CHAPTER 2

THEORETICAL FOUNDATION

2.1 Theoretical Foundation

2.1.1 Cellular phone

Cellular phone which is also known as mobile phone, wireless phone, hand-phone can be defined as a type of short-wave analog or digital telecommunication in which a subscriber has wireless connection from a mobile telephone to a relatively nearby transmitter [5].

2.1.1.1 History of Cellular phone

Cellular phone was first developed and built by Martin Cooper on the 3rd of April 1973 [6]. In March 6th 1983, it was made available for purchase, named Motorola DynaTAC 8000X. The first approval was given by the U.S. Federal Communications Commission becoming the world's first commercial handheld mobile phone, sold for $3,995 [5, 7]. Weighing of 2 pounds, it had a cool size of 13 x 1.75 x 3.5 inches. Along with the time, the cellular phone size is getting smaller.

Figure 1: Motorola DynaTAC 8000X

Image taken from phonereport.info

Initially, cellular phone was using analog network standard (1G). As the traffic crowded another solution was searched. In the 1989, GSM (Global System for Mobile Communications) was accepted as international digital cellular telephone standard (2G). The earliest commercial GSM phone call was made by Radiolinja's network in Finland [8] stated the first officially opened GSM network. Another digital standard, CDMA IS-95A was finalized in 1993 giving far more capacity than GSM [9, 10]. The CDMA (Code Division Multiple Access) network was commercially opened in 1995.

That time cellular phone only allows voice to voice telecommunication, until on December 3, 1992 Short Message Service was first sent by Neil Papworth containing "Merry Christmas" to his colleagues at Vodafone. SMS was not booming until 1999, seven years later, after the short messages could be sent to different networks [11].

As the world demanding for more advanced technology, GPRS (General Packet Radio Service) standard appeared as a development of the GSM standard classified as 2.5G [12]. It uses Packet Switching technology to transfer data also offering internet

connection. Another evolution, EDGE (Enhanced Data Rates for GSM Evolution) standard came allowing higher data rate transfer, stated as 2.75G [13].

The demand got increased for much higher data rate transfer, faster, and secure. In 1999, CDMA2000 1X and WCDMA were decided as the next standard (3G) to answer the growing demand. Not long after that, in 2000, the world's first 3G CDMA2000 commercial service was officially opened [9].

In 2001, it was the first time cellular phone had color screen and in 2002, the initial introduction of cellular camera phone. By the year of 2005, there were 200 million commercial CDMA2000 subscribers and 1.5 billion GSM customers worldwide [8, 9]. In the future there already waiting to launch 4G.

2.1.1.2 GSM and CDMA

Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA) are two primary competing cellular phone technologies. GSM is a combination of FDMA (analog) and TDMA (signal). FDMA divides frequency of 25MHz bandwidth into 124 carrier frequencies spaced 200 kHz apart and assigns those carrier frequencies to each base station [14]. Moreover TDMA divides those carrier frequencies in time. GSM operates at 900MHz and 1.8GHz bands.

CDMA is a radio transmitted communication technology which employs a spread-spectrum technology to send the data in small parts over specified range or frequencies at any time [10]. The spectrum radio transmitted is always at the same wide-band chunk of spectrum. Each of the user’s signals is spread over by unique spreading code and the

receiver will receive the unique code to recover the signal. CMDA operates at 800MHz and 1.9GHz bands.

2.1.1.3 SMS

Short Message Service (SMS) is a wireless service that enables the transmission of short text messages between mobile subscribers and external systems such as electronic mail, paging, and voice-mail systems [15]. The message being transmitted must not contain images or graphics and must not be longer than 160 alphanumeric characters.

