DEAKIN UNIVERSITY

SECURELY SHARING DYNAMIC MEDICAL INFORMATION IN E-HEALTH

By

Fahed Matar Al-Neyadi
MSc in Information Systems

Submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

Deakin University
2016
I am the author of the thesis entitled

**Securely Sharing Dynamic Medical Information in E-Health**

submitted for the degree of **Doctor of Philosophy (Information Technology)**

This thesis may be made available for consultation, loan and limited copying in accordance with the Copyright Act 1968.

'I certify that I am the student named below and that the information provided in the form is correct'

Full Name: Fahed Matar alneyadi

Signed: Signature Redacted by Library

Date: 5/8/2016
I certify the following about the thesis entitled:

Securely Sharing Dynamic Medical Information in E-Health

submitted for the degree of Doctor of Philosophy (Information Technology)

a. I am the creator of all or part of the whole work(s) (including content and layout) and that where reference is made to the work of others, due acknowledgment is given.

b. The work(s) are not in any way a violation or infringement of any copyright, trademark, patent, or other rights whatsoever of any person.

c. That if the work(s) have been commissioned, sponsored or supported by any organisation, I have fulfilled all of the obligations required by such contract or agreement.

I also certify that any material in the thesis which has been accepted for a degree or diploma by any university or institution is identified in the text.

"I certify that I am the student named below and that the information provided in the form is correct"

Full Name: Fahed Matar alneyadi

Signed: [Signature Redacted by Library]

Date: 5/8/2016
# AUTHORSHIP STATEMENT

## 1. Details of publication and executive author

<table>
<thead>
<tr>
<th>Title of Publication</th>
<th>Publication details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. An Authentication Framework for e-Health Systems,</td>
<td>in Institute of Electrical and Electronics Engineers (IEEE) (eds), ISSPIT 2007 Proceedings of the 7th IEEE International Symposium on Signal Processing and Information Technology, pp. 616-620, Institute of Electrical and Electronics Engineers (IEEE) , United States</td>
</tr>
<tr>
<td>4. A privacy preserving service broker architecture for data sharing,</td>
<td>in Kim, Tai-hoon; Lee, Young-hoon; Kang, Byeong-Ho and Sleczak, Dominik (eds), Future generation information technology, pp. 450-458, Springer-Verlag, Berlin, Germany</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of executive author</th>
<th>School/Institute/Division if based at Deakin; Organisation and address if non-Deakin</th>
<th>Email or phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Al-Neyadi, F</td>
<td>School of Information Technology</td>
<td><a href="mailto:fmalneya@deakin.edu.au">fmalneya@deakin.edu.au</a></td>
</tr>
</tbody>
</table>

## 2. Inclusion of publication in a thesis

Is it intended to include this publication in a higher degree by research (HDR) thesis? | Yes | If Yes, please complete Section 3  
If No, go straight to Section 4. |

## 3. HDR thesis author’s declaration

<table>
<thead>
<tr>
<th>Name of HDR thesis author if different from above. (If the same, write “as above”)</th>
<th>School/Institute/Division if based at Deakin</th>
<th>Thesis title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Al-Neyadi, F.</td>
<td>School of Information Technology</td>
<td>Securely Sharing Dynamic Medical Information In E-Health</td>
</tr>
</tbody>
</table>

If there are multiple authors, give a full description of HDR thesis author’s contribution to the publication (for example, how much did you contribute to the conception of the project, the design of methodology or experimental protocol, data collection, analysis, drafting the manuscript, revising it critically for important intellectual content, etc.)

60%

I declare that the above is an accurate description of my contribution to this paper, and the contributions of other authors are as described below.

<table>
<thead>
<tr>
<th>Signature and date</th>
<th>9/08/2016</th>
</tr>
</thead>
</table>

## 4. Description of all author contributions

<table>
<thead>
<tr>
<th>Name and affiliation of author</th>
<th>Contribution(s) (for example, conception of the project, design of methodology or experimental protocol, data collection, analysis, drafting the manuscript, revising it critically for important intellectual content, etc.)</th>
</tr>
</thead>
</table>
Al-Neyadi, F.,  Design of methodology, co-develop and refined algorithms, experimental protocol, data collection, analysis and drafting the manuscript.

Abawajy, J.  Did preliminary research, develop conception of the project, co-develop and refined algorithms, theoretical design and analysis and revising the paper critically for important intellectual content.

5. Author Declarations
I agree to be named as one of the authors of this work, and confirm:

i. that I have met the authorship criteria set out in the Deakin University Research Conduct Policy,

ii. that there are no other authors according to these criteria,

iii. that the description in Section 4 of my contribution(s) to this publication is accurate,

iv. that the data on which these findings are based are stored as set out in Section 7 below.

If this work is to form part of an HDR thesis as described in Sections 2 and 3, I further

v. consent to the incorporation of the publication into the candidate’s HDR thesis submitted to Deakin University and, if the higher degree is awarded, the subsequent publication of the thesis by the university (subject to relevant Copyright provisions).

<table>
<thead>
<tr>
<th>Name of author</th>
<th>Signature*</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Al-Neyadi, F.,</td>
<td>Signature Redacted by Library</td>
<td>9/08/2016</td>
</tr>
<tr>
<td>Abawajy, J.</td>
<td>Signature Redacted by Library</td>
<td>3/08/2016</td>
</tr>
<tr>
<td>Deris, M.</td>
<td>Signature Redacted by Library</td>
<td>8/08/2016</td>
</tr>
</tbody>
</table>

6. Other contributor declarations
I agree to be named as a non-author contributor to this work.

<table>
<thead>
<tr>
<th>Name and affiliation of contributor</th>
<th>Contribution</th>
<th>Signature* and date</th>
</tr>
</thead>
</table>

* If an author or contributor is unavailable or otherwise unable to sign the statement of authorship, the Head of Academic Unit may sign on their behalf, noting the reason for their unavailability, provided there is no evidence to suggest that the person would object to being named as author.

7. Data storage
The original data for this project are stored in the following locations. (The locations must be within an appropriate institutional setting. If the executive author is a Deakin staff member and data are stored outside Deakin University, permission for this must be given by the Head of Academic Unit within which the executive author is based.)

<table>
<thead>
<tr>
<th>Data format</th>
<th>Storage Location</th>
<th>Date lodged</th>
<th>Name of custodian if other than the executive author</th>
</tr>
</thead>
</table>

This form must be retained by the executive author, within the school or institute in which they are based.

If the publication is to be included as part of an HDR thesis, a copy of this form must be included in the thesis with the publication.
Acknowledgements

First and foremost, I would like to thank my supervisor Prof. Jemal Abawajy for his valuable advice, guidance and support throughout and during the course of my study from the formation of the research problem till the completion of the thesis. His continual encouragement to work hard and persevere to achieve good research outcomes played a significant role in the successful completion of this work. I am grateful for his supervision and thank him very much.

I would like to express my sincere gratitude to H.H. Shaikh Hazza Bin Zayed for giving me the chance to go through this experience, which enlightened me in so many ways.

Also, I would like to acknowledge my parents, brothers and sisters for their love, trust, guidance, support, confidence, and patience throughout the years of my studies and research; without them, I doubt that I would have achieved what I have today, thanks for believing in me.

I would like to express my deepest gratitude to my wife, for her understanding and support through all the good times and especially through the bad times. She was always there with great advice and a listening ear.

Last but not least, my dearest circle of friends who were always encouraging me and showering me with their love and support through all the times, may God bless them all.

