

*Master Thesis*  
*Computer Science*  
*Thesis no: MCS-2007:13*  
*June 2007*



# **Reviewing Security and Privacy Aspects in Combined Mobile Information System (CMIS) for health care systems**

**Al-Leddawi Mustafa  
Kunwar Ramesh**

Department of  
Software Engineering and Computer Science  
School of Engineering  
Blekinge Institute of Technology  
Box 520  
SE – 372 25 Ronneby  
Sweden

This thesis is submitted to the Department of Computer Science and Software Engineering, School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Software Engineering and Computer Science. The thesis is equivalent to 20 weeks of full time studies.

**Contact Information:**

Author(s): Al-Leddawi, Mustafa  
Address: Kungsmarksvägen 71 LGH 1312  
371 44 Karlskrona  
Sweden  
E-mail: [mustafa.leddawi@gmail.com](mailto:mustafa.leddawi@gmail.com)

**Contact Information:**

Author(s): Kunwar, Ramesh  
Address: Kungsmarksvägen 69 LGH 1426  
371 44 Karlskrona  
Sweden  
E-mail: [rameshkunwar@hotmail.com](mailto:rameshkunwar@hotmail.com)

University advisor(s):

Guohua Bai

E-mail: [guohua.bai@bth.se](mailto:guohua.bai@bth.se)

Department of Software Engineering and Computer Science  
Blekinge Institute of Technology

School of Engineering  
Blekinge Institute of Technology  
Box 520  
SE – 372 25 Ronneby  
Sweden

Internet : [www.bth.se/tek](http://www.bth.se/tek)  
Phone : +46 457 38 50 00  
Fax : + 46 457 271 25

# Abstract

Medical area has been benefited by the use of ICT (Information and Communication Technology) in recent days. CMIS (Combined Mobile Information System), our proposed model system, is such a system targeted for health care system. IMIS (Integrated Mobile Information System), a system for diabetic healthcare, which is being developed in Blekinge Institute of Technology will be taken as a case study for our proposed system. CMIS is a multi-role system with core service being medical-care related and others like self-monitoring, journal-writing, communicating with fellow patients, relatives, etc. The main reason for not using CMIS could be the security and privacy of the users' information. Any system connected to Internet is always prone to attack, and we think CMIS is no exception. The security and privacy is even more important considering the legal and ethical issues of the sensitive medical data. The CMIS system can be accessed through PDA (Personal Digital Assistant), smart phones or computer via Internet using GPRS (General Packet Radio Service)/UMTS (Universal Mobile Telecommunication System) and wired-communication respectively. On the other hand, it also increases the burden for security and privacy, related to the use of such communications. This thesis discusses various security and privacy issues arising from the use of mobile communication and wired communication in context of CMIS i.e., issues related to GPRS (mobile) and web application (using wired communication). Along with the threats and vulnerabilities, possible countermeasures are also discussed. This thesis also discusses the prospect of using MP2P (Mobile Peer-to-Peer) as a service for some services (for example, instant messaging system between patients) in CMIS. However, our main concern is to study MP2P feasibility with prospect to privacy. In this thesis, we have tried to identify various security and privacy threats and vulnerabilities CMIS could face, security services required to be achieved and countermeasure against those threats and vulnerabilities. In order to accomplish the goal, a literature survey was carried out to find potential vulnerabilities and threats and their solution for our proposed system. We found out that XSS (cross-site scripting), SQL injection and DoS attack being common for a web application. We also found that attack against mobile communication is relatively complex thus difficult to materialize. In short, we think that an overall planned security approach (routinely testing system for vulnerabilities, applying patches, etc) should be used to keep threats and attacks at bay.

**Keywords:** Privacy, Security, MP2P, CMIS, DoS, XSS (Cross-Site scripting), SQL Injection, Eavesdropping.

## **Acknowledgements**

*We would like to express our heartiest gratitude to our supervisor Prof. Guohua Bai, Docent for his suggestion, guidance, encouragement, and patience throughout the period of thesis. We would like to express our sincere thanks to Professor Rune Gustavsson for accepting us and giving an opportunity to work in this field. We would also like to thank Mr. Peng Zhang for his sincere suggestion and help providing information. To our family, who gave us all support over the years. To our friends who supported us during the work by discussing and reviewing. Last but not the least; we would like to thank Sweden and its people for giving us a chance to get high-quality education at no cost.*

*Mustafa Al-Leddawi  
Ramesh Kunwar  
June 1, 2007  
Karlskrona, Sweden*

# Table of Contents

<b>LIST OF FIGURES.....</b>	<b>V</b>
<b>CHAPTER 1 INTRODUCTION.....</b>	<b>1</b>
1.1 BACKGROUND AND MOTIVATION .....	1
1.2 RESEARCH QUESTIONS .....	3
<b>CHAPTER 2 RELATED WORK .....</b>	<b>5</b>
2.1 INTEGRATED MOBILE INFORMATION SYSTEM (IMIS) .....	6
2.2 GSM RELATED MOBILE HEALTHCARE .....	7
2.3 WEAKNESS OF CURRENT APPROACH.....	8
2.4 SOME ATTACKS OVER THE GSM .....	8
2.4.1 Attacks on algorithm A3/8 .....	8
2.4.2 Flaw in A5/1 & A5/2 algorithm .....	8
2.4.3. Attack on SIMcard .....	8
2.4.4 False base-station.....	8
2.5 COUNTERMEASURE FOR THE ATTACKS .....	9
2.5.1 New A3/A8 implementation.....	9
2.5.2 GSM A5/3 Ciphering.....	9
2.5.3 GPRS/UMTS .....	9
2.5.4 UMTS – Two-way authentication .....	9
<b>CHAPTER 3 LITERATURE STUDY AND VALIDITY .....</b>	<b>10</b>
3.1 INTRODUCTION .....	10
3.1.1 Literature survey.....	10
3.1.2 Analysis procedure.....	11
3.1.3 REVIEW AND EVALUATION PROCEDURE.....	11
3.2 THE RESEARCH VALIDITY .....	11
3.3.1 TYPES OF VALIDITY AND RESEARCH VALIDITY .....	11
3.3.2 THE RESEARCH QUALITY VALIDITY .....	12
3.3.3 THE RESEARCH INTERPRETATION VALIDITY .....	12
<b>CHAPTER 4 SECURITY SERVICES .....</b>	<b>13</b>
4.1 CONFIDENTIALITY .....	13
4.2 INTEGRITY .....	13
4.3 AVAILABILITY .....	13
4.4 AUTHENTICATION.....	13
4.5 NON-REPUDIATION .....	14
4.6 ANONYMITY .....	14
4.7 SUMMARY .....	14
<b>CHAPTER 5 VULNERABILITIES AND THREATS RELATED TO MOBILE COMMUNICATION IN CMIS.....</b>	<b>15</b>
5.1 HISTORY OF MOBILE COMMUNICATIONS SYSTEMS .....	15
5.2 THREATS AGAINST GSM .....	15
5.3 THREATS AGAINST GPRS .....	16
5.3.1 GPRS Overview .....	16
5.3.2 GPRS Architecture.....	16
5.3.3 Security functions in GPRS.....	18
5.3.4 GPRS Security Process .....	19
5.3.5 Security Threats to GPRS .....	20
5.3.5.1 Attack on availability .....	20
5.3.5.2 Confidentiality .....	20
5.3.5.3 Integrity.....	20
5.3.5.4 Authentication and authorization.....	20
5.3.6 Solutions of the attack.....	21

5.3.6.1 Using logical tunnel from GGSN to network: .....	21
5.3.6.2 Limiting traffic rate: .....	21
5.3.6.3 Inspecting stateful packets: .....	21
5.3.6.4 Implementing Ingress or Egress Packet Filtering: .....	21
5.4 OTHER THREATS .....	21
5.5 SUMMARY .....	22
<b>CHAPTER 6    WEB APPLICATION SECURITY .....</b>	<b>23</b>
6.1 ENCRYPTION, DIGITAL SIGNATURE, AND CERTIFICATES .....	23
6.1.1 Encryption.....	23
6.1.2 Digital signature:.....	23
6.1.3 Certificates.....	24
6.2 SECURE CLIENT-SERVER INTERACTION.....	24
6.2.1 User authentication.....	24
6.2.2 Authorization .....	24
6.2.3 end-to-end security.....	24
6.3 CLIENT SECURITY ISSUES .....	24
6.3.1 Preserving privacy.....	24
6.3.2 Mobile code security.....	25
6.3.3 Phishing and web spoofing .....	25
6.3.4 Desktop security.....	25
6.4 SERVER-SIDE SECURITY.....	25
6.4.1 Cross site scripting (XSS).....	25
6.4.2 SQL injection .....	25
6.4.3 vulnerability of server-side scripting language .....	26
6.4.4 Service availability.....	26
6.5 SUMMARY .....	26
<b>CHAPTER 7    MOBILE PEER-TO-PEER (MP2P) ON CMIS AS A SERVICE WITH THE PERPECTIVE OF PRIVACY.....</b>	<b>27</b>
7.1 INTRODUCTION.....	27
7.2 MOTIVATION.....	27
7.3 PARADIGM OF MP2P .....	28
7.5 PRIVACY PROTECTION MECHANISM.....	29
7.5.1 Location-based privacy mechanism.....	29
7.5.2 Content-based privacy scheme.....	29
7.6 CONCLUSION.....	31
<b>CHAPTER 8    FUTURE WORK AND CONCLUSION.....</b>	<b>32</b>
8.1    FUTURE WORK .....	32
8.2    CONCLUSION .....	32
<b>REFERENCES .....</b>	<b>33</b>

## LIST OF FIGURES

Figure 2.1: Multiple proposed healthcare telemedicine system with mobile communication link support [12]. .....	5
Figure 2.2: IMIS overview .....	6
Figure 2.3: Authentication and Cipher Key .....	7
Figure 5.1: GSM/GPRS Architecture [28]. .....	17
Figure 5.2: Ciphering key (Kc) generating algorithm .....	18
Figure 5.3: Authentication Algorithm (A3).....	19
Figure 5.4: The GPRS Encryption Algorithm .....	19
Figure 7.1: Mobile Client's Protocol Stack [50]. .....	29
Figure 7.2: Preserving privacy using buddy [54]. .....	30

---

# Chapter 1 INTRODUCTION

---

This chapter introduces and presents the baseline of this master thesis to provide the reader with an overview of the whole paper and the important issues that will be discussed and investigated.

## 1.1 BACKGROUND AND MOTIVATION

In the last few years, the evolution of computer science and mobile communication has been developed rapidly. This revolution of technology has been annexed to commercial services, military use, medical records and others.

Recently, there are many extensive researches in different medical areas using mobile communication systems, especially in USA and Europe [1] [2]. During the IT evolution, many attempts were made to build what the researchers called an Integrated Systems. However such system should offer trustworthy and confidential services. The researchers worked harder to achieve the mentioned systems especially those related to medical and healthcare. Many of the standards, such as D-AMPS (Digital Advance Mobile Phone Systems) - USA based, GSM (Global System for Mobile communications) - European based, and others have been built to serve the use(r) of digital cellular technology communities regardless to healthcare and medical communities [3]. So, more interest is given to the healthcare communities nowadays.

Computing and communication become more important to healthcare communities, not only from the technical viewpoint, but also from the humanitarian point of view. Humanitarian in the sense, that it will be helpful to save people's life. Also, it might help to cure patients faster.

CMIS (Combined Mobile Information System for Health care) is a system aimed for various areas such as diabetic, asthmatic patient, etc. CMIS is a system which uses both mobile and wired (combined) communication system. The tradition for diabetic patients has been to contact their care providers (doctors, nurses, relatives, etc.) regularly for support, treatment, and education. It is evident that better communication facility between the patients and care-providers will help to reduce visit time and help to improve the quality of life of the patients. Also, if a visit is necessary and if patient and care-providers are able to communicate before the visit, then the planned visit would be more worthwhile [4].

