". NOSQL database are non-relational databases that scale out better than relational databases and are designed with web applications in mind. They do not use SQL to query the data and do not follow strict schemas like relational models.

With NoSQL, ACID (Atomicity, Consistency, Isolation, and Durability) features are not guaranteed always.

Why it makes sense to learn SQL after NOSQL?

With the advantages of NOSQL databases outlined above that scale out better than relational models, you might be thinking why one would still want to learn about SQL database?

Well, NOSQL databases are sort of highly specialized systems and have their special usage and limitations. NOSQL suit more for those who handles huge volumes of data. The vast majority use relational databases and associated tools.

Relational databases have the following advantages over NOSQL databases;

- SQL (relational) databases have a mature data storage and management model. This is crucial for enterprise users.
- SQL databases support the notion of views which allow users to only see data that they are authorized to view. The data that they are not authorized to see is kept hidden from them.
- SQL databases support stored procedure SQL which allow database developers to implement part of the business logic into the database.
- SQL databases have better security models compared to NoSQL databases.

The world has not deviated from use of relational databases. There is growing a demand for professionals who can handle relational databases. Thus, learning databases and SQL still holds merit.

5.2 Database Environment

One of the major aims of a database is to supply users with an abstract view of data, hiding a certain element of how data is stored and manipulated. So, the starting point for the design of a database must be an abstract and general description of the information requirements of the organization that is to be represented in the database. And hence you will require an environment to store data and make it work as a database.

What is a Database Environment?

A database environment is a collective system of components that comprise and regulates the group of data, management, and use of data which consist of software, hardware, people, techniques of handling database and the data also. Here, the hardware in a database environment means the computers and computer peripherals that are being used to manage a database and the software means the whole thing right from the operating system (OS) to the application programs that includes database management software like M.S. Access or SQL Server. Again, the people in a database environment include those people who administrate and use the system. The techniques are the rules, concepts, and instructions given to both the people and the software along with the data with the group of facts and information positioned within the database environment.

Components of DBMS

DBMS have several components, each performing very significant tasks in the database management system environment. Below is a list of components within the database and its environment.

Software

This is the set of programs used to control and manage the overall database. This includes the DBMS software itself, the Operating System, the network software being used to share the data among users, and the application programs used to access data in the DBMS.

Hardware

Consists of a set of physical electronic devices such as computers, I/O devices, storage devices, etc., this provides the interface between computers and the real-world systems.

Data

DBMS exists to collect, store, process and access data, the most important component. The database contains both the actual or operational data and the metadata.

Procedures

These are the instructions and rules that assist on how to use the DBMS, and in designing and running the database, using documented procedures, to guide the users that operate and manage it.

Database Access Language

This is used to access the data to and from the database, to enter new data, update existing data, or retrieve required data from databases. The user writes a set of appropriate commands in a database access language, submits these to the DBMS, which then processes the data and generates and displays a set of results into a user readable form.

Query Processor

This transforms the user queries into a series of low-level instructions. This reads the online user's query and translates it into an efficient series of operations in a form capable of being sent to the run time data manager for execution.

Run Time Database Manager

Sometimes referred to as the database control system, this is the central software component of the DBMS that interfaces with user-submitted application programs and queries, and handles database access at run time. Its function is to convert operations in user's queries. It provides control to maintain the consistency, integrity and security of the data.

Data Manager

Also called the cache manger, this is responsible for handling of data in the database, providing a recovery to the system that allows it to recover the data after a failure.

Database Engine

The core service for storing, processing, and securing data, this provides controlled access and rapid transaction processing to address the requirements of the most demanding data consuming applications. It is often used to create relational databases for online transaction processing or online analytical processing data.

Data Dictionary

This is a reserved space within a database used to store information about the database itself. A data dictionary is a set of read-only table and views, containing the different information about the data used in the enterprise to ensure that database representation of the data follow one standard as defined in the dictionary.

Report Writer

Also referred to as the report generator, it is a program that extracts information from one or more files and presents the information in a specified format. Most report writers allow the user to select records that meet certain conditions and to display selected fields in rows and columns, or also format the data into different charts.

5.3 Database Architecture

What Is Database Architecture?

Database architecture uses programming languages to design a particular type of software for businesses or organizations. Database architecture focuses on the design, development, implementation and maintenance of computer programs that store and organize information for businesses, agencies and institutions. A database architect develops and implements software to meet the needs of users.

The design of a DBMS depends on its architecture. It can be centralized or decentralized or hierarchical. The architecture of a DBMS can be seen as either single tier or multi-tier. The tiers are classified as follows:

1. 1-tier architecture
2. 2-tier architecture
3. 3-tier architecture
4. n-tier architecture

1-tier architecture:

One-tier architecture involves putting all of the required components for a software application or technology on a single server or platform.

Basically, a one-tier architecture keeps all of the elements of an application, including the interface, Middleware and back-end data, in one place. Developers see these types of systems as the simplest and most direct way.

2-tier architecture:

The two-tier is based on Client Server architecture. The two-tier architecture is like client server application. The direct communication takes place between client and server. There is no intermediate between client and server.

3-tier architecture:

A 3-tier architecture separates its tiers from each other based on the complexity of the users and how they use the data present in the database. It is the most widely used architecture to design a DBMS.

This architecture has different usages with different applications. It can be used in web applications and distributed applications. The strength in particular is when using this architecture over distributed systems.

- Database (Data) Tier – At this tier, the database resides along with its query processing languages. We also have the relations that define the data and their constraints at this level.
- Application (Middle) Tier – At this tier reside the application server and the programs that access the database. For a user, this application tier presents an abstracted view of the database. End-users are unaware of any existence of the database beyond the application. At the other end, the database tier is not aware of any other user beyond the application tier. Hence, the application layer sits in the middle and acts as a mediator between the end-user and the database.
- User (Presentation) Tier – End-users operate on this tier and they know nothing about any existence of the database beyond this layer. At this layer, multiple views of the database can be provided by the application. All views are generated by applications that reside in the application tier.

n-tier architecture:

N-tier architecture would involve dividing an application into three different tiers. These would be the:

1. logic tier,
2. the presentation tier, and
3. the data tier.

It is the physical separation of the different parts of the application as opposed to the usually conceptual or logical separation of the elements in the model-view-controller (MVC) framework. Another difference from the MVC framework is that n-tier layers are connected linearly, meaning all communication must go through the middle layer, which is the logic tier. In MVC, there is no actual middle layer because the interaction is triangular; the control layer has access to both the view and model layers and the model also accesses the view; the controller also creates a model based on the requirements and pushes this to the view. However, they are not mutually exclusive, as the MVC framework can be used in conjunction

with the n-tier architecture, with the n-tier being the overall architecture used and MVC used as the framework for the presentation tier.

5.4 Relationship – Terminologies and Types

What is a Relationship?

In relational database design, a relationship is where two or more tables are linked together because they contain related data. This enables users to run queries for related data across multiple tables. Relationships are a key element in relational database design.

Primary Key vs Foreign Key

Relationships are achieved using a primary key and a foreign key. In the above example, City. CityId is the primary key, and Customer. CityId is the foreign key.

The primary key is a unique identifier. Because it is unique, the foreign key can reference it, with complete confidence that it is referencing only one record.

So, in a relationship, the foreign key in one table matches the primary key in the other table. That is, any value in the foreign key field should have a matching value in the primary key field in the referenced table. The foreign key and primary key fields should also have the same data type (with a few possible exceptions).

A common convention is to give the foreign key field the same name as the primary key field that it references, but this is not a requirement.

Creating a Relationship

Once you've created the tables, you then need to establish the relationship. Most relational database management systems will allow you to create a relationship via the GUI. However, you can also do it using programmatically using SQL.

Types of Relationships

There are three types of relationships in database design:

- One-to-One: A row in table A can have only one matching row in table B, and vice versa.
- One-to-Many (or Many-to-One): A row in table A can have many matching rows in table B, but a row in table B can have only one matching row in table A.
- Many-to-Many: A row in table A can have many matching rows in table B, and vice versa.

What are the Benefits of Relationships?

Relationships are the basis of any relational database management system (RDBMS). Relationships are a very powerful tool to use in database design.

Here are some key benefits of relationships in database design:

- Reduces storage requirements
- Helps maintain data integrity
- Helps increase usability for end users
- Easier data maintenance
- Helps with security
- Helps with scalability or expansion of the database

These are explained in more detail below.

Reduces storage requirements: Storing an ID is typically more efficient than storing the full text – especially if the text is long.

Helps maintain data integrity: By entering the data once, then referencing that one record, there is less room for error.

Helps increase usability for end users: By creating a relationship, you can now provide users with a widget for selecting the desired option (a drop down/combo box for example). So, instead of having to type the full city name, they simply select the city from the drop-down list. You can do this easily, by populating the drop-down list with the contents of the table.

Easier data maintenance: Updates to data only need to be done in one place. For example, if a city's name changes (yes, it does happen), you can update it once – in the City table.

You won't need to update thousands, or even millions, of records that hold city information, because they only store the CityId. And because the CityId stays the same, you won't even need to look at the Customer table or any other table.

