Salwa Ghaffar

Info 101 milestone 4

The Evolution of Technology

Table of Contents

[Introduction 2](#_Toc26658239)

[Chapter 1 - Intro to Computing and Security Technology 5](#_Toc26658240)

[Chapter 2 - The Internet and the WEB 10](#_Toc26658241)

[Chapter 3 - Components of Computing Devices 12](#_Toc26658242)

[Chapter 4 - Server, Clients, Virtual Machines and Other Devices 16](#_Toc26658243)

[Chapter 5 - Databases and Data Management 20](#_Toc26658244)

[Chapter 6 - Cyber Security and Cyber Warfare 24](#_Toc26658245)

[Chapter 7 - Identity Theft and Individual Cyber Security 29](#_Toc26658246)

[Chapter 8 - Linux and Open Source 34](#_Toc26658247)

[Chapter 9 - Command Line Interface 37](#_Toc26658248)

[Chapter 10 - Computing Technology Management and Administration 39](#_Toc26658249)

[Cloud Systems Administrator 40](#_Toc26658250)

[Web Content Manager 40](#_Toc26658251)

[Database Administrator 40](#_Toc26658252)

[Device Administrator 41](#_Toc26658253)

[Network Administrator 41](#_Toc26658254)

[Project Administrators 41](#_Toc26658255)

[Software Application Administrator 41](#_Toc26658256)

[System Administrator 42](#_Toc26658257)

[Conclusion 42](#_Toc26658258)

[References 44](#_Toc26658259)

# Introduction

In this paper, it is intended to critically appraise the evolution of technology, if we think about the gadgets that we are using every day, it has created amazing tools and resources putting at our fingertips. Now let’s think about the time when these gadgets did not exist. If we think about 30’s or 40’s over that time no one knew about these technologies and there were some inventions, but they were not known to most of the people. The world first program-controlled computer Z1 was created in Germany in 1935 – 1938 by Konrad Zues, but it was not known by everyone in fact most of our thinking is the technology innovations started in United States. This paper will be stating interesting facts about the technology evolution and why it is so important in our lives now a days. In this paper we will be discussing about how the IT industry evolved from the time when there were no known computers to the time where we can get all the data in a small gadget like smartphones and smartwatches.

1. Introduction to computing and Security Technology: we have a lot of software’s and gadgets that is being used for computing and security which we didn’t had in the past. One of the main reasons for this could be that the online banking and shopping which needs more security because the more the technology evolve the more it has threat.
2. The Internet and the Web: over the past decades the internet and web evolved a lot.In the past internet was not even available to everyone except army, and web browser or search engine like google were created to handle the enormous number of data available on online.
3. Components of Computing Devices: in the past there weren’t any digital computers, people who were using computers they were analog even the first computer invented was calculator which was a big invention in the past.
4. Servers, Clients, Virtual Machines, and Other Devices: client and servers were used to use mainframes and connect to dumb terminals until when the personal computers started and replaced terminals. Now a days the client and server are used to form a network that connects multiple users. As we know that virtual machines can be used to act as hypervisor and runs another operating system in you***r*** actual computer, it is also called a guest host which emulate different OS systems and hardware platforms.
5. Databases and Data Management: database management is often used for storing and organizing computer data. In the early time there weren’t any software’s and tools to use for data management. In early years punch cards were used managing data it was fast way to enter data and retrieve it.
6. Cyber Security and Cyber Warfare: in the past there wasn’t that much use of cyber security because the technology was not that advance. Even the cybersecurity began at the time when there weren’t any malicious software’s. the threats to computers at that time were known and clear. The first program of self-replicating worm was made at that time by Ray Tomlinson. Cyber warfare is defined as a technology to damage electronic and physical assets of a state or organization by using viruses, worms, and also ransomware.
7. Identity Theft and Individual Cyber Security: since the technology has evolved the risk of Identity theft has also been increased with it. Most common identity thefts could be achieved by the internet, hacking, and phishing. Now a days the identity theft has become easy for criminals because of the use of technology.
8. Linux and Open Source: when we talk about open source technology the first word that comes to our mind is Linux. Linux is an operating system and since it is open source so anyone can use, copy, study, and change the software in any way. Linux is another version of UNIXthis which was developed in the mid-1970s and was originally developed as a multitasking system for minicomputers and mainframes.
9. Command Line Interface: before having the command line it was hard to save files to disk and have multiple running applications with multiple users. The idea of command line was evolved from UNIX in 1969 but was also influenced by a program RUNCOM. The earliest command-line systems combine teletypes with computers, which were originally invented for automatic telegraph.
10. Computing Technology Management and Administration: as the technology has evolved so as the management of computing technology and administration. Computing technology management usually focus on system’s hardware, software, database, and networks.

This paper chapters will be about these ten topics and how it has evolved to this modern technological world.

# Chapter 1 - Intro to Computing and Security Technology

If we think about technology that we are using now it doesn’t seem like we have enough of it. We have greatly developed in technology like computers which never existed in some earlier eras. We can advance more, for instance we have smartphones which works like computers. Nonetheless there was a time when these things did not exist previously. These chapters will address some of the inventions that we don’t know the history of. Most of them we don’t know who created them. We are using all these devices whether they are created by Microsoft or Apple, but we don’t know when they started, how they created these devices, and who started programming for computers. We play video games now a days and we even have careers which are for Computer Science, Cyber Security, Gaming, and Data Management, but we don’t know when we had them and who invented them.

Now that the discussion about computing has begun, we will talk about who invented the first computer, and when the computer was invented. The first computer that was invented was a calculator, it was invented by Charles Babbage who is also known as “The Father of Computer.” He wanted to mechanically calculate mathematical tables. In 1812 or 1813 he made a small calculator, which was able to perform certain computations to eight decimals. In the mid-1830s Babbage developed plans for an Analytical Engine, the ancestor of the modern digital computer. In his device he planned the capability of any arithmetical operations (Britannica, n.d.). Babbage was an English mathematician and inventor who created the first digital computer. He developed a plan for an Analytical Engine in the mid-1830s even though it was never completed but it had most of the basic elements of a present-day computer. His Analytical Engine was used later to do the first programming.

Later, in 1843 Augusta Ada, who was an associate of Babbage, annotated an article which was about Babbage’s analytical machine elements. Augusta elaborated on her annotation and proposed the idea that the Analytical Engine can be programmed. She has been addressed as a first programmer in the history who not only gave the idea about codes which can be used to handle symbols and letters along with numbers, but also made the theory for the looping in computer programming. She is like an idol for girls in computing. There were also women who got recognition in the computing world. She was the first programmer and her idea about looping is still being used in programming language (Britannica, n.d.). There is still a lot of people who don’t believe or support women in IT and think that they don’t qualify enough but the history has its own records that the first programming language was started by a woman. In 1980 a new computing language was developed and named “Ada” after Augusta. However, the analytical engine was never completed, but his notebook was discovered in 1937. In 1991 Doron Swade led the Science Museum library in London to construct Difference Engine 2 accurate to 31 digits. Doron Swade used Babbage’s design as reference for this development (News, 2000). Just like Charles Babbage and Augusta Ada there are also some other people who contributed to the development of computing and computer security like Alan Turing.