Figure 2 (see below) shows how SMS works in a GSM network [16]. As you can see, once the sender sent a message, the message is then received by a Short Message Service (SMSC). In order to get proper receiver, SMSC sends a SMS request to Home Location Register (HLR) to discover the roaming customer. After HLR receives the requests, it responds back to SMSC with the subscriber's status (inactive or active and roaming location). If the status is inactive then SMSC will hold the message until the HLR sends a sent notification. SMSC transfer the message to GSM message delivery system in a Short-Message Delivery Point to Point format. The system pages the device and if it responds, delivers the message. If the message is received by the receiver, SMSC will set the message as sent status and will not attempt to send it again.

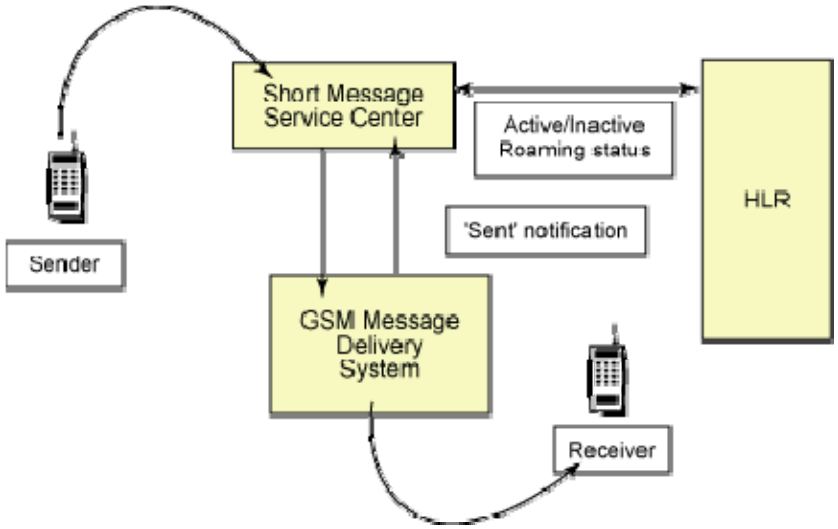


Figure 2: SMS Delivery System

Image taken from www.ibm.com

Here are some SMS benefits:

- Guarantee the message is received by target receiver.
- Having notification delivery
- Cheap

2.1.1.4 MMS

Multimedia Messaging Service (MMS) is a messaging protocol that enables the transmission of multimedia messages such as text, images, graphics, sound, and video. It uses both of WAP and SMS technology to send the message.

The process of sending and receiving MMS message works like this [17]:

- First the sending phone establishes TCP/IP connection through GPRS, and then performs an HTTP POST to an MMSC of the MMS message containing content of the message, header information and a list of intended receiver.

- After MMSC receives the message, it validates the message sender and then stores the content of the message and makes it available as a dynamically generated URL link.
- MMS notification message which is generated by MMSC is sent to receiver via WAP Push over SMS. It contains a URL pointer to the dynamically generated MMS content.
- When receiver receives MMS notification message, it initiates a TCP/IP connection through GPRS and performs an HTTP get to retrieves the message from MMSC.

2.1.2 Security

In information technology, security is the protection of information assets through the use of technology, processes, and training [18]. In order to have a secure system, it must have at least three aspects in it. The three aspects are described as [19]:

- *Confidentiality* means that assets (protected data, information or resources) can be access by authorized user only. Confidentiality is sometimes called secrecy or privacy.
- *Integrity* means that assets can be modified by authorized user only or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating.
- *Availability* means that assets are available to authorized user whenever it is needed. Availability is sometimes known by its opposite, denial of service.

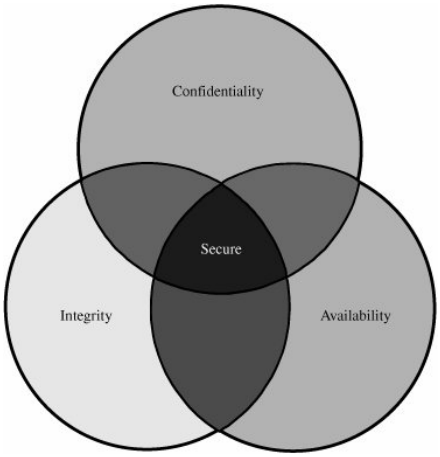


Figure 3: Relationship between Confidentiality, Integrity, and Availability

Image taken from Security in Computing

These three aspects cannot be separated one to the other. When these three aspects are fulfilled then the goal of security is accomplished.