Fahed Matar Al-Neyadi
Abstract

There is a need to share privacy-sensitive data among autonomous but cooperating organisations. However, security concerns and compliance to privacy regulations requiring confidentiality of the data renders unrestricted access to organisational data by others undesirable. The challenge is how to guarantee privacy preservations for the owners of the information that are willing to share information with other organisations while keeping some other information secret. Therefore, there is a need for privacy preserving database operations for querying data residing at different parties.

To offer the best possible care for their patients, health care providers need coordinated data obtained from the physicians’ own patient database, other physicians, pharmacies, and drug reference databases. Certainly, increased access to medical data leads to more effective and satisfactory care. However, data sharing in dynamic, multi-institutional health care organizations is, necessarily, highly controlled, with resource providers and consumers defining clearly and carefully in restricting with what is shared, who is allowed to share, and the conditions under which sharing occurs. Hence, this thesis addresses the following major topics:

- How to dynamically exchange electronic health record (EHR) information among disparate health care service providers?
- How to ensure that access to the patient records is provided to the authorized person only?
- How to ensure data privacy concerns when data is shared between multiple health care organizations?

The study discusses a proposed solution for the above mentioned specific dilemmas by suggesting the implementation of the following mechanism:

- An architectural framework that enables a flexible and dynamic conglomeration of data across any combination of the participating heterogeneous data sources to maximize knowledge sharing
- A privacy preserving service broker architecture for data sharing in virtual health care environment
- Context-based e-health system access control mechanism for virtual health care environment
- An authentication framework for e-health systems in virtual health care environment and
Finally, an authorization policy management framework for dynamic medical data sharing in virtual health care environment

To investigate the performance of proposed solution model, a sufficient number of test records sample were formulated and used. Many analysis test factors are used to measure and evaluate the effectiveness of the proposed prototypes.
Publications

Conference paper


Book Chapter

# Contents

Chapter 1 ......................................................................................................................................... 11
  1.1 Background ................................................................................................................................. 11
  1.2 Significance ................................................................................................................................. 14
  1.3 Problem Statement ....................................................................................................................... 18
  1.4 Thesis Contribution ...................................................................................................................... 20
  1.5 Thesis Organisation ..................................................................................................................... 21

Chapter 2 ......................................................................................................................................... 23
  2.1 Introduction ................................................................................................................................... 23
  2.2 E-Health System .......................................................................................................................... 24
  2.3 Electronic Health Record ............................................................................................................. 27
  2.4 Data Interoperability Issues ......................................................................................................... 31
  2.5 Health Data Sharing Issues ......................................................................................................... 34
  2.6 Information security ..................................................................................................................... 36
  2.7 Authentication and Authorization Issues ..................................................................................... 39
  2.8 Information Access Control ........................................................................................................ 42
  2.9 Authenticity of the Shared Data ................................................................................................. 45
  2.10 Authorized Data Disclosure ....................................................................................................... 47
  2.11 Privacy and Security Issues ....................................................................................................... 49
  2.12 Chapter Summary ....................................................................................................................... 53

Chapter 3 ......................................................................................................................................... 56
  3.1 Introduction ................................................................................................................................... 56
  3.2 Virtual Healthcare System .......................................................................................................... 57
    3.2.1 Medical Data Ontology ......................................................................................................... 60
    3.2.2 User Authentication Framework ......................................................................................... 63
  3.3 Conceptual Framework Implementation ...................................................................................... 65
    3.3.1 Healthcare Database Peering .............................................................................................. 65
    3.3.2 Ontologies .............................................................................................................................. 66
    3.3.2 Authentication ....................................................................................................................... 78
  3.4 Chapter Summary ........................................................................................................................ 86

Chapter 4 ......................................................................................................................................... 87
  4.1 Introduction ................................................................................................................................... 87
  4.2 Distributed Healthcare Provider Community Framework .......................................................... 89
    4.2.1 Access Credentials .............................................................................................................. 91
    4.2.2 Membership Maintenance ................................................................................................. 92
    4.2.3 Authorization Policy .......................................................................................................... 95
    4.2.4 Authorization Brokerages .............................................................................................. 98
  4.3 Policy-based Collaborative Authorization Management Framework .......................................... 100
  4.4 Security Analysis ........................................................................................................................ 103
    4.4.1 Secure Interaction ............................................................................................................. 103
    4.4.2 Authentication Policy Behavior ......................................................................................... 104
    4.4.3 Verification of Security Attributes .................................................................................... 106
  4.5 Conclusion .................................................................................................................................. 106

Chapter 5 ......................................................................................................................................... 108
  5.1 Introduction .................................................................................................................................. 108
Chapter 6 ......................................................................................................................................... 132
6.1 Introduction................................................................................................................................. 132
6.2 Developing a Privacy Preserving Query Processing Solution .............................................. 133
6.3 Layered System Architecture Model ...................................................................................... 134
6.3.1 Service Provider ...................................................................................................................... 136
6.3.2 Service Customer ................................................................................................................... 137
6.3.3 Service Broker ....................................................................................................................... 137
6.4 Privacy-preserving Data Sharing Framework ......................................................................... 138
6.5 Implementation and Analysis .................................................................................................. 141
6.5.1 System functionality .............................................................................................................. 142
6.5.2 Data Query Page ................................................................................................................... 146
6.5.3 Query Translation page ........................................................................................................ 148
6.6 Conclusion ................................................................................................................................. 150
Chapter 7 ......................................................................................................................................... 151
7.1 Introduction ................................................................................................................................. 151
7.2 Thesis Contributions ................................................................................................................ 151
7.3 Future directions ...................................................................................................................... 152
References ...................................................................................................................................... 154
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Attribute Certificate</td>
</tr>
<tr>
<td>ACA</td>
<td>Attribute Certificate Authority</td>
</tr>
<tr>
<td>CC</td>
<td>Content Certificate</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CCA</td>
<td>Consent Certificate Authorities</td>
</tr>
<tr>
<td>CSS</td>
<td>Central Server Scheme</td>
</tr>
<tr>
<td>E-Commerce</td>
<td>Electronic Commerce</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Healthcare Record</td>
</tr>
<tr>
<td>EMR</td>
<td>Electronic medical record</td>
</tr>
<tr>
<td>FPS</td>
<td>Forwarding Pointer Scheme</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HAS</td>
<td>Health care Authentication Server</td>
</tr>
<tr>
<td>HIV</td>
<td>Human Immunodeficiency Virus</td>
</tr>
<tr>
<td>HL7</td>
<td>Health Level7</td>
</tr>
<tr>
<td>HMO</td>
<td>Health Maintenance Organizations</td>
</tr>
<tr>
<td>HP</td>
<td>Healthcare Professionals</td>
</tr>
<tr>
<td>HPC</td>
<td>Health care Provider Community</td>
</tr>
<tr>
<td>HS</td>
<td>Hierarchical Scheme</td>
</tr>
<tr>
<td>ICA</td>
<td>Identity Certificate Authority</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ISG</td>
<td>Information security governance</td>
</tr>
<tr>
<td>ISM</td>
<td>Information security management</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>LDA</td>
<td>Local Data Agent</td>
</tr>
<tr>
<td>LGW</td>
<td>Local Gateway</td>
</tr>
<tr>
<td>MDP</td>
<td>Message Delivery Protocol</td>
</tr>
<tr>
<td>MRI</td>
<td>Magnetic resonance imaging</td>
</tr>
<tr>
<td>PHR</td>
<td>Personal Health Records</td>
</tr>
<tr>
<td>PDMS</td>
<td>Plant Design Management System</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-Peer</td>
</tr>
<tr>
<td>PKI</td>
<td>Public-Key Infrastructure</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Based Access Control</td>
</tr>
<tr>
<td>RHIO</td>
<td>Regional Health Information Organisations</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SOA</td>
<td>Service Oriented Architecture</td>
</tr>
<tr>
<td>TIHI</td>
<td>Trusted Interoperation of Healthcare Information</td>
</tr>
<tr>
<td>TTP</td>
<td>Trusted Third Party</td>
</tr>
<tr>
<td>RGW</td>
<td>Remote Gateway</td>
</tr>
<tr>
<td>XACML</td>
<td>Extensible Access Control Markup Language (XACML)</td>
</tr>
</tbody>
</table>
# Notation and Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Data objects</td>
</tr>
<tr>
<td>U</td>
<td>Users</td>
</tr>
<tr>
<td>C</td>
<td>Context information</td>
</tr>
<tr>
<td>R</td>
<td>Set of roles</td>
</tr>
<tr>
<td>P</td>
<td>Set of Permission</td>
</tr>
<tr>
<td>l</td>
<td>Implies to</td>
</tr>
<tr>
<td>O</td>
<td>Operation</td>
</tr>
<tr>
<td>l</td>
<td>Authentication trust level</td>
</tr>
<tr>
<td>S</td>
<td>Sets</td>
</tr>
<tr>
<td>≥</td>
<td>Greater than or equal to</td>
</tr>
<tr>
<td>≤</td>
<td>Less than or equal to</td>
</tr>
<tr>
<td></td>
<td>Union</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Background