Studies in the USA and in Sweden showed that the self-treatment and supervision of diabetic patients can greatly increase their quality of their daily life if they are provided with reliable and easy access to their care providers [4].

Therefore, the necessity of a multi role system, which could help patients to communicate with their care providers as well as self-monitor them, brings the system like CMIS into existence. CMIS, which aims to provide reliable and easy communication between patient, care providers, and relatives on both stationary and mobile platform. CMIS could be based on Engström's triangle model in Activity Theory [4] [12]. The benefit of using it is that CMIS can be used to integrate and coordinate various health care activities under the same fundamental activity system [4].

CMIS focuses on shared information sharing and reliable communication between different stakeholders like patient, doctors, nurses, relatives, etc.

A patient can join CMIS by providing certain individual data to CMIS system administration. The patient and his/her family get login information and education. Users have option of mobile or wired communications to access CMIS. All information of a user will be stored in a database server; no data will be saved locally. Information is encrypted while being exchange to boost security. Different access levels are made regarding the access of data.

CMIS also facilitates a user to chat with other fellow diabetic patients, write diary, activities, etc. and send queries to a special doctor, nurse [4].

There are two scenarios for CMIS. In one scenario, the patient is given focus and thus, provided with mobile-network communication platform which will assist patient regarding preparation before visiting doctor, supervising herself/himself, and to extent self-treatment as well. Under another scenario, the care providers are given focus with same mobile-network communication that will be able to access the patient's information. The seamless-communication between the patients and care-providers will provide better care to patient as well as will reduce unnecessary visits to doctor.

The term P2P generally refers to systems or applications that share resources in a distributed and decentralized way. Unlike traditional client-server model, P2P network relies on the bandwidth and computing power of the peers (users) to exchange information rather than computing power and bandwidth of few servers. This greatly helps to lessen the burden of few servers by distributing bandwidth and computing power. There is no concept of client or server in P2P; however, nodes are connected with equal peers. Napster [10] was the first popular to use P2P system for file transfer. Other popular P2P services like Gnutella [13] and Freenet are considered as pure P2P system because they use P2P structure for all purpose [11]. The advantages of using P2P technology are like improved scalability, lower cost of ownership, self-organized, greater fault tolerance, etc.

The networking capabilities, with the advent of smartphones, increasing users, better services (like 3G), of mobile devices are rapidly growing. This has drawn a lot of attraction for the adoption of P2P technology in mobile phones too, despite having low networking, storage, and processing capabilities. MP2P file-sharing client like Symella [47], a Gnutella [14] file-sharing client, are already available for Symbian smartphone (for S60 Platform 2nd & 3rd edition). Gnutella is mostly used and fully distributed (also called as pure) P2P protocol.

P2P, which is considered as one of the major revolutions the Internet has experienced, has become a very popular medium to share information. Its popularity can be depicted by the fact that 80% of the total traffic in a high speed IP backbone link was generated by P2P [9]. Thus, we shall also discuss the possibilities of benefiting CMIS with P2P through the security perspective

Though all personal information are considered sensitive, healthcare information is considered even more sensitive. Protecting users' data is a big challenge for CMIS especially in the current situation where privacy is at stake, when attacks on various systems are in rise. Since, CMIS uses both mobile and conventional wired communication, so extra care should be given for information security. Security is a hot issue in vital systems like transportation, telecommunications, healthcare, and financial services. A large segment of society may be adversely affected if it is compromised. Thus, the research in this field could be justified.

While talking about security of a system we must keep in mind about the security aspects that provide mitigation against many threats. They are [7]:

- Integrity: The property of information that has not been changed by unauthorized parties.
- Confidentiality: The protection of transmitted data from unauthorized parties.

- Authentication: The assurance that the communicating entity is the one which has claimed to be.
- Availability: The property of a system or a system resource to be accessible and usable at any time by an authorized system entity.
- Non-repudiation: It prevents either or sender or receiver from denying a transmitted message.

The importance of above could be felt particularly when the threats possessed in wireless or wired communication is observed carefully. Some of the most common threats faced today are:

- DoS attack
- Spoofing
- Sniffing
- Eavesdropping
- Social Engineering

Medical records are highly sensitive. Any alteration on such data can lead to fatality. Therefore, a system must assure the security of the system to its users. To know more about the persistent threats it is important to know the environment in which the system operates. Security is considered as one of the most affecting factor for the reliability of any software; especially that uses Internet, which is not secured any more [8].

The users for CMIS system would be expecting a secure system which they can rely on; especially, when the attack attempts and unauthorized entrance to systems are increasing. The threats could be internal or external. So, a secure system should not only protect against outside attack, but also provides reliable framework for the safety of information internally too. However, internal threat is not the scope of our study and we shall not discuss it.

Healthcare is a humanitarian area and, therefore, the subject matter motivates us to work in this area. Obviously, the beneficiary of the CMIS will be the society.

## **1.2 RESEARCH QUESTIONS**

The thesis focuses on the security issues arising from the use of CMIS. Security is one of the most vital aspects in the healthcare systems.

Following research questions were considered for this thesis:

- What are the potential threats to CMIS, arising with the use of the mobile technology?
- What are the possible threats for the security and privacy in CMIS as a web application?
- What could be the possible solution to address those threats?
- Is MP2P suitable technology for CMIS with the perspective of privacy?

A detail study of the CMIS and literature survey will be done to find answers of above questions. We have listed the expected outcomes below:

- A detail study of various threats will be carried out to find different vulnerabilities.
- A study of the provisions to counter threats by CMIS will be carried out.
- A general suggestion and/or recommendation will be presented.

The remainder of the thesis is structured as follows. Chapter 2 presents the related work. Chapter 3 discusses the literature study and validity that has been followed during the research. Chapter 4 holds discussion about security services. Chapter 5 includes investigation of the attack on the mobile communication. Chapter 6 holds a discussion for web-application security. Chapter 7 is about using mobile peer-to-peer (MP2P) system on CMIS with perspective of security and privacy. Finally Chapter 8 holds an expected and future work and the conclusions.

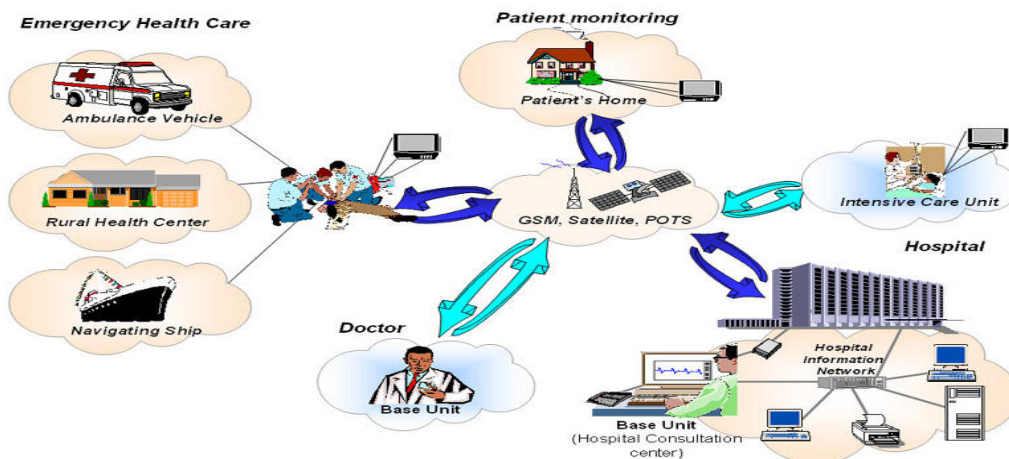
---

## Chapter 2 RELATED WORK

---

In this part of the study, we try to discuss some of the research that has been done on the security issue. We also try to refer these researches in specific category according to the way that they concern in security. Some of these researches are designed and constructed by their units with the concern of processing of medical data in the telecommunication sector [12], while some of them are dealing with other techniques or security mechanisms.

Kyriacou et al. proposed a Multi-Purpose Healthcare Telemedicine Systems with mobile communication link support [12]. This system is designed and examined according to multiple criteria; the most important one is the security needs. Therefore, security and privacy can be taken into account at the beginning of system development life cycle. This system is supposed to integrate two main modules; the first module is based on the patient's site which is called Telemedicine Unit. The second one is based on the care providers which is called the Base Unit. The system's design and implementation based on a detailed user requirements analysis. The communication over the system's unit's sites is done using TCP/IP.



**Figure 2.1: Multiple proposed healthcare telemedicine system with mobile communication link support [12].**

The main purpose of proposing the Multi-Purpose Healthcare Telemedicine System is to deliver the health care services and also to share the medical knowledge. Thus, for supervise the emergency care and provide expert healthcare using telecommunication and information technologies.

Blowfish cipher encryption algorithm has been used to encrypt the exchanged data [12]. Therefore, security was designed to concern processing of sensitive medical data over the communication system. Blowfish algorithm was designed to be easy to implement and to have high execution speed [7] [11]. It is significantly faster and more flexible as it allows for a variable key size. Also, Blowfish uses a large number of sub-keys for encryption or decryption and these keys must be pre-computed before any of the encryption or decryption processes are being carried out [7]. In the Base Unit, the data size of the information is reduced by using a compression algorithm called lossless ECG compression which is based on Huffman coding algorithm [18].

The Multi-Purpose Healthcare Telemedicine System uses a secure database system which is password protected and encrypted. Further, to enhance the security different levels of access depending upon the users' group are defined. This ensures availability of needy (sanctioned by the organization) information to a user depending upon his/her role or right.

## 2.1 INTEGRATED MOBILE INFORMATION SYSTEM (IMIS)

We have taken a system that is being developed in Blekinge Institute of Technology but not yet deployed. Integrated Mobile Information System for Diabetic Healthcare (IMIS) is a project financed by VINNOVA [4].

Functions of the IMIS can be summarized as [4]:

- Monitoring:
  - Online monitoring of vital signs, such as EKG, blood pressure, blood glucose, body temperature, etc.
- Communication /accessibility:
  - Vital signs are recorded in a database. In case of any anomaly, an alarm should be send to the pre-defined care providers. Other factors are booking visiting time, renewing prescriptions, and queries.
- Knowledge and decision making:
  - Patient's medical history can be stored to seek decision support and advices from care providers. Other services like making diagnoses, detecting trends and reacting on it.
- Support relatives and social life:
  - Pproviding psychological support to contact with relatives by video chat. Setting up 'community' forum where people exchange experience and advices.

IMIS grows up to achieve the need for communication and information accessibility between care-providers and their shared patients [6]. IMIS is used to integrate and coordinate several healthcare activities by sharing the same primary activity structure to help the healthcare organizations to communicate with each other and to get access to the right information [4].