2.1.2.1 Eavesdropping

Eavesdropping is a process of listening, monitoring data (such as e-mail, username, password, credit card, calling card number, etc) intentionally without their permission or knowledge [20, 21]. If a message is publicly broadcasted, then it will not be counted as eavesdropping.

There are several eavesdropping techniques and some of them are [22]:

- Listening to a telephone conversation between two people sharing secret information
- Wiretapping / Telephone tapping, which is figuring out what information is being sent from telephone conversation. It uses special devices that can intercept the electromagnetic emission from the wires.

- A man in the middle attack, which is when the attacker positions himself so that all communication between two people first passes through him.

2.1.2.2 Mobile Spy

Mobile Spy is a hybrid software or service which allows you to monitor smartphone in real time [23]. It is compatible with three operating systems: Windows Mobile, Symbian OS and Apple iPhone. Supported features are calls log, SMS (text message) log, web site URLs log and log summary.

Figure 4 (see below) shows how it works.

A. Customer purchases Mobile Spy software and install it to targeted phone, after that set configurations about the monitoring needs.
B. While targeted user performs SMS and call activities, Mobile Spy records and uploads it to Mobile Spy server.
C. Customer login through their account and view activities recorded as seen in figure 5.

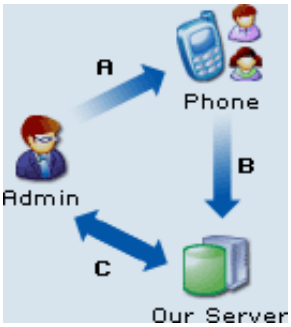


Figure 4: Mobile Spy System

Image taken from www.mobile-spy.com

Figure 5: SMS Logs Mobile Spy

Image taken from www.mobilespylogs.com

2.1.3 Steganography

Steganography is the art and science of hiding message where it comes from Greek word steganos (covered or secret) and graphein (writing or drawing) [24]. The goal of Steganography is to hide secret message (usually known as covert file) within a larger one (usually know as overt file) in such a way that others cannot discern the presence or contents of the hidden message [3]. Steganography is different from cryptography. While cryptography scrambles a message into a code to obscure its meaning, Steganography hides the message entirely [4]. Steganography can be used together with cryptography, for example encrypting the message first and then hiding it in host file. Host file can be image files, sound / movies files, word documents, or html file.

People who use Steganography must have a reason for communicating, so that no one monitors their communication and suspects them. For example anime lovers could exchange pictures of their favorite anime, while actually they are passing secret information.

Based on level of security which hidden message is embedded, transmitted and read, there are three types of Steganography approaches, which are [25]:

- Pure Steganography

  Pure Steganography is the least secured method among the others since it doesn't use any key to hide secret message. So if someone know that there is a hidden message then it is relatively easy to be cracked. It can be called secure if only the sender and the receiver know there is a hidden message and Steganography is used in the process.

- Private key Steganography

  Private Key Steganography uses symmetric key for encrypting and hiding secret message, so both parties which is sender and receiver must have the same key. It can be called secure as long as the key are not being compromised.

- Public key Steganography

  Public key Steganography is the most secure one among the others since it uses key paired system (public key and private key). In order to receive message, receiver sends his own public key to the sender. Then sender uses the given public key to encrypt the message. The encrypted message can only be decrypted by the receiver's private key.

While based to hiding techniques, Steganography can be categories as [4]:

- Insertion-based

  Insertion-based technique discovers sections in a file that are ignored by the processing application so that when the data is added, it has no effect on the representation (visual or audio reproduction) of the data. In some file there is an EOF (end of file) flag that is used to mark the end of the file. Application will read the file until it reach EOF flag and ignoring other data after it. In this case hidden data can be allocated after EOF flag.