Helps with security: Sensitive data can be stored in a table that has certain privileges applied. When a user logs in, the system provides users with access to only those tables that they're allowed to have access to. For example, a receptionist might be able to see other employees' details but not their salary. However, the pay clerk would have access to their salary.

Helps with scalability or expansion of the database: Having certain data in a separate table allows you to add records that aren't necessarily needed now but may be needed in the future. For example, you could add new cities to the City table even if no other record references it yet.

5.5 Relational Data Model

What is Relational Model?

The relational model represents the database as a collection of relations. A relation is nothing but a table of values. Every row in the table represents a collection of related data values. These rows in the table denote a real-world entity or relationship.

The table name and column names are helpful to interpret the meaning of values in each row. The data are represented as a set of relations. In the relational model, data are stored as tables. However, the physical storage of the data is independent of the way the data are logically organized.

Some popular Relational Database management systems are:

- DB2 and Informix Dynamic Server - IBM
- Oracle and RDB – Oracle
- SQL Server and Access - Microsoft

Relational Model Concepts

1. Attribute- Each column in a Table. Attributes are the properties which define a relation. e.g., Student_ Roll no, Name, etc.
2. Tables – In the Relational model the, relations are saved in the table format. It is stored along with its entities. A table has two properties rows and columns. Rows represent records and columns represent attributes.
3. Tuple – It is nothing but a single row of a table, which contains a single record.
4. Relation Schema: A relation schema represents the name of the relation with its attributes.
5. Degree: The total number of attributes which in the relation is called the degree of the relation.
6. Cardinality: Total number of rows present in the Table.
7. Column: The column represents the set of values for a specific attribute.
8. Relation instance – Relation instance is a finite set of tuples in the RDBMS system. Relation instances never have duplicate tuples.
9. Relation key - Every row has one, two or multiple attributes, which is called relation key.
10. Attribute domain – Every attribute has some pre-defined value and scope which is known as attribute domain

Relational Integrity constraints

Relational Integrity constraints is referred to conditions which must be present for a valid relation. These integrity constraints are derived from the rules in the mini world that the database represents.

There are many types of integrity constraints. Constraints on the Relational database management system is mostly divided into three main categories are:

- Domain constraints
- Key constraints
- Referential integrity constraints

Domain Constraints

Domain constraints can be violated if an attribute value is not appearing in the corresponding domain or it is not of the appropriate data type.

Domain constraints specify that within each tuple, and the value of each attribute must be unique. This is specified as data types which include standard data types integers, real numbers, characters, Booleans, variable length strings, etc.

Example:

Create DOMAIN CustomerName
CHECK (value not NULL)

The example shown demonstrates creating a domain constraint such that Customer Name is not NULL

Key constraints

An attribute that can uniquely identify a tuple in a relation is called the key of the table. The value of the attribute for different tuples in the relation has to be unique.

Example:

In the given table, Customer ID is a key attribute of Customer Table. It is most likely to have a single key for one customer, Customer ID =1 is only for the Customer Name =" Google".

Customer ID	Customer Name	Status
1	Google	Active
2	Amazon	Active
3	Apple	Inactive

Referential integrity constraints

Referential integrity constraints are based on the concept of Foreign Keys. A foreign key is an important attribute of a relation which should be referred to in other relationships. Referential integrity constraint state happens where relation refers to a key attribute of a different or same relation. However, that key element must exist in the table.

Example:

In the above example, we have 2 relations, Customer and Billing.

Tuple for CustomerID =1 is referenced twice in the relation Billing. So, we know CustomerName=Google has billing amount $300

Operations in Relational Model

Four basic update operations performed on relational database model are: Insert, update, delete and select.

- Insert is used to insert data into the relation
- Delete is used to delete tuples from the table.
- Modify allows you to change the values of some attributes in existing tuples.
- Select allows you to choose a specific range of data.

Whenever one of these operations are applied, integrity constraints specified on the relational database schema must never be violated.

Best Practices for creating a Relational Model

- Data need to be represented as a collection of relations
- Each relation should be depicted clearly in the table
- Rows should contain data about instances of an entity
- Columns must contain data about attributes of the entity
- Cells of the table should hold a single value
- Each column should be given a unique name
- No two rows can be identical
- The values of an attribute should be from the same domain

5.6 Entity Relationship Model

What is the ER Model?

The ER or (Entity Relational Model) is a high-level conceptual data model diagram. Entity-Relation model is based on the notion of real-world entities and the relationship between them.

ER modeling helps you to analyze data requirements systematically to produce a well-designed database. So, it is considered a best practice to complete ER modeling before implementing your database.

History of ER models

ER diagrams are a visual tool which is helpful to represent the ER model. It was proposed by Peter Chen in 1971 to create a uniform convention which can be used for relational database and network. He aimed to use an ER model as a conceptual modeling approach.

What are ER Diagrams?

Entity relationship diagram displays the relationships of entity set stored in a database. In other words, we can say that ER diagrams help you to explain the logical structure of databases. At first look, an ER diagram looks very similar to the flowchart. However, ER Diagram includes many specialized symbols, and its meanings make this model unique.

Facts about ER Diagram Model:

- ER model allows you to draw Database Design
- It is an easy to use graphical tool for modelling data
- Widely used in Database Design
- It is a GUI representation of the logical structure of a Database
- It helps you to identifies the entities which exist in a system and the relationships between those entities

Why use ER Diagrams?

Here, are prime reasons for using the ER Diagram

- Helps you to define terms related to entity relationship modeling
- Provide a preview of how all your tables should connect, what fields are going to be on each table
- Helps to describe entities, attributes, relationships
- ER diagrams are translatable into relational tables which allows you to build databases quickly
- ER diagrams can be used by database designers as a blueprint for implementing data in specific software applications
- The database designer gains a better understanding of the information to be contained in the database with the help of ERP diagram
- ERD is allowed you to communicate with the logical structure of the database to users

Components of the ER Diagram

This model is based on three basic concepts:

1. Entities
2. Attributes
3. Relationships

Example

For example, in a University database, we might have entities for Students, Courses, and Lecturers. Students entity can have attributes like Rollno, Name, and DeptID. They might have relationships with Courses and Lecturers.

What is entity?

A real-world thing either living or non-living that is easily recognizable and non-recognizable. It is anything in the enterprise that is to be represented in our database. It may be a physical thing or simply a fact about the enterprise or an event that happens in the real world.

An entity can be place, person, object, event or a concept, which stores data in the database. The characteristics of entities are must have an attribute, and a unique key. Every entity is made up of some 'attributes' which represent that entity.

Examples of entities:

- Person: Employee, Student, Patient
- Place: Store, Building
- Object: Machine, product, and Car
- Event: Sale, Registration, Renewal
- Concept: Account, Course
- Notation of an Entity

Entity set:

An entity set is a group of similar kind of entities. It may contain entities with attribute sharing similar values. Entities are represented by their properties, which also called attributes. All attributes have their separate values. For example, a student entity may have a name, age, class, as attributes.

Example of Entities:

A university may have some departments. All these departments employ various lecturers and offer several programs. Some courses make up each program. Students register in a particular program and enroll in various courses. A lecturer from the specific department takes each course, and each lecturer teaches a various group of students.

Relationship

Relationship is nothing but an association among two or more entities. E.g., Tom works in the Chemistry department.

For example

- You are attending this lecture
- I am giving the lecture
- Just looking at entities, we can classify relationships according to relationship-types:
- A student attends a lecture
- A lecturer is giving a lecture.

Weak Entities

A weak entity is a type of entity which doesn't have its key attribute. It can be identified uniquely by considering the primary key of another entity. For that, weak entity sets need to have participation.

In above example, "Trans No" is a discriminator within a group of transactions in an ATM.

Let's learn more about a weak entity by comparing it with a Strong Entity

Strong Entity Set	Weak Entity Set
Strong entity set always has a primary key.	It does not have enough attributes to build a primary key.
It is represented by a rectangle symbol.	It is represented by a double rectangle symbol.
It contains a Primary key represented by the underline symbol.	It contains a Partial Key which is represented by a dashed underline symbol.
The member of a strong entity set is called as dominant entity set.	The member of a weak entity set called as a subordinate entity set.
Primary Key is one of its attributes which helps to identify its member.	In a weak entity set, it is a combination of primary key and partial key of the strong entity set.
In the ER diagram the relationship between two strong entity set shown by using a diamond symbol.	The relationship between one strong and a weak entity set shown by using the double diamond symbol.

Strong Entity Set	Weak Entity Set
The connecting line of the strong entity set with the relationship is single.	The line connecting the weak entity set for identifying relationship is double.

Attributes

It is a single-valued property of either an entity-type or a relationship-type.
For example, a lecture might have attributes: time, date, duration, place, etc.

An attribute is represented by an Ellipse

Types of Attributes	Description
Simple attribute	Simple attributes can't be divided any further. For example, a student's contact number. It is also called an atomic value.
Composite attribute	It is possible to break down composite attribute. For example, a student's full name may be further divided into first name, second name, and last name.
Derived attribute	This type of attribute does not include in the physical database. However, their values are derived from other attributes present in the database. For example, age should not be stored directly. Instead, it should be derived from the DOB of that employee.
Multivalued attribute	Multivalued attributes can have more than one values. For example, a student can have more than one mobile number, email address, etc.