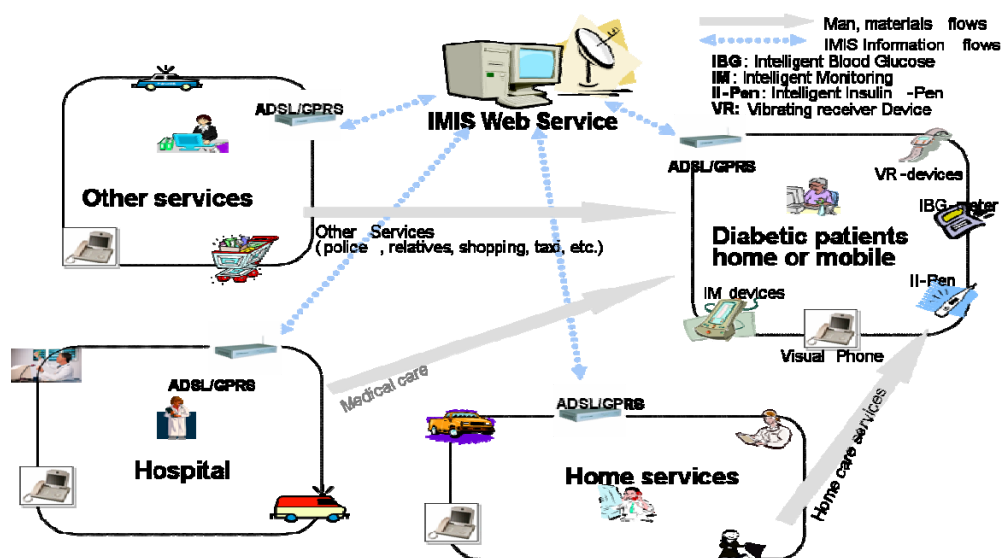


Fig. 2.2 IMIS overview [4]

## 2.2 GSM RELATED MOBILE HEALTHCARE

The multiple proposed healthcare telemedicine systems with mobile communication link support based its network on a digital mobile telephone system GSM (Global System for Mobile communication) which is common in Europe [1][9]. GSM is the wireless telephone standard in Europe [1]. The initial GSM standard provides an encryption of speech and data transmissions over the radio path [9], hence to support security services through mobile transmissions. The main purpose of designing GSM is to satisfy the need of a secure mobile system over the (air transmission) wireless transmission encryption.

The GSM security is designed to protect the privacy of a mobile user against eavesdropping, unauthorized access, and unauthorized tracing of the user's location and identity when they are mobile. The protection against an unauthorized access is done via strong authentication. Eavesdropping is prevented through encryption of the information channel. To prevent from disclosing users identity and location, the appropriate radio signaling channels are also encrypted and a temporary identity (TMSI) is used instead of the actual identity (IMSI). So the encryption algorithm plays a vital role for secure GSM [9]. Figure 2.2 describes briefly the authentication process and the cipher key generation.

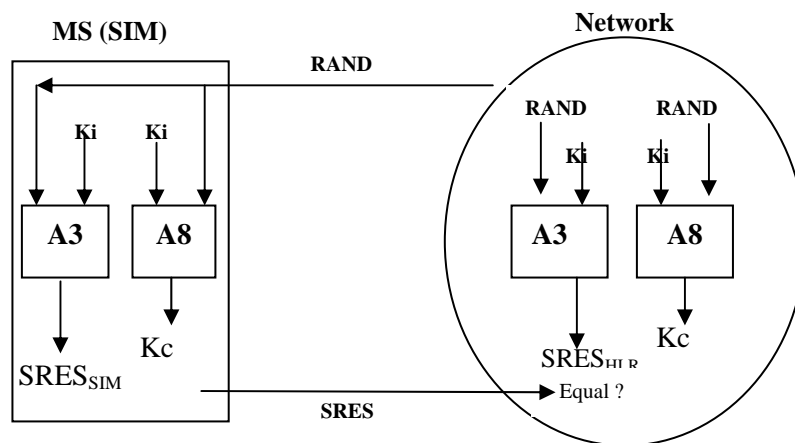


Figure 2.3: Authentication and Cipher Key generation [9].

The figure above, the party authentication key (Ki), the authentication algorithm (A3), the cipher key generation algorithm (A8), and the encryption algorithm (A5) all of them are part of the subscriber identity module (SIM) which are programmed by the operator[9]. The authentication algorithm (A3) is used to generate the signed response (SRESSIM) using the Random Number (RAND) and the secret key (Ki). Similarly, A3 authentication algorithm is used to calculate the signed response (SRESHLR) using the random number (RAND) and the secret key (Ki). Both signed responses (SRESSIM, SRESHLR) are compared, SIM is considered to be authenticated if it is equal and avail the service of operator otherwise denied.

The algorithm COMP128 (A3 and A8 implemented together) is a common algorithm which is used by operators for the cipher key generation and the authentication algorithms [14] [15]. The COMP128 algorithm uses the key (Ki) of length 128 bit and a random number (RAND) of length 128 bit as input to generate an output of 128 bits and a signed response (SRES) of 32 bit and cipher key (Kc) of 54 bit [15].

## **2.3 WEAKNESS OF CURRENT APPROACH**

This section presents some of the familiar weak points with GSM; these weak points could allow some attacks and eavesdropping.

As in the case of the authentication process and the cipher key generation, the general authentication process of GSM suffers from some weakness points. The general description of the authentication is that the authentication SIM used to identify the party to the operator. The operator can check the responses which come from the user after he had sent many issues to the user and the user encrypts these issues using the authentication algorithm (A3). As a result, the SIM user can authenticate itself on the network but the network can not authenticate itself to the SIM user, thus, it is one way authentication. This may help the attacker to play an important role that he could deceive to be a network and launch man-in-the-middle-attack.

In addition, GSM does not protect against some kinds of attacks. For example, an active attack involves some modification of the data stream or the creation of a false stream [7]. Thus, the cipher keys and the authentication tokens [17] could be sent over the network insecurely, so an attacker could intercept (capture) this communication and he could also impersonate the user or network elements.

Moreover, the security elements over the GSM network are already available, but the challenge here is that these elements need to upgrade and improve. For instance, the used encryption and authentication algorithms are already available, but have not been completely deployed.

## **2.4 SOME ATTACKS OVER THE GSM**

### **2.4.1 ATTACKS ON ALGORITHM A3/8**

COMP128 is a new version. If 16000 RAND-SRES pair is collected then Ki can be find out. Wagner& Goldberg claimed to crack COMP128 algorithm in 1998.

### **2.4.2 FLAW IN A5/1 & A5/2 ALGORITHM**

Attacks made by Biryukov, Shamir and Wagner [57]. A database of algorithm states and related key state is prepared. After that, a key search in database is made to find out a matching key stream. The database provides correct algorithm when a match is found. After simple computing Kc can be find out.

### **2.4.3. ATTACK ON SIMCARD**

Since SIM is implemented on smartcard, any vulnerability on a smart card will directly affect the security of SIM as IMSI & Ki are stored on it. The research operation of the smart card processor can be interrupted if it is exposed to an electric camera flash bulb [58].

### **2.4.4 FALSE BASE-STATION**

GSM security provides unilateral authentication. Unlike MS or ME authenticated to BS, BS is not authenticated to mobile equipment. Therefore, it facilitates attack by using of false BS.

## **2.5 COUNTERMEASURE FOR THE ATTACKS**

### **2.5.1 NEW A3/A8 IMPLEMENTATION**

New algorithms COMP128-2 and COMP128-3 has been introduced. COMP128-3 uses 64-bit Kc, however, COMP128-2 still uses the 10-bit ciphering Kc. COMP128-2 and COMP128-3 has stopped SIM cloning which makes extraction of Kc over the air infeasible.

### **2.5.2 GSM A5/3 CIPHERING**

In 2002, GSM added a much stronger algorithm than A5/1 and A5/2 which is A5/3. The A5/3 is based on Kasumi core (the core encryption used for UMTS).

### **2.5.3 GPRS/UMTS**

In GPRS, ciphering occurs in LLC (Logical Link Control) layer. In UMTS, it occurs at RLC/MAC layer. The FEC is then applied at physical layer.

### **2.5.4 UMTS – TWO-WAY AUTHENTICATION**

The 2-way authentication procedure removes the possibility of imitating the network. The network sends the AUTN (Authentication Token) along with the RAND. AUTN consist of a sequence number (SQN) encrypted using RAND and root key (K). The SIM keeps track of sequence number to stop attacker from replaying the legitimate network's authentication request.

---

# Chapter 3 LITERATURE STUDY AND VALIDITY

---

This chapter is based to discuss our research methodology. It defines the activity of the research, explanation of necessary information, how the research proceeds and how to measure the progress. It also provides a brief description of the way that the study was done and explanation of how the data was analyzed and explanation of methodological problems and solutions.

## 3.1 INTRODUCTION

Theoretical study has been conducted in order to carry out the research questions and to find out what is the thing that the potential reader could ask. The research method architecture aims to describe how the literature survey, analysis, reviewing and evaluating have been carried out in order to clear the research primary methodologies.

### 3.1.1 LITERATURE SURVEY

The literature survey is widely used and comprehensive. Therefore, it is the state of the art and identifies gaps in the body of the knowledge. On other hand, the literature survey identifies clearly the relevant work to locate useful expertise; also it keeps abreast of developments around the world [18]. These reasons could be carried out to make it easy to gather the required, relevant and related literature materials, i.e., textbooks, articles, journals (e.g. security issues journals), World Wide Web, newspapers and conference proceedings which concerns in the subject that the research is describing. However, the literature survey is not only a simple list of papers or a descriptive list of available materials but also it is a guiding concepts or a critical assessment.

Since, the main purpose of the thesis is about reviewing different security aspects of the CMIS system. The survey should be managed and constructed in a systematic manner in order to minimize the efforts and time. Therefore, the literature survey has been managed and controlled according to the following limitation:

- Analyzing the major security threats over CMIS system.
- The possibilities of using Mobile Peer-to-Peer (MP2P) in the CMIS system through the security perspective.
- Reviewing the defensive aspects against the threats.

The available databases like, except from the various books, IEEEExplore, ACM digital library, Springer Link and others have been used to perform the search for the needed data. In addition, some of different search engines like Google, Google Scholar, Yahoo, Ayna [19], CiteSeer [25] and others have been used in order to search various subject related literatures using an advanced search to assure more comfortable and suitable results. For example, searching for a specific file format and searching for the current and/or recent published articles etc. The main reason for using multiple search engines and citation site like CiteSeer is to gain variety outputs and cited literatures thus to be useful, non-biased and related to relevant materials. Although the search engines have some known advantages, but they cannot cover and provide the all required resources. However, some of the printed books are available as an electronic form, so we can access it. In other hand, some of these

books are not available as an electronic form and they are not freely accessible. Thus, the search in the university library for the printed materials is more suitable.

### **3.1.2 ANALYSIS PROCEDURE**

The routine procedure is followed to make sure if the collected literature materials are relevant by reading the abstract and the conclusion parts of the materials. If these materials are relevant, more concentration will be given to these materials and they will be chosen. Then, the chosen materials will be inspected carefully to verify facts.

During the collection process, and at the same time, reading the chosen materials was done more than one time to help in understanding the purpose of the materials and explaining certain idea. These steps could help to determine whether the material helps to make the content clear and meaningful or to give us a sense about what we are doing. Moreover, more concentration was given on each literature thus to grasp enough by making basic notes for the most important aspects. Also these materials have been documented to use as references. In addition, all elements inside these materials could be important and it should be reviewed and understood, thus to find out the reason of its existence. This could help to add more understanding in the area of the study. Moreover, our previous knowledge which has been built from the taken courses at the school and the discussion with teachers and students was used to contribute in this research.

Finally, the more one know the better it is in order to improve the quality of the discussion. Therefore, various materials were discussed for a related topic from different angles.

### **3.1.3 REVIEW AND EVALUATION PROCEDURE**

The analyzing, classifying and evaluating of the study is, especially, difficult because the strategies and techniques have not been well defined [24]. Every study should nevertheless struggle to have a general analytic strategy. It is argued that adopting some approaches implies taking different perspective in addition to our point of view, which could help in building the classification and evaluation from that adoption in utilizing the research. However, talking about security aspects over the CMIS system, which could poses various threats, provides mitigation against threats; the assumption contribute mainly in utilizing positive approaches. The main assumption behind the positive paradigm is that there is an objective truth which exists in the world which can be revealed through the scientific method where the focus is on discussing and comparing the variant approaches (techniques) that have some similarity and/or concepts. Thus, this could help mainly in discovering the main diversities and similarities between different approaches.

