**Chapter 4**

**Server, Clients, Virtual Machines and Other Devices**

There are many computers that we use every day and it has many different devices and systems which support our daily activities. There are different kind of computers which can be used for different tasks. There are different types of computers which can be used for different tasks for example the Stand-alone, Workstation and Client-Server. Virtual Machines and VPN are another interesting way in which we can use computers.

Stand-alone computers are computers which has no network connection. They do not require any local area network (LAN) or wide area network (WAN). Sometimes they are connected to a network, but the network is not mandatory for its general use. An example of stand-alone computer could be creating documents for instance presentation or a spread sheet. When computer is running local applications without internet access, the machine is technically a stand-alone PC. In 1990’s throughout the offices, millions of PCs were hooked up to a local network for file sharing which were called workstations (PC Encyclopedia, n.d.).

If we look in depth to a Workstation also known as Personal Computer, traditionally a computer on a network which is primarily used for an employee’s access and day-to-day activities. They were developed in the “U.S. in 1981 by the National Aeronautics and Space Administration for it’s Apollo space program and was commercially introduced in 1983” (Britannica, n.d.). A workstation processes activity which do not require permission from any other device on a network. A pure workstation normally has only two types of connections for example a connection to the internet and a directly connected printer. Some workstation are primarily individual, solo computers which do not require other computers to complete normal function and day-to-day tasks. Some tasks performed by workstation could be:

* Checking e-mails
* Viewing websites
* Writing document
* Designing logo
* Modifying a photo

Aside from stand-alone and workstation there are other devices or networks devices which can be used on computers. In order to store and retrieve data the internet requires the use of network devices with many names. These devices hold and display movies, text, photos and many other products and services in the world. Some examples of that will be Client, Server, Hubs, Switches, and Routers. As mentioned earlier that workstations were introduced in the 1990s, client-server networking grew popularity during that time too.

A Client performs all the functions of a Workstation with a few special modifications. A Client request services, access, or permissions from another computer called “Server”. Essentially, a client computer must ask a Server for approval for many functions a user might attempt on a client. Many clients require a user to input a “username” and “password” prior to using client. When the username and password are typed by the user, the information is sent to a server for approval. Examples of a client will be computers in a Library or Cybercafés and staff computer in a company (Spencer, 2018)

There are also Thin-Clients which are created to essentially access server in some other location and interact with it. The user cannot tell but all transactions, saves, modifications and tasks are not occurring at the user’s location. These types of devices are used at mall kiosks, McDonalds counters for cash registers and doctor’s offices for nursing stations.

As mentioned earlier about “Server” it is a system that gives out stuff or hold stuff. There are many types of servers in operation such as:

* Web servers which hold and display websites
* Video server which allow access to movies online
* E-mail servers for transmitting and receiving texts and documents
* Domain Name Servers which allow users to find internet websites using friendly names

“Hub” is one of the oldest devices used in networks this device essentially multiplies physical connections to a network. If there is a single connection which leads to the internet in a building. The hub would allow multiple devices access to this single connection. These devices could be a computer, printer and even cameras. “Switch” is a device which operates much like hub except that it compensates for some of disadvantages associated with hubs.

Computer networks include many elements which were discussed earlier in the chapter. They are workstations, clients and servers which provide many different functions for company, business or enterprise. Working with server’s technology there is a need to develop experience using many different operating systems and devices. Many of these platforms are extremely expensive. There is an option which will allow a person to spend little or almost no money in order to practice and develop skills for administer and managing servers and workstation. This option is called “Virtualization”. (Spencer, 2018)

Virtualization is far from a new concept, but it has significantly evolved over the years. Originally developed in the 1960s as a way to share valuable mainframe resources (Lowe, 2004). Virtualization is process of using “make pretend” software which can duplicate the functions of real-life computers and servers. Literally, a person can install virtual software on a computer and perform a large number of activities and tasks which would be required on an actual server or workstation. The virtual servers are often called “Virtual Machines” or simply “VM’s”.