Alan Turing, who is known as “The Father of Computer Security or Modern Computing”, was a computer scientist, cryptanalyst, and a brilliant mathematician. His biggest invention was the Turing Machine which he created in 1936. It was a simple machine but could simulate any computer algorithm, no matter how complicated it is. During World War II he worked with wartime cryptanalytic headquarters. He created a computer that was used to decode the German Enigma machine which Germans were using during war to encode their messages in which they were discussing war related plans. The Polish Bombe which they used against Germany**~~’s~~** was a more powerful device. It could break any Enigma message where a small portion of plaintext could be guessed correctly (Hodges, n.d.). More details about cyber security and cyber warfare will be discussed later in chapters. There were also some people who can be credited of making the Electronic Numerical Integrator and a commercial computer for business.

John (William) Mauchly and J. Presper Eckert are the scientists credited with the invention of the Electronic Numerical Integrator and Computer (ENIAC) in 1943-1944. ENIAC was funded as a technology that could be used in war, but the war was over at that time. However, the ENIAC was employed by the military, this invention was revealed in February 1946. They also designed the Electronic Computing System for The U.S. Census Bureau which was the first commercial computer for business and government applications in 1946 (Lemelson-MIT Celebrating invention, inspiring youth, n.d.). In 1949 their company also launched the BINAC Binary Automated Computer which was using magnetic tape to store data. While they were being funded by the Census Bureau, they delivered their first UNIVAC computer to the Census Bureau in June 1951. Just like John William Mauchly and J. Presper Eckert there were two scientists who created the integrated circuit or computer chip. Although they did not work together, their invention was at the same time and the idea to make an integrated circuit came to them around the same time.

Jack Kilby and Robert Noyce, they came up with the idea of putting all elements of an electronic circuit to a single silicon chip. In 1947 they created their integrated circuit which is also known as a microchip. The integrated circuit made it possible to incorporate a roomful of equipment into a device that could be held in the palm of the hand. It also made electronic equipment dramatically cheaper to manufacture. Microchips now control most electrical devices, including all computers (BBC UK, n.d.). In the 1940s to 1950s more people were involved in the industry and bringing their invention. There was also another woman who could be credited for developing the first programming languages.

Grace Hopper was a computer scientist, mathematician and a navy officer. During World War II she joined the U.S. Navy and was assigned to program the Mark I Computer. After the war ended, she continued to work in computing. She was leading the team that created the first computer language compiler, which led to the popular COBOL language in 1953 (Biography, n.d.). After some time of COBOL another programming language FORTRAN was created.

In 1954 John Backus created a programming language called FORTRAN, in full, Formula Translation. His new program made computer programing more accessible because previous programs were written in machine language, which required the programmer to write instructions in binary or hexadecimal arithmetic. Since Backus was frustrated with this hard programming language, he was led to find a simpler way. Backus led IBM employees to create a language that combined a form of English shorthand with algebraic equations. FORTRAN was a faster writing computer program than the other program that ran nearly as efficiently as programs that had been laboriously. He made it as easy as possible because at that time most of the people didn’t have any computers, so it was hard for them to manage writing those long programs. It was expensive for them to afford programming languages because at that time using computers was not common (Britannica FORTRAN , n.d.). Now a days we are using a lot of programming languages, specially Python and JavaScript, also required for almost every technology student to take for their major. There are languages like Java and C++ to name a few. There were also some other inventions rather than programming we all are using now a days, like the mice for computers and the graphical user interface.

Douglas Engelbart was an American inventor who invented the computer mouse in the 1950s. He also developed the basic of graphical user interface which is known as GUI. He also created a groupware which is a type of computer program that shares data between more than one computer for processing. He also won the A.M. Turing Award which is the highest honor in computer science. In 1963 he was funded by SRI for his own laboratory where he worked on inventing and perfecting various devices such as the computer mouse, the multiple window display and hypermedia. His work made it possible for ordinary people to use computers. There were a lot of inventions and mentioning all of them will take chapters to write them down (Hall, n.d.).

As mentioned earlier there were not that many computers to be used by everyone. In 1974-1977 the personal computer, like Scelbi and Mark-8, were an early model of microcomputers based on Intel 8008 processor and CPU, reached the market. In 1975 Bill Gates and Paul Allen formed their own software company Microsoft after their success of writing down a software for the Altair using the new BASIC language. Yes, Microsoft whose products are the most famous ones they started their company in 1975 and after one year another famous and well-known company was formed; Apple, whose products we are using everyday now a days. Steve Jobs and Steve Wonzniak started their Apple Computers on April 1, 1976. Steve Wonzniak was used to work on internal computer and Steve Jobs worked on the external computer. Although there were computers being used by people, Apple took the stage because of their designs and it could be seen even now of how they design their products.

Nevertheless, there were a lot of inventions that came after time to time, but all these modern technologies could never have been possible without the hard work of these inventions. Now a days we have so many devices at home but back in 1812 or 1813 the biggest invention was a calculator which was called a computer those days. If we talk about programming than it was started by women. Women were the ones who led the programming world and Augusta Ada was such a brilliant woman who even gave the idea of looping which we are using in JavaScript and python etc. to make our codes easier.

# Chapter 2 - The Internet and the WEB

The internet, what do we know about it? Who invented it? It’s a global network system which connects millions of computers that uses TCP/IP protocol, but what are protocols and what do they do? Now a days we are using this internet regularly whether it’s for communications, or if we want to collect any information. Most of the people don’t know who made this. It will be hard to credit one person for this invention because many scientists, engineers and programmers developed new features and technologies which we can use now. To make it simple many scientist had visions of wireless systems, but it was not invented until the computer scientists developed “packet switching” in the 1960s.

With packet switching, a message that is sent from one computer to another is broken down into small packets of digital data. Each packet is given an address to travel to and is then routed to its destination (Brian Donnelly, n.d.). In 1973 there were 37 nodes in the operation. Even though packet switching was created in the 1960s it was kept in secret until the 1970s. It was revealed based on national security because academic institutions were involved with the research of ARAPANET Department of Defense. Regardless of what type of computer is on a network, there must be software to allow it to be managed and allow it to communicate. This is where the scientists like Vinton Cerf and Robert Kahn came up with the basic idea of “protocol”, a software for computer communications between 1973 and 1974. Protocol is a method for communication between computers on small and large networks. The protocol is a combination of TCP/IP (Andrew, 2019).