Cardinality

Defines the numerical attributes of the relationship between two entities or entity sets. Different types of cardinal relationships are:

- One-to-One Relationships
- One-to-Many Relationships
- Many to One Relationships
- Many-to-Many Relationships

1) One-to-one: One entity from entity set X can be associated with at most one entity of entity set Y and vice versa. Example: One student can register for numerous courses. However, all those courses have a single line back to that one student.
2) One-to-many: One entity from entity set X can be associated with multiple entities of entity set Y, but an entity from entity set Y can be associated with at least one entity. For example, one class is consisting of multiple students.
3) Many to One: More than one entity from entity set X can be associated with at most one entity of entity set Y. However, an entity from entity set Y may or may not be associated with more than one entity from entity set X.
4) Many to Many: One entity from X can be associated with more than one entity from Y and vice versa.

ER- Diagram Notations

ER- Diagram is a visual representation of data that describe how data is related to each other.

- Rectangles: This symbol represent entity types
- Ellipses: Symbol represent attributes
- Diamonds: This symbol represents relationship types
- Lines: It links attributes to entity types and entity types with other relationship types
- Primary key: attributes are underlined

Best Practices for Developing Effective ER Diagrams

- Eliminate any redundant entities or relationships
- You need to make sure that all your entities and relationships are properly labeled
- There may be various valid approaches to an ER diagram. You need to make sure that the ER diagram supports all the data you need to store
- You should assure that each entity only appears a single time in the ER diagram
- Name every relationship, entity, and attribute are represented on your diagram
- Never connect relationships to each other
- You should use colors to highlight important portions of the ER diagram

Summary

- The ER model is a high-level data model diagram
- ER diagrams are a visual tool which is helpful to represent the ER model
- Entity relationship diagram displays the relationships of entity set stored in a database
- ER diagrams help you to define terms related to entity relationship modeling
- ER model is based on three basic concepts: Entities, Attributes & Relationships
- An entity can be place, person, object, event or a concept, which stores data in the database
- Relationship is nothing but an association among two or more entities
- A weak entity is a type of entity which doesn't have its key attribute
- It is a single-valued property of either an entity-type or a relationship-type
- It helps you to defines the numerical attributes of the relationship between two entities or entity sets
- ER- Diagram is a visual representation of data that describe how data is related to each other
- While Drawing ER diagram you need to make sure all your entities and relationships are properly labeled.

5.7 Data Schemas

Database systems comprise of complex data structures. Thus, to make the system efficient for retrieval of data and reduce the complexity of the users, developers use the method of Data Abstraction. There are mainly three levels of data abstraction:

- Internal Level: Actual PHYSICAL storage structure and access paths.
- Conceptual or Logical Level: Structure and constraints for the entire database
- External or View level: Describes various user views.

Internal Level/Schema

The internal schema defines the physical storage structure of the database. The internal schema is a very low-level representation of the entire database. It contains multiple occurrences of multiple types of internal record. In the ANSI term, it is also called "stored record'.

Facts about Internal schema:

- The internal schema is the lowest level of data abstraction
- It helps you to keeps information about the actual representation of the entire database. Like the actual storage of the data on the disk in the form of records
- The internal view tells us what data is stored in the database and how
- It never deals with the physical devices. Instead, internal schema views a physical device as a collection of physical pages

Conceptual Schema/Level

The conceptual schema describes the Database structure of the whole database for the community of users. This schema hides information about the physical storage structures and focuses on describing data types, entities, relationships, etc. This logical level comes between the user level and physical storage view. However, there is only single conceptual view of a single database.

Facts about Conceptual schema:

- Defines all database entities, their attributes, and their relationships
- Security and integrity information
- In the conceptual level, the data available to a user must be contained in or derivable from the physical level

External Schema/Level

An external schema describes the part of the database which specific user is interested in. It hides the unrelated details of the database from the user. There may be "n" number of external views for each database.

Each external view is defined using an external schema, which consists of definitions of various types of external record of that specific view. An external view is just the content of the database as it is seen by some specific particular user. For example, a user from the sales department will see only sales related data.

Facts about external schema:

- An external level is only related to the data which is viewed by specific end users.
- This level includes some external schemas.
- External schema level is nearest to the user
- The external schema describes the segment of the database which is needed for a certain user group and hides the remaining details from the database from the specific user group

Goal of 3 level/schema of Database

Here, are some Objectives of using Three schema Architecture:

- Every user should be able to access the same data but able to see a customized view of the data.
- The user need not to deal directly with physical database storage detail.
- The DBA should be able to change the database storage structure without disturbing the user's views
- The internal structure of the database should remain unaffected when changes made to the physical aspects of storage.

Summary

- There are mainly three levels of data abstraction: Internal Level, Conceptual or Logical Level or External or View level
- The internal schema defines the physical storage structure of the database
- The conceptual schema describes the Database structure of the whole database for the community of users
- An external schema describes the part of the database which specific user is interested in DBMS Architecture allows you to make changes on the presentation level without affecting the other two layers

5.8 Conversion of ER Model to Relational Model

The ER Model is intended as a description of real-world entities. Although it is constructed in such a way as to allow easy translation to the relational schema model, this is not an entirely trivial process. The ER diagram represents the conceptual level of database design meanwhile the relational schema is the logical level for the database design. We will be following the simple rules:

1. Entities and Simple Attributes:

An entity type within ER diagram is turned into a table. You may preferably keep the same name for the entity or give it a sensible name but avoid DBMS reserved words as well as avoid the use of special characters.

Each attribute turns into a column (attribute) in the table. The key attribute of the entity is the primary key of the table which is usually underlined. It can be composite if required but can never be null.

It is highly recommended that every table should start with its primary key attribute conventionally named as TablenameID or ID.

Taking the following simple ER diagram:

The initial relational schema is expressed in the following format writing the table names with the attributes list inside a parentheses as shown below for

- Persons (personid, name, lastname, email, phone)
- Persons are Table. name, lastname, are Table Columns (Attributes).
- *personid is the primary key for the table: Person*

2. Multi-Valued Attributes

A multi-valued attribute is usually represented with a double-line oval. If you have a multi-valued attribute, take the attribute and turn it into a new entity or table of its own. Then make a 1: N relationship between the new entity and the existing one. In simple words.

1. Create a table for the attribute.
2. Add the primary (id) column of the parent entity as a foreign key within the new table as shown below:
    - Persons (personid , name, lastname, email)
    - Phones (phoneid , personid, phone)
    - "personid" within the table Phones is a foreign key referring to the "personid"of Persons

3. Relationships

To keep it simple and even for better performances at data retrieval, I would personally recommend using attributes to represent such relationship. For instance, let us consider the case where the Person has or optionally has one wife. You can place the primary key of the wife within the table of the Persons which we call in this case Foreign key as shown below.

Persons (personid , name, lastname, email , wifeid)
Wife (wifeid , name)

Or vice versa to put the personid as a foreign key within the Wife table as shown below:

Persons (personid, name, lastname, email)
Wife (wifeid , name , personid)

For cases when the Person is not married i.e. has no wifeID, the attribute can set to NULL

4. 1:N Relationships

This is the tricky part! For simplicity, use attributes in the same way as 1:1 relationship but we have only one choice as opposed to two choices.

4. N:N Relationships

We normally use tables to express such type of relationship. This is the same for N – ary relationship of ER diagrams. For instance, The Person can live or work in many countries. Also, a country can have many people. To express this relationship within a relational schema we use a separate table as shown below:

It should convert into:

Persons(personid , name, lastname, email)
Countries (countryid , name, code)
HasRelat (hasrelatid , personid , countryid)

Relationship with attributes:

It is recommended to use table to represent them to keep the design tidy and clean regardless of the cardinality of the relationship.

5.9 The Enhanced ER Model (Generalization, Specialization and Aggregation)

As the complexity of data increased in the late 1980s, it became more and more difficult to use the traditional ER Model for database modelling. Hence some improvements or enhancements were made to the existing ER Model to make it able to handle the complex applications better. Hence, as part of the Enhanced ER Model, along with other improvements, three new concepts were added to the existing ER Model, they were:

1. Generalization
2. Specialization
3. Aggregation

Let's understand what they are, and why were they added to the existing ER Model.

Generalization: Generalization is a bottom-up approach in which two lower level entities combine to form a higher-level entity. In generalization, the higher-level entity can also combine with other lower level entities to make further higher-level entity. It's more like Superclass and Subclass system, but the only difference is the approach, which is bottom-up. Hence, entities are combined to form a more generalized entity, in other words, sub-classes are combined to form a super-class.

Specialization: Specialization is opposite to Generalization. It is a top-down approach in which one higher level entity can be broken down into two lower level entity. In specialization, a higher-level entity may not have any lower-level entity sets, it's possible.

Aggregation: Aggregation is a process when relation between two entities is treated as a single entity.

In the diagram above, the relationship between Center and Course together, is acting as an Entity, which is in relationship with another entity Visitor. Now in real world, if a Visitor or a Student visits a Coaching Center, he/she will never enquire about the center only or just about the course, rather he/she will ask to enquire about both.