Virtual machines provide support for many of the major functions an actual server performs. Activities such as installing printers, hosting websites, storing shared documents and many other functions. VM’s can also interact with real world in activities such as communicating with real computers on a network or allowing access to the internet. Nevertheless, there is disadvantage to VM’s, they behave as an independent computer. Each VM, like all other computers require RAM. Essentially, the amount of RAM used by a VM is subtracted from the actual RAM on the real computer. (Spencer, 2018)

Similarly, to the idea of VM’s is VPN (Virtual Private Network) which was introduced in 1996 by a Microsoft employee while developing the peer-to-peer tunneling protocol (PPTP) (Le VPN, 2018). PPTP creates a more secure and private connection between a computer and the internet, which was later replaced by VPN due to security reason. The VPN is a private network on the internet, which creates a private connection between multiple people and devices. This is safe and encrypted network like the internet. VPN has the effect of creating a virtual area in the internet or other insecure location, which imitates like more secure private network (Kinkela & Yonker, Servers, Clients, Virtual Machines and Other Devices, 2019).

**Chapter 5**

**Databases and Data Management**

A database management System allows a person to organize, store, and retrieve data from a computer. The databases are major components in today’s internet technology.  All internet services that we use on a consumer basis are built around what is referred to as Client Server Architectures. This is called a Three Tiered Topology when connecting to the database through software on the Internet. As we learned in the earlier chapters about punch cards and how they were used for programming, they were used for input, output and data storage. It was a fast way to enter data, and to retrieve it. In 1980 Herman Hollerith adapted the punch cards which acted as the memory for mechanical tabulating machine.

There are many types of databases now a days, and most companies develop their own databases to adapt them to their needs. Although, there are many different types of Database Models, this chapter will concentrate more on a Relational Model because it is most widely used database model. The RDBMS (Relational Database Management System) which was presented in June 1970 by Dr. Edgar F. Codd, an IBM research scientist, in the paper “A Relational Model of Data for Large Shared Databanks”. The RDBMS is where the industry started. It was very popular and structured database, this means all the data are available in the form of Tables which consists of Rows and Columns. Each and every table contains a Primary Key and a Foreign Key (Quora, n.d.)

The primary key of a relational table uniquely identifies each record in the table.  Primary keys must contain unique values. Each table should have a primary key, and each table can have only ONE primary key. A foreign key is a referential constraint between two tables.  A foreign key is a field in a relational table that matches a unique key of another table.  Usually this is the primary key in another table.  The foreign key can be used as a bridge to cross-reference tables.

In data modeling, the cardinality of one data table with respect to another data table is a critical aspect of database design. Cardinality expresses minimum and maximum number of entity occurrences associated with one occurrence of related entity. Relationships between data tables define cardinality when explaining how each table links to another. In the relational model, tables can be related as any of: many-to-many, many-to-one (one-to-many), or one-to-one. These particular aspects are said to be the cardinality of a given table in relation to another.