In any society, health care system represents one of the building blocks representing the quality of public service. In the past and recent years, countries across the globe have used various resources and policies to improve the service of health care system. One of the common choice made by the countries include migration from traditional paper-based health care system into modern electronic health care. The electronic health care system has greater advantages, which include greater convenience and expedite access to medical data. A consequence of this will be less treatment delays, lesser medical errors, cost effective system, fraud detection mechanism where, shorter refund delays for patients covered by health insurance schemes.

In spite of the above mechanism and benefits, people are still sceptical about the new electronic based health care system and are reluctant to embrace the system. One of the reasons could be the lack of assurance given by the medical agencies about safe handling of patient data and also about maintaining patients’ privacy. Hence, there is a need for proper strategies and measure for handling people data confidentially keeping both security and privacy in mind.

During the last few years, there has been a swing from administrative health systems that are concerned mainly with billing practices to clinical Electronic Healthcare Record (EHR) that provide support for providers of health care. There are many advantages of using EHRs (Donyai et al. 2007; Franklin, Jacklin & Barber 2008; Henry et al. 1998; Hillestad et al. 2005; King et al. 2003; Schiff & Rucker 1998; Sim et al. 2001). The use of automated prescription delivery (e-prescription), lead up to increased legibility, warnings against drug interactions and previous
allergic reactions and possibly automated dose calculation, reduce errors associated with prescription of medication (Donyai et al. 2007; Franklin, Jacklin & Barber 2008; Hillestad et al. 2005; Schiff & Rucker 1998). Apart from daily care, EHR systems are also used for the other applications such as clinical research, quality assurance and education.

EHRs have the potential to facilitate coupling of distributed healthcare processes and communications among multiple specialists and the patient (Hillestad et al. 2005). They are also more easily aggregated from various geographic locations to support large clinical research studies compared to their paper counterparts. Moreover, EHRs have potential to help healthcare to be provided based on evidence and best practice in order to achieve better quality and efficiency (Barretto et al. 2003; Henry et al. 1998; Sim et al. 2001). But perhaps the most promising potential of EHRs is its ability to close the loop between clinical practice, research and education (Van der Lei 2002).

At present health care systems, patients’ health data are spread out over numerous healthcare providers that do not share information. This makes it very difficult for physicians and clinicians to obtain a complete clinical history of patients. Thus, although considered advantageous compared to paper-based records, EHRs still have a long way to go in realising its full potential as an integral part of a safe, effective and efficient health care system. However, advances in networking technology have created a new window of opportunity for information communication, dissemination and assimilation. It has made it possible to interconnect independent and geographically distributed e-health systems such that healthcare professionals (i.e., physicians, nurses, etc.) are able to access patient health data and related information from any location at any time. For example, using interconnected e-health infrastructure, data like images, lab results and clinical information (e.g., pharmacy and drug allergy data) can be shared rather fast and thus, guarantee an optimized care process.
In order to understand how to treat a patient, the healthcare providers need to understand what has and has not worked well for the patient in the context of his/her health records and the treatments (diagnostics) available at any point in time. In order to consider the requirement for data sharing, let us consider an experimental scenario and investigate how data sharing can be carried out in different conditions. For instance, let Dr. Ahmed be the paediatrist who treated Mr. Khan in the Aftab hospital. During his stay in the hospital Mr Khan has to undergo various tests. Suppose Mr Khan, who has just been discharged from the Aftab hospital after a serious illness, visited his family physician Dr. Faisal for post-hospital follow up. During this check-up Dr. Faisal does not have any information about the tests that are carried out at Aftab hospital and he prescribes different medicine to Mr. Khan. He states that Dr. Faisal changed several of his medications on discharge and is confused as to which ones to take (he did not bring them with him for his visit). What is important for patient care here is for the two physicians to share their records with each other – they need to reconcile her medication lists, Dr. Ahmed needs the labs Dr. Faisal just got while Dr. Faisal needs the Cath report from the hospitalization, etc.

Sharing medical data among different healthcare providers has the great potential and by doing this whole contributed healthcare providers will benefit significantly. Since these healthcare providers handle very important patient’s information (private data) they may be unwilling to share their health care data. This necessitates a mechanism that can facilitate the health care providers to dynamically share EHR in a transparent manner.

There are many significant benefits in sharing enablement of the data. EHR will lead to a better and safer care with better data availability. Reliable patient care and consistent medical systems are only possible by making the clinical data made available to all the related health care providers (Mohammad & Stergioulas 2010; Yun Sik 2005). By sharing the complete patient information, his/her health records can be fully analysed and the proper diagnosis can be made on time. This can significantly improve the health care services, reducing cost and improving
proficiency and welfare of the patients (Donyai et al. 2007). In case, a patient from one local community is unwell and resides far from home and obliged to receive treatment (health care service) in another health care provider - or any health care provider sends patients to other - physicians and nurses at each of the health care systems will be able to clearly and swiftly access invaluable information about the patient's medications, allergies and health conditions, permitting them to postulate the right kind of treatment at the right time and circumvent unintentional results like adverse medication interactions. Moreover, considerable reduction of health care costs, which well-designed EHR systems with well-trained health care workers have proven to do (Liang et al. 2010; Tianlong & Zhuangzhi 2007), but really is focused on the improvement of patient care. This could also lessen the health care cost by reducing repetitions of investigations, and minimize risks of medical error by obtaining up-to-date medical history and allergy information available at the point of care (Ray & Wimalasiri 2006; Wan 2010).

1.2 Significance

With increasing mobility of populations, patient data may be distributed over many locations in different electronic health care (e-health) systems. While interaction between various health care providers becomes more important and the response to the clinical analysis is becoming the main issue, the access of data anywhere/anytime in a clinical environment is contemplated as an important aspect of quality of care. Hence, with improvement of people’s living standard and increasing mobility of people’s activities, an effective and ubiquitous health care system for both physicians and patients is a must.