  The main characteristic of insertion-based technique is adding data to file and not modifying the existing contents of the file. The advantages of this technique are quality of the image is unaffected and unlimited hidden message (you can add data as much as you want). However the disadvantage is someone will suspect it if the file is so big. For example, the size of file containing only word “Hi how are you?” is 5MB.

- Substitution-based

  Substitution-based technique discovers insignificant information in a file, so that the insignificant information can be substituted with data that wants to be added without having any impact. This technique must be done carefully since substituting wrong information can make file unusable or visually flawed.

  The advantage of this technique is size of the file has not changed. However the disadvantages are quality of the image is affected and limited hidden message (limited to the quantity of insignificant information in the file).

- Generation-based

  Unlike insertion-based and substitution-based technique that requires the host file / over file, generation-based technique uses the covert file to create overt file. For example, covert file is used to create a fractal image with given angle, length and color for each line created. This technique appears to solve stego detection problem which exist in insertion-based and substitution-based method. For example, if someone has both original file and file with hidden data, they can know the difference by comparing the binary composition.

Here are some products that implement Steganography:

- S-Tools is a freeware program with a drag and drop interface which mostly runs in Windows 95 or latter. It hides data in GIF or BMP image file and wav sound file using three least significant bits of each byte of data. Moreover, it can do encryption with IDEA, DES, Triple-DES, and MDC.
- Hide and Seek is a freeware program which hides data in GIF image file using least significant bit of each data byte. It runs under DOS.
- J-Steg is a program with simple built-in wizard. It hides data in JPEG image file using compression coefficient. JPEG images use a Discrete Cosine Transform (DCT) compression scheme which involves rounding floating point calculation. This rounding must be decided by the programs whether rounding up or rounding down. By modulating the decision, message can be embedded in the DCT coefficient.

Like other security technologies which are not one hundred secure, Steganography also have flaws, which are as follows:

- If someone knows there is a hidden message and knows the algorithm used, and unfortunately the message is not being encrypted, then he/ she can read the message.
- The hidden message can easily be destroyed without have to destroy the host file. For example, least significant bit is used to hide message in an image, then when the image is converted to another format, it is not impossible that the bit composition become changed. Even slight changes can destroy the message.

2.1.3.1 History of Steganography

Steganography was first published by Johaness Trithemius in 1499 in his book titled “Steganographia” [4]. The idea comes from Histiaeus which was a prisoner of a rival king. He used his slave to pass a secret message to his army. In order to do that, he shaved his slave’s head and tattoos the message on it and delivered the hidden writing as the slave's hair grew back.

In World War II, invisible inks which sources are milk, vinegar, fruit juice and urine that get darken when heated were used with much success [26]. However with the improving technology, it became easy to decode invisible inks.

Another way proposed was to use null cipher. In null chipper, a naive sounding message was used to camouflage the real message. For example, “Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming any day” message have a

hidden message of “Send Lawyers, Guns, and Money” by taking the third letter in each word. However with the improving message detection, this technique is no longer used.

Latter on microdots technology is developed by Germans. Microdots are very small photographs, the size of a printed period, which contain very clear text when magnified [27]. Through the development and time, another advanced technology appears up till now.

2.1.3.2 Digital Watermarking

Digital watermarking is a means by which an image is marked such that the owner of a file can rightfully identify any instance of that file to be his own [28]. For example, companies which sell photographs for website/ advertisement use watermarks to identify whether the used image has been paid or not. The trick of watermarking is to provide a subtle element that doesn’t overwrite anything else in the image, but that is significant enough to validate the image [4].

Although digital watermarking hides data in a file just like Steganography, it used only for protecting and proving ownership, not for transmitting information. It is commonly used by companies that sell images and audio recordings.