## **3.2 THE RESEARCH VALIDITY**

### **3.3.1 TYPES OF VALIDITY AND RESEARCH VALIDITY**

The research validity is the best available approximation to the truth of a given proposition, inference or conclusion [20]. Usually, we have to make conclusions or inferences in our daily life. We have been often involved in making or drawing a conclusion during our daily academic activities and writing up as a thesis or research papers. The research validity is concerned with the manner of how much the conclusion is valid and if the conclusion is close to the truth. However, different researchers have developed their own concepts of validity, and they have also generated or adopted what they consider to be more appropriate term of validity. There are four major types of validity according to Trochim [20], construct validity, internal validity, external validity and conclusion validity. However, some qualitative researchers have argued that the term validity is not applicable to qualitative research; they have realized at the same time the need for some kind of qualifying check or

measure for their research [23]. [21] Suggests that the validity is affected by the researcher's perceptions of validity in the study and his/her choice of paradigm assumption. In other words, winter [22] described that the construct validity is concerned with determining whether the study measures what it is intended to measure. Thus, it is clear that the construct validity is more related to the quantitative research than qualitative research. In that way, this thesis is classified as qualitative research and this type of (construct) validity is considered as irrelevant. Internal validity is concerned with the issue cause-and-effect between the treatment and the outcomes [22]. It is also used to describe what was observed and experienced, thus the internal validity could be used with the experimental research. Therefore, internal validity is irrelevant to this thesis. External validity is concerning in generalizing the results of the research [22]. It is applicable to experiment research which involves the use of sample from a certain population. So, external validity is not related to the thesis because of there is no generalization carried out.

Conclusion validity is the degree to which conclusions we reach about relationships in our data are reasonable [20]. Conclusion validity is the most important type since it is relevant whenever we are trying to decide if there is a relationship in our observations. It is also relevant to the qualitative research. Thereby, the conclusion is based on our interpretation of the techniques that will be used to study the possibility of using a mobile P2P in CMIS system. In order to improve the conclusion validity, we think that it is so important to discuss the quality validity and interpretation validity especially they are related to each other. More interpretation leads to high quality.

### **3.3.2 THE RESEARCH QUALITY VALIDITY**

Quality is one of the most important issues in research, deprivation of it in literature resources is considered as one of the setback in the quality of the thesis. So, we try to defeat against systematic biases and nonsystematic biases by following the organized and systematic search procedures. If the different techniques like observation, interviews and other have been applied in the research, this could lead to more reliable results. Moreover, one data source could validate another by comparing the sources; we try to compare different literature sources to see if they are homogenous and if they are validate to each other. Although using many resources are considered as enough helpful, but it needs more efforts and might not be possible to follow this approach as we want; especially, some sources not always available.

### **3.3.3 THE RESEARCH INTERPRETATION VALIDITY**

Interpretation, in most research, attempts to make clear underlying sense of an object of the research. This object could, therefore, be in one way is confused, incomplete, cloudy, seemingly contradictory, and in another way unclear or misunderstanding concepts inside the literature documents. In order to decrease this ambiguousness, we have referred to some researches from different viewpoints. Moreover, we tried to confab different texts as a whole and the interpretation of its parts thus to gain good understanding. As a result, we will try to analyze the different security concepts and the need for secure system especially in CMIS system to light an underlying coherence.

---

## Chapter 4 SECURITY SERVICES

---

Security could be the basis of privacy. To enhance privacy and security in CMIS, it needs to address security services. Security services include confidentiality, integrity, authentication, non-repudiation, availability, and anonymity. Security services should be thoroughly addressed in order to provide a better security. The most common security services are as follows:

### 4.1 CONFIDENTIALITY

Confidentiality ensures that information is able to be accessible only to authorized party. All information may not be of equal value. For instance, the most sensitive information such as healthcare and military requires protection against unauthorized destruction, modification or disclosure. Essentially, confidentiality protects the transmitted data from passive attacks [7]. Modification of such information to various adversaries could have destructing consequences.

### 4.2 INTEGRITY

As with confidentiality, integrity is about ensuring the accuracy and completeness of information. It guarantees prevention of unauthorized modification of information such as messages. Only the authorized parties are allowed to modify the information or messages. There are various ways that could compromise information integrity such as human errors when data is entered, errors could occur during the information transmission and system bugs and viruses, etc. However, these threats could be minimize by data backup, using security mechanisms to control information access, preventing invalid input by validating through user interfaces and using error detection and fault tolerant software when transmitting data. Thus, integrity is achieved by preventing unauthorized insertion, modification or destruction of information or messages. The destruction of data is also covered under integrity service. Thus, it addresses both message stream modification and denial of service.

### 4.3 AVAILABILITY

Availability concerns with protecting the system as well as its data to ensure it would be available when required. i.e. the service should be available most of the time excluding downtime related to upgrade or repair or other development activity. Also a variety of attacks can result the unavailability. However, some of these attacks are responsive to automated countermeasures such as authentication and encryption whereas others require some sort of actions to prevent or recover from loss of availability of services of a system. Availability protects a system to ensure its availability despite of various attacks. On other hand, abuse model describes how a malicious actor may attempt to break the system availability by deleting some files or using DoS attack [26].

### 4.4 AUTHENTICATION

Generally, an authentication service is referred to assure that a communication is genuine. Thus, to assure that communicating parties is one that it claims to be to access the system

resources [7]. Without authentication, an attacker could masquerade a system to gain an unauthorized access to the system and hold the information. Moreover, the attacker's attempts could interfere with the operations of the other parties on the system [7].

## **4.5 NON-REPUDIATION**

Non-repudiation ensures that the originators of the messages cannot deny the fact that the message was sent by them. Thus, when a receiver receives a message, s/he can prove that this message was from the claimed sender. Moreover, the sender also can prove that the message was received by the intended receiver. On other hand, non-repudiation is also considered useful for detection and isolation of compromised nodes.

## **4.6 ANONYMITY**

Nowadays everybody wants anonymity. Anonymity is the stage of being unknown or hidden. Violation of anonymity could also result in a breach in privacy.

## **4.7 SUMMARY**

In this chapter, the common security services have been described briefly. Authorization is another security service that could be concerned to a certain application. Confidentiality and Integrity (CI) are the two services that have high importance that computers and network security should cover. Despite these services have to be protected, the attack against these services are possible. Access control is another security service which is important to have control for who should have access to resources and with certain conditions. It gives access to services for authorized party and denying an unauthorized party. However, achieving a good tradeoff among these services is basic challenge to enhance security and privacy in CMIS system.

---

# Chapter 5 VULNERABILITIES AND THREATS RELATED TO MOBILE COMMUNICATION IN CMIS

---

Since CMIS operates using mobile communications as well as stationary. Therefore, we shall discuss various types of attacks on the mobile communication systems like GSM, GPRS and UMTS along with their short description. We think it is necessary to assess these threats, though mobile communication is considered secure than the stationary one. However, due to the importance of sensitive medical data, it is necessary to understand the security of the communication being used. This will help to increase the privacy of users as well as boost trust for the system.

## 5.1 HISTORY OF MOBILE COMMUNICATIONS SYSTEMS

The rapid evolution of mobile communications systems is continuous from the first-generation to the commencement of fourth generation (mobile devices with IP address). The first generation (1G) has been based on analog technology for traffic [28]. The capacity of the 1G network was lower than that of current cellular networks; also the support for mobility in this network was weaker. There were different companies that adopted the 1G like: Nordic Mobile Telephone (NMT), Total Access Communications systems (TACS) and Advanced Mobile Phone Service (AMPS) [28]. However, most of these 1G systems have been already closed with the new advanced telecommunications infrastructures.

The second-generation (2G), Global System for Mobile communications (GSM), Personal Digital Cellular (PDS), Interim Standard (IS) and Code Division Multiple Access (CDMA) have been based on digital technologies for voice-oriented traffic [28]. It is obvious that the difference between the 1G and 2G is analog/digital split. The capacity of the 2G networks is higher than 1G system. The channel's capacity is divided among several users either by code or time division [28].

The rapid growth of wireless communications, the growth of the Internet, and the increasing use of mobile systems and mobile communications increased the need for new generations of mobile systems. The third generation (3G) systems have also been based on digital technologies for mixed voice, data, and multimedia traffic [29]. Thus, rapid progress in the new technologies could satisfy and provide the user needs.

## 5.2 THREATS AGAINST GSM

The Global System for Mobile communication (GSM) provides solutions to some aspects of privacy and security such as subscriber authentication, subscriber identity confidentiality, and confidentiality of voice and data over the system communication. GSM provides security controls. In one hand, the operator of the network wants to ensure that the subscriber requesting the service is valid i.e. authentication (see section 4.4). On the other hand, the subscriber wants to have access to the services without compromising the privacy.

However, the GSM specifications have been designed in secrecy and distributed only on a need-to-know basis to hardware and software vendors and GSM network operators, thus protecting the GSM from being exposed to expert communities and preventing from studying the enclosed authentication and enciphering algorithms. The GSM community

depends on abstruseness, for instance, it could be harder to crack the algorithms if they were not widely available. In this part, we attempt to introduce the GSM security model and we try to investigate the weak points in this model in order to show the possibilities that these points can be attacked by the hackers, malicious network operator or malicious users, a GSM interceptor and phone call eavesdropper [30]. During investigating the different points of attack in the GSM system, we will try to discuss some threats and claims of eavesdrop on a GSM phone call that some of the researchers made.

Biham et al. claimed that his team uncovered a possible means of cracking the GSM mobile phone network encryption code; they claimed that they opened the door to attack and could enable eavesdroppers to listen into phone calls. Biham et al. discovered weaknesses in the encryption scheme used in GSM networks [31]. This attack allows an eavesdropper to hear a conversation. The attack starts while the call is being set up and the receiver's phone still ringing. After this step the call can be overheard. The author further stress that it is possible to impersonate callers or steal calls using a special device in the middle of a call. Consequently, the effect on user privacy could be imagined due to such attack.

The essential mistake made by GSM developers in creating a system increased the gap of the security [31]. This type of cracking does not affect 3G phones, which use different protocols and security mechanisms than GSM and GPRS.

On other hand, [30] has different view point. The GSM phones are not vulnerable and there is no risk to subscribers. Thus, the process and the function design offer strongest level of wireless security. Moreover, there is no risk of over-the-air eavesdropping. The level of encryption used by GSM makes the over-the-air eavesdropping approximately impossible. However, these contradictions lead to born a new data service.

## **5.3 THREATS AGAINST GPRS**

This part of the study discusses the important threat against GPRS. Since, CMIS also uses GPRS, thus, studying threat against GPRS is important.

GPRS makes the connection to the Internet/Intranet always available to the user. Some of the sensitive information and services might require a high level of privacy. This section briefly covers the threats related to GPRS and the measures to avoid attack

### **5.3.1 GPRS OVERVIEW**

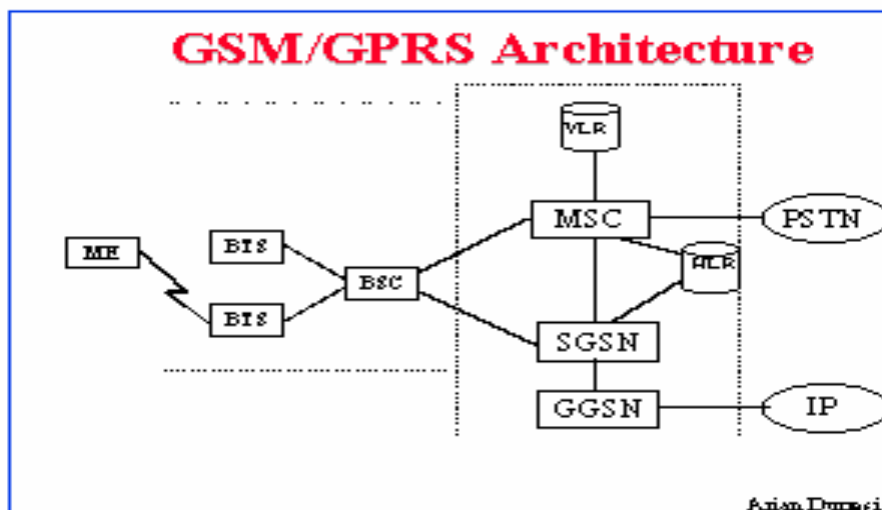
GPRS (General Packet Radio Service) is a method to enhance the 2G phones to enable them to send and receive data more rapidly [32]. It is the second phase of the GSM service; hence most of the security threats which are exist in the GSM has been inherited in the GPRS.