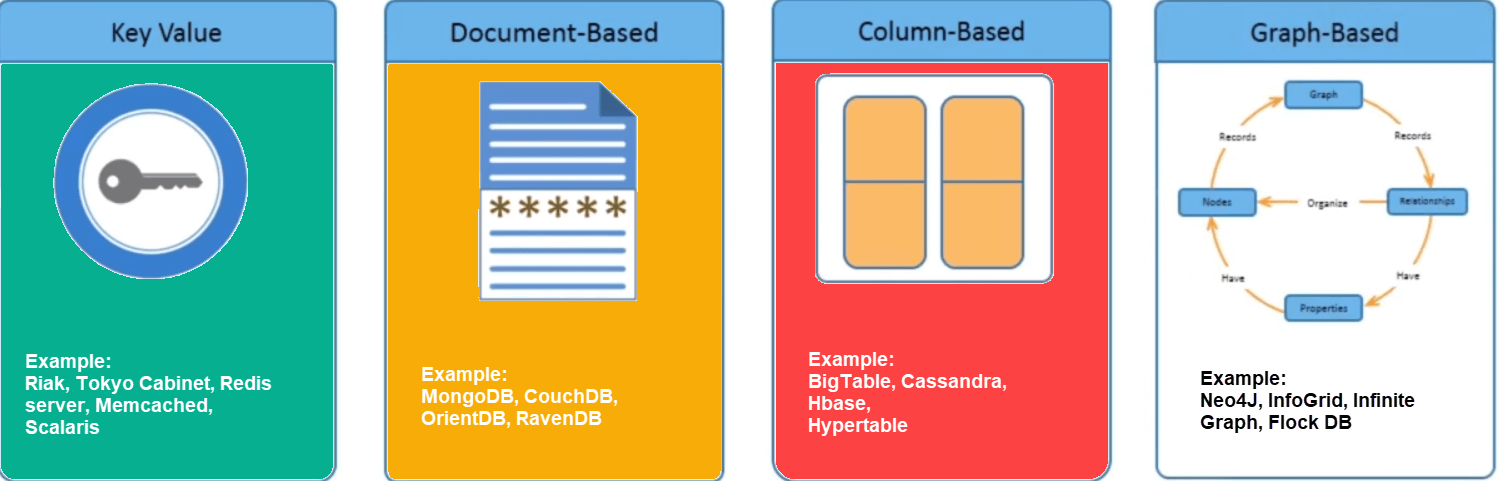
 In many-to-many relationships a mapping/translation table is created that maps the primary keys of the two entities involved in the many-to-many relationship. This creates two one-to-many relationships towards the mapping table. When there is a one to one relationship, one typically leaves it intact.  It is the desirable cardinality in a relational database. A one-to-one relationship is mostly used to split a table in two in order to optimize access or limit the visibility of some information. When there is a one to one relationship, one of two actions typically occur.  The first is to combine the two tables into a single table.  The second is to keep the two tables separated.  When this action is taken one table becomes the primary key table and the other becomes the foreign key table. The most frequently accessed table is typically assigned as the primary key table in the relationship (Nelson, 2018)

There is an alternative to this traditional Relation Database called NoSQL Databases which are especially useful for working with large sets of distributed data. NoSQL was first used in 1998 by Carlo Strozzi when he was naming his open-source “relational” database which did not use SQL. Later in 2009 Eric Evans and Johan Oskarsson came up with this name again when they were describing their non-relational databases. The term NoSQL can mean either “No SQL system” or the “Not only SQL” because systems might system SQL-like query languages. Not only can NoSQL systems handle both structured and unstructured data, but they can also process unstructured Big Data quickly. This led to organizations such as Facebook, Twitter, LinkedIn, and Google adopting NoSQL systems. These organizations process tremendous amounts of unstructured data, coordinating it to find patterns and gain business insights. Big Data became an official term in 2005 (Foote, 2018)

NoSQL uses data stores optimized for specific purposes. Normally, NoSQL stores data in one of four categories:

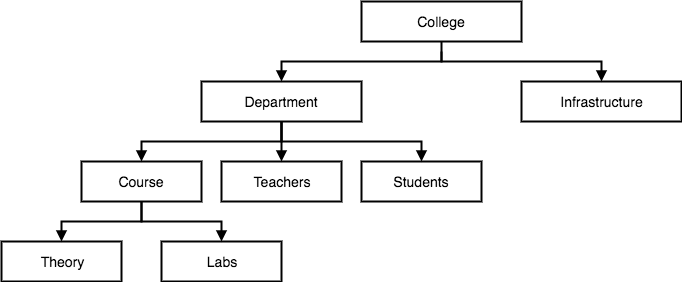
* **Key-Value Database** - Key-value databases store data in unique key-value pairs, meaning each key is associated only with one value in a collection, like in a dictionary. This makes querying a key-value data store fast because of its simple model. There’s no query language needed. Data retrieval is a simple matter of using get, put, and delete commands (Vargas, 2019)
* **Document Oriented Database** - Document databases use JSON, XML, or BSON documents to store data. You can pretty much fill in a document with whatever data you want (Vargas, 2019)
* **Wide Column Database** - wide-column database use columns to store data. You can group related columns into column families. Individual rows then constitute a column family (Vargas, 2019)
* **Graph Database** - Nodes and relationships are the bases of graph databases. A node represents an entity, like a user, category, or a piece of data. A relationship represents how two nodes are associated. Graph databases use nodes that contain lists of relationship records (Vargas, 2019)

**Figure 5.1**



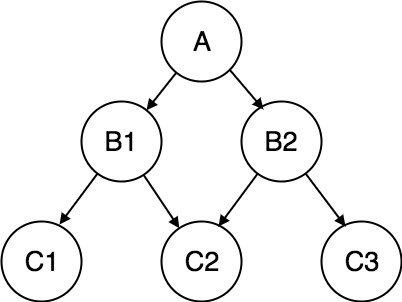
There are other database models too like Hierarchical Model and Network Model. The hierarchical model is a database that organizes data in a tree-like-structure with a single root to which all other data is linked (Study Tonight, n.d.). This structure was developed by IBM in the 1960’s and was used in early database systems. Below is an example of Hierarchical Model.