There are two types of watermarks, which are visible and invisible (see figure 6). In visible watermarks, copyright information overlay the original image, so that even the image is printed or scanned, copyright information will be visible. Unlike visible watermarks, invisible watermarks create a pattern to an image so that human eye cannot detect it, however a computer can. It is better if the image has smaller pixels in order to have people less chance to notice the slight changes of them. The advantage of invisible

watermarks is the image quality is not degraded. While the disadvantage is when the image is printed, copyright information will be gone.

Figure 6: Visible (left) and invisible (right) watermarks

Image taken from Hiding in Plain Sight: Steganography and the Art of Covert Communication

Here are some characteristic of digital watermarking:

- Does not impair the image - not to block large portion of the image or the entire image.
- Cannot be removed - make it to be impossible to remove digital watermarking without seriously degrading the image.
- Embeds a small amount of information - since it only be used as copyright protection/ ownership proven.
- Repeats data – place copyright information in more than one place to make sure that digital watermarking cannot easily removed.

There is one tool used to attack digital watermarks called StirMark. The first version of StirMark developed by Fabien Petitcolas was published in November 1997 as a tool to test the robustness of image watermarking algorithms [29]. StirMark Benchmark 4.0 is freely available today.

2.1.3.3 Steganalysis

Steganalysis is the art and science to detect whether a file has hidden message or not [30]. The one who does Steganalysis is called steganalyst. Steganalysts must have sufficient knowledge of Steganography and techniques of hiding data as well as good pattern recognition skills.

First step in Steganalysis is to discover hidden message which known as attack [31]. There are some attacks depending on available information to the steganalyst, which are:

- Stego-only attack – only stego-object is known
- Known cover attack – stego-object and original medium are known. In order to detect hidden message, stego-object and original cover object are compared.
- Known message attack – hidden message and stego-image are known. It can be used to analyze pattern which could decipher such message in future.
- Known stego attack – Steganography algorithm, stego-object and original medium are known
- Chosen stego attack – Steganography algorithm and stego-object are known
- Chosen message attack – stego-object is created from Steganography tool or algorithm of a chosen message in order to find the patterns in stego-object.

After hidden message is discovered another step taken is to disable or destroy the hidden message. This can be done by image manipulation or multiple manipulations which includes cropping (removing portion of image), rotating, blurring (decreasing the contrast between pixels), sharpening (increasing contrast between pixels), adding/ removing noise, re-sampling, converting between bit densities, converting from digital

to analog to digital (print and rescan the image), adding bit wise message, adding transform message.

2.1.3.4 Related Study on Steganography

- Stealth Steganography in SMS [32]. Considering information security issue, this paper describes a method to hide information in black and white picture in SMS message. After the user receives a picture message which contains hidden information, the decoder program extracts that information and immediately deletes the information from the picture, so that the picture saved on receiver's mobile phone will not contain any hidden information. The program was built with J2ME technology and has been tested on Nokia 6680 mobile phone.
- Sending Mobile Software Activation Code by SMS Using Steganography [33]. Considering much mobile software need to insert an activation code based on IMEI code, this paper describes a method to send mobile software activation code hidden in a SMS picture message. After user receives a picture message which contains activation code, the program extracts that activation code and compares it with the code which is generated based on the user's mobile phone IMEI code. If the codes are the same then software is activated. Program was built with J2ME technology and has been tested on Nokia N71 mobile phone.
- Improving Mobile Banking Security Using Steganography [34]. Considering the issue of security which is faced by m-banking, this paper describes a method for increasing security information requested by users. The requested information is hidden in a picture by password and is put on a site then the address is sent to the user. After user receives it, he/she downloads the picture then enters password to

extract the information. Program was built with J2ME technology and has been tested on Nokia N71 and Nokia 6680 mobile phone.