5.10 Database Normalization

Database Normalization is a technique of organizing the data in the database. Normalization is a systematic approach of decomposing tables to eliminate data redundancy(repetition) and undesirable characteristics like Insertion, Update and Deletion Anomalies. It is a multi-step process that puts data into tabular form, removing duplicated data from the relation tables.

Normalization is used for mainly two purposes,

- Eliminating redundant(useless) data.
- Ensuring data dependencies make sense i.e. data is logically stored.

Problems Without Normalization

If a table is not properly normalized and have data redundancy then it will not only eat up extra memory space but will also make it difficult to handle and update the database, without facing data loss. Insertion, Updating and Deletion Anomalies are very frequent if database is not normalized. To understand these anomalies let us take an example of a Student table.

Rollno	name	branch	hod	office_tel
401	Akon	CSE	Mr. X	53337
402	Bkon	CSE	Mr. X	53337
403	Ckon	CSE	Mr. X	53337
404	Dkon	CSE	Mr. X	53337

In the table above, we have data of 4 Computer Sci. students. As we can see, data for the fields branch, hod(Head of Department) and office_tel is repeated for the students who are in the same branch in the college, this is Data Redundancy.

Insertion Anomaly

Suppose for a new admission, until and unless a student opts for a branch, data of the student cannot be inserted, or else we will have to set the branch information as NULL.

Also, if we have to insert data of 100 students of same branch, then the branch information will be repeated for all those 100 students. These scenarios are nothing but Insertion anomalies.

Updation Anomaly

What if Mr. X leaves the college? or is no longer the HOD of computer science department? In that case all the student records will have to be updated, and if by mistake we miss any record, it will lead to data inconsistency. This is Updation anomaly.

Deletion Anomaly

In our Student table, two different informations are kept together, Student information and Branch information. Hence, at the end of the academic year, if student records are deleted, we will also lose the branch information. This is Deletion anomaly.

Normalization Rule

Normalization rules are divided into the following normal forms:

1) First Normal Form
2) Second Normal Form
3) Third Normal Form
4) BCNF

5) Fourth Normal Form

First Normal Form (1NF)

For a table to be in the First Normal Form, it should follow the following 4 rules:

1) It should only have single(atomic) valued attributes/columns.
2) Values stored in a column should be of the same domain
3) All the columns in a table should have unique names.
4) And the order in which data is stored, does not matter.

Second Normal Form (2NF)

For a table to be in the Second Normal Form,

1) It should be in the First Normal form.
2) And, it should not have Partial Dependency.

Third Normal Form (3NF)

A table is said to be in the Third Normal Form when,

1) It is in the Second Normal form.
2) And, it doesn't have Transitive Dependency.

Boyce and Codd Normal Form (BCNF)

Boyce and Codd Normal Form is a higher version of the Third Normal form. This form deals with certain type of anomaly that is not handled by 3NF. A 3NF table which does not have multiple overlapping candidate keys is said to be in BCNF. For a table to be in BCNF, following conditions must be satisfied:

1) R must be in 3rd Normal Form
2) and, for each functional dependency ($X \rightarrow Y$), X should be a super Key.

Fourth Normal Form (4NF)

A table is said to be in the Fourth Normal Form when,

1) It is in the Boyce-Codd Normal Form.
2) And, it doesn't have Multi-Valued Dependency.

What is First Normal Form (1NF)?

1st Normal Form which is more like the Step 1 of the Normalization process. The 1st Normal form expects you to design your table in such a way that it can easily be extended, and it is easier for you to retrieve data from it whenever required. If tables in a database are not even in the 1st Normal Form, it is considered as bad database design.

Rules for First Normal Form

The first normal form expects you to follow a few simple rules while designing your database, and they are:

Rule 1: Single Valued Attributes

Each column of your table should be single valued which means they should not contain multiple values. We will explain this with help of an example later, let's see the other rules for now.

Rule 2: Attribute Domain should not change

This is more of a "Common Sense" rule. In each column the values stored must be of the same kind or type.

For example: If you have a column dob to save date of births of a set of people, then you cannot or you must not save 'names' of some of them in that column along with 'date of birth' of others in that column. It should hold only 'date of birth' for all the records/rows.

Rule 3: Unique name for Attributes/Columns

This rule expects that each column in a table should have a unique name. This is to avoid confusion at the time of retrieving data or performing any other operation on the stored data. If one or more columns have same name, then the DBMS system will be left confused.

Rule 4: Order doesn't matter

This rule says that the order in which you store the data in your table doesn't matter. Using the First Normal Form, data redundancy increases, as there will be many columns with same data in multiple rows, but each row as a whole will be unique.

What is Second Normal Form?

For a table to be in the Second Normal Form, it must satisfy two conditions:

1) The table should be in the First Normal Form.
2) There should be no Partial Dependency.

What is Partial Dependency? Do not worry about it. First let's understand what is Dependency in a table?

What is Dependency?

Let's take an example of a Student table with columns student_id, name, reg_no(registration number), branch and address(student's home address).

student_id	name	reg_no	branch	Address

In this table, student_id is the primary key and will be unique for every row, hence we can use student_id to fetch any row of data from this table

Even for a case, where student names are same, if we know the student_id we can easily fetch the correct record.

student_id	name	reg_no	branch	address
10	Akon	07-WY	CSE	Kerala

11	Akon	08-WY	IT	Gujarat

Hence, we can say a Primary Key for a table is the column or a group of columns (composite key) which can uniquely identify each record in the table.

I can ask from branch name of student with student_id 10, and I can get it. Similarly, if I ask for name of student with student_id 10 or 11, I will get it. So, all I need is student_id and every other column depends on it or can be fetched using it.

This is Dependency and we also call it Functional Dependency.

What is Partial Dependency?

Now that we know what dependency is, we are in a better state to understand what partial dependency is. For a simple table like Student, a single column like student_id can uniquely identfy all the records in a table.

But this is not true all the time. So now let's extend our example to see if more than 1 column together can act as a primary key. Let's create another table for Subject, which will have subject_id and subject_name fields and subject_id will be the primary key.

subject_id	subject_name
1	Java
2	C++
3	Php

Now we have a Student table with student information and another table Subject for storing subject information. Let's create another table Score, to store the marks obtained by students in the respective subjects. We will also be saving name of the teacher who teaches that subject along with marks.

score_id	student_id	subject_id	marks	teacher
1	10	1	70	Java Teacher
2	10	2	75	C++ Teacher
3	11	1	80	Java Teacher

In the score table we are saving the student_id to know which student's marks are these and subject_id to know for which subject the marks are for. Together, student_id + subject_id forms a Candidate Key for this table, which can be the Primary key.

How this combination can be a primary key?

See, if I ask you to get me marks of student with student_id 10, can you get it from this table? No, because you don't know for which subject. And if I give you subject_id, you would not know for which student. Hence, we need student_id + subject_id to uniquely identify any row.

But where is Partial Dependency?

Now if you look at the Score table, we have a column names teacher which is only dependent on the subject, for Java it's Java Teacher and for C++ it's C++ Teacher & so on.

Now as we just discussed that the primary key for this table is a composition of two columns which is student_id & subject_id but the teacher's name only depends on subject, hence the subject_id, and has nothing to do with student_id.

This is Partial Dependency, where an attribute in a table depends on only a part of the primary key and not on the whole key.

How to remove Partial Dependency?

There can be many different solutions for this, but our objective is to remove teacher's name from Score table. The simplest solution is to remove columns teacher from Score table and add it to the Subject table. Hence, the Subject table will become:

subject_id	subject_name	teacher
1	Java	Java Teacher
2	C++	C++ Teacher
3	Php	Php Teacher

And our Score table is now in the second normal form, with no partial dependency.

score_id	student_id	subject_id	marks
1	10	1	70
2	10	2	75
3	11	1	80

Quick Recap

- For a table to be in the Second Normal form, it should be in the First Normal form and it should not have Partial Dependency.
- Partial Dependency exists, when for a composite primary key, any attribute in the table depends only on a part of the primary key and not on the complete primary key.
- To remove Partial dependency, we can divide the table, remove the attribute, which is causing partial dependency, and move it to some other table where it fits in well.

What is Third Normal Form (3NF)

In our last tutorial, we learned about the second normal form and even normalized our Score table into the 2nd Normal Form.

Requirements for Third Normal Form

For a table to be in the third normal form,

1) It should be in the Second Normal form.
2) And it should not have Transitive Dependency.

What is Transitive Dependency?

With exam_name and total_marks added to our Score table, it saves more data now. Primary key for our Score table is a composite key, which means it's made up of two attributes or columns → student_id + subject_id.

Our new column exam_name depends on both student and subject. For example, a mechanical engineering student will have Workshop exam, but a computer science student won't. And for some subjects you have Prctical exams and for some you don't. So, we can say that exam_name is dependent on both student_id and subject_id.

And what about our second new column total_marks? Does it depend on our Score table's primary key?

Well, the column total_marks depend on exam_name as with exam type the total score changes. For example, practicals are of less marks while theory exams are of more marks.

But, exam_name is just another column in the score table. It is not a primary key or even a part of the primary key, and total_marks depend on it.

This is Transitive Dependency. When a non-prime attribute depends on other non-prime attributes rather than depending upon the prime attributes or primary key.

How to remove Transitive Dependency?