**Figure 5.2**



In 1969 Charles Bachman developed the Network Model and was later introduced in 1971. This model allows each record to have multiple parent and child records. Some of its benefits could be simple concept, ability to manage more relationships and easy access to data. Nevertheless, this model also has drawbacks like System Complexity and Functional Flaws (Techopedia, n.d.). Below is an example of Network Model

**Figure 5.3**



**Chapter 6**

**Cyber Security and Cyber Warfare**

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Criminals who perform these illegal activities are often referred to as hackers (Cybercrime, n.d.) There are many conversation in the cyber-security and computer world reference to the term “Hackers” but there are also lesser known terms given to different types of hackers for example “White Hat Hacker”, “Black Hat Hacker”, and “Grey Hat Hacker”. All of these terms are attempting to define the experts in the computer field who have a great understanding of computer language and computer communication software.

White Hat Hacker identify and exploit areas in which a computer or network system can be damaged or compromised. This person work for businesses which create options for computer security or antivirus software.

Black Hat Hackers participate in compromising or damaging computers and other network devices. They primarily work as contractor or individual/group, this person has a goal of participating in malicious activities concerning computer data, services or operation. Some examples of these could be:

* Stopping or destroying computer data using virus or network attacks (Trojan, Phishing, DoC, etc.)
* Accessing and distributing confidential data (Movies, credit card and personal data, etc.)
* Stopping an internet business being accessed by users (i.e., Netflix, Sony PlayStation, etc.).

Grey Hat hacker is between Black Hat Hacker and a White Hat Hacker. They do not have malicious intentions. Literally the Grey Hat Hacker does what a White Hat Hacker does, but illegally. Although there is a distinction made between these “Hackers”, their abilities are the same, but their motives define their classification. Depending on the situation and affiliations, they could be the “good guys” or “bad guys” depending on their perspective and the matter at hand.

There many types of cyber crimes like online bank information theft, identity theft, online predatory crimes, and unauthorized computer access. More serious crimes like cyber terrorism are also of significant concern (Kinkela & Yonker, Cyber Security and Cyber Warfare, 2019). These cyber criminals use a variety of programs like Computer Virus and Malware to accomplish their targets.

A virus is a program which was created to carry out malicious activities on a computer. Viruses come in multiple forms, but they all have at least two elements in common which are damaging effects and ability to replicate. A computer virus spreads between computer systems using some type of transmission or common contact area such as file, storage area (Flash drive, SD card, Website, etc.) or even an e-mail. All viruses do not immediately attack a computer or user, but usually stay inactive on a system until the user performs a specific activity. The first virus that attacked MS-DOC is called Brain and was written by two brothers Basit Farooq Alvi and Amjad Farooq Alvi in 1986 Lahore, Pakistan. This virus infected the boot sector of storage media formatted with the DOS file Allocation Table (FAT) file system. The two brothers made this virus for themselves, but they didn’t know that it will become such a growing into a global-sized monster, with powers beyond capabilities (Radiska, 2016). Some of the categories on viruses will be the following:

* **Spyware** – spyware is installed without a computer owner’s permission in order to gather private information often by reporting the data in the form of an e-mail. The information could include, internet activities, visited websites, keystrokes (keylogging), saved documents and passwords. Spyware made its first significant public impact in 1999, when the popular freeware game Elf Bowling was discovered to be laced with tracking software (Finjan, n.d.)
* **Adware** – adware use began in 1995 and some industry experts considered it to be a spyware, but they are variant, and it will cause a computer browser homepage to change or initiate visiting unknown websites without the users request or display commercials randomly on a computer.
* **Trojan** – Trojan was first developed by computer programmer John Walker in 1975. This virus is created to look innocent. Often it will look like a normal document such as a “docx” or “pdf”. It also disguised as an e-mail attachment. Traditionally, Trojans do not replicate automatically and require a user to perform some type activity to activate them. Once the virus is being activated, they perform several attacks like recording the keys pressed on a keyboard, deleting files, changing filenames or making files invisible.
* **Worm** – Worm travel between computers in order to send copies of date back to the creator of worm. Normally this data is credit card, social security numbers, and customer databases, etc. An important aspect involving a Worm is that it is normally “self-replicating”. Once launched on a computer, until erased, a Worm is totally self-sufficient. The first internet worm called “Morris Worm” was released in 1988.
* **Macro** – this virus originates from the function available in programs to automatically perform several tasks after activating a key combination or clicking on a single icon. A macro virus install itself into any files or documents created with that program. In December 1994, the researcher Joel McNamara wrote the first real macro virus for demonstration purposes. In 1995 this virus was accidently included on CD-ROM by Microsoft to hundreds of corporations (Tech Target, n.d.)
* **Hijackware** – this type of virus modifies the settings of Internet Explorer, Google Chrome, and Firefox. The result of hijackware is evident when a user’s internet search is randomly searched. Often time, the home page of the user or the default search engine is also changed.

In addition to the danger of viruses, there are people who use their knowledge of computer code and software to create applications to actively attack and disable computers and entire networks. These individuals can literally access a computer system and attempt to compromise computer settings. The following are some types of active system attacks:

* **Brute Force Attack** – this type of attack occurs when several randomly selected numbers, usernames, passwords and phrases are attempted to access a computer or network resources. This process is totally “Trial and Error”. Either an actual person can be used to attempt a brute force attack or software can be used to attempt thousands of random combinations.
* **Dictionary Attack** – this type of attack requires the use of some type of database of specific numbers, usernames, passwords and phrases. The reason it is called a dictionary attack is due to the predetermined numbers, usernames, passwords and phrases selection is much likely that which appears in a dictionary.
* **Social Engineering** – this is the art of manipulating people and uses human interaction in order to derive confidential information. Using everyday seemingly normal conversations, the attacker is attempting to gain information such as passwords, confidential data locations.
* **Baiting** – making convenient access to a device such as a flash drive to a computer user who the attacker wants to compromise. The person who picks up the flash drive and uses it does not know that the flash drive has software on it which will automatically install various things like monitoring or remote access software.
* **Phishing** – this usually happens via telephone, e-mail, and text messaging. Essentially, a message is received informing of some important occurrence like Lottery Winner and Bank Account Confirmation. Somewhere in the communication there will be a request to send the message sender some type of confidential data. Once the data is sent, the attacker now can either steal data or launch attacks against the user’s servers.

Cyber Warfare refers to the use of technology to launch attacks on nations, governments and citizens, causing comparable harm to actual warfare using weaponry. The problem with cyber warfare is that its very hard to work out who launched the attack in the first place (McCallion, 2019). The most common technique that has been used in cyber warfare is (DoS) Denial of Service attack, it is the major tool of Cyber Warfare. This attack is usually intended to shut down a machine or network, making it inaccessible to its users.

The first-ever DoS attack occurred in 1974 by a 13-year-old high school student. He learned a new command that could be run on PLATO terminal (PLATO was the first generalized computer-assisted instruction system). He was curious to see how it would be like for a room full of users to be locked out at once, he wrote a program that would send the “ext” command to many PLATO terminals at the same time. Dennis went over to Computer-Based Education Research Laboratory and testes his program, which succeeded in forcing all 31 users to power off at once. There is also Distributed Denial-of-Service attack which is abbreviated as DDoS. DoS is different from DDoS because DoS usually uses one computer and on internet connection to flood a targeted system or resource. The DDoS attack uses multiple computers and internet connections to flood the targeted resources. DDoS attacks are often global attacks, distributed via botnets (Beal, n.d.). There are several DoS attacks that has happened in the history by using DDoS method which are mentioned below.