The European Telecommunication Standard Institute (ETSI) defines the GPRS as the standard for providing packet data services in GSM networks [32]. The GPRS has come and designed to move 2G networks closer to the performance of 3G networks. The benefit from designing 3G is to make it capable to transfer large amount of data at high speed.

The GPRS not only encourages the threats that exist in the GSM, but also it encourages new challenges. Since, the GPRS is connected to the Internet and it employs IP technology [34]. Moreover, some of these threats are during the data transmission at the air interface and operators handling of data that are transmitted or stored in their network.

### **5.3.2 GPRS ARCHITECTURE**

Figure 5.1 illustrate the GPRS architecture. This part describes briefly the main elements in the GPRS system. It includes components that already known in the GSM system.



17

**Figure 5.1: GSM/GPRS Architecture [28].**

- ME – Mobile Equipment  
It is a device that is used to connect to the GPRS network or avail GPRS service.
- MS – Mobile Station  
Mobile station is the combination of a Mobile Equipment (ME) and SIM-card.
- SIM – Subscriber Identity Module  
Contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication
- BTS – Base Transceiver Station  
Handles the radio-link protocols with the Mobile Station
- BSC – Base Station Controller  
Handles radio-channel setup, frequency hopping, and handover
- HLR – Home Location Register  
All the administrative information of each subscriber, and the current location of the mobile
- VLR – Visitor Location Register  
Contains selected information for call control and services for mobiles located in its geographic area
- MSC – Mobile Services Switching Center  
Normal switching node of the PSTN (Public Switched Telephone Network), plus functionality for registration, authentication, location updating, handover, and call routing to roaming subscriber
- EIR – Equipment Identity Register  
It contains the mobile equipment identity information which could help in block calls from stolen, unauthorized access, or defective mobile stations.
- AuC – Authentication Center  
It Stores a copy of the secret key of each subscriber's SIM card for using in authentication and encryption.
- SGSN – Serving GPRS Support Node  
The main function of the SGSN is to provide data support services to the MS, ciphering and authentication, mobility management, and session management. It also provides

forwarding incoming and outgoing IP packets addressed to/from a MS which is attached within the SGSN area service. The SGSN is logically connected to a Gateway GPRS Support Node (GGSN) [28].

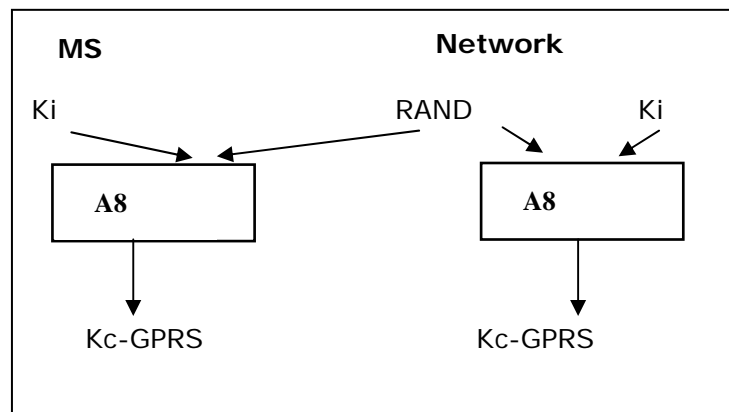
- GGSN – Gateway GPRS Support Node  
It provides the data gateway to external networks such as the public Internet. It provides GPRS session management with communication setup towards external network.

### 5.3.3 SECURITY FUNCTIONS IN GPRS

In this section, we will discuss about security mechanisms of GPRS. The security functions in GPRS are similar to the existing GSM security functions [33], [34]. The Denial-of-Service attack is one of the most common and widely used where legitimate users are denied access to services [7]. This attack may have a specific target. For example, the disruption of an entire network either by disabling the network or by overloading or victimizing a single entity target such as a specific server of a popular services.

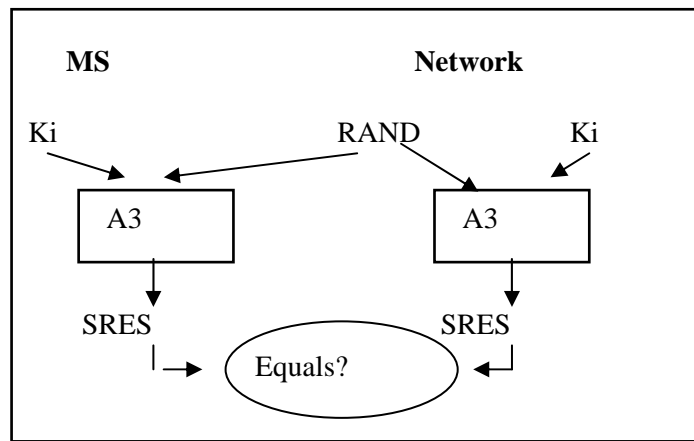
Mobile Station (MS) is formed from SIM-card and Mobile Equipment (ME). The SIM-card contains the identity of the subscriber. When the SIM-card been inserted into a ME, it directly authenticates an MS to be ready to get access to the network. The SIM-card contains the IMSI (International Mobile Subscriber Identity),  $K_i$ , the cipher key generating algorithm (A8), the authentication algorithm (A3), and the GPRS encryption algorithm (A5).

Figure 5.2 illustrate the ciphering key generating algorithm (A8). This algorithm is using the combination of the key ( $K_i$ ) and the 128-bit random number (RAND) to generate the 64-bit ciphering key ( $K_c$ ), which is GPRS-key. This is used with the encryption algorithm (A5) to cipher the data stream between the Mobile Station (MS) and the GPRS network.



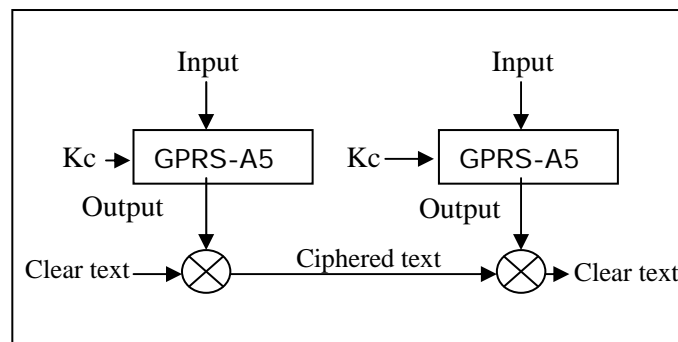
**Figure 5.2: Ciphering key ( $K_c$ ) generating algorithm**

Figure 5.3 illustrates the Authentication algorithm (A3). This algorithm uses the random number (RAND) with the authentication key ( $K_i$ ) to produce a signed response (SRES). This signed response is used by the network to authenticate the mobile station (MS) and to make use of the secret authentication key ( $K_i$ ).



**Figure 5.3: Authentication Algorithm (A3).**

The GPRS encryption algorithm (GPRS-A5) has been based on the Mobile Equipment (ME) [35]. Figure 5.4 illustrates the use of the GPRS-A5 algorithm. This algorithm is used in the GPRS ciphering process over the-air-transmissions between the mobile station (MS) and the GPRS network during transferring data.



**Figure 5.4: The GPRS Encryption Algorithm**

### 5.3.4 GPRS SECURITY PROCESS

The authentication request is being sent to the network from the mobile station (MS). The request arrives to the Serving GPRS Support Node (SGSN) and then sends to the Home Location Register (HLR) and to Authentication Center (AuC). And then the triplets will be generated. These triplets are the random number (RAND), the signed response (SRES), and the encryption key (GPRS-Kc). The RAND and the SRES are used to authenticate the smart card in the mobile station as a response. The data between the MS and SGSN is encrypted using the key Kc. Then, GPRS-Kc and SRES are calculated from the RAND using the authentication algorithm A3/8 [35]. The triplets RAND, SRES, and GPRS-Kc are sent to the SGSN which sends RAND to the MS. The same authentication algorithm A3/8 used by the MS and SIM card (Smart Card) is used to generate SRES and GPRS-Kc. This SRES will be sent back to the SGSN thus to compare this SRES with the SRES in the authentication triplets. However, if the two SRES's are identical, then the MS must have the correct authentication algorithm A3/8 and Ki. Therefore, this is judge to be authentic.

If both of the MS and the SGSN have the same GPRS-Kc, then both of them can use Kc to encipher the session between the MS and SGSN.

The GPRS has following measures which could be vital for the privacy needed in the CMIS system thus it uses GPRS network.

- Identity Confidentiality (IC)

The main goal of (IC) is to provide privacy to the subscriber. It is done by avoiding an intruder to identify the subscriber on the radio path. However, it is difficult to identify the subscriber from his signal over the radio and connections to the SGSN [36].

- Identity Authentication (IA)

The authentication process is described in [37]. The RAND and SRES have been come from the HLR/AuC and stored within the SGSN. So, the authentication is performed within the SGSN. The SGSN and RAND could be compared to decide if the two SRES's are identical to make sure that the smart card (SIM) has the correct authentication algorithm A3/8 and the correct Ki.

- User and Signaling data Confidentiality

The user and signaling data such as IMEI and IMSI need to be protected. As in GSM, the signaling key (GPRS-Kc) and the user data are derived from the use of the authentication algorithm A3/8. All of the user information such as short messages which is transferred over a signaling channel should be protected. Moreover, the user information on the physical connections over the radio channel should be protected in order to achieve confidentiality.

### 5.3.5 SECURITY THREATS TO GPRS

The main purpose of any attack is either to harm the system or steal information. GPRS, like any other system, could be used for same purpose i.e., to harm or steal the information. Actually, sometimes there could be different motivation of an attack. An attack on such a system could be a dream of the sophisticated white-collar criminal [38]. After the information has been stolen, the intruders have the opportunity to sell this information to gain money or they are lured by sheer fame.

Here, we will be discussing about security threats on Gi interface. Since, CMIS is a web-based application, therefore, we think it is relevant to discuss about Gi interface as Gi interface connects with the Internet, corporate networks and other service providers network [36]. As a result of using Gi interface, CMIS is also exposed to all sorts of threats that a normal application poses due to Internet. We shall discuss different attacks related to security services.

#### 5.3.5.1 ATTACK ON AVAILABILITY

Denial of Service (DoS) is the biggest threat for availability.

**Gi bandwidth saturation:** A link from PDN (Packet Data Network) to mobile operator might be flooded resulting a DoS attack.

**MS flooding:** Targeting a particular MS by flooding traffic could also result a DoS attack to the respective user.

#### 5.3.5.2 CONFIDENTIALITY

If application layer or IP security is not used than an intruder can see the data passing from MS to public network.

#### 5.3.5.3 INTEGRITY

As described above, if no security is maintained than a possible intruder can change the data.

#### 5.3.5.4 AUTHENTICATION AND AUTHORIZATION

One MS may access the network of another user if layer 2 or layer 3 tunnels are not used at the GGSN (Gateway GPRS Support Node). This happens because the MS or hosts beyond it can create packets of any address whatever the IP address may be assigned to MS. Hence, source address of network can not be relied for authentication and authorization [36].

## 5.3.6 SOLUTIONS OF THE ATTACK

### 5.3.6.1 USING LOGICAL TUNNEL FROM GGSN TO NETWORK:

GGSN should be able to separate corporate network in layer 2 or layer 3 tunnels. Thereby, the prohibiting corporate routing from Internet to network or between networks.