Recently, how to access this distributed patient data to provide the best possible care has received attention both from governments, health care providers and researchers (Hillestad et al. 2005). These efforts are vital for making patient information readily available to health care providers, reducing medical errors, and streamlining administrative functions. However, given
the highly sensitive nature of personal health data, the protection of data integrity, availability, authenticity, confidentiality and privacy as well as compliance with personal data protection regulations are critical factors towards achieving users’ trust and acceptance of e-health systems (Henry et al. 1998).

In order to realise data sharing among health care providers, some subtle challenges must be addressed. Sharing electronic health records in a single medical institution and in a large-scale manner is a difficult and challenging problem (Donyai et al. 2007). There are several elements that contribute to this issue. First, health information systems are intrinsically scattered and autonomously managed. While most of the health information systems are privately-owned and often only serve one particular department within a health care institute (Franklin, Jacklin & Barber 2008), search and access to clinical data across health care enterprises is quite hard if not impossible (Jinyuan & Yuguang 2010). Further, the privately owned health care systems has also contributed to the heterogeneous formats used to store the data and access methods together with the lack of inter-operability among the information repositories of such data sets. Moreover, both legal and ethical issues prevent sharing of the health care information among the health care providers.

While it is important that a way to allow health professionals have access to the necessary patient data and information to do their job the best way, increasing automation of the electronic medical record presents, among others, significant patient privacy and confidentiality issues that could expose the health care providers and users to liability (McGraw, et. al., 2013; Hripcsak, et. al., 2014; Yaraghi, et. al.; 2014). Moreover, each e-health system in the network is independently and autonomously managed by the health care providers with authority to control access to their locally managed patient health data and information. In addition, the health care providers are responsible for defining access-rules to protect resources and each brings its own set of concerns. Also, legal responsibilities and accountabilities pertinent to health data collection and
management are the driving force behind health care providers guarding patient data and related information securely. Therefore, research in secure mechanisms to prevent and protect the confidential information and privacy-sensitive patient data as well as fostering trust between health care consumers and providers is paramount in e-health infrastructure.

In health care information systems, the need for privacy, confidentiality and security protection takes on new meanings and challenges (Meingast, Roosta & Sastry 2006a). Typically, health care providers have different security policies that state a diverse set of security requirements and capabilities. Authentication and authorization mechanisms for health care professions may also be different. The physician-patient relationship is confidential. Were that not the case, patients would be reluctant to divulge information necessary to the diagnosis and treatment of their problems. Confidentiality is a significant mechanism by which a patient's right to privacy is maintained and respected.

In general, several non-trustworthy members with unreliable past connections intend to share data instead carry out certain tasks. Healthcare providers differ significantly with their way of operation, scope, ideology, structure, population, and sociology. Nonetheless, vigilant investigation of principal technology necessities indicates us to recognise a comprehensive set of mutual interests and needs. Especially, there is a need for extremely adaptable sharing systems for complex and detailed levels of control over how shared supplies are used, including fine-grained and multi-stakeholder access control, delegation, and application of local and global policies. There are also requirements for sharing of variety of resources, which include programs, files, data to computers, sensors, and networks, and to use different modes, ranging from single user to multi-user and from performance sensitive to cost-sensitive and hence embracing issues of quality of service, scheduling, co-allocation, and accounting.
Different health care systems were implemented at different times and on different platforms. This limits the ability of these health care systems to share data quite severely. Some of the reasons for limitations of data sharing are explained below in brief:

- **Privacy and consent**
  Each health care provider uses different privacy policies. Physicians have an ethical duty to maintain the confidentiality of the patients. Hence, the sharing of patients’ data solely depends on privacy and consents.

- **Access of accurate information**
  In order to access the patients’ information accurately, both physicians and the healthcare providers need to have complete access to the patient information. Some privacy legislation explicitly specifies patients with the ability to restrict access to their personal health information. This type of restriction stops both physicians and health care providers in accessing important patients’ information.

- **Secondary data usage**
  Personal data collected from the patients (secondary data) are sometimes useful in conducting further research, however, due to different data sharing policies and data platforms the usage of these data could be severely restricted (Mangalmurti, Murtagh & Mello 2010).

Formulating EHRs interoperability is one of the requirements for supporting data sharing in increasingly spread and distinct health care systems. Getting innovative information into EHRs for decision support is a vital stage to promote evidence based care. By providing continuous education, knowledge in the form of instructions needs to be circulated and applied in practice. This recurring flow of information and knowledge between care, research and education must be expedited in order to accomplish a safer and more efficient health care system. Hence, an interoperable EHR outline can enable
the sharing of data, information and knowledge not only between people who are using the system but also for contributing software systems.

1.3 Problem Statement

The need to engage in collaborative processes is fundamental to health care. Currently, patient data collected by different EHR systems are not readily sharable with other systems. This situation is sometimes described as islands of EHR systems where data are trapped in their originating system. Such isolated islands are no doubt limiting EHRs to realising its full potential to support clinical practice, research and education.

To offer the best possible care for their patients, health care providers need coordinated data obtained from the physicians’ own patient database, from other physicians’ database, pharmacies, and drug reference databases. Certainly, increased access to medical data leads to more effective and safer care. However, data sharing in dynamic, multi-institutional health care organizations is, necessarily, highly controlled, with resource providers and consumers defining clearly and carefully just what is shared, who is allowed to share, and the conditions under which sharing occurs. The specific problems addressed in this thesis are:

- How to dynamically exchange EHR information among disparate health care service providers?
- How to ensure that access to the patient records is provided to the authorized person only?
- How to ensure data privacy concerns when data is shared between multiple health care organizations?

At present, a patient’s health information may be spread out over a number of different health care providers that do not share information, which makes it challenging for physicians and clinicians to obtain a full clinical history of a patient. Therefore, there is a need for a mechanism
that enables health care providers to dynamically exchange EHR information among disparate health care service providers.

While there is scope for easy availability of individual’s health care information to physicians and authorized individuals, this could also increase the potential risk for abusing the system (accessing the patient’s private data). Hence, as health care providers gradually move to render their business processes and data to external third party organizations, the security concerns of guaranteeing their clients for the safeguard of private data, such as Personal Health Records (PHRs) and EHRs, are accurately validated and authorized is becoming a major worry. Though, both EHR and PHR shares patients data, however, there is huge differences between them. The differences between EHR and PHR are explained below in brief:

- In EHR, either the hospital or the health care provider has control over the documents, but in PHR, it is the individual who has the control over the documents.
- In EHR, all the data are documented electronically, but in PHR the data are documented either manually or electronically.
- EHR is data created by many practitioners and health care providers, whereas the person himself creates PHR (Roblin et al. 2009).

There is a need to share privacy-sensitive data among autonomous but cooperating organisations. However, security concerns and compliance to privacy regulations requiring confidentiality of the data renders unrestricted access to organisational data by others undesirable. The challenge is how to guarantee privacy preservations for the owners of the information that are willing to share information with other organisations while keeping some other information secret. Therefore, there is a need for privacy preserving database operations for querying data residing at different parties.
### 1.4 Thesis Contribution

The following are the key contributions made in this thesis:

1. An architectural framework that enables a flexible and dynamic conglomeration of data across any combination of the participating heterogeneous data sources to maximize knowledge sharing.