In February 2000 Michael Calce also known as Mafia Boy (a security expert and former computer hacker) launched a highly publicized DoS attack against large commercial websites, including Yahoo, Amazon, eBay, Fifia.com etc. To mention some other attacks In January 2001, Register.com was targeted, DNS servers were used as reflector in that attack. On two occasions to date, attackers have performed DNS Backbone DDoS Attacks on the DNS root servers. The first occurred in October 2002 and disrupted service at 9 of the 13 root servers. The second occurred in February 2007 and caused disruptions at two of the root servers. Even CERT/CC, one of the Internet's leading network security sites, was also suffered from DDoS attack in May 2001. In the same year, DDoS attack was launched targeting Whitehouse.gov domain. In January 2004, MyDoom attacked 1 million computers. In February 2007, more than 10,000 online servers in games such as such as Return to Castle Wolfenstein, Halo, Counter-Strike and many others were attacked. After one year, WordPress.com was attacked resulting in 15 minutes of outage. The incidents citing DDoS attacks are endless. These attacks demonstrate the potential of attackers (Arora, 2011)

# Works Cited

Arora, K. (2011). Impact Analysis of Recent DDoS Attacks. *International Journal on Computer Science and Engineering*, 4.

Beal, V. (n.d.). *webopedia.com*. Retrieved from webopedia: https://www.webopedia.com/TERM/D/DDoS\_attack.html

Britannica, E. o. (n.d.). *britannica.com*. Retrieved from britanicca: https://www.britannica.com/technology/workstation

*Cybercrime*. (n.d.). Retrieved from techopedia.com: https://www.techopedia.com/definition/2387/cybercrime

Finjan. (n.d.). *Finjan Cyber Security*. Retrieved from Finjan Cyber Security Web site: https://blog.finjan.com/the-past-and-present-state-of-spyware/

Foote, K. D. (2018, June 18). *Dataversity.net*. Retrieved from Dataversity: https://www.dataversity.net/a-brief-history-of-non-relational-databases/

Kinkela, M. P., & Yonker, V. (2019, November 3). Cyber Security and Cyber Warfare. Philadelphia, PA, USA.

Kinkela, M. P., & Yonker, V. (2019, October 23). Servers, Clients, Virtual Machines and Other Devices. Philadelphia, PA, USA.

*Le VPN*. (2018, August 17). Retrieved from levpn.com: https://www.le-vpn.com/history-of-vpn/

Lowe, S. (2004, November 3). *TechRepublic*. Retrieved from techrepublic.com: https://www.techrepublic.com/article/solutionbase-an-introduction-to-virtual-machines/

McCallion, J. (2019, September 20). *IT Pro*. Retrieved from IT Pro Web site: https://www.itpro.co.uk/security/28170/what-is-cyber-warfare

Nelson, C. (2018, May). Database Management Systems. PA, U.S.

*PC Encyclopedia*. (n.d.). Retrieved from pcmag.com: https://www.pcmag.com/encyclopedia/term/51969/stand-alone-pc

Quora. (n.d.). *Quora*. Retrieved from https://www.quora.com/What-are-the-different-types-of-databases

Radiska, T. (2016, September 8). *The Vitage News*. Retrieved from The Vitage News Web site: https://www.thevintagenews.com/2016/09/08/priority-brain-first-computer-virus-created-two-brothers-pakistan-just-wanted-prevent-customers-making-illegal-software-copies/

Spencer, R. (2018). *Foundations of Windows Computers 2.0.* Middletown.

*Study Tonight*. (n.d.). Retrieved from studytonight.com: https://www.studytonight.com/dbms/database-model.php

*Tech Target*. (n.d.). Retrieved from Tech Target Web site: https://searchsecurity.techtarget.com/definition/macro-virus

*Techopedia*. (n.d.). Retrieved from techopedia.com: https://www.techopedia.com/definition/30613/network-model-databases

Vargas, K. (2019, August 20). *Studio 3T*. Retrieved from studio3t.com: https://studio3t.com/knowledge-base/articles/nosql-database-types/

<https://www.studytonight.com/dbms/images/hierarchical-dbms-model.png>

<https://www.studytonight.com/dbms/images/network-dbms-model.png>

[https://miro.medium.com/max/2998/1\*cCpM0QPSUXftgwAfkZyEuQ.png](https://miro.medium.com/max/2998/1*cCpM0QPSUXftgwAfkZyEuQ.png)