Transmission Control Protocol (TCP) attempts to assure the dependable transmissions of data between networks and devices. Internet Protocol (IP) attempts to define the path that data, signals, packets, etc., will travel between a sending device and destination. In 1982 the Defense Department implemented the use of TCP/IP protocol on ARAPANET which at that time contained 100 nodes. In the late 80s the government removed restrictions on the internet which gave access to several researchers and scholars to computer networks. In 1989 computer scientist Tim Berners-Lee invented the World Wide Web, which gave the online world more recognition.

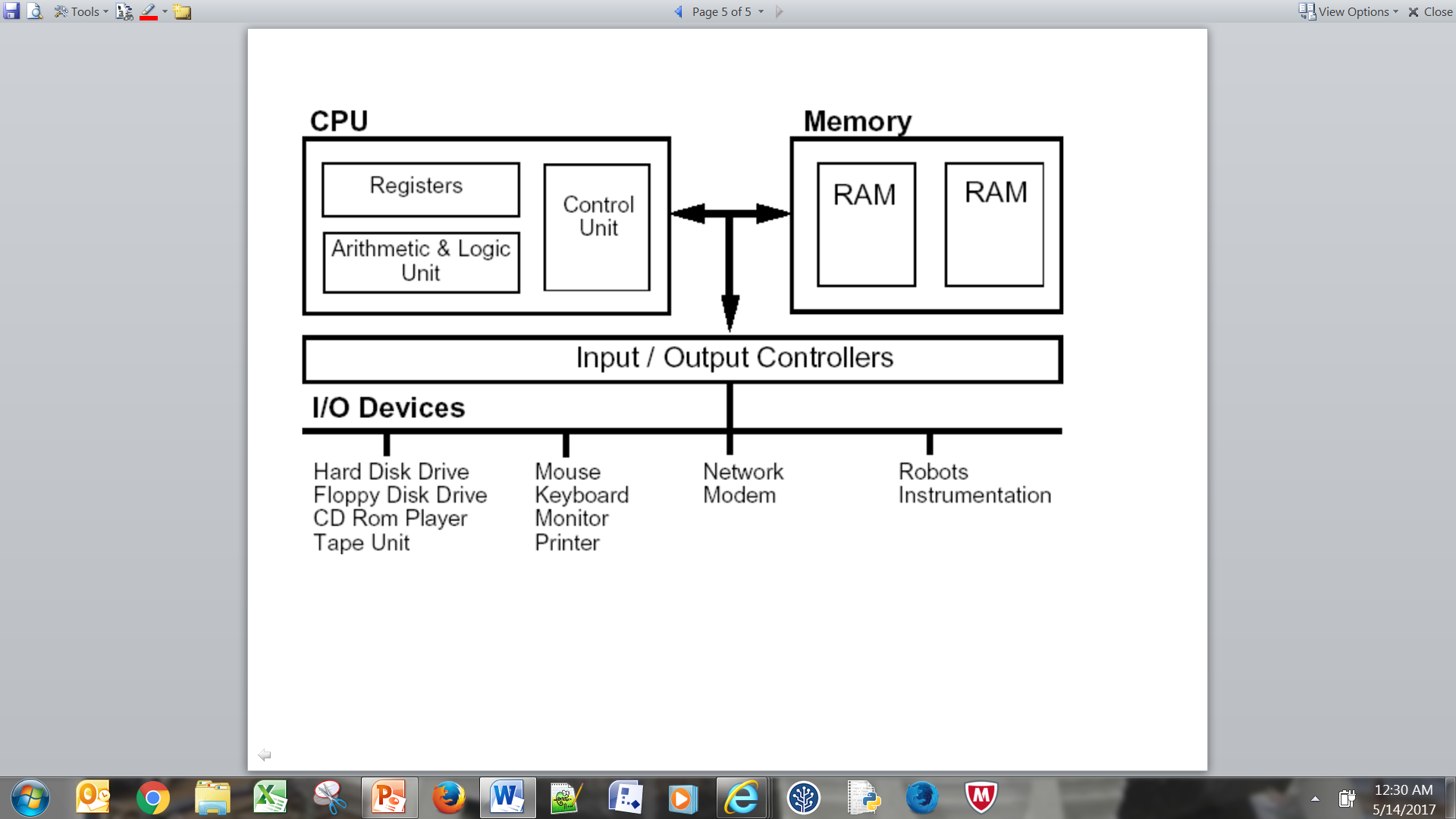
Tim Berners-Lee compiled code which allowed access to the global bank of knowledge www via using code such as HTML (Hypertext Markup Languages), URLs (Uniform Resource Locators), communication protocols such as HTTP (Hypertext Transfer Protocol) and internet browsers (Mozilla Firefox, Internet Explorer, and Google Chrome). The term “internet” is used synonymously with www (World Wide Web) but there is a difference between the internet and www. Think of the internet as a large book with many pages and chapters. Www is like a “table of contents” for that book which the reader uses to locate the specific item in it. The things we are searching for could be either small sentences or big chapters, it could also be a video, music or graphics (Spencer).

# Chapter 3 - Components of Computing Devices

In all computer systems, there are two major categories of which all other groups of computer aspects fall within: computer hardware versus computer software. You can also call them the components of computers. Hardware is all the parts you can touch, break, throw or trip. These are physical devices related to the computer. Examples of hardware could include the computer case, monitor, printer, hard drive etc. Software is a collection of instructions, files and codes which are written out, stored digitally and utilized by a computer to perform operations, tasks and functions. Comparing a person with a computer, while the human body would be hardware for example “eyes, mouth and hands”, software would be more like a person’s spirit for example “ideas, morals, ethics, and dreams.”

If we talk about the history of software than we can reference back to our chapter one where we talked about computer programming, and who was the first computer programmer. This can give us an idea about the software as well, because software consists of instruction sets created by programmers using many types of programming languages or Computer Code. In early time punch cards were being used for programming. Later, they were replaced by reels of magnetic tape. In the late 1950s several different programming software were created but it was only available to computer scientists and large businesses. They were used to make their own software which could be used specifically for that one system or device. Nevertheless, when ordinary people started using computers, they were not able to create their own software. The ones made by the company were not useful for them because it was specifically made for the companies and couldn’t work for other systems. During that time Operating Systems like MS-DOS was introduced which would operate the computer. MS-DOS was used to operate many early IBM computers. The first commercial software was available to average customers by IBM in the late 1960s and early 1970s (Designer, n.d.).