The proposed model is based on three technologies; they are “peer-to-peer (P2P), mobile agents and ontology”. The main aim of this framework is to deliver a universal and collaborative (shared) health care system to support both clinicians and health care providers in making optimal decision-making. The system aims to provide safe and secure patients data sharing between several hospitals and medical related entities, thus improving the medical data sharing facility. To this end, we propose an innovative ontology-based software agent and P2P networking model to deliver an adaptable and dynamic accumulation of data across any combination of the participating heterogeneous data sources to maximize information (data) sharing.

2. A privacy preserving service broker architecture for data sharing in virtual health care environment

Much of the data in the health care domain is considered private and confidential. Clearly, preservation of privacy when sharing data in a dynamic environment is very challenging. To address this challenge, we propose a new computationally efficient framework that enables organizations to share privacy-sensitive data. The proposed framework is able to answer queries without revealing any useful information to the data sources or to the third parties.

3. Context-based e-health system access control mechanism for virtual health care environment

E-Health systems logically demand a sufficiently fine-grained authorization policy for access control. The access to medical information should not be just role-based but should also
include the contextual condition of the role to access data. In this thesis, we present a mechanism to extend the standard role-based access control to incorporate contextual information for making access control decisions in e-health application. We present an architecture consisting of authorization and context infrastructure that work cooperatively to grant access rights based on context-aware authorization policies and context information.

4. An authentication framework for e-health systems in virtual health care environment

The high-level sensitivity of medical information mandates stronger authentication and authorization mechanisms to be used in e-Health systems. This thesis describes the design and implementation of certificate-based e-Health authentication and authorization architecture. This architecture was developed to authenticate e-Health professionals accessing shared clinical data among a set of affiliated health institutions based on peer-to-peer networks. The architecture had to accommodate specific medical data sharing and handling requirements, namely the security of professionals' credentials.

5. An authorization policy management framework for dynamic medical data sharing in virtual health care environment

To enable resource sharing between multiple heterogeneous health care enterprises, an authorization policy management framework is required. To solve these problems in a loose-coupling way, we propose a dynamic, distributed and heterogeneous authorization policy management framework for sharing medical information among autonomous and disparate health care information systems.

1.5 Thesis Organisation

In this chapter, we motivated and formulated the problem statement and its significance is discussed. The rest of thesis is organized as follows:
• Chapter 2 explains comprehensive literature reviews of the research study. Issues related to the problem address in this thesis are also explained in detail.

• Chapter 3 proposes an architectural framework that enables an adaptable and dynamic accumulation of data across any combination of the participating diverse data sources to increase knowledge sharing. The proposed method is based on ontologies, mobile agents and P2P technology for bringing together independent diverse and highly dispensed health care services.

• Chapter 4 discusses Authorization Policy Management and privacy preserving service broker architecture for data sharing. In addition to presenting the proposed Context-based e-health system access control mechanism.

• Chapter 5 presents an authentication framework for virtual e-health system together with a depiction of the design and implementation of certificate-based e-Health authentication and authorization architecture. In addition, this chapter presenting test results

• Chapter 6 illustrates a privacy preserving query processing solution and authorization policy management framework for dynamic medical data sharing.

• Chapter 7 addresses the Conclusion and Future Directions
Chapter 2

Literature Review

2.1 Introduction

The use of computers revolutionised the diagnosis and therapy in medical everyday life. Magnet Resonance Therapy and Computer Tomography would not be possible without the aid of computers. Computer aided surgery and computer aided diagnosis helped to improve the medical treatment significantly. Another key element within the health sector that recently got a lot of attention is the EHR. They (EHR’s) contain patient information such as laboratory test, observations, diagnosis, treatments, therapies, patient identification, legal permissions, information on allergies etc. The International Organization for Standardization (ISO) defines EHRs as repositories of information regarding the health status of a subject of care, in computer process-able form (Lewis, Chang & Friedman 2005).

In recent times due to the advancement in pervasive computing and electronic surveillance, the requirement for control tools which respect the privacy of the users are in more demand. In general, users have put full faith on government agencies and central organisations on managing and accessing their personal data. Moreover, users will not know whether any data held by the government agencies are either being communicated or been sold to the third parities. This situation clearly puts users in a risky situation.

Privacy and information security is a growing issue in the health care. The research literature on information security in health care published in both non-information system and information system. EHR contain variety of data that is used for different purposes by different persons involved in health care. It includes computerized medical records, electronic medical record, electronic patient record, integrated care record, personal health record. EHR has become the
most widely used in recording health in electronic form (Hartley and Jones, 2012). Vast majority of health record are still on non-electronic form across many institutions. Increasing popularity of internet and electronic communication devices has made the work easier (Barrett, Silverman and Byrnes, 2011). Health information system is the most important factor in US health care quality and reduces costs. Information system in the discipline such as sociology and psychology analyse the role of employees and individual in information security risks management. EHR enables efficiency and exchange of health information, enhance productivity, removes administrative burden, reduce costs, open up new opportunity and moreover reduce costs. It helps in improving efficiency, accessing and quality of health care services. EHR infrastructure is the reusability and interconnection of all health recorded information. Patient medical record is share with organization such as insurance, medical. For example, a large body research focus on developing technological solution as it ensures in privacy of patient when the information is processed, shared and stored (Sofiev and Bergmann, 2012).

Over the years, researchers have developed various techniques and measures to permit individual users to take in charge of their own data, so that they can access, manage and protect their own information. These methods are usually titled as privacy-preserving protocols. In this chapter, we survey the research literature on the state-of-art health information sharing and various concern such security and privacy in that may arise when sharing health information.

2.2 E-Health System

In this thesis, we refer to e-health system as health care systems and services that are interconnected and can work together easily and effectively, while maintaining patient and professional confidentiality, privacy, and security. We assume a multidisciplinary team environment where patients will be treated by a potentially large team of health providers geographically distributed in various locations. Each health care provider operates autonomously
within distinct domain and has different health care information systems to support local patient care. The health care providers and their systems deal with a whole range of sensitive issues related to patient information such as diagnostic reports, MRI images, pathological test results, diagnosis reports, prescriptions, and so on. In the rest of the paper, we define Healthcare Professionals (HP) as any person involved in any kind of health care related services that include physicians, nurses, administrative staff, support staff and IT staff.

Since health professionals have to provide a wide range of distinctive services, the roles of various types of HPs differ widely, which requires differentiated access roles to the users of the e-health system. Also, individuals have the right to expect that their identifiable health information will not be disclosed without their express informed consent. Moreover, accessing patient related data must be on demanding and on need bases. In addition, as the custodian of patient information, each health care provider is responsible for protecting patient information in patient database against un-authorized use.

E-health is the application of communication and information technologies across the whole range of function that affects health. The benefit of e-health is the improvement in health care and the quality of patient care. Health care is the key driving forces pushing health initiatives (Brent, 2015). E-health involves electronic patient administration system such as electronic messaging system, laboratory and radiology information system, and telemedicine telepath logy. E-health care refers to use of computer system by general pharmacists and practitioners to manage patient, electronic prescribing and medical records. It allows the sharing of necessary information between cares provider across discipline, medical and institution. It is an essential element of health care renewals. It delivers the information for health consumer and health professional through telecommunication and internet. Using the power of e-commerce and IT improves the public health services through training and education of health care (Johnson, 2011). This is the system of using e-business and e-commerce practices in health management.
system. E-health provides new method of using health resources such as money, medicines and information and help in improving the efficient of resources. The internet provides new medium of information dissemination and collaboration and interaction among health professional, institutions and health providers and the public (Chuan et.al., 2014). E-health system helps in preventing unsafe drug interaction, speed up access to information, reduces duplication and allows secure access to information to health providers. E-health improves the quality and efficiency of health system. It optimizes the clinical processes, facilitates the works of health worker and improves the communication between people. Tele-health includes health promotion, surveillance and public health function. It includes computer assisted telecommunication that support management. It is used for telecommunication to treat disease and diagnose and ill health (Sofiev and Bergmann, 2012).