- Proposed Secure Mechanism for Identification of Ownership of Undressed Photographs or Movies captured Using Camera Based Mobile Phones [35]. Considering potential misuse of phones with camera capability, this paper describes a method to embed phone number or mobile machine ID (serial ID) to the captured images/ movies without user knowledge. If there is an inappropriate image/ movie, it can be used to prove and catch the owner of the image/ movie.

2.1.4 Mobile Platform Development

2.1.4.1 J2ME

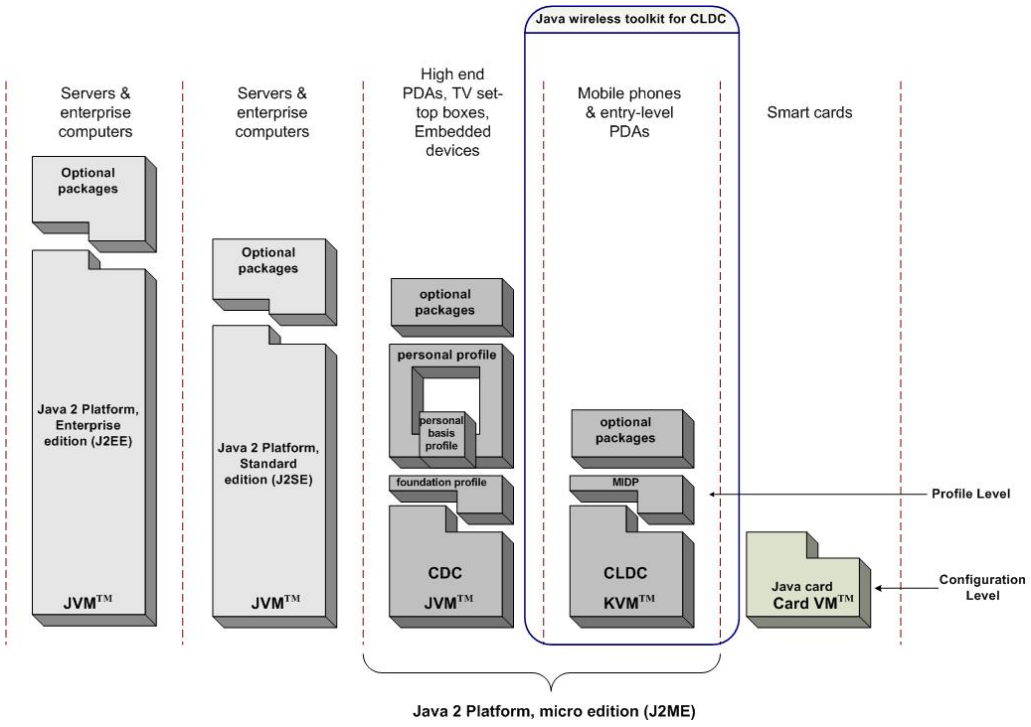


Figure 7: Java 2 Platform

Image taken from ikt.hia.no/aml

Java which is known as Java 2 Platform is divided into three editions which are Java 2 Standard Edition (J2SE), Java 2 Enterprise Edition (J2EE), and Java 2 Micro Edition (J2ME) [36]. They are targeted for different devices/ systems. J2SE is designed for desktop-based application, J2EE is designed for server-based application, and J2ME is designed for handheld and embedded devices.

J2ME (a scaled down version of J2SE) is a collection of packages and classes for application development on mobile devices or less memory and low processing power devices. It first introduced by sun in 1999.

J2ME architecture is divided into four different levels:

- KVM (Kilobyte Virtual Machine)/ CVM – a subset of Java Virtual Machine is used as a pool for running small java program/ code on the device.
- Configuration – Java runtime environment which includes virtual machine, native code, and a set of core classes derived primarily from J2SE. There are two different configurations which are Connected Limited Device Configuration (CLDC) and Connected Device Configuration (CDC). CLDC is used for low end PDAs and limited devices such as cellular phone, pagers and smart cards while CDC is used for capable devices such as high end PDAs. KVM is virtual machine for CLDC while CVM is virtual machine for CDC.
- Profiles – extensions to fill out missing functionality and support specific implementation such as user interface classes for building interactive application and record management to store persistent data. CLDC-profile is called Mobile

Information Device Profile (MIDP) while CCD-profile is called Personal Digital Assistant Profile (PDAP).