Again, the solution is very simple. Take out the column's exam_name and total_marks from Score table and put them in an Exam table and use the exam_id wherever required.

Score Table: In 3rd Normal Form

score_id	student_id	subject_id	marks	exam_id

The new Exam tables

exam_id	exam_name	total_marks
1	Workshop	200
2	Mains	70
3	Practicals	30

Advantage of removing Transitive Dependency

The advantage of removing transitive dependency is,

1) Amount of data duplication is reduced.
2) Data integrity achieved.

What is Boyce-Codd Normal Form (BCNF)

Boyce-Codd Normal Form or BCNF is an extension to the third normal form and is also known as 3.5 Normal Form.

Rules for BCNF

For a table to satisfy the Boyce-Codd Normal Form, it should satisfy the following two conditions: It should be in the Third Normal Form.

1) And, for any dependency A → B, A should be a super key.
2) The second point sounds a bit tricky, right? In simple words, it means, that for a dependency A → B, A cannot be a non-prime attribute, if B is a prime attribute.

Fourth Normal Form (4NF)

Fourth Normal Form comes into picture when Multi-valued Dependency occur in any relation. In this tutorial we will learn about Multi-valued Dependency, how to remove it and how to make any table satisfy the fourth normal form.

In our last tutorial, we learned about the boyce-codd normal form, we suggest you follow the last tutorial before this one.

Rules for 4th Normal Form

For a table to satisfy the Fourth Normal Form, it should satisfy the following two conditions:

1) It should be in the Boyce-Codd Normal Form.
2) And, the table should not have any Multi-valued Dependency.

Let's try to understand what multi-valued dependency is in the next section.

What is Multi-valued Dependency?

A table is said to have multi-valued dependency, if the following conditions are true,

1) For a dependency A → B, if for a single value of A, multiple value of B exists, then the table may have multi-valued dependency.
2) Also, a table should have at-least 3 columns for it to have a multi-valued dependency.
3) And, for a relation R (A, B, C), if there is a multi-valued dependency between, A and B, then B and C should be independent of each other.

If all these conditions are true for any relation(table), it is said to have multi-valued dependency.

5.11 Database Management Systems

What is a Database?

A database is a collection of related data which represents some aspect of the real world. A database system is designed to be built and populated with data for a certain task.

What is DBMS?

Database Management System (also known as DBMS) is a software for storing and retrieving users' data by considering appropriate security measures. It allows users to create their own databases as per their requirement.

It consists of a group of programs which manipulate the database and provide an interface between the database. It includes the user of the database and other application programs. The DBMS accepts the request for data from an application and instructs the operating system to provide the specific data. In large systems, a DBMS helps users and other third-party software to store and retrieve data.

Let us see a simple example of a university database. This database is maintaining information concerning students, courses, and grades in a university environment. The database is organized as five files:

- The STUDENT file stores data of each student
- The COURSE file stores contain data on each course.
- The SECTION stores the information about sections in a particular course.
- The GRADE file stores the grades which students receive in the various sections
- The TUTOR file contains information about each professor.

To define a database system:

- We need to specify the structure of the records of each file by defining the different types of data elements to be stored in each record.
- We can also use a coding scheme to represent the values of a data item.
- Basically, your Database will have 5 tables with a foreign key defined amongst the various tables.

Characteristics of Database Management System

- Provides security and removes redundancy
- Self-describing nature of a database system
- Insulation between programs and data abstraction
- Support of multiple views of the data
- Sharing of data and multiuser transaction processing
- DBMS allows entities and relations among them to form tables.
- It follows the ACID concept (Atomicity, Consistency, Isolation, and Durability).
- DBMS supports multi-user environment that allows users to access and manipulate data in parallel.

DBMS vs. Flat File

DBMS	Flat File Management System
Multi-user access	It does not support multi-user access
Design to fulfill the need for small and large businesses	It is only limited to smaller DBMS system.
Remove redundancy and Integrity	Redundancy and Integrity issues
Expensive. But in the long-term Total Cost of Ownership is cheap	It's cheaper

DBMS	Flat File Management System
Easy to implement complicated transactions	No support for complicated transactions

Users in a DBMS environment

Following, are the various category of users of a DBMS system

Component Name	Task
Application Programmers	The Application programmers write programs in various programming languages to interact with databases.
Database Administrators	Database Admin is responsible for managing the entire DBMS system. He/She is called Database admin or DBA.
End-Users	The end users are the people who interact with the database management system. They conduct various operations on database like retrieving, updating, deleting, etc.

Popular DBMS Software

Here, is the list of some popular DBMS system:

- MySQL
- Microsoft Access
- Oracle
- PostgreSQL
- dBASE
- FoxPro
- SQLite
- IBM DB2
- LibreOffice Base
- MariaDB
- Microsoft SQL Server etc.

Application of DBMS

Sector	Use of DBMS
Banking	For customer information, account activities, payments, deposits, loans, etc.
Airlines	For reservations and schedule information.
Universities	For student information, course registrations, colleges and grades.
Telecommunication	It helps to keep call records, monthly bills, maintaining balances, etc.
Finance	For storing information about stock, sales, and purchases of financial instruments like stocks and bonds.
Sales	Use for storing customer, product & sales information.

Sector	Use of DBMS
Manufacturing	It is used for the management of supply chain and for tracking production of items. Inventories status in warehouses.
HR Management	For information about employees, salaries, payroll, deduction, generation of paychecks, etc.

Types of DBMS

Four Types of DBMS systems are:

- Hierarchical, Network, Relational & Object-Oriented DBMS

Hierarchical DBMS

In a Hierarchical database, model data is organized in a tree-like structure. Data is Stored Hierarchically (top down or bottom up) format. Data is represented using a parent-child relationship. In Hierarchical DBMS parent may have many children, but children have only one parent.

Network Model

The network database model allows each child to have multiple parents. It helps you to address the need to model more complex relationships like as the orders/parts many-to-many relationship. In this model, entities are organized in a graph which can be accessed through several paths.

Relational model

Relational DBMS is the most widely used DBMS model because it is one of the easiest. This model is based on normalizing data in the rows and columns of the tables. Relational model stored in fixed structures and manipulated using SQL.

Object-Oriented Model

In Object-oriented Model data stored in the form of objects. The structure which is called classes which display data within it. It defines a database as a collection of objects which stores both data members values and operations.

Advantages of DBMS

- DBMS offers a variety of techniques to store & retrieve data
- DBMS serves as an efficient handler to balance the needs of multiple applications using the same data
- Uniform administration procedures for data
- Application programmers never exposed to details of data representation and storage.

- A DBMS uses various powerful functions to store and retrieve data efficiently.
- Offers Data Integrity and Security
- The DBMS implies integrity constraints to get a high level of protection against prohibited access to data.
- A DBMS schedules concurrent access to the data in such a manner that only one user can access the same data at a time
- Reduced Application Development Time

Disadvantage of DBMS

DBMS may offer plenty of advantages but, it has certain flaws-

- Cost of Hardware and Software of a DBMS is quite high which increases the budget of your organization.
- Most database management systems are often complex systems, so the training for users to use the DBMS is required.
- In some organizations, all data is integrated into a single database which can be damaged because of electric failure or database is corrupted on the storage media
- Use of the same program at a time by many users sometimes lead to the loss of some data.
- DBMS can't perform sophisticated calculations

When not to use a DBMS system?

Although, DBMS system is useful. It is still not suited for specific task mentioned below: Not recommended when you do not have the budget or the expertise to operate a DBMS. In such cases, Excel/CSV/Flat Files could do just fine.

Summary

- A database is a collection of related data which represents some aspect of the real world
- Database Management System (also known as DBMS) is a software for storing and retrieving users' data by considering appropriate security measures.
- DBMS Provides security and removes redundancy
- DBMS has many advantages over tradition Flat File management system
- End-Users, Application Programmers, and Database Administrators are they type of users who access a DBMS
- DMBS is widely used in Banking, Airlines, Telecommunication, Finance and other industries
- Four Types of DBMS systems are 1) Hierarchical 2) Network 3) Relational 4) Object-Oriented DBMS
- DBMS serves as an efficient handler to balance the needs of multiple applications using the same data
- Cost of Hardware and Software of a DBMS is quite high which increases the budget of your organization

5.12 DBMS Transaction

What is a Database Transaction?

A transaction is a logical unit of processing in a DBMS which entails one or more database access operation. In a nutshell, database transactions represent real-world events of any enterprise. All types of database access operation which are held between the beginning and end transaction statements are considered as a single logical transaction. During the transaction the database is inconsistent. Only once the database is committed the state is changed from one consistent state to another.

Facts about Database Transactions

- A transaction is a program unit whose execution may or may not change the contents of a database.
- The transaction is executed as a single unit
- If the database operations do not update the database but only retrieve data, this type of transaction is called a read-only transaction.
- A successful transaction can change the database from one CONSISTENT STATE to another
- DBMS transactions must be atomic, consistent, isolated and durable
- If the database were in an inconsistent state before a transaction, it would remain in the inconsistent state after the transaction.

Why do you need concurrency in Transactions?