Now a days we have a lot of software that we are using regularly. Software can be divided into many different categories such as operating system software and Application Software. Application software allow a user to create documents, spreadsheet, send e-mail, view web pages and many other daily technology-related activities. Firmware is also software which allow an operating system to communicate with specific devices such as speakers and printers. Nonetheless, for this software to operate there is another important component, the hardware portion. Deprived of this hardware the computers can’t work automatically. Hardware of today’s computers are the Stored Program which follows the concept of Von Neumann architecture designed in 1945 by John Von Neumann. His concept was that programs and data are stored in a separate storage unit called memories and are treated the same. The Von Neumann machine consists of a central processor with an arithmetic/logic unit along with control unit, memory, mass storage, and input/output (Techopedia, n.d.). Below is a diagram of his design.



There are many types of hardware which can be either Internal (Inside of the computer case), External (connecting to the outside of the case), or Peripheral (not required for operation of a computer).

Internal Hardware:

* Motherboard
* Power Supply
* Hard Drive
* Optical Drive (e.g. DVD/BD/CD drive)

External Hardware:

* Monitor
* External Hard Drive

Peripheral Hardware:

* Scanners
* Microphones
* Speakers
* Mouse

Some of the hardware parts are “Optical Drive” which allows access as well as storage for data such as documents, files, programs, movies, music and installation of software. “Hard drive” is used as a long-term storage for data. “Motherboard” provides the connection for all internal components such as optical drive, hard drive, CPU, etc. Electricity flows thru motherboard between all devices connected both internally and externally to the computer. There is also “Expansion Card” which can be added to a computer to enhance or add additional functionality to a computer. Some examples of expansion card will be USB Card, Sound Card, Network Interface Card, and Video Card. The most necessary part in the hardware will be the “Power Supply” provides power to all internal devices. The internal devices require at least three different voltages 3.3V, 5V, and 12V (Spencer).

* 3.3V: Motherboard, RAM, onboard ports i.e. USB, NIC, etc.
* 5V: Hard drive circuits, higher-end RAM and standard graphic cards.
* 12V: Hard drive and optical drive motors, fans and High-end graphic cards.

There are a lot of internal hardware and external hardware, and one of them is the Mouse. We have discussed about the invention of this important hardware earlier. The creation of the mouse was discussed in chapter one, it was invented by Douglas Engelbart in the 1950s.

# 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 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 ***have*** 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.).

**A Workstation also known as Personal Computer, is 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 its 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 introduced in 1980 and it is 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. Such as*** they are unable to differentiate between the devices on the network. If one computer is trying to reach another on a hub-based network, the computer will send the message to every other computer on the network, consuming bandwidth for each transfer.

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.

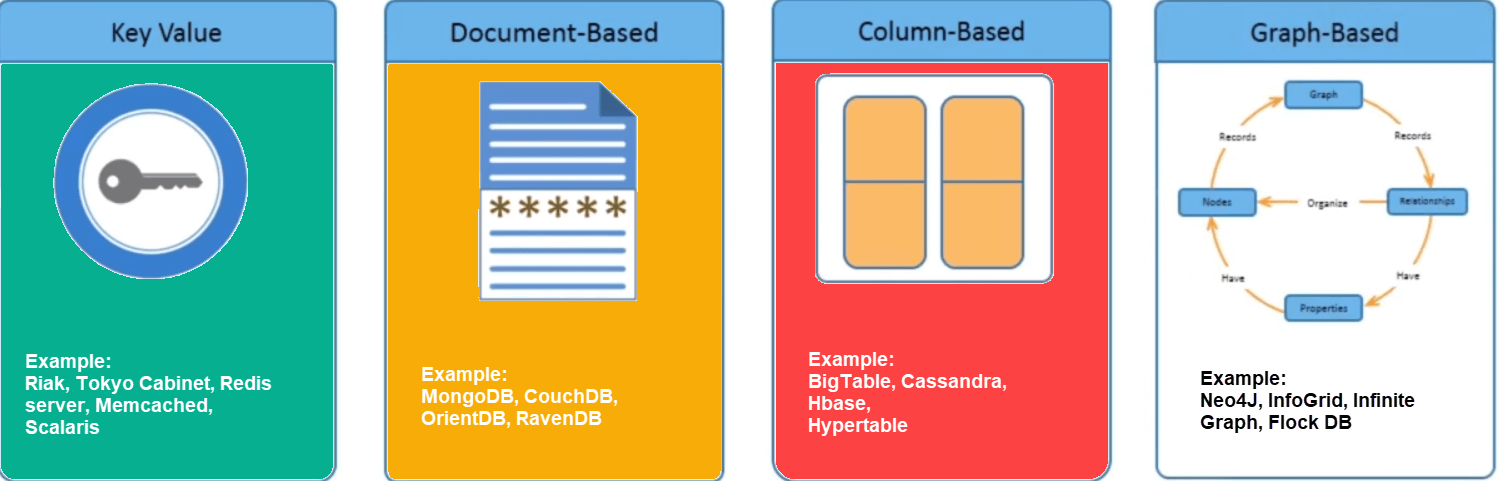
 In many-to-many relationships, a mapping/translation table is created that maps the primary keys of the two entities involved in the many-to-many relationship. This creates two one-to-many relationships towards the mapping table. When there is a one to one relationship, one typically leaves it intact.  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:

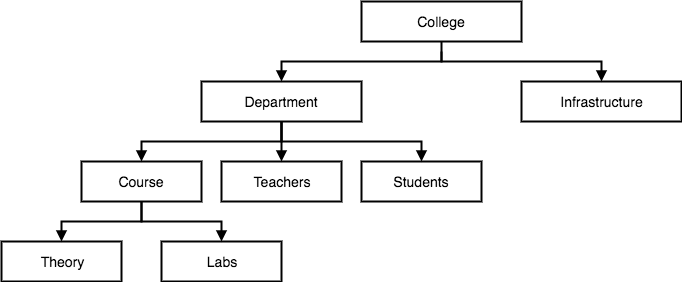
* **Key-Value Database** - Key-value databases store data in unique key-value pairs, meaning each key is associated only with one value in a collection, like in a dictionary. This makes querying a key-value data store fast because of its simple model. There’s no query language needed. Data retrieval 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**



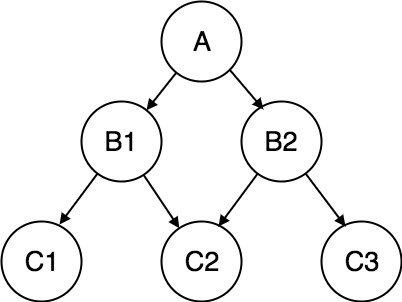
There are other database models too like Hierarchical Model and Network Model. The hierarchical model is a database that organizes data in a tree-like-structure with a single root to which all other data is linked (Study Tonight, n.d.). This structure was developed by IBM in the 1960’s and was used in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



***Should include a citation for images.***

# 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 works 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 cybercrimes 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 *(DOS)*** 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 this software became a handy for bad people and was used for for crimes,** 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 it’s 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 ***tested*** 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)

# Chapter 7 - Identity Theft and Individual Cyber Security

Have ever been a target of cybercrime. As we addressed different types of cybercrime in previous chapter. This chapter will concentrate more on individual cyber security. There are a lot of cases where a common man has been becoming a target of these Hackers. Where they ask for money by using the Ransomware methods and there are some other methods as well where you will be targeted by hackers. Since this chapter will be discussing about personal attacks on your computer, this will also put some light on anti-virus or anti-malware. We will discuss about some of the famous software’s which we can use to protect ourselves from being a target of hacking. We will also mention some of the open source software’s as well.