### 5.3.6.2 LIMITING TRAFFIC RATE:

There could be separate physical interface for corporate traffic and Internet traffic or corporate traffic should be prioritized.

### 5.3.6.3 INSPECTING STATEFUL PACKETS:

Enforcing a security policy allowing only MS to initiates communication to corporate network. Stateful packet filtering should be used to make sure traffic initiated by network is always hidden to MS.

### 5.3.6.4 IMPLEMENTING INGRESS OR EGRESS PACKET FILTERING:

To prevent the possible spoofed MS thereby eliminating chances of DoS, DDoS attack.

**Ingress Filtering:** Ingress filtering allows controlling the incoming packets. Following simple rules could be implemented.

- i. Inbound traffic should not bear a source IP address that is not assigned to host network.
- ii. Inbound traffic should not bear a private (non-routable) IP address.

**Egress Filtering:** Egress filtering allows controlling the outgoing packet there by preventing being a zombie host. Following simple rule could be implemented.

- i. Outbound traffic should not bear a source IP address that is not assigned to host network.
- ii. Outbound traffic should not bear a private (non-routable) IP address.

## 5.4 OTHER THREATS

There are also other threats apart from described above. These threats arise due to the fact that data are transmitted over the air. Thus, the attack could be also on the data at the air interface or the stored data in the network.

There could be another threat especially between the different GPRS operators; the trusted people in different networks could attempt to misuse the position and they could do different actions like:

- Eavesdropping: The intruder could eavesdrop the subscriber's traffic or s/he could eavesdrop signal and control.
- Masquerading: It takes place on when a party pretends to be a different entity [7]. For example, user A may send a message to user C pretending to be user B.
- Traffic Analysis: when user a sends a message to user C, user B observes pattern of the message that sent from A to C. The common technique for masking the contents of the message is an encryption.

Moreover, Cryptography can increase security in user authentication techniques [40]. Cryptography is the basis for several advanced authentication methods.

However, many attacks that degrade the network services (viruses, DoS attack) might have serious consequences for medical practice [38].

## **5.5 SUMMARY**

GPRS provides a better bandwidth for mobile phones. Due to its higher bandwidth and Internet support, it is attracting many Internet-based applications such as CMIS to be implemented in mobile platform. However, it is necessary to provide data security and availability to be successful technology. In this chapter, we discussed different types of threat arising to security services as well as ways to address them. Internet, being a dynamic field, is quite volatile especially in case of security. Hence, it is necessary to be ahead or within the attacker's knowledge-boundary to take advance, preemptive or prompt action against any possible threats. It is quite necessary when we talk about CMIS because it consist very important medical data.

---

# Chapter 6 WEB APPLICATION SECURITY

---

In this chapter we will describe about the different aspects of security threats in a web application and measures to address them. CMIS being a web application, posses all the threats a normal web application do.

Web applications are publicly available to many users may be in the form of Intranet or Internet. Internet-exposed application is visible to the whole world and posses even bigger threat for the privacy, anonymity and secrecy of the legitimate users.

CMIS, being a web application, must fulfill the following security aspects on behalf of its client:

1. Security of client node and personal data.
2. Securing information while being transmitted.
3. Security of the server and data stored in it.

Further, as we discussed in chapter 4, it should able to address following security services.

- Confidentiality
- Integrity
- Non-repudiation
- Authentication
- Authorization
- Availability
- Privacy

Now, we will discuss some security measures a web-based application should adopt, most common threats that CMIS could face and its countermeasure as well.

## 6.1 ENCRYPTION, DIGITAL SIGNATURE, AND CERTIFICATES

### 6.1.1 ENCRYPTION

It is a way of transferring plain text into unreadable (cipher) using some mathematical functions. It is the best way to protect message being viewed by other party. However, without the use of strong encryption algorithm or key, it is likely to protect information. Also, strong encryption with larger key size can result in additional burden on overhead of the communication and affect the performance. Hence, CMIS can use stronger encryption algorithm for its user authentication. However, to boost performance, a light-weight authentication may also be used [41]. A tradeoff between security and performance has to be done.

### 6.1.2 DIGITAL SIGNATURE:

They are used for message authentication based on public key [11]. They are also basis to guarantee integrity, non-repudiation, and authenticating identities [42]. A sender at first calculates hash value for the message and signs the hashed message with his private key. The receiver than decrypts the message with sender public key thus obtaining hashed value. Now the receiver calculates the hash value of obtained message. If both are same, receiver will be

sure the message was indeed send by the sender and the receiver could not say it was not signed by him as he is the only who could have signed the message. This ensures non-repudiation and authentication as well.

### **6.1.3 CERTIFICATES**

In asymmetric cryptography, one party might not be assured regarding other party public key. Chances are high that someone might publish a key impersonating other party. Therefore, the need of a trusted Certificate Authority (CA) is necessary. Then, each party verifies their public key through the CA and in return the CA will sign the party's public key with its digital signature. VeriSign is such an example.

## **6.2 SECURE CLIENT-SERVER INTERACTION**

### **6.2.1 USER AUTHENTICATION**

It concerns with the verification of user's identity. The most common and widely used authentication mechanism is the user login/password system. Generally, SSL connections are used to authenticate a user.

### **6.2.2 AUTHORIZATION**

It concerns with what an authenticated user is allowed to do. It is like fixing role and responsibility of a user. There are various access control mechanisms for this purpose. We can take example of windows operating system which has privilege like administrator, guest, power user, etc. This is necessary because all the users do not posses same privilege and hence, it will help against unauthorized access of the system resource.

### **6.2.3 END-TO-END SECURITY**

For a web service, end-to-end security is of crucial importance. Web service helps to realize complex business process. For example, web services interact through the exchange of SOAP (Simple Object Access Protocol).

Generally more than two communicating entities might be involved in online transaction. Like, a patient is interacting with a doctor; however, the patient might need to communicate with a laboratory to obtain the results of tests. Here, the communication between patient and doctor can be secured by previously introduced transport level security (SSL, TLS (Transport Layer Security)). Now an end-to-end security is needed between the patient and the laboratory. This can be referred as a message level security, which means the security information is contained within the message. The will help a part of the message to be transported without intermediaries parties viewing or modifying it.

## **6.3 CLIENT SECURITY ISSUES**

### **6.3.1 PRESERVING PRIVACY**

Preserving client issue is always a challenging and most issue. A SSL-secured authentication and communication allows users to transfer their personal information without being compromising. Similarly, the service provider should handle the users' data very carefully and should be able to keep potential attackers at bay by implementing different sort of security mechanisms like efficient access-control system, reliable authentication, well-configured and strong firewall and other related issues.

### **6.3.2 MOBILE CODE SECURITY**

To enhance the usability and performance of a web application, a web application might use mobile codes written in JavaScript (most common), Java applets, ActiveX, etc. The real problem with the mobile code is they are executed in the host computer. Several threats exist such as eavesdropping being the common. These threats could be addressed by using sandbox (a way to execute Java applets) or signing the code. This is very vital in the system like CMIS due to the vital medical data.

### **6.3.3 PHISHING AND WEB SPOOFING**

Phishing is an attempt to steal user private information such as user name and password. It is a trick laid down by an attacker to fool a user to sign up in their page instead of legitimate one. An intruder might be interested in getting a VIP patient's (say a member of parliament or a celebrity) information through CMIS using a phishing technique. Hence, it is necessary for CMIS to address it by implementing certain techniques, like one adopted by Yahoo! [43].

### **6.3.4 DESKTOP SECURITY**

It is evident many commercial application carry some sort of adware, whereas some malicious-intention but useful-looking application might also carry spyware or trojan within them. Hence, it is necessary for the CMIS to make its client to trust it.

## **6.4 SERVER-SIDE SECURITY**

### **6.4.1 CROSS SITE SCRIPTING (XSS)**

It is a way of inserting a malicious (illegitimate) HTML code to acquire information in dynamically generated web pages. The malicious HTML code may be embedded inside form fields (changing hidden form value) or cookies or URL parameters. This problem happens when parameters are not checked before passing. According to CERT advisory [44] the attack could be motivated for obtaining confidential information (credit card number, changing the behavior of forms and exposing SSL-encrypted connections). The way to fix the problem is to encode HTML meta-characters into the corresponding numerical representation like `#&<n>` syntax, where 'n' is the numerical representation of enclosed character.

### **6.4.2 SQL INJECTION**

Generally, web application use data input by user to construct SQL queries. A disgruntled or malicious use might take advantage of vulnerability by executing arbitrary SQL query against the database [45].

*Prevention of SQL injection:*

*Parameter verification:* The syntax of the parameters before processing should be verified. Certain characters like “ ' ” or “ ; ” or “ = ” should be checked and avoided execution of such query if found.

*Prepared Statement:* Parameters are sent to the database separately in prepared statements. They are generally considered immune to SQL injection attack. It is generally considered immune to SQL injection attack. The database uses bind variable values and does not interpret the contents of the variable in any way.

### **6.4.3 VULNERABILITY OF SERVER-SIDE SCRIPTING LANGUAGE**

Vulnerabilities in the server-side scripting language could always jeopardize all the security measures. Hence, along with the other security measure, it is necessary to look for any vulnerability either through rigorous penetration testing, through vendor security bulletin or independent security bulletin. For example, there was a known issue of XSS by the use of .NET framework 2.0. Microsoft has classified this vulnerability as “could allow information disclosure” [46]. However, a patch has already been issued to resolve this vulnerability. There were other known security issues which could be found in Microsoft security bulletin along with their patches.

### **6.4.4 SERVICE AVAILABILITY**

#### **6.4.4.1 Denial of service (DoS) attack**

This is one of the most widely used methods of attack. It aims to block the legitimate user from accessing resources from a system or web application. This type of attack is aimed to starve a system’s resources like CPU, disk space or memory.

#### **6.4.4.2 Host security**

We discussed about different type of security attacks and to extent their counter measures as well. However, any sort of attack is possible due to discovery of unknown vulnerability in operating system or third party software. Thus, it is necessary to keep the system always up-to-date. Critical security patches should never be missed. Also, the security is concerned with the use of well-configured firewall and inspecting successptible ports like 443, 137, etc.

## **6.5 SUMMARY**

Considering the fact that CMIS operates in insecure environment i.e., Internet [8], a vigilant activity is always required to protect it. New sort of attacks and new vulnerabilities are common and growing. Hence, a good effort must be given to ensure the security of CMIS and thereby privacy as well.

---

# **Chapter 7 MOBILE PEER-TO-PEER (MP2P) ON CMIS AS A SERVICE WITH THE PERSPECTIVE OF PRIVACY**

---

CMIS is a multi-role system. It could tap the opportunity of a dynamic distributed networking system called P2P (Peer-to-Peer). Non-core functionalities like instant messaging could be migrated to use P2P architecture as a service to relieve the burden of CMIS server. A seamless integration between the CMIS system and the proposed MP2P system is expected. We are particularly interested about the use of MP2P (mobile peer-to-peer) system with the perspective of privacy. Since privacy, anonymity and security has been our core issues in thesis, we again are giving emphasis on privacy issue. There are lots of privacy-related issues but we are going to address only few of them due to the constraint that this subject matter not being the core topic of our thesis.