A database is a shared resource accessed. It is used by many users and processes concurrently. For example, the banking system, railway, and air reservations systems, stock market monitoring, supermarket inventory, and checkouts, etc. Not managing concurrent access may create issues like:

- Hardware failure and system crashes
- Concurrent execution of the same transaction, deadlock, or slow performance

States of Transactions

The various states of a Database Transaction are listed below

State	Transaction types
Active State	A transaction enters into an active state when the execution process begins. During this state read or write operations can be performed
Partially Committed	A transaction goes into the partially committed state after the end of a transaction.
Committed State	When the transaction is committed to state, it has already completed its execution successfully. Moreover, all of its changes are recorded to the database permanently.

State	Transaction types
Failed State	A transaction considers failed when any one of the checks fails or if the transaction is aborted while it is in the active state.
Terminated State	State of transaction reaches terminated state when certain transactions which are leaving the system can't be restarted.

State Transition Diagram for a Database Transaction

Let's study a state transition diagram that highlights how a transaction moves between these various states.

1. Once a transaction states execution, it becomes active. It can issue READ or WRITE operation.
2. Once the READ and WRITE operations complete, the transactions becomes partially committed state.
3. Next, some recovery protocols need to ensure that a system failure will not result in an inability to record changes in the transaction permanently. If this check is a success, the transaction commits and enters into the committed state.
4. If the check is a fail, the transaction goes to the Failed state.
5. If the transaction is aborted while it's in the active state, it goes to the failed state. The transaction should be rolled back to undo the effect of its write operations on the database.
6. The terminated state refers to the transaction leaving the system.

What are ACID Properties?

For maintaining the integrity of data, the DBMS system you have to ensure ACID properties. ACID stands for **A**tomicity, **C**onsistency, **I**solation, and **D**urability.

- **Atomicity:** A transaction is a single unit of operation. You either execute it entirely or do not execute it at all. There cannot be partial execution.
- **Consistency:** Once the transaction is executed, it should move from one consistent state to another.
- **Isolation:** Transaction should be executed in isolation from other transactions (no Locks). During concurrent transaction execution, intermediate transaction results from simultaneously executed transactions should not be made available to each other. (Level 0,1,2,3)
- **Durability:** · After successful completion of a transaction, the changes in the database should persist. Even in the case of system failures.

Example of ACID

Transaction 1: Begin X=X+50, Y = Y-50 END
Transaction 2: Begin X=1.1*X, Y=1.1*Y END
Transaction 1 is transferring $50 from account X to account Y.

Transaction 2 is crediting each account with a 10% interest payment.

If both transactions are submitted together, there is no guarantee that the Transaction 1 will execute before Transaction 2 or vice versa. Irrespective of the order, the result must be as if the transactions take place serially one after the other.

Types of Transactions

Based on Application areas

- Non-distributed vs. distributed
- Compensating transactions
- Transactions Timing
- On-line vs. batch

Based on Actions

- Two-step
- Restricted
- Action model

Based on Structure

- Flat or simple transactions: It consists of a sequence of primitive operations executed between a begin and end operations.
- Nested transactions: A transaction that contains other transactions.
- Workflow

What is a Schedule?

A Schedule is a process creating a single group of the multiple parallel transactions and executing them one by one. It should preserve the order in which the instructions appear in each transaction. If two transactions are executed at the same time, the result of one transaction may affect the output of other.

Example

Initial Product Quantity is 10

Transaction 1: Update Product Quantity to 50

Transaction 2: Read Product Quantity

If Transaction 2 is executed before Transaction 1, outdated information about the pro duct quantity will be read. Hence, schedules are required.

Parallel execution in a database is inevitable. But Parallel execution is permitted when there is an equivalence relation amongst the simultaneously executing transactions. T his equivalence is of 3 Types.

Result equivalence:

If two schedules display the same result after execution, it is called result equivalent schedule. They may offer the same result for some value and different results for another set of values.

For example, one transaction updates the product quantity, while other updates customer details.

View Equivalence

View Equivalence occurs when the transaction in both the schedule performs a similar action. Example, one transaction inserts product details in the product table, while another transaction inserts product details in the archive table. The transaction is the same, but the tables are different.

CONFLICT Equivalence

In this case, two transactions update/view the same set of data. There is a conflict amongst transaction as the order of execution will affect the output.

What is Serializability?

Serializability is the process of search for a concurrent schedule who output is equal to a serial schedule where transaction ae execute one after the other. Depending on the type of schedules, there are two types of serializability:

- Conflict
- View

Summary:

- A transaction is a logical unit of processing in a DBMS which entails one or more database access operation
- It is a transaction is a program unit whose execution may or may not change the contents of a database.
- Not managing concurrent access may create issues like hardware failure and system crashes.
- Active, Partially Committed, Committed, Failed & Terminate are important transaction states.
- ACID stands for Atomicity, Consistency, Isolation, and Durability
- Three DBMS transactions types are Base on Application Areas, Action, & Structure.
- A Schedule is a process creating a single group of the multiple parallel transactions and executing them one by one.
- Serializability is the process of search for a concurrent schedule who output is equal to a serial schedule where transaction ae execute one after the other.

5.13 DBMS Query

When the relational model was launched for the first time, one of the chief criticisms often cited was the inadequate presentation of queries. Since then, a significant amount of research has been committed to developing highly proficient algorithms for processing and dealing with queries. There are a lot of ways for doing a complex query can be performed, and one of the targets of query processing is to decide which one is the most cost-effective. In first generation network and hierarchical database systems, the low-level procedural query

language is generally implanted in a high-level programming language such as COBOL, and it is the job of the programmers to select the most appropriate execution strategy. In contrast, with declarative languages such as SQL, the user identifies what data is required rather than how it is to be retrieved.

In this chapter, you will be given a general idea of query processing and examine the main segments of this activity. Here you will examine the first phase of query processing, namely query decomposition, which transforms a high-level query into a relational algebra query and ensures that it is syntactically and semantically correct.

Overview of Query Processing

This query processing activity involved in parsing, validating, optimizing, and executing a query. The target of query processing is to change a query written in a high-level language, (usually SQL) into a correct and efficient execution strategy expressed in a low-level language (using the relational algebra) and to perform the strategy to retrieve the required data. An important aspect of query processing is query optimization. The activity of choosing an efficient execution strategy for processing a query is known as Query optimization. As there are many correspondent transformations of the same high-level query, the main aim of optimizing a query is to choose the one that minimizes resource usage. Generally, you will try reducing the total execution time of the query which is the total of the execution times of all individual operations that make up the query.

Both methods of query optimization rely on database statistics to assess properly the different options that are available. The accuracy and currency of these statistics have a significant bearing on the efficiency of the execution strategy chosen.

Comparison of Different Processing Strategies

Find all DBAs who work at a Dhaka branch.

You can write this query in SQL as:

```
SELECT *
FROM Staff s, Branch b
WHERE s.branchNo = b.branchNo AND
(s.position = 'DBA' AND b.city = 'Dhaka');
```

The 3 equivalent relational algebra queries corresponding to the above SQL statement are:

σ(position='DBA') ∧ (city='Dhaka') ∧ (Staff.branchNo=Branch.branchNo)

(((Staff × Branch)

σ(position='DBA') ∧ (city=' Dhaka')(Staff branchNo=Branch.branchNo Branch)

(σposition='DBA'(Staff)) Staff.branchNo=Branch.branchNo (σcity=' Dhaka'(Branch))

What is Query Decomposition in DBMS?

Query decomposition is the first phase of query processing. The primary targets of query decomposition are to transform a high-level query into a relational algebra query and to check that the query is syntactically and semantically correct. The typical stages of query decomposition are analysis, normalization, semantic analysis, simplification, and query restructuring.

Structured Query Language (SQL)

Structured Query Language is a standard Database language which is used to create, maintain and retrieve the relational database. Following are some interesting facts about SQL.

- SQL is case insensitive. But it is a recommended practice to use keywords (like SELECT, UPDATE, CREATE, etc) in capital letters and use user defined things (liked table name, column name, etc) in small letters.
- We can write comments in SQL using "–" (double hyphen) at the beginning of any line.
- SQL is the programming language for relational databases (explained below) like MySQL, Oracle, Sybase, SQL Server, Postgre, etc. Other non-relational databases (also called NoSQL) databases like MongoDB, DynamoDB, etc do not use SQL
- Although there is an ISO standard for SQL, most of the implementations slightly vary in syntax. So, we may encounter queries that work in SQL Server but do not work in MySQL.

What is Relational Database?

Relational database means the data is stored as well as retrieved in the form of relations (tables). Table 1 shows the relational database with only one relation called STUDENT which stores ROLL_NO, NAME, ADDRESS, PHONE and AGE of students.

STUDENT

ROLL_NO	NAME	ADDRESS	PHONE	AGE
1	RAM	DELHI	9455123451	18
2	RAMESH	GURGAON	9652431543	18
3	SUJIT	ROHTAK	9156253131	20
4	SURESH	DELHI	9156768971	18

TABLE 1

These are some important terminologies that are used in terms of relation.

Attribute: Attributes are the properties that define a relation. e.g.; ROLL_NO, NAME etc.
Tuple: Each row in the relation is known as tuple. The above relation contains 4 tuples, one of which is shown as:

1	RAM	DELHI	9455123451	18

Degree: The number of attributes in the relation is known as degree of the relation. The STUDENT relation defined above has degree 5.