In order to protect yourself from the hackers first thing you need to do is learn about the Phishing and Spoofing threats. We have briefly defined phishing in the earlier chapters. Spoofing and phishing are both techniques used by scammers to mislead e-mail recipients. Both involve posing as a different sender to trick the recipient into carrying out an action. Spoofing is a technical measure used to change the apparent sender details on an e-mail, while phishing is an attempt to make the recipient hand over sensitive information such as log-in details. The two techniques may be used either separately or simultaneously: in simple terms, spoofing refers to what a scammer does, while phishing refers to what a scammer is trying to achieve (Lister, n.d.).

Phishing is the rapid evolution in the hacking history. The earliest phishing in the history was an Algorithm Phishing in 1990 which was flagged by (AOL) American Online. During that time, the first phishers [created an algorithm](https://en.wikipedia.org/wiki/Phishing#History) to generate random credit card numbers in order to get an original card’s match from the AOL accounts. Once matched, the phishers accessed this data to manipulate it. By the time AOL caught up to the scam – after 1995 – phishers had already moved to newer technologies (Sys Cloud, n.d.). There are different categories of Phishing listed below:

* Vishing – Vishing refers to phishing done over phone calls. Since voice is used for this type of phishing, it is called vishing. Considering the ease and enormity of data available in social networks, it is no surprise that phishers communicate confidently over a call in the name of friends, relatives or any related brand, without raising any suspicion (Sys Cloud, n.d.)
* Search Engine Phishing - Search engine phishing is the type of phishing that refers to the creation of a fake webpage for targeting specific keywords and waiting for the searcher to land on the fake webpage. Once a searcher clicks on the page link, s/he will never recognize that s/he is hooked until it is too late (Sys Cloud, n.d.)
* Spear Phishing - spear phishing is typically targeted in nature, and the emails are carefully designed to target a particular user. These attacks have a greater risk because phishers do a complete social profile research about the user and their organization – through their social media profile and company website. Spear phishing is the most commonly used type of phishing attack – on individual users as well as organizations (Sys Cloud, n.d.).
* Whaling - Whaling is not very different from spear phishing, but the targeted group becomes more specific and confined in this type of phishing attack. In this phishing they target the enterprise top executives and they are always high value.

There are different ways to protect yourself from different types of hackings. Although there is no perfect method of protecting data, computers, server and networks. There are several practices which can be done in order to avoid any threats to your systems. UAC is one of the practices which will be helpful to secure your system and it was originally introduced in 2008 when Windows launched Vista. UAC stops users from making changes to a computer’s operating systems. By the default, only the user with administrator account can make changes. Therefore, if someone tries to download change something in the operating system the user account control dialog box appears requesting credentials. If the credentials are not those of Administrator, the UAC will stop the installation.

Another method which is useful to protect yourself from Cyber threats is TPM (Trusted Platform Module). The origin of TPM can be traced back to 1951 when preventive maintenance was introduced in Japan. This is a security feature that has been developed an increasing implemented over the last few years on for laptops and desktops. The system requires inter-related microchips circuitry which is part of the motherboard, BIOS and hard drive to provide hardware specific security. TPM has the ability to provide better confidentiality of data as well as storage of security elements such as passwords, certificates and encryption keys. These elements allow security and confidentiality when accessing the computer or when the computer is being used to access online resource such as websites or gateway servers.

BitLocker is another method for protection which was initially released on January 30, 2007. This method performs manipulation of the data on a hard drive via changing the order and arrangement of “bits” in messages and documents. BitLocker can Utilize either 128 bit or 256-bit encryption. BitLocker also protects the physical hard drive from being accessed by any operating system other than the one which originally communicated with the hard drive. The hard drive is also “married” to the motherboard to which the hard drive is originally connected to so if the hard drive is removed from the computer and replaced in a different system, the drive will be unusable because BitLocker requires a connection to both the original operating system and motherboard (Spencer, Foundations of Windows Computers 2.0, 2018)

A firewall is a software or device which monitors access to a computer. The first firewall proposal, or packet filter, came in 1989 by Jeff Mogul of Digital Equipment Corp (DEC) (Brodbeck, n.d.). Essentially, the firewall will look for activity which falls outside of a “baseline”. When activity disconnect the connection or inform a computer user of the activity. As a comparison, think of computer as a very popular “nightclub” with a dress code requiring a tie for a male. At the door of the club, there are staff members who assure all males have ties. If a male attempts to enter without a tie, this would be “outside of the baseline” which will either cause the club staff to reject the male or ask which will either cause the eager club goer should be allowed to enter (Spencer, Foundations of Windows Computers 2.0, 2018)

Beside these you can always use “antivirus” or “anti-malware” software to keep your stuff safe. Some software are expensive and some are cheap you can also find open source software as well. The picture attached below shows some of the well-known security software for computers.



Since Identity Theft is a major part of cybercrime and usually involve computers, so we will highlight some information about it in this chapter. Identity theft is the act of a person obtaining information illegally about someone else. Thieves try to find such information as full name, maiden name, address, date of birth, social security number, passwords, phone number, e-mail, and credit card numbers. The thief can then use this information to gain access to bank accounts, e-mail, [and smartphones](https://www.computerhope.com/jargon/s/smartphone.htm), identify themselves as you, or sells your information (Hope, 2019). There are some cases where hackers have used phishing in order to gain identities illegally and it was previously described in this chapter. Below are some methods which you can use to protect yourself from identity theft by (cmu.edu, n.d.)