- Optional Packages – additional sets of APIs that is not included in configuration or profile. One example of optional package is Bluetooth support.

2.1.4.2 Symbian OS

Symbian OS is an open source operating system for mobile phones primarily used on Nokia advanced or data enabled smart phones [37]. It runs in three major platforms, which are Nokia S60, Nokia Series 80, and UIQ.

Symbian Limited, which is the developer of Symbian OS, was originally founded by Psion, Nokia and Ericsson in July 1998, with Motorola joining later that year, Matsushita in 199 and Siemens in 2002 [38]. It was originally designed for mobile phone with limited resources.

2.1.4.3 BREW

BREW, which is an acronym for Binary Runtime Environment of Wireless, was introduced in January 2001 and developed by Qualcomm [39]. Originally it was used only for CDMA, however today it can be used also for SMA, GPRS and UTMS.

BREW is less developer friendly than other mobile development since testing application created by BREW is more difficult. In order to test the application, developer cannot just upload and run it on mobile phone. However the application must include a digital signature which can be obtained by becoming the content provider or a Qualcomm Authenticated BREW Developer. Moreover once digital signature is obtained, other barriers must be overcome.

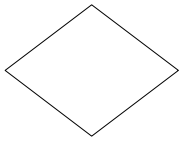
2.1.5 Diagram

Analysts and designers use diagrams to build models of systems. Diagrammatical model are used extensively by systems analysts and designers in order to communicate ideas, generate new ideas and possibilities, test ideas and make predictions also understand structure and relationship [40].

2.1.5.1 Flowchart

Flowchart is a simple pictorial representation which shows an algorithm or process to analyze, design and manage a process or program. There are four major elements of flowchart as shown below:

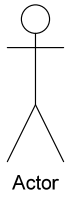
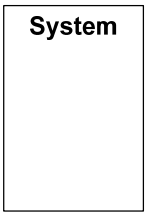
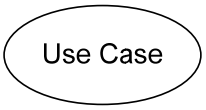
Table 1: Elements of a Flowchart Diagram

Element	Terms
	Terminator – show start or end points in a process
	Process – represents a processing step
	Decision – represents a logical condition or branch in the process flow
	Arrow – shows the flow of control

2.1.5.2 Use Case Diagram

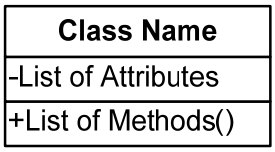
Use Case diagram shows interaction between system, external systems and users, which means who will use the system and in what ways the user expects to interact with the system [41]. There are four major elements of use case as shown below:

Table 2: Elements of a Use Case Diagram

Element	Terms
	Actor - person who interacts with the system it self
	System boundary – represents the scope of the system
	Use case – system functionality. It can extend / use another use case
	Relationship – links actor with use case

2.1.5.3 Class Diagram

Class diagram shows object classes that the system composed of as well as the relationship between those object classes [41]. Class entity is shown below:



2.1.5.4 Statechart Diagram

Statechart Diagram is used to model the dynamic behavior of a particular object [41]. It shows an object's life cycle. There are five major elements of statechart diagram as shown below:

Table 3: Elements of a Statechart Diagram

Element	Terms
	Initial State – start point
	State – represents the scope of the system
	Final State – denote the ending
	Relationship – links actor with use case
	Synchronization Bar –control the splitting or joining of sequential paths

Horrocks (1999) relates the use of statecharts to coding and testing of the user interface [37]. The process involves five tasks, which are:

- Describe the high-level requirements and main user tasks
- Describe the user interface behavior
- Define user interface rules
- Draw the statechart
- Prepare an event-action table