Cardinality: The number of tuples in a relation is known as cardinality. The STUDENT relation defined above has cardinality 4.

Column: Column represents the set of values for a particular attribute. The column ROLL_NO is extracted from relation STUDENT.

ROLL_NO
1
2
3
4

The queries to deal with relational database can be categories as:

Data Definition Language: It is used to define the structure of the database. e.g.; CREATE TABLE, ADD COLUMN, DROP COLUMN and so on.

Data Manipulation Language: It is used to manipulate data in the relations. e.g.; INSERT, DELETE, UPDATE and so on.

Data Query Language: It is used to extract the data from the relations. e.g.; SELECT

So first we will consider the Data Query Language. A generic query to retrieve from a relational database is:

1. SELECT [DISTINCT] Attribute_List FROM R1,R2….RM
2. [WHERE condition]
3. [GROUP BY (Attributes)[HAVING condition]]
4. [ORDER BY(Attributes)[DESC]];

Part of the query represented by statement 1 is compulsory if you want to retrieve from a relational database. The statements written inside [] are optional. We will look at the possible query combination on relation shown in Table 1.

Case 1: If we want to retrieve attributes ROLL_NO and NAME of all students, the query will be:

```
SELECT ROLL_NO, NAME FROM STUDENT;
```

ROLL_NO	NAME
1	RAM

2	RAMESH
3	SUJIT
4	SURESH

Case 2: If we want to retrieve ROLL_NO and NAME of the students whose ROLL_NO is greater than 2, the query will be:

```
SELECT ROLL_NO, NAME FROM STUDENT
WHERE ROLL_NO>2;
```

ROLL_NO	NAME
3	SUJIT
4	SURESH

CASE 3: If we want to retrieve all attributes of students, we can write * in place of writing all attributes as:

```
SELECT * FROM STUDENT
WHERE ROLL_NO>2;
```

ROLL_NO	NAME	ADDRESS	PHONE	AGE
3	SUJIT	ROHTAK	9156253131	20
4	SURESH	DELHI	9156768971	18

5.14 Database Replication

Data Replication is the process of storing data in more than one site or node. It is useful in improving the availability of data. It is simply copying data from a database from one server to another server so that all the users can share the same data without any inconsistency. The result is a distributed database in which users can access data relevant to their tasks without interfering with the work of others.

Data replication encompasses duplication of transactions on an ongoing basis, so that the replicate is in a consistently updated state and synchronized with the source. However, in data replication data is available at different locations, but a particular relation has to reside at only one location.

There can be full replication, in which the whole database is stored at every site. There can also be partial replication, in which some frequently used fragment of the database is replicated, and others are not replicated.

Types of Data Replication

1. Transactional Replication
2. Snapshot Replication

3. Merge Replication

Replication Schemes

1. Full Replication – The most extreme case is replication of the whole database at every site in the distributed system. This will improve the availability of the system because the system can continue to operate as long as at least one site is up.

Advantages of full replication

- High Availability of Data.
- Improves the performance for retrieval of global queries as the result can be obtained locally from any of the local site.
- Faster execution of Queries.

Disadvantages of full replication

- Concurrency is difficult to achieve in full replication.
- Slow update process as a single update must be performed at different databases to keep the copies consistent.

2. No Replication – The other case of replication involves having No replication – that is, each fragment is stored at only one site.

Advantages of No replication

- The data can be easily recovered.
- Concurrency can be achieved in no replication.

Disadvantages of No replication

- Since multiple users are accessing the same server, it may slow down the execution of queries.
- The data is not easily available as there is no replication.

3. Partial Replication – In this type of replication some fragments of the database may be replicated whereas others may not. The number of copies of the fragment may range from one to the total number of sites in the distributed system. The description of replication of fragments is sometimes called the replication schema.

Advantages of Partial replication

- The number of copies of the fragment depends upon the importance of data.

Advantages of Data Replication

Data Replication is generally performed to:

- To provide a consistent copy of data across all the database nodes.
- To increase the availability of data.
- The reliability of data is increased through data replication.
- Data Replication supports multiple users and gives high performance.

- To remove any data redundancy, the databases are merged, and slave databases are updated with outdated or incomplete data.
- Since replicas are created there are chances that the data is found itself where the transaction is executing which reduces the data movement.
- To perform faster execution of queries.

Disadvantages of Data Replication

- More storage space is needed as storing the replicas of same data at different sites consumes more space.
- Data Replication becomes expensive when the replicas at all different sites need to be updated.
- Maintaining Data consistency at all different sites involves complex measures.

5.15 Distributed DBMS

In a distributed database, there are several databases that may be geographically distributed all over the world. A distributed DBMS manages the distributed database in a manner so that it appears as one single database to users. In the later part of the chapter, we go on to study the factors that lead to distributed databases, its advantages and disadvantages.

A distributed database is a collection of multiple interconnected databases, which are spread physically across various locations that communicate via a computer network.

Features

- Databases in the collection are logically interrelated with each other. Often, they represent a single logical database.
- Data is physically stored across multiple sites. Data in each site can be managed by a DBMS independent of the other sites.
- The processors in the sites are connected via a network. They do not have any multiprocessor configuration.
- A distributed database is not a loosely connected file system.
- A distributed database incorporates transaction processing, but it is not synonymous with a transaction processing system.

Distributed Database Management System

A distributed database management system (DDBMS) is a centralized software system that manages a distributed database in a manner as if it were all stored in a single location.

Features

- It is used to create, retrieve, update and delete distributed databases.
- It synchronizes the database periodically and provides access mechanisms by the virtue of which the distribution becomes transparent to the users.
- It ensures that the data modified at any site is universally updated.

- It is used in application areas where large volumes of data are processed and accessed by numerous users simultaneously.
- It is designed for heterogeneous database platforms.
- It maintains confidentiality and data integrity of the databases.

Factors Encouraging DDBMS

The following factors encourage moving over to DDBMS –

- Distributed Nature of Organizational Units – Most organizations in the current times are subdivided into multiple units that are physically distributed over the globe. Each unit requires its own set of local data. Thus, the overall database of the organization becomes distributed.
- Need for Sharing of Data – The multiple organizational units often need to communicate with each other and share their data and resources. This demands common databases or replicated databases that should be used in a synchronized manner.
- Support for Both OLTP and OLAP – Online Transaction Processing (OLTP) and Online Analytical Processing (OLAP) work upon diversified systems which may have common data. Distributed database systems aid both these processing by providing synchronized data.
- Database Recovery – One of the common techniques used in DDBMS is replication of data across different sites. Replication of data automatically helps in data recovery if database in any site is damaged. Users can access data from other sites while the damaged site is being reconstructed. Thus, database failure may become almost inconspicuous to users.
- Support for Multiple Application Software – Most organizations use a variety of application software each with its specific database support. DDBMS provides a uniform functionality for using the same data among different platforms.

5.16 Functional Dependencies

What is a functional dependency?

Functional Dependency is when one attribute determines another attribute in a DBMS system. Functional Dependency plays a vital role to find the difference between good and bad database design.

Example:

Employee number	Employee Name	Salary	City
1	Dana	50000	San Francisco
2	Francis	38000	London
3	Andrew	25000	Tokyo

In this example, if we know the value of Employee number, we can obtain Employee Name, city, salary, etc. By this, we can say that the city, Employee Name, and salary are functionally depended on Employee number.

A functional dependency is denoted by an arrow →
The functional dependency of X on Y is represented by X →Y

Key terms

Here, are some key terms for functional dependency:

Key Terms	Description
Axiom	Axioms is a set of inference rules used to infer all the functional dependencies on a relational database.
Decomposition	It is a rule that suggests if you have a table that appears to contain two entities which are determined by the same primary key then you should consider breaking them up into two different tables.
Dependent	It is displayed on the right side of the functional dependency diagram.
Determinant	It is displayed on the left side of the functional dependency Diagram.
Union	It suggests that if two tables are separate, and the PK is the same, you should consider putting them. together

Rules of Functional Dependencies

Below given are the Three most important rules for Functional Dependency:

- Reflexive rule –. If X is a set of attributes and Y is_subset_of X, then X holds a value of Y.
- Augmentation rule: When x -> y holds, and c is attribute set, then ac -> bc also holds. That is adding attributes which do not change the basic dependencies.
- Transitivity rule: This rule is very much similar to the transitive rule in algebra if x -> y holds and y -> z holds, then x -> z also holds. X -> y is called as functionally that determines y.

Types of Functional Dependencies

- Multivalued dependency:
- Trivial functional dependency:
- Non-trivial functional dependency:
- Transitive dependency:

Multivalued dependency in DBMS

Multivalued dependency occurs in the situation where there are multiple independent multivalued attributes in a single table. A multivalued dependency is a complete constraint

between two sets of attributes in a relation. It requires that certain tuples be present in a relation.

Note: You need to remember that transitive dependency can only occur in a relation of three or more attributes.