## **7.1 INTRODUCTION**

Massive popularity, mobility and increasing computing power of mobile devices has opened a door for P2P (peer-to-peer) application in such devices under a new name MP2P (Mobile Peer-to-Peer) system. P2P systems have revolutionized the way we share information unlike the traditional client-server model. The term P2P generally refers to systems or applications that share resources in a distributed and decentralized way. Unlike traditional client-server model, P2P network relies on the bandwidth and computing power of the peers (hereafter we shall interchangeably use 'peers' or 'users') to exchange information rather than computing power and bandwidth of few servers. Though its popularity due to sharing of music, movies, and other stuffs has legal issues, however, it provides an excellent way to distribute personal as well as commercial contents. It offers the ability to share huge amount of data through the network by dividing computing power, storage space, bandwidth, and total cost of ownership. It can either be used to transfer files or can be used as a service like Skype. Recent advancement in mobile technologies and growing demand of mobility has emphasized on development of mobile ad-hoc networks (MANET). Mobile ad-hoc networks provide opportunity for mobile P2P network applications—such as mobile patient monitoring, distributed command and control system, etc. Mobile devices like mobile phones, PDA has now become an integral part of our life. Due to their decreasing size, growing computing power and storage, increase in networking capabilities and better services (UMTS) by the service provider has made them even more powerful. The very popular P2P system could take advantage of this mobility, thus creating a mobile P2P (MP2P) system. One such example is Symella (Symbian, Gnutella) [47], which is a file sharing client for Nokia S60 (based on Symbian) 2nd & 3rd generation Smartphones. Symella is based on Gnutella.

## **7.2 MOTIVATION**

We have decided to discuss about MP2P system rather than P2P system with the context of CMIS. We have decided to do so as P2P system are now quite general and is used many sector, however, MP2P sector is quite new, and slowly gaining momentum and could be more useful for patients due to its mobility. We believe a bright future for MP2P system due

to the growing demand of mobility. Hence, system like CMIS can leverage the use MP2P-based application as it is not guaranteed that patients will be always at home.

## 7.3 PARADIGM OF MP2P

Mobile Peer-To-Peer (MP2P) systems are slowly driving a major paradigm shift in the era of distributed computing. Major industrial players believe “P2P react society better than other types of computer architecture [48]”. In short, a P2P system can be characterized by the following properties [49]:

- No central database
- No central coordination
- Peers without global view of the system
- Autonomous peers
- Unreliable communication

The strength of MP2P lies in the capability of collecting large number of users (peers) located in various geographical areas. It also provides seamless integration of new users as they do not need to be validated or authenticated against a centralized server. This vary nature of MP2P facilitates scalability.

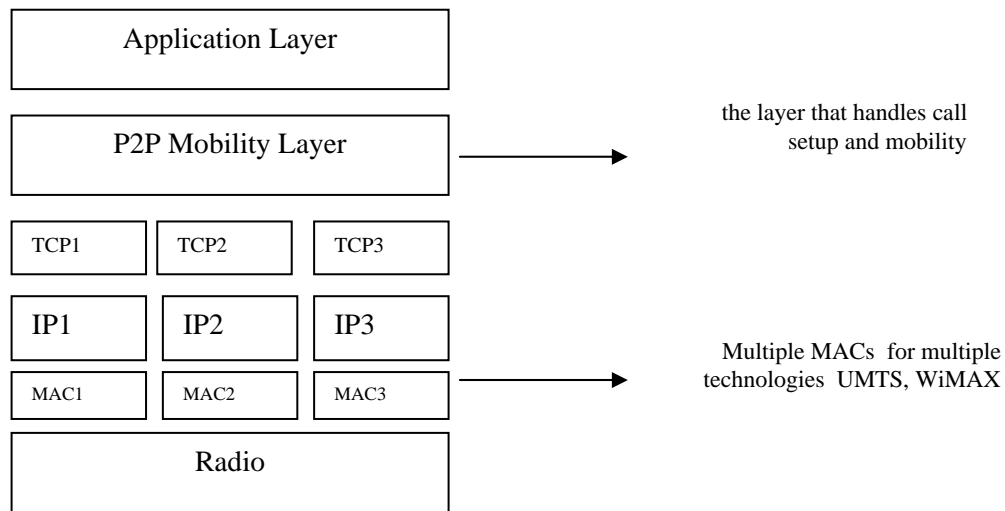
MP2P can be applicable in two type of environment:

1. *Distributively-owned peers:*  
General, Normal world P2P scenario. Here, the users operate under fully decentralized system without the knowledge of other peers.
2. *Peers owned by particular organization:*  
Peers are controlled in some way regarding accountability of their actions. It is an advantage to an organization if it wants to facilitate seamless integration of other nodes in their system. This approach is better suited for CMIS. Hybrid-P2P architecture with secure peer authentication could be the best possible solution.

A MP2P system may be classified according to the type of communication they use.

1. *Ad-hoc communication:*  
A MP2P application may operate using short-range communication systems like Bluetooth, ZigBee, and WLAN (Wireless Local Area Network).
2. *GSM/UMTS communication:*  
Like orthodox P2P, MP2P application uses Internet to communicate between peers. Peers will use mobile phones with Internet access to communicate with other peers.

CMIS could use both type. However, the main problem using both communication-ready (say UMTS and WLAN) is in location management and handover [50]. Eren et al. describes about handover using different communication system such as UMTS to WLAN [50]. During handover mobile clients maintain more than one IP address (figure 7.1). For the location management, a moving client should update its IP address to a common lookup server (having fixed IP address) through which another mobile client can contact it.



**Figure 7.1: Mobile Client's Protocol Stack [50].**

## 7.5 PRIVACY PROTECTION MECHANISM

Privacy itself can have different meaning depending on the context. If an MP2P application is used for a location-based service, then the compromise of the user location could be privacy breach. Similarly, there could be trust-based mutual cooperation between requester and supplier; any violation could lead to privacy breach. Here, we have classified privacy as per the context or scenario.

### 7.5.1 LOCATION-BASED PRIVACY MECHANISM

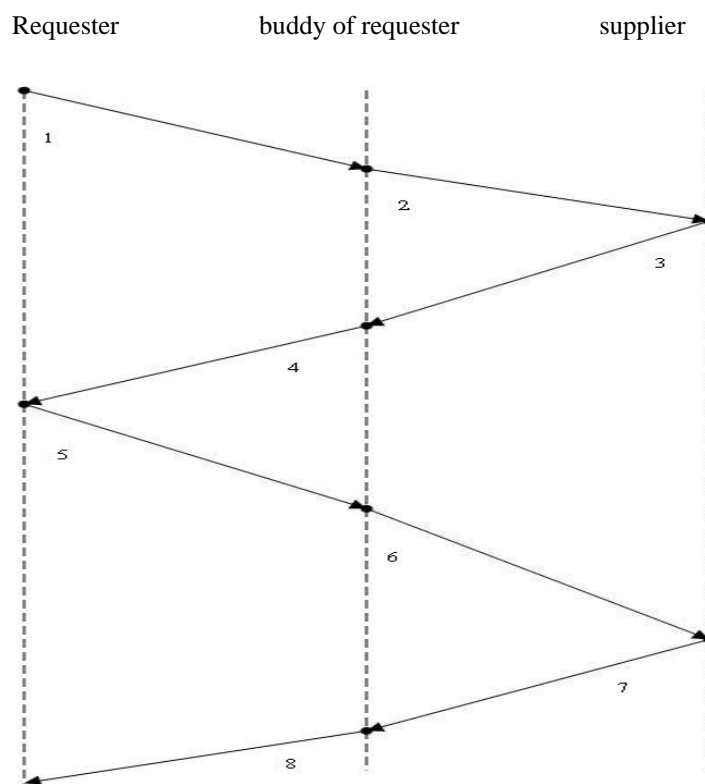
For certain location-base applications, like an application which guides tourist about a nearby tourist spot or restaurant or ATM. Generally, the tourist has to report his/her location to a centralize server to get the direction of the desired location. With the use of untrusted servers, it might poses privacy threat to a user. Someone might be interested in tracking a user's habit or location of visit, etc. In fact GPS device has already been misused for stalking girl-friend [53].

This scenarios arises due to the use of centralized database server, however, using MP2P system could address such problem. A mobile client could work together with other clients to conceal their exact location without any help from centralized server or any trusted third party [54]. Further, [54] has proposed P2P spatial cloaking algorithm to strengthen the privacy. In the algorithm, users at first search for peers using single or multiple hops. After that mobile user performs spatial cloaking by forming a group of  $k-1$  (many similar) peers and tries to hide the exact location with a spatial location. By this, they could achieve  $K$ -anonymity [55]. The algorithm also addresses the problem of locating a users using mobile positioning technique. Here any client is chosen randomly and acts as an agent on behalf of the actual querying client. More information about this P2P spatial cloaking algorithm can be found in [54].

### 7.5.2 CONTENT-BASED PRIVACY SCHEME

As we have mentioned previously, privacy is also dependent upon the type of context. On certain context like multimedia streaming or file sharing, when users exchange data, they also send certain information. A user generally does not want a third-party to observe these data as they could breach ones privacy. Probably, most of us do not want others to know if we are exchanging certain things (say adult material or a patient suffering from AIDS only wants his doctor to know about this fact), however, disclosure of certain overheads like requester id, data handle, content type could reveal the things being transferred.

A peer, instead of requesting herself, can request another peer (buddy, hereafter one who serves as a proxy on behalf of requester or supplier) for the desired data. When the desired data and supplier is located, the buddy will work as a proxy to serve the data. However, other peers might have knowledge that someone is requesting data but not the exact peer. The scenario could be described from the figure [51] below.



**Figure7.2: Preserving privacy using buddy [54].**

Through this way the privacy of the requester is preserved. However, the buddy of requester knows the information of requester, hence; the privacy relies upon the trustworthiness and reliability of the buddy.

Lu et al. has tried to address these issues using various methods listed here [51].

- *Protecting data handle:* Data handle is not revealed at the beginning. Only a partial hashed value of handle is revealed which is send to a buddy (step 1 and 2 in figure 7.2). The peer sends back a candidate set with his/her certificate of public key to requester. There might be some match. In this case a Bloom filter [56] is sent back to buddy and finally to requester (step 3 and 4 in figure 6.1). The requester than can eliminate peers having incomplete data. Then requester encrypts the request with supplier key and put a

request via buddy (step 5, 6 and step 7, 8 shows the data received). Here, privacy is improved as malicious nodes need to compromise buddy and both Bloom filter and hash function.

- *Hiding the data content:* We need to protect the privacy of the data content as well because a buddy can still compromise requester privacy if buddy can see the data content. The best way is to encrypt the data handle and data content for improvement in privacy and eavesdropping. Here, requester encrypts data using supplier public key. In order to prevent man-in-the-middle-attack by buddy, s/he is required to sign the packet as non-repudiation evidence. Now, a possible intruder needs to compromise buddy, Bloom filter, hash function, and encryption key.
- *Both entity privacy:* Previously discussed measures were to protect requester privacy but what about supplier privacy? A buddy (requester's) can collude with supplier to reveal the interest of requester. This will also violates supplier privacy due to the fact it will reveal the content of the data. As a measure, supplier can also use his own buddy and it functions in similar way as we described in previous section. Supplier's buddy cannot violate privacy because the request will be protected with Bloom filter, hash function and end-to-end encryption.

## **7.6 CONCLUSION**

In this section, we talked about privacy issue focusing mainly two situations, location-based and content-based. Non-core functions such as instant messaging will be incorporated to MP2P seamlessly. We gave more emphasis to privacy because of the nature of CMIS. Medical-related data are always vital and a patient has full right for its privacy. Also, privacy may be treated or defined differently in different situation and depending upon the user. In some scenario, a user might not be concerned whether his location is disclosed; however, he might be more concerned about keeping the content of the data private. Further, the issue of privacy invasion might arise due to any vulnerability in the technology used.