Over the past decade, in many countries the health care delivery system has transformed as simple patient – physician relationship into a multifaceted network linking patients to several stakeholders. Emergence of Information technology, Internet services and their implementation into health care industry are most likely to expand health care delivery quality, minimise health care cost, and improve the medical technological services (Song et al. 2006). Due to the advancement of web and Internet technologies, security and privacy issues are rising over traditional medical services (Agrawal et al. 2004). Nevertheless, this revolution has increased the impending information security risk and privacy abuse. The privacy issue is very important for such systems because most medical data are about individual patients and holds highly sensitive information. Inapplicable revelations of those data cause privacy breaches to patients, which in turn lead to serious legal and financial penalties to the medical hospitals. At the same time, the privacy issue is especially challenging in e-Health systems due to its complex design and also implementation of such systems (Agrawal & Johnson 2007; Yuan et al. 2008). In USA it is projected that health care fraud involves about 10% of total health expenditure (Dixon & Shofer
Furthermore, with emergence in digital technology of health records, medical identity theft has developed a larger frightening issue, costing both taxpayers and patients. Failure to protect sensitive medical and patient information is also a major issue of E-health. Hence, there is a need for suitable privacy preserving E-health systems which can tackle the above shortcomings (Gajanayake, Iannella & Sahama 2011).

2.3 Electronic Health Record

Because of the growing use of information technologies in health care industries, patient records are regularly created and shared in an electronic form (Choudhri et al. 2003). In USA, health care information systems are mainly considered as the single most significant element in improving health care quality and lessening associated costs (Dixon & Shofer 2006). Latest government initiatives forecast implementation of a universal Electronic Health Record (EHR) by all Health Maintenance Organizations (HMO) by year 2014 (Goldschmidt 2005). Recent research study conducted at USA shows that it could save up to $81 billion annually by adopting into EHR system (Hillestad et al.). Nevertheless information technology (IT) expenditure in health care division imprints that of several other industries, usually in 3-5% of revenue, far behind industries such as financial facilities where closer to 10% are the standard (Bartels 2006).

Electronic health record collects health related data and information of an individual and retrieved by different health care provider including doctor for health care related purposes in electronic format. EHR system provides information regarding infrastructure and efficient platform for health care provider e.g. clinics and hospitals. Health care provider and recipients choose to participate to the needs and joining consent to EHR sharing system. EHR implementation enhances private-public partnership in health care sector and helps in redressing private public imbalance. The system brings the maximum benefit to the children, senior citizen and people who frequently use private health care services and public at the same time (Chuan
et al., 2014). The system is not merely an IT project. It also requires addressing privacy, legal and security issues of institutional issues and patient records including governance of emerging EHR sharing holding infrastructure and transferring the vast amount of health data of majority of population (Uden, 2013). EHR processes involve technical complexity, investment, numerous challenges and change in workflow. It promotes widespread adoption use of IT health and health information technology for economic and clinical health. The provision includes incentive payment program and assistance technical for the eligible health professional and hospital to implement, adopt and upgrade the electronic health records and achieving the meaning of health information technology. In achieving the aim of Health Information Technology for Economic and Clinical Health Act (HITECH) legislation was created in 2009 to stimulate the adoption of electronic health record and supporting the technology in United States, the organization does not successfully implement the meaningful and optimal use of EHR that involves numbers of challenges. The purpose of literature review is to provide how an organization optimizes and implements an EHR and from the standard for performing and reporting on Peer standards that provide information on administering, planning, performing, reporting that reviewed publication and gray literature. The different stages in EHR process are planning, workflow and software design, vendor selection, training and user support and modification (Cruz-Cunha, Tavares and Simoes, 2010). EHR relates to some topic such as patient outcome, cost saving, activity work pattern, time cost and other points. To guarantee the success in EHR system implementation the essential thing is to have good understanding of the factor that contribute to stakeholder. EHR improves the efficiency, delivery, safety and quality.

Modern health care systems use large networks to manage patient data information. Apart from the medical diagnostics, the patient's medical information could be used for other purposes; for instance, data could be used for improving the competence within health care system, public policy improvement and administration at state and central level, and also for conducting
research in advanced medical science (Hodge 2003). Apart from this, patients’ medical records could be also being shared with payer organizations such as private medical insurance companies and government agencies such as Medicare service to rationalize payment of services rendered by physicians. Additionally, health care providers may use patients’ medical records to manage their operations, to evaluate service attribute, and to recognise quality-upgrading prospects. Medical data of patients is also used for “public health management, hospital accreditation, medical research, and for managing social and welfare systems via central and local government organisations” (Appari and Johnson, 2010).

Healthcare delivery is an extremely intricate process involving many individuals and organizations. Providing voluntarily admission to amalgamated health care information at the point of care remotely involves a system architecture that facilitates partnership and coordination among health care services and facilitates the mobility of health care professionals (Koufí, Malamateniou & Vassilacopoulos 2010). In order to be part of the global network databases, peers only need to define local mappings to a small set of associated databases and hence no global semantic co-operation is required. Once a database sends a query to its immediate neighbours via local mapping links, its neighbours after processing the query circulate the query to their own neighbours, and so on until the query reaches to all or a set of predefined set of databases. The way the query spreads across the network imitates the way communications are transmitted in a Peer-to-Peer (P2P) system, hence it is also termed as Peer Data Management Systems (Tatarinov & Halevy 2004). With the current arrival of middleware technologies that facilitate sharing EHRs through independently managed heterogeneous health care information systems across different health care enterprises, regardless of the fact that they may be scattered throughout the world, and that they may not know each other personally. For instance, under the assumption that the health care providers form a Gnutella-like P2P community, an ontology-
based P2P approach for facilitating heterogeneous medical information sharing between health care providers is proposed in (Arenas et al. 2003).

In the past few years, P2P applications have emerged as a popular way of sharing data in decentralized and distributed environments. There are mainly two types of P2P technologies; they are untrusted approach such as Free net (Clarke et al. 2001) and the structured approach based on Distributed Hash Table (DHT) such as Chord (Stoica et al. 2001). However, these two technologies don’t care about the semantic meaning of the nodes. In order to overcome the above obstacles some of the approaches were used recently, such as semantic P2P network using Virtual Hierarchical Tree Gird Organization (VIRGO). It uses the decentralised approached and hence can connect directly in P2P ways and share information (Lican 2009).

- “Electronic medical record (EMR) is the record that contains clinical data, which is stored in a structured manner, while clinical data is the information, which comes under fully within the medical domain (Lewis, Chang & Friedman 2005). EMR stores data electronically for managing medical data collected by a hospital or clinician practice (Meingast, Roosta & Sastry 2006a). However, EMRs don’t include non-medical data which include social or mental health information”.

- “Electronic patient record (EPR) is the method to store the individual health care data for primary patient care usage (Von Solms 1998)”.