Advantages of Functional Dependency

- Functional Dependency avoids data redundancy. Therefore, same data do not repeat at multiple locations in that database
- It helps you to maintain the quality of data in the database
- It helps you to defined meanings and constraints of databases
- It helps you to identify bad designs
- It helps you to find the facts regarding the database design

Summary

- Functional Dependency is when one attribute determines another attribute in a DBMS system.
- Axiom, Decomposition, Dependent, Determinant, Union are key terms for functional dependency
- Four types of functional dependency are 1) Multivalued 2) Trivial 3) Non-trivial 4) Transitive
- Multivalued dependency occurs in the situation where there are multiple independent multivalued attributes in a single table
- The Trivial dependency occurs when a set of attributes which are called a trivial if the set of attributes are included in that attribute
- Nontrivial dependency occurs when A->B holds true where B is not a subset of A
- A transitive is a type of functional dependency which happens when it is indirectly formed by two functional dependencies
- Normalization is a method of organizing the data in the database which helps you to avoid data redundancy
- Functional dependency helps you to maintain the quality of data in the database

5.17 Database Security

Data is a valuable entity which must have to be firmly handled and managed as with any economic resource. So, some part or all of the commercial data may have tactical importance to their respective organization and hence must have to be kept protected and confidential. In this chapter, you will learn about the scope of database security. There is a range of computer-based controls that are offered as countermeasures to these threats.

1. What is Database Security?
2. What is a Threat?
3. Computer-Based Controls
4. What are Access Controls?
5. Backup and Recovery

1. What is Database Security?

Database security is the technique that protects and secures the database against intentional or accidental threats. Security concerns will be relevant not only to the data resides in an organization's database: the breaking of security may harm other parts of the system which may ultimately affect the database structure. Consequently, database security includes hardware part, software part, human resource, and data. To efficiently do the uses of security needs appropriate controls, which are distinct in a specific mission and purpose for the system. The requirement for getting proper security while often having been neglected or overlooked in the past days; is now more and more thoroughly checked by the different organizations.

We consider database security about the following situations:

- Theft and fraudulent.
- Loss of confidentiality or secrecy.
- Loss of data privacy.
- Loss of data integrity.
- Loss of availability of data.

These listed circumstances mostly signify the areas in which the organization should focus on reducing the risk that is the chance of incurring loss or damage to data within a database. In some conditions, these areas are directly related such that an activity that leads to a loss in one area may also lead to a loss in another since all of the data within an organization is interconnected.

2. What is a Threat?

Any situation or event, whether intentionally or incidentally, can cause damage which can reflect an adverse effect on the database structure and consequently the organization. A threat may occur by a situation or event involving a person, or the action or situations that is probably to bring harm to an organization and its database.

The degree that an organization undergoes as a result of a threat's following which depends upon some aspects, such as the existence of countermeasures and contingency plans. Let us take an example where you have a hardware failure occurs corrupting secondary storage; all processing activity must cease until the problem is resolved.

3. Computer-Based Controls

The different forms of countermeasure to threats on computer systems range from physical controls to managerial procedures. In spite of the range of computer-based controls that are preexisting, it is worth noting that, usually, the security of a DBMS is merely as good as that of the operating system, due to the close association among them.

Most of the computer-based database security is listed below:

- Access authorization.
- Access controls.
- Views.

- Backup and recovery of data.
- Data integrity.
- Encryption of data.
- RAID technology.

4. What is Access Controls?

The usual way of supplying access controls to a database system is dependent on the granting and revoking of privileges within the database. A privilege allows a user to create or access some database object or to run some specific DBMS utilities. Privileges are granted users to achieve the tasks required for those jobs.

The database provides various types of access controls:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

5. Backup and Recovery

Every Database Management System should offer backup facilities to help with the recovery of a database after a failure. It is always suitable to make backup copies of the database and log file at the regular period and for ensuring that the copies are in a secure location. In the event of a failure that renders the database unusable, the backup copy and the details captured in the log file are used to restore the database to the latest possible consistent state.

What Is Database Security and Why Is It Important?

Database security, and data protection, are stringently regulated. Although the law struggles to keep up with the constant changes of an evolving digital world, there are regulations in force which demand certain standards from any business with an online component. Users across the globe expect their privacy to be taken seriously and modern commerce must reflect this wish. If your company has an online component, then you must consider database security as a priority.

What is database security?

As a general rule now, if your company collects any data about customers, suppliers, or the wider community, it is stored on a database somewhere. This data may be sensitive and private and can be subject to strict privacy agreements including those referred to above. For example, your customers may provide you with an email address, postal address, and phone number when they purchase something from you. However, if this data is accessed without authority, sold to third parties, or otherwise misused, you could be subject to strict legal action from the people whose privacy has been compromised.

Basically, database security is any form of security used to protect databases and the information they contain from compromise. Examples of how stored data can be protected include:

- Software – software is used to ensure that people can't gain access to the database through viruses, hacking, or any similar process.

- Physical controls – an example of a physical component of database security could be the constant monitoring of the database by company personnel to allow them to identify any potential weaknesses and/or compromises.
- Administrative controls – this refers to things like the use of passwords, restricting the access of certain people to certain parts of the database, or blocking the access of some company personnel altogether.

Why is database security important?

Database security is more than just important: it is essential to any company with any online component. Sufficient database security prevents data bring lost or compromised, which may have serious ramifications for the company both in terms of finances and reputation. Database security helps:

- Company's block attacks, including ransomware and breached firewalls, which in turn keeps sensitive information safe.
- Prevent malware or viral infections which can corrupt data, bring down a network, and spread to all end point devices.
- Ensure that physical damage to the server doesn't result in the loss of data.
- Prevent data loss through corruption of files or programming errors.

As you will see, database security places an obligation on you and your business to keep sensitive data stored correctly and used appropriately. Complying with regulations and the applicable law not only reduces the risk of information being mishandled, but it protects you from both costly legal ramifications and lost customer confidence. Investment in Database security will ensure you have done your due diligence in terms of data protection.

5.18 Platform Hardening

Commercial and open-source system configurations such as Windows, Linux and Oracle do not always have all the necessary security measures in place to be deployed immediately into production. These configurations often have features and functionalities enabled by default, which can make them less secure, especially given the sophistication and resourcefulness of today's cybercriminals.

A system hardening program can help address this issue by disabling or removing unnecessary features and functionalities. This enables security teams to proactively minimize vulnerabilities, enhance system maintenance, support compliance and, ultimately, reduce the system's overall attack surface.

Unfortunately, many companies lack a formal system hardening program because they have neither an accurate IT asset inventory nor the resources to holistically maintain or even begin a program. An ideal system hardening program can successfully track, inventory and manage the various platforms and assets deployed within an IT environment throughout their life cycles. Without this information, it is nearly impossible to fully secure configurations and verify that they are hardened.

Planning and Implementing Your System Hardening Program

System hardening is more than just creating configuration standards; it also involves identifying and tracking assets in an environment, establishing a robust configuration management methodology, and configuring and maintaining system parameters to expected values. To manage and promote system hardening throughout your organization, start by initiating an enterprise wide program plan. Most companies are engaged in various stages of a plan but suffer from inconsistent approaches and execution.

A plan builds on the premise that hardening standards will address the most common platforms, such as Windows, Linux and Oracle, and IT asset classes, such as servers, databases, network devices and workstations. These standards will generally address approximately 80 percent of the platforms and IT asset classes deployed in an environment; the remaining 20 percent may be unique and require additional research or effort to validate the most appropriate hardening standard and implementation approach. By adopting the 80/20 rule, hardening will become more consistent, provide better coverage and increase the likelihood of continued success. Let's take a closer look at the components of a system hardening program plan and outline the steps you can take to get started on your hardening journey, gain companywide support of your strategy and see the plan through to completion.

1. Confirm Platforms and IT Asset Classes
2. Determine the Scope of Your Project
3. Establish Configuration Standards
4. Implement Your System Hardening Standards
5. Monitor and Maintain Your Program

System Hardening Has Never Been So Crucial

Implementing and managing an effective system hardening program requires leadership, security knowledge and execution. Obtaining executive commitment, management support and sufficient investment for the program is also crucial. If you carefully choose a combination of easy-to-implement platforms and IT asset classes and more challenging, longer-term hardening efforts, you'll see incremental improvements in program execution and support.

Companies everywhere and across industries face an ever-accelerating rate of change in both the threat and technology landscapes, making system hardening more crucial than ever. A hardening program isn't built in a day, but an effective, thoughtfully constructed plan can significantly lower your company's risk posture.

5.19 Security Best Practices

Database security requires extensive experience handling sensitive data and current knowledge of new cyber threats. Your business database contains information that cyber-criminals target to steal identities, credentials, and financial information. Below are 7 database security best practices to help keep your company database safe.

1. Keep security controls of database server on maximum
2. Separate servers and web servers

3. Encrypt all files and backups
4. Put a database firewall and web application firewall in place
5. Regularly update patches
6. Hack/audit your database to check your security
7. Keep an encrypted copy of your database on backup

Cloud backup allows you to recover any deleted or accidentally changed file to the version you require. Backup all pertinent databases using a reliable, cloud backup company focused on security. This will mean you always have a copy of all-important customer and company information stored away in case of an unforeseen problem and can retrieve the information upon request. Look into cloud backup companies that offer unlimited previous file versions (critical if a ransomware virus strikes) and military-grade security. These companies will offer the most thorough backup and recovery solutions and will keep your data safe no matter what.