1. [Protect your Social Security number](javascript:void(0);)
2. [Fight phishing - do not take the bait](javascript:void(0);)
3. [Keep your identity from getting trashed](javascript:void(0);)
4. [Control your personal financial information](javascript:void(0);)
5. [Shield your computer from viruses and spyware](javascript:void(0);)
6. [Click with caution](javascript:void(0);)
7. [Check your bills and bank statements](javascript:void(0);)
8. [Stop pre-approved credit offers](javascript:void(0);)
9. [Ask questions](javascript:void(0);)
10. [Check your credit reports - for free](javascript:void(0);)

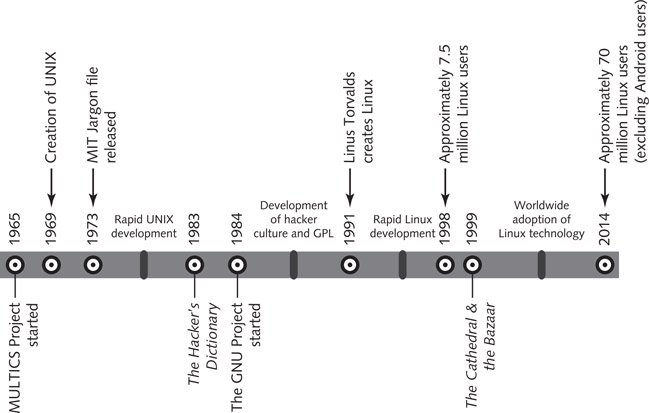
# Chapter 8 - Linux and Open Source

“Open Source” (OSS) a software in which the source code and software can be obtained free of charge and can be modified. The term “Open Source”, although popular now, has only been defined as an actual term since its inception in the late 70’s and early 80’s. This chapter will talk about the open source software and the rest of chapter will concentrate on Linux which is the most popular and commonly used open source software.

In 1980s Richard Stallman had the idea to create free software that users could adapt when needed, and that led him to GNU project. The GNU operating system is a completely free software system, upward-compatible with UNIX. GNU stands for “GNU's Not Unix”.  A longer version called the [GNU Manifesto](https://www.gnu.org/gnu/manifesto.html) was also published in March 1985. It has been translated into several [other languages](https://www.gnu.org/gnu/manifesto.html#translations) (gnu.org, n.d.).

There were a lot of movements in the history of open source. In 1992 first widely-used web browser NCSA Mosaic was developed at the National Center for Supercomputing Applications and its team also created a commercial web browser, Netscape Navigator in 1994, which leads in user share. In 1995 Apache HTTP Server development began. In 1998 Netscape Browser releases its source code, and at the same year the “Open Source” label was created in Palo Alto, California strategy session. In 1999 the Microsoft Internet Explorer takes the lead in market share. A free Open Source version of Netscape which known as Mozilla Firefox now was being released in 2002, and at the same year Apple releases Safari for OS X. Subsequently, the first version of Safari for Microsoft Windows was released in 2007. After one year in “2008” Google released Google Chrome for Microsoft Windows, but then they released their first stable Google Chrome to support OS X and Linux in 2009. In 2012 the Red Hat became the first one-billion-dollar Open Source Company (Kinkela & Yonker, Linux and Open Source)

The rest of our chapter will discuss about Linux, it is referred to as Open Source Software (OSS) as well, because Linux is published under the GNU Public License. [Linux](javascript://) is an operating system that is used today to run a variety of applications on a variety of different hardware. Linux has the ability to manage thousands of tasks at the same time, including allowing multiple users to access the system simultaneously. Hence, Linux is referred to as a [multiuser](javascript://) and [multitasking](javascript://) operating system. Linux is based on the UNIX operating system developed by Ken Thompson and Dennis Ritchie of AT&T Bell Laboratories in 1969 and was developed through the efforts of many people as a result of the hacker culture that formed in the 1980s (Eckert). The picture shows the Timeline of Linux and UNIX development by (Eckert).



The core component of the Linux operating system is called the Linux [kernel](javascript://). The first Linux kernel was released in September 1991. The Linux kernel and supporting software (called function libraries) are written almost entirely in the C programming language, which is one of the most common languages that software developers use when creating programs.

The Linux kernel was developed collaboratively and was centrally managed; however, many Linux add-on packages were developed freely worldwide by those members of the hacker culture who were interested in their release. Linux was a convenient focal point for free software developers. During the early- to mid-1990s, Linux development proceeded at full speed, with hackers contributing large amounts of their time to what turned into a large-scale development project. All this effort resulted in several distributions of Linux. A [distribution](javascript://) of Linux is a collection or bundle of software containing the commonly developed Linux operating system kernel and libraries, combined with add-on software specific to a certain use (Eckert). Well-known distributions of Linux include [Red Hat](javascript://), [Ubuntu](javascript://), [OpenSUSE](javascript://), Slackware, Debian, Ubuntu, Linux Mint and TurboLinux.

We will end this chapter with mentioning some of the advantages of using Linux:

* Risk reduction
* Meeting business needs
* Stability and security
* Flexibility for different hardware platforms
* Ease of customization
* Ease of obtaining support
* Cost reduction

# Chapter 9 - Command Line Interface

The Command Line Interface (CLI) requires an in-depth understanding of the structure of operating systems. In order to activate elements and functions in the operating system, a user is required to type out the exact word which initiates a function. Spelling must be perfect in order to manipulate a CLI operating system. Many present-day operating systems offer access to the CLI. On Windows-based operating systems the CLI is often confused with an operating system which is no longer used called (DOS) Disk Operating System.

One of the most misunderstood options available on operating system is entitled the “Command Line Interface” normally abbreviated as “CLI”. Many people who have some knowledge of computers will refer to this access method as “DOS”. The “look” of DOS and the CLI are very similar.

DOS (Disk Operating System) is an extremely outdated operating system used by Microsoft between 1980 and 1998. Essentially, the operating system DOS used “command-words” to perform functions. If a user did not understand the correct format for the “words” they would be unable to utilize a computer. About 1993, one of the first GUI’s (Graphical User Interface) entitled “Windows for Workgroups”, was produced. This GUI was installed on top f DOS which allowed functions to be performed using pictures referred to as “icon” and “buttons”. The buttons interacted with DOS as a control feature. DOS was replaced by Windows 98 but the ability to use command line was retained using the command or “cmd” in the search field of a “Start Menu”. Many technicians referred to the search field as the “Run” option.