- “Personal health record (PHR) is a person-centred system intended to track and support health activities across one’s whole life experience. It is not restricted to any single health organisation or medical service provider (Meingast, Roosta & Sastry 2006a). The PHR is a set of computer based tools that allow people to access and manage their lifelong health information and make appropriate parts of it available to those who need it” (Schoder & Fischbach 2003).

In this thesis, the term of EHR is used since it has a broader use for distinctive medical, health and personal information of patients during their lifespan.
2.4 Data Interoperability Issues

There is a growing need for sharing patient records among health care providers and their associated facilities, in order to provide the best care and clinical outcomes for patients. The broader problem we are trying to resolve is how to make use of IT to deliver valuable support for accessing medical data for clinical care, medical research, teaching, health services administration, and patient care. The problem, however, is that health care providers typically use many heterogeneous health care information systems that do not interoperate, which makes it arduous for physicians and clinicians to capture a complete medical history of a patient. Moreover, health care information systems tend to store health information in various copyrighted (privately-owned) formats. This variety of data arrangements forms a major obstacle in sharing patient information/data among medical providers. The non-interoperability of IT systems represents the biggest single problem in transferring data securely between different parts of a health care system.

In a recent study, Yaraghi (2015), show that healthcare information exchange (HIE) can reduces the number of orders for laboratory tests and radiology examinations per patient by 52% and 36% respectively in the emergency departments. Similarly, Vest et. al., (2015) found that HIE can reduce patient readmission by 57%. While without interoperability, sustained acceptance of current EMR technologies will stimulate information silos that already exist in today's paper based medical records leading to privately-owned control by information designers (Brailer 2005).

Since healthcare institutions maintain their patient data often behind the firewall, enabling access to these data is expensive and complex due to factors such as heterogeneity, sensitivity and time criticality of health data makes it sharing with other healthcare institution quite challenging (Mandl and Kohane, 2015. Furthermore, privacy and security in instituting an interoperable health information exchange remain major problems.
Interoperability issues in e-health are important to deliver the quality health care and reducing the cost of health care. Important cases includes the coordinating the chronic patients and enabling the cooperation in different e-health system such as electronic health record system, Personal health care system and wireless health care devices enabling the use of EHR for clinical research able to share the lifelong EHR among different health care provider. Achieving e-health interoperability is a challenge because their competent standards and clinical information (Koutsouris and Lazakidou, 2005). Successful industry such as integrating the health care enterprises as large scale deployments such National Health information system. Its task exists between two application accepting data included in the form service request and performing the task judged by the user of the receiving system. The two applications are in the three layer interoperability stack the communication and transport layer which involves the exchange the document and messages as well coding and business process involves choreography of interaction. Agreement between two applications on the interface is not practical because it requires new interface for each application for implementation to communicate with. Variety of different standard is used in different layer of interoperability stack and application to conform to different standards the problem continues. Overcoming with the challenges by determining the combination of standard used and restricting further them to ensure interoperability (Wei, Rykowski and Dixit, 2013).

Establishment of fully practical interoperable EHR scheme remains a major challenge. Recent research studies have recommended Service Oriented Architecture (SOA) models for EHR in various situations encompassing clinical decision support systems (Catley, Petriu & Frize 2004), collective medical imaging analysis (Catley, Petriu & Frize 2004), and health clinic setting (Catley, Petriu & Frize 2004; Raghupathi & Kesh 2007). These SOA based EHRs are expected to be accessible to allow inter-enterprise impressions such as Regional Health Information Organizations (RHIO), and federation of such RHIOs could produce health information networks
both nationally and globally (Catley, Petriu & Frize 2004; Raghupathi & Kesh 2007). Solomon (Solomon 2007) carried out a case study, where he investigated the performances of three budding RHIO, namely the “Indian Health Information Exchange, the Massachusetts Health Data Consortium, and the Santa Barbara County Care Data Exchange”. He prompted numerous elements that inspire innovation and diffusion, adjustment, and change management of RHIOs. Among them, security and privacy of patient information are main fears impeding the implementation of clinical IT across the RHIOs. Those fears could persist in the near future as the technology benchmarks for data interoperability are still in the development stage (Dogac 2006; Eichelberg et al. 2005).

Initiatives such as IHE (RSNA 2007) dictate how complex standards such as HL7 (HL7 2007) and DICOM (DICOM 2007) should be utilized when implementing hospital workflows. An important step towards accomplishing this objective has been realised through years of teamwork among health care experts, resulting in the international standard for storing and allocating health data: The Health Level Seven Version 3 (HL7 v3) Standard. HL7 v3 initiates an exclusive Reference Information Model (RIM) that administers stability of stored and shared data across distinct domains within health care. Nevertheless, the present criterions have focused on only on syntactic issues, which in most instances still need human intervention in order to maintain service integration. In order to improve interoperability, semantics are required to permit software to grasp the significance of data and a service’s tenacity permitting better-quality service discovery, automated planning and facilitation. The significance of semantics for interoperability is well documented in Paul (2004). Nevertheless, currently semantic web technologies are not popular among leading vendors.
2.5 Health Data Sharing Issues

In health care division, it is most important to share medical information/data across organisational limits to support the main interest of the agencies and also the multiple stakeholders. Progresses in medical technology have transformed multiple health records into single databases, which also support researchers involved in developing such tasks. An important and growing research in the field of technology and diverse range of frameworks offers methodologies to reduce or control the disclosure risk of patient information – which include “*global and local recoding* (Samarati 2001), *micro-aggregation* (Domingo-Ferrer et al. 2006; Domingo-Ferrer & Mateo-Sanz 2002), *data perturbation* (Muralidhar & Sarathy 2005), *data swapping* (Reiss 1984), and *data encryption* (Hui-Mei, Chin-Ming & Shaou-Gang 2002).

Conversely, some researchers debate that it is not possible to entirely delink patients’ identities from their health information for numerous reasons, which include the sighting of errors or variability in care endowment necessitates identification of the patient for corrective follow-up care. Poor control on research legitimacy and potential scams if de-identified cannot be traced back to original source, and increase in cost of data preservation(Behlen & Johnson 1999). More recently, researchers recommended SQL searching schemes of encrypted data (Susilo & Win 2007) and attribute protection boost to “*k-anonymity*” algorithm (Truta & Vinay 2006) to preserve privacy of patients during data disclosure for secondary reasons such as medical research. Similarly, set theory is used to build “*k-unlinkability*” that could offer security from hackers who may match publicly available information such as imprints of location visits to re-identify a patient (Malin 2007a). Riedl et al. (2007) developed an innovative architecture for producing a safe pseudonymous connection between patient and their health record that will let authorization to specific people, which include, health care providers, close relatives of patients, and medical researchers. Recent developments on data masking research, discussed above, are well supported with industrial research and technological advances such as “*Hippocratic*
database” (Agrawal et al. 2002b) and “Sovereign Information Sharing platform” (Agrawal, Evfimievski & Srikant 2003). Hippocratic database is an integrated set of technologies that empowers effective administration of information disclosure from patients’ health records in agreement with regulatory criterions without hampering the lawful flow of information to support activities related to individual level care endowment and public health management (Agrawal & Johnson 2007). These developments have encouraged wider research on problems concerned to acquiring privacy preferences from patients under the guidance of E-Health applications built on Hippocratic database platform (Yuan et al. 2007).