---

# Chapter 8 FUTURE WORK AND CONCLUSION

---

## 8.1 FUTURE WORK

CMIS for health care holds tremendous potential for future. Like any system, security and privacy are vital for the success of a system. We have tried to focus on most common vulnerabilities and threat on web applications. CMIS, our model application, being a web application inherits all the threat poses by any web application. Our theoretical-based work could be a basis to conduct a real/live test in a system similar to CMIS. Further, a similar test could be carried out for the threats possessed by using GPRS communication. Looking at the nature and trend of attack, it is becoming more complex and sophisticated, so the future work could also evolve around these new types of attacks which do not rely on application vulnerability but skills of an attacker to penetrate a system. We have also discussed a prospect of using MP2P system. Hence, issues related to privacy, anonymity, and security could be a good future study. Moreover, CMIS can tap the advantage of new generation mobile communication system i.e. 4G which is suppose to provide real IP and better bandwidth with many other advantages. In this case, it will be interesting to study about its security, privacy and anonymity.

## 8.2 CONCLUSION

Security, privacy and anonymity are vital for the success of any application, especially, for the application like CMIS. In this thesis, we have overviewed the challenges and solution to some of the threats arising due to use of mobile communication (GPRS) and wired communication (CMIS being a web application). In this thesis, we have discussed our first research question “*What are the potential threats to CMIS, arising with the use of the mobile technology?*” in chapter 5. We found that privacy-and-anonymity-based issues like identity confidentiality, identity authentication, and user-and-signal data confidentiality are well addressed in GPRS. Since GPRS inherits some of the threats of GSM, in chapter 2 we have discussed these attacks against A3/8, A5 and A8 algorithms. However, we found that these attacks are very difficult to materialize. Regarding another research question, “*What are the possible threats for the security and privacy in CMIS as a web application?*”, we have discussed in chapter 6. We came to conclude that XSS, SQL injection, and DoS being the bigger and common threats, as with the other web application. The most common solution is always safe coding by identifying vulnerabilities, training users about common security mistakes, input filtering, checking parameters before passing, and using prepared statement; however, DoS attack is still difficult to address. The last research question “*Is MP2P suitable technology for CMIS with the perspective of privacy?*” is discussed in chapter 7. MP2P system seems to be feasible with the perspective of privacy and security but by adopting some security and privacy measures. Privacy and security could be preserved using buddy (proxy), K-anonymity, P2P spatial cloaking algorithm, and encryption is always essential. We also found various other privacy, anonymity and security mechanism proposed by different authors during our literature survey. We do admit we have certain shortcomings in our thesis and have described part of the shortcoming in the section as a part of future work.

# REFERENCES

- [1] D.A. Perendina and A. Allen, "Telemedicine technology and clinical applications", *JAMA*, Vol. 273, No. 6, 1995, pp. 483-488, available at: <http://www.hoise.com/vmw/99/articles/vmw/RI-VM-07-99-1.html>.
- [2] N.M. Fisk, S. Bower, W. Sepulveda, "Fetal telemedicine: Interactive transfer of real time ultrasound and video via ISDN for remote consultation", *J. Telemedicine and Telecare*, Vol. 1, No. 1, pp. 38-44, 1995.
- [3] R. Istepanian, "Integrated mobile telemedical systems: current status and future prospects", *IEEE Trans. Inform. Technol. Biomed*, Vol 3, No. 2, JUNE 1999.
- [4] IMIS: [www.IMISCare.org](http://www.IMISCare.org), (May 2007).
- [5] [http://www.diabetes.org.uk/Research/Publications/Research\\_Strategy/](http://www.diabetes.org.uk/Research/Publications/Research_Strategy/) (January 2007).
- [6] B., Wei, "Agent-based Interface Approach with Activity Theory: Human-Computer interaction in diabetic health care system", <http://www.diva-portal.org/vxu/abstract.xsql?dbid=915>
- [7] W. Stallings: *Network Security Essentials*, Second Edition, Pearson Education, Inc., ISBN 0-13-20271-5, 2003
- [8] L. Chaung, B. Nixon., E. Yu., and J. Mylopoulos., *Non-Functional Requirements in Software Engineering*, Kluwer International Series in Software Engineering, ISBN: 0792386663, London, 1999.
- [9] R. Pandy: *Mobile and Personal Communication Services and Systems*, Series Edition, John B. Anderson., IEEE, Inc. ISBN 0-7803-4708-0, 2002.
- [10] M. Kis., "Information Security Antipatterns in Software Requirements Engineering", 9<sup>th</sup> *Conference of Pattern Languages of Programs (PloP)*, Member IEEE, 2002, PP. 1-7.
- [11] B. Schneier: *Applied Cryptography*, Second Edition, John Wiley & Sons, Inc. ISBN: 0-471-11709-9, 1996.
- [12] E. Kyriacou, S. Pavlopoulos, A. Berler, M. Neophytou, A. Bourka, A. Georgoulas, A. Anagnostaki, D. Karayiannis, C. Schizas, C. Pattichis, A. Andreou, D. Koutsouris, "Multi-purpose HealthCare Telemedicine Systems with mobile communication link support", *BioMedical Engineering OnLine*, 2003, doi:10.1186/1475-925X-2-7, Available At : <http://www.biomedical-engineering-online.com/content/2/1/7>
- [13] Gnutella, <http://www.gnutella.com/>
- [14] Anon., CrackA5: <http://jya.com/crack-a5.htm>
- [15] Olivier B., Nora D., Laurent G., Pierre G., Helena H., David N., Stephane S., Claire W., "Mobile Terminal Security", *Cryptology ePrint Archive*, Report 2004:158, Available at : <http://eprint.iacr.org/>
- [16] [http://en.wikipedia.org/wiki/Brute\\_force\\_attack](http://en.wikipedia.org/wiki/Brute_force_attack)
- [17] Bitpipe, Available at : <http://www.bitpipe.com/tlist/Security-Tokens.html>. Bitpipe, Inc. 1998-2007..
- [18] Cooper., H., *Synthesizing Research: A Guide for Literature Reviews*. Thousand Oaks, California: Sage Publications. (call number H62 C5859), 1998.
- [19] Ayna, Advanced Search, <http://www.ayna.com/index.en.html>, last check: March07, 2007.
- [20] W. Trochim, *Research Methods Knowledge Base*, Atomic Dog Publishing Inc. ISBN: 1-931442-48-7, 2006, available at <http://socialresearchmethods.net/kb/introval.htm>.
- [21] J. Creswell et al., "Determining validity in qualitative inquiry", *Theory into Practice*, 39(3), 2000, pp. 124-131.
- [22] G. Winter, "A comparative discussion of the notion of 'validity' in qualitative and quantitative research", *The Qualitative Report*, Vol. 4, (3&4). 2000, available at: <http://www.nova.edu/ssss/QR/QR4-3/winter.html>, last check: March 01, 2007.

- [23] N. Golafshani, "Understanding Reliability and Validity in Qualitative Research ", the Qualitative Report, Vol. 8, University of Toronto, 2003, available at: <http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf> , last check: March 03, 2006.
- [24] J. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Method Approaches*, Sage Pubns, 2nd edition, 2003, ISBN-10: 0-7619-2442-6.
- [25] <http://citeseer.ist.psu.edu/>.
- [26] J. McDermott & C. Fox, "Using abuse case models for security requirements analysis", *Computer Security Applications Conference, IEEE*, 1999.
- [27] H. Lawrence, L. Richard, K. Roman, *3G Wireless Demystified*, McGraw-Hill. ISBN: 0-07-136301-7, 2002.
- [28] H. Gunnar, S. Holger, *GPRS: gateway to third generation mobile networks*, series, Artech House mobile communication series, ISBN: 1-58053-159-8, 2003.
- [29] B. Walke, *Mobile Radio Networks*, Wiley, 2nd Edition, ISBN : 978-0-471-49902-2, 1999.
- [30] Anon., GSM Alliance Clarifies False & Misleading Reports of Digital Phone Cloning, [referred 01.05.2007], Available At: <http://jya.com/gsm042098.txt>.
- [31] E. Barkan et al, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", *International Association for Cryptologic Research*. 2003.
- [32] S. Alex et al, "Mobile VPNs for Next Generation GPRS and UMTS Networks", Lucent Technologies.Inc. 2000.
- [33] ETSI EN 301 344. Digital cellular telecommunications system (Phase 2+); "General Packet Radio Service (GPRS)", Service description; Stage 2. European Telecommunications Standards Institute., 2000.e
- [34]H. Kari., Available At: <http://www.cs.hut.fi/~hhk/GPRS/>, [www.cs.hut.fi/~hhk/GPRS/gprs\\_own.html](http://www.cs.hut.fi/~hhk/GPRS/gprs_own.html).
- [35] <http://portal.etsi.org/dvbandca/GEA3/Gea3specs.asp>.
- [36] B. Alan, "GPRS Security Threats and Solution Recommendations", *Juniper Networks, Inc.*, 2004.
- [37] B. Charles, "GPRS Security", Charles Brookson, 2001. Available At: <http://www.brookson.com/gsm/gprs.pdf> , Last Review: May, 2007.
- [38] R. Anderson., *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, Inc. ISBN: 0-471-38922-6, 2001.
- [39] H. Lasse, "Authentication and Security in GPRS Environment: An Overview", Helsinki University of Technology, 1998.
- [40] B. Matt, *Introduction to Computer Security*, Addison Wesley Professional, ISBN 0-321-24744-2, 2005.
- [41] H. Johnson , *Toward Adjustable Lightweight Authentication For Network Access Control*, ISSN 1653-2090, ISBN 91-7295-077-3, 2005
- [42] Gerti et al. (editor), *Web Engineering: The discipline of systematic development of web applications*, Chapter 13: Security for web applications-Martin W., Alfons K., Stefan S., John Wiley & Sons, Ltd., ISBN: 3-89864-234-8, 2006
- [43] Yahoo! Phishing protection, Available At : <https://protect.login.yahoo.com/login/>, Last Visit: May,2007.
- [44] CERT, Coordination Center Software Engineering Institute, Copyright 2000 Carnegie Mellon University, Available At: <http://www.cert.org/advisories/CA-2000-02.html>, Last Visit: May,2007.
- [45] S. David, S. Richard, "Abstracting Application-Level Web Security", *ACM* 1-58113-449 5/02/0005, 2002.
- [46] Microsoft Security Bulletin MS06-033, Available At: <http://www.microsoft.com/technet/security/Bulletin/MS06-033.msp> , 2006.
- [47] Symella, Available At: <http://symella.aut.bme.hu>. Last Visit: May, 2007.
- [48] D. Clark, "Face-to-Face with Peer-to-Peer Networking", *IEEE Computer*, January 2001.

- [49] K. Aberer & Z. Despotovic, "Managing trust in a Peer-2-Peer information system", ACM, 2001.
- [50] K. Eren et al., "A Peer-to-Peer Architecture for Mobile Communications", *Motorola Inc., IEEE*, 2005.
- [51] Y. Lu, W. Want, D. Xu & B. Bhargava, "Trust-based privacy preservation for peer-to-peer data sharing", in *J. IEEE transactions on systems, man and cybernetics*, 2006.
- [52] G. Kortuem et al, "When Peer-to-Peer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad hoc Networks", *IEEE*, 2002.
- [53] Man accused of stalking ex-girl friend with GPS, <http://www.foxnews.com/story/0,2933,131487,00.html>. (Last visit 2007-04-29).
- [54] M. F. Mokbel & C-Y. Chow, "Challenges in preserving location privacy in peer-to-peer environments", in *proceedings of the seventh international conference on web-age information management workshops, IEEE*, 2006.
- [55] Sweeney, "K-anonymity: A model for protecting privacy", *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 2002.
- [56] B. Bloom, "Space/time trade-offs in hash coding with allowable errors", *Communications of The ACM*, vol. 13, No. 7, July 1970.
- [57] A. Biryukov et al, "Real time cryptanalysis of A5/1 on a PC", *Springer Verlag, FSE 2000, LNCS No. 1978*, 2000.
- [58] S. Skorobogatov, R. Anderson, "Optical Fault Induction Attacks", *IEEE Symposium on Security and Privacy*, 2000.