In the field of computer/server technology, there are many CLI functions used. One of the reasons which supports CLI functions is that the command words do not often change. The “buttons” and “icons” normally change between operating systems or even between different versions of the same operating systems. The command “ping” for example is the same on Linux, Unix, Windows and even Cisco Router and the Switch operating systems. All are run from a CLI. The following are some well-known CLI commands performed on Windows:

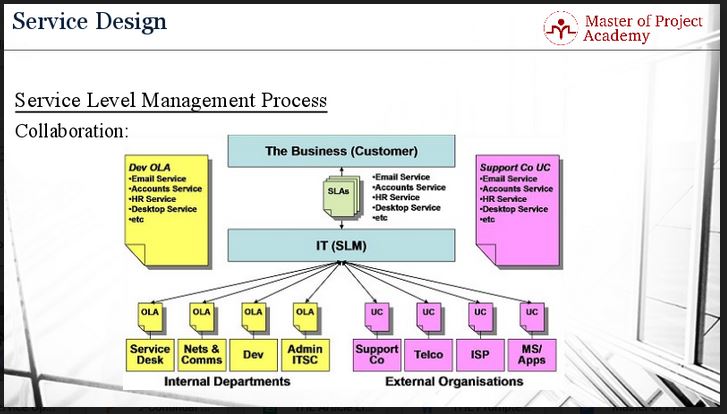
* Dir – Displays the contents of the directory presently being viewed.
* Cls – Removes previous command results from the CLI.
* Cd – Redirects the focus of the command prompt to a directory with in the present directory.
* Cd\ - Redirects the focus of the command prompt to the root (Top) of the drive being viewed.
* Cd .. – Redirects the focus of the command prompt back one level to the previous or containing directory.
* Mkdir <name> – Creates a directory that is named in the command.
* Rmdir <name> – Eliminates a directory that is named in the command.

Just like Microsoft there are many more Command Line Interfaces in Linux and Mac OS terminal as well. Bourne shell is a UNIX Shell and was developed at AT&T. The Bourne shell family includes Korn shell, bash and zsh. Bash shell was for GNU’s project which was released in 1989 to replace it with Bourne shell (Kinkela & Yonker). The table below show some comparison between the commands used on Mac OSx, Linux, and DOS from (Kinkela & Yonker).

|  |  |  |  |
| --- | --- | --- | --- |
| **Description** | **DOS Command** | **Linux Command** | **Mac OSX Command** |
| **Change Directory** | **cd** | **cd** | **cd** |
| **Clear the screen** | **cls** | **clear** | **clear** |
| **Copy a file** | **copy** | **cp** | **cp** |
| **Display text on screen** | **echo** | **echo** | **echo** |
| **Find a file** | **if exist** | **locate, grep, find** | **locate, grep, find** |
| **Leave the shell** | **exit** | **exit** | **exit** |
| **List files** | **dir** | **ls, dir** | **ls** |
| **Create new directory** | **md** | **mkdir** | **mkdir** |
| **Move a file** | **move** | **mv** | **mv** |

# Chapter 10 - Computing Technology Management and Administration

As the technology has been evolved it has also opened a lot of jobs opportunities in different types of technology managements and administration. Since this chapter is about computer technology management, we will mention SLM over here referred to a Service Level Management is one of five components in the ITIL Service Delivery area. The practice of Service Level Management (SLM) gives assurance to the service consumer that a provider will deliver a level of service that meets their needs. The purpose of the SLM practice is to set clear business-based targets for service performance, so that the delivery of a service can be properly assessed, monitored, and managed against these targets. SLM involves the definition, documentation, and active management of service levels (Blog, n.d.). The picture below show the process of SLM by Master of Project Academy.



This chapter will talk more about some of the jobs available for us now in this field which are listed below.

## Cloud Systems Administrator

A Cloud Systems Administrator is responsible for working in a mixed Windows and Unix software environment. The responsibility of the individual is to manage the instances of the cloud infrastructure services and the multiple cloud servers. The professional also leads, oversees and maintains, multiuser computing environment as per the requirements of the organization. The primary job responsibilities of the cloud administrator are to work in coordination with the IT department to develop and support cloud, windows or Unix infrastructure. They usually provide technical assistance on windows, cloud-based systems, and resolve operational problems. Anybody interested in taking on a cloud systems administrator position must have a bachelor’s degree in computer science, information technology, electronics, or telecommunications (Engineer, n.d.)

## Web Content Manager

Web content managers typically oversee the content presented on websites. They may also monitor website traffic, make sure the website is working properly and respond to website feedback. A career in this field usually requires education and experience in a computer-related field. In addition, employers may require knowledge of website development or content management systems. They also work with the site's content producers, determining the type, quality and quantity of content needed for the website. They may assign projects, edit content and manage the employees who work with the website's content. Individuals interested in becoming a web content manager will usually need a certificate or an undergraduate degree in a computer science field (Study.com, 2019)

## Database Administrator

Database administrators (DBAs) are employees who work with technology, using specialized types of software to store and organize a company's data. This could include a variety of information, from confidential financial numbers, to payroll data, to customer shipping records. A DBA makes sure that data is available to users, and that it's kept secure from unauthorized access or accidental loss or corruption. A DBA must have a minimum of a four-year college degree in a related field and relevant experience. They requireA bachelor's degree in information technology or computer science.

## Device Administrator

Provide expertise and direction in the development and modifications of mobile solutions (e.g. laptops, tablets, smart phones) to enhance performance and availability. Support end users with mobile devices, mobile device training and issue management of mobile solutions. Analyzes and tests smart phones, tablets and other mobile devices and associated applications to ensure they are supportable within an environment (Kinkela & Yonker, Computing Technology Management and Administration)

## Network Administrator

A network administrator is responsible for keeping an organization’s computer network up-to-date and operating as intended. Any company or organization that uses multiple computers or software platforms needs a network admin to coordinate and connect the different systems. Their areas of expertise include local area networks (LANs), wide area networks (WANs), and intranets. Network administrators organize, install, and provide support for these systems (Erstad, 2018)

## **Project Administrators**

Project Administrator assist with project management duties. They oversee and performing administrative functions concerned with a project. This may include calling contractors, making appointments, ordering supplies, doing site visits and preparing reports. Administrators work in several industries including engineering, pharmaceutical, health care, and research. Employers prefer that Project Administrators possess a first degree in Business. They can also possess a High School Diploma but with many years of experience and a record of accomplishment. Having Project Management qualifications, certifications, or diplomas is an asset. Senior Project Administrators usually hold a master’s degree (Job, n.d.)

## Software Application Administrator

Software application administrator’s main duty is for all licensed and developed software applications. They install, update, tune, and diagnose both internal and third-party applications. Software Application Administrator provides IT support services to company’s clients, documents and coordinates technical implementation and support services. Administrators make recommendations for future upgrades for both hardware and software. They are required to have associate’s or bachelor’s degree in computer science or a related field, or equivalent work experience (Bourne, 2014)

## System Administrator

A system administrator is a professional who is held accountable for network setup, annual server maintenance such as mail servers and file servers, and much more. System Administrator requirements include an in-depth understanding of computer software, hardware, and networks. The IT System Administrator must design, organize, modify and support the organization’s computer systems. These professionals must upgrade and manage the software and hardware. The IT System Administrator should handle any issues related to [Local Area Networks (LAN)](https://www.fieldengineer.com/blogs/what-is-wireless-lan), Wide Area Networks, and Network segments. It is the System Administrator who maintains operating systems, business applications, security tools, web-servers, email, laptop, and desktop PCs. The basic requirement is a bachelor’s degree in [computer science](https://www.fieldengineer.com/blogs/software-engineering-vs-computer-science), information system management, [information technology](https://www.fieldengineer.com/blogs/it-engineering/) or other related fields (Engineer, Field Engineer, n.d.)

### Conclusion

While writing this paper a lot of things were being researched. They were some old stuff which we learned in this while going through each chapter. We learned how the technology has evolved through these decades. In the first chapter some of the important aspects in history of technology were discussed like who discovered these new technologies and when were they discovered.

In the second chapter “The Internet and the web” we got familiarized TCP/IP protocol and packet switching. We also learned about a bit of its history of when was it introduced which was interesting to know it. The third chapter “components of computing devices” was more about the hardware and software of computer. In chapter four we got into more in depth with the evolution of technology and learned about switches, router, and virtual machines. While switches and clients are systems in which one hold stuff and another request and use that stuff, virtual machine is a software which can duplicate the functions of real-life computers and servers.

Chapter five concentrated on a database management System which allows a person to organize, store, and retrieve data from a computer. Chapter six cyber security and cyberwarfare addressed some important aspects cyber security and the chapter also addressed the evolution of cyber security. Where as chapter seven got more in depth with cyber security and talked about the threats that we can face individually in our own computers. Chapter eight was giving some information about the free sources we can get for our devices. The chapter concentrated more on Linux which is the biggest distributor of open source technology.

In chapter nine we talked about command line which is a text-based user interface used to view and manage computer files. In chapter ten we did not talk about the evolution and history because this chapter was addressing some of the jobs available in field which was more about current stuff going on. This research was a good practice and we were able to get a good grasp of information in the field of IT. We were able to encounter some aspects of the evolution of these modern technologies which we are using now a days as well.

# References

Andrew, E. (2019, March 2019). *History Who Invented Internet*. Retrieved from https://www.history.com/news/who-invented-the-internet

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

*BBC UK*. (n.d.). Retrieved from http://www.bbc.co.uk/history/historic\_figures/kilby\_and\_noyce.shtml

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

*Biography*. (n.d.). Retrieved from https://www.biography.com/scientist/grace-hopper

Blog, B. (n.d.). *BMC BLOG*. Retrieved from BMC Blog Web Site: https://www.bmc.com/blogs/itil-service-level-management/

Bourne, K. (2014, February 14). *techradar*. Retrieved from https://www.techradar.com/news/software/what-does-an-application-administrator-do-1219241

Brian Donnelly, C. J. (n.d.). *Lawyering in the Digital Age*. Retrieved from http://www2.law.columbia.edu/donnelly/lda/index.html

*Britannica*. (n.d.). Retrieved from https://www.britannica.com/biography/Charles-Babbage

*Britannica FORTRAN* . (n.d.). Retrieved from https://www.britannica.com/technology/FORTRAN

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

Brodbeck, C. (n.d.). *Ostec*. Retrieved from Ostec Blog: https://ostec.blog/en/perimeter/firewall#:~:targetText=The%20first%20firewall%20proposal%2C%20or,%2C%20therefore%2C%20the%20first%20generation.

cmu.edu. (n.d.). *cmu.edu*. Retrieved from cmu.edu: https://www.cmu.edu/iso/aware/idtheft/protect/index.html

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

Designer, B. (n.d.). *BSC Designer*. Retrieved from The History and Significance of Software: https://bscdesigner.com/software-history.htm

Eckert, J. (n.d.). Introduction to Linux Chapter 1. In J. Eckert, *CompTIA Linux+ Guide to Linux Certification.*

Engineer, F. (n.d.). *Field Engineer*. Retrieved from Field Engineer Website: https://www.fieldengineer.com/skills/cloud-systems-administrator

Engineer, F. (n.d.). *Field Engineer*. Retrieved from Field Engineer Web Site: https://www.fieldengineer.com/skills/what-is-a-system-administrator

Erstad, W. (2018, August 16). *Rasmussen College*. Retrieved from Rasmussen College Web Site: https://www.rasmussen.edu/degrees/technology/blog/what-does-a-network-administrator-do/

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/

gnu.org. (n.d.). *gnu.org*. Retrieved from gnu.org: https://www.gnu.org/gnu/gnu-history.en.html

Hall, M. (n.d.). *Britannica* . Retrieved from https://www.britannica.com/biography/Douglas-Engelbart

Hodges, A. (n.d.). *Alan Turing*. Retrieved from turing.org: https://www.turing.org.uk/publications/dnb.html

Hope, C. (2019, 11 16). *Computer Hope*. Retrieved from Computer Hope Web site: https://www.computerhope.com/jargon/i/identhef.htm#:~:targetText=Identity%20theft%20is%20the%20act,mail%2C%20and%20credit%20card%20numbers.

Job, J. i. (n.d.). *Job is Job*. Retrieved from Job is Job Web Site: https://www.jobisjob.com/project+administrator/job-description

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.

Kinkela, M. P., & Yonker, V. (n.d.). Computing Technology Management and Administration. Philadelphia.

Kinkela, M. P., & Yonker, V. (n.d.). Linux and Open Source. Philadelphia, PA, USA.

Kinkela, M., & Yonker, V. (n.d.). Command Line Interface. Philadelphia, PA, USA.

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

*Lemelson-MIT Celebrating invention, inspiring youth*. (n.d.). Retrieved from Lemelson-MIT: https://lemelson.mit.edu/resources/john-mauchly-j-presper-eckert

Lister, J. (n.d.). *It Still Works*. Retrieved from It Still Works Web site: https://itstillworks.com/difference-between-phishing-spoofing-2602.html

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.

News, B. (2000, April 13). *BBC News*. Retrieved from Babbage Printer Finally Runs: http://news.bbc.co.uk/2/hi/science/nature/710950.stm

*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.

Spencer, R. (n.d.). *Foundations of Windows Computers 2.0.* Philadelphia.

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

Study.com. (2019, September 28). *Study.com*. Retrieved from Study.com: https://study.com/articles/Web\_Content\_Manager\_Job\_Description\_and\_Requirements.html

*Sys Cloud*. (n.d.). Retrieved from Sys Cloud Web site: https://blog.syscloud.com/types-of-phishing/

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

*Techopedia*. (n.d.). Retrieved from https://www.techopedia.com/definition/32480/von-neumann-architecture

*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/