An electronic health known as the health delivers and enhances health information and services through the technology and internet. Health informatics includes health knowledge management, consumer health informatics, and medical research using health grids. The technologies facilitate the provision of medical information to different users such as physician, care team, patient, pharmacy, and medical researchers. It includes medication, demographics, immunization, radiology images, laboratory test results, allergies and billing information. There is need to create a computer science tool intendment to general medicine and governed by same profession from several considerations (Markey, 2014). The sharing data is possibly to bring professional senility to many dynamics and operation imposed by informative system far managed and governed by others. Advancements in informational technology provide new opportunity for research to share data and helps to build another work. Informatics is the ability to maintain large database and combine the information to many sources. The importance of sharing data is advancing health and strongly endorse by the H8 group of global health organization. NO H8 group is team of students and photographers who promote marriage, gender and human equality via education. In some fields such as physics and genetics, the sharing data establishes and accelerates the research progress and application for public good. The sharing data improves the public health researches it is time consuming and expensive. Charitable and public research believes in
marketing research to set available data to investors and beyond the original researcher (Yang and Ma, 2013). It generates three benefits such as fast progress in improving health, better valuation of money, higher quality science. Funding institution works on its own operational and legal framework that is committed towards working goals. It establishes joint working groups and generates health routine services and statistics and other type of health data adopt the similar approach. It establishes the guideline to desired goals and principle. It recognizes the variety of approaches and flexibility needed to balance the right of individual and communities that contribute to data, the investigator that design collect and research the analyse data, the scientific community that productivity use of data for further research.

In the recent past, researchers have focused mainly on developing theoretical solutions for secure data disclosure. Nevertheless, each health care provider may not use advanced technology, integrated with modern algorithms, to reveal data for secondary reasons. Understanding the operational usefulness of data disclosure technology from the field may help hospital management in modifying data disclosure procedures, as well as selecting proper data disclosure technology solutions.

2.6 Information security

There are various different terms need to be considered when talking about information security. Most important among them are briefly described below:

- **Information security** is used to protect information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities” (Serour 2006). It includes the use of physical and logical data access controls to ensure the appropriate use of data and to inhibit “unlawful or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets” (Guah & Currie 2004). Information
security comprises the totality of security precautions needed to deliver a satisfactory protection level for a system and for information treated by a system (Meingast, Roosta & Sastry 2006a; Papazafeiropoulou & Gandecha 2007).

- “Data protection refers to the set of privacy-motivated laws, policies and procedures that aim to minimise intrusion into respondents’ privacy caused by the collection, storage and dissemination of personal data (Meingast, Roosta & Sastry 2006a) (Glossary of Statistical Terms)”.

- “Confidentiality is the privacy interests that arise from specific relationships (e.g., doctor/patient, researcher/subject) and corresponding legal and ethical duties (Wiederhold et al. 2000). It signifies to the property that information is not disclosed to unauthorized individuals, entities, or processes (Kluge 2004) ensuring that information are accessible only to those authorized to have access (Serour 2006). Confidentiality is to safeguard sensitive information from unauthorized disclosure (Coiera & Clarke 2004) or intelligible intervention (Win 2005)”.

- “Integrity is the property that data have not been altered or destroyed in an unauthorized manner ensuring that information is accurate and complete (Coiera & Clarke 2004) in storage and transport; that is correctly processed” (Meingast, Roosta & Sastry 2006a).

- “Availability is the property of being accessible and usable upon demand by an authorized entity (ISO/IEC TR 13335-1, 1996, pp.5) ensuring that information is available to those who are authorized to have it, when and where they should have it (Talia & Trunfio 2003)”.

- “Privacy is technically defined as the condition of being isolated from view, or secret. Privacy can be seen more concerned with social aspects, which is generally known as the ability to control information about oneself”. (Papazafeiropoulou & Gandecha 2007) provided some definitions of privacy they are listed as below:
Privacy in health sector is the individual’s right to control the acquisition, use and disclosure of their identifiable health information.

- **Auditability** (usually called accountability) is the ability of inquiry, which guarantees that the actions of an object may be traced uniquely to the entity (Kluge 2004).

- “**Information security management (ISM)** signifies to the structured process for the implementation and on-going management of information security in an organization” (Coiera & Clarke 2004).

- “**Information security governance (ISG)** defines the procedure of how information security is tackled at an executive level” (Win 2005).

- **Authenticity**: According to Von Solms (1998), authenticity is, “the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information” It can also be denoted as the criterion that ensures the reliability (integrity) of the identity (Meingast, Roosta & Sastry 2006a).

The security and privacy of the information is the prime importance to all individual, private sector and government agencies of the organization. The protection of information is more sensitive issue in the health care sector (Ying and Mun, 2011). Like all other industry health care is becoming more efficient in delivering the clinical results and most effective cost through the use of computers, information technology, application, electronic networks and other
technologies. Theses technology increases the exchange of information among the health provider and poses privacy and security personal health information and risk to information. Health information discloses an unauthorized individual, tampered with, accessed incorrectly and loosing those results an impact on patient health or even the life (Meyers, 2012). The documentation framework and action plan implements on security priorities need to adapt the complexities and size of various health care organizations. The guideline has two versions: information security for health care sector resources and information for community based and private medical based. Other is information and resources for complex organization. Developing security risk sets up a risk management program, health care organization is better prepared to protect the reputation and maintaining the confidence and trust of the patients, it reduces the liability to implement the security program and complete the legal requirement based on Personal Information Protection and Electronic Documents Act PIPEDA, and Personal Health Information Protection Act PHIPA, operation by clarifying responsibilities and goals. It is essential to authenticate the health care system to achieve security of health system. PIPEDA is an act, which passed on 2001 and implemented on 2004, which is Personal Information Protection and Electronic Documents act. PHIPA is personal health information protection act is a tools of health information protection act.

2.7 Authentication and Authorization Issues

Authentication means maintaining the set of user credential such as passwords, username and biometrics. The approach is used for few application and services. This particular approach provides severe security risks. Many different credentials lead to many insecure practices like using one password for all accesses, writing down password, using of simple credential. The process allows user authentication and identity in order to access the multiple applications. Many implementations are processed such as MIT Kerberos. The implementation is adequate to small
network environment, but fails in scalability. Kerberos provides cross organizational protocol bindings and manage the user credential and principle key becomes complex (Muth, 2014).

Web services are increased in organizations and enterprises to expose the data to their business partners the resource and services are spreading to different administrative domains and controlling the accesses becomes a crucial issue. Accesses control mechanism is currently using to face the risk of unauthorized access. The mechanism takes several forms use different technology and involves varying degree of complexities. The implementation to several access control model is proposed in literature (Yogesan, 2009). The model arises from the need of change in organizational structures and technologies and not forming deficiencies in security provided by earlier methods. List of such role is given to access the control decision and resources on the basis of matching between the user role and role defined in the list. The drawback of the role is defined in the organization which is unrealistic in service oriented architecture.

Authentication in networked e-health system is important and challenging. An authentication service conveys proof that the identity of an object or subject has indeed the identity it claims to have, while the authorization means the granting of permission on the basis of authenticated identification. Without proper authentication mechanism, the provision, continuity and safety of health care system could easily be compromised. A large number of techniques may be used to authenticate a user and a survey of existing tools showed that there is no single best approach for providing an authentication and authorization infrastructure for e-health systems (Lopez, Oppliger & Pernul 2004). A PKI and smart card based e-Health authentication architecture to authenticate health professionals accessing a regional platform for sharing clinical data among a set of affiliated health institutions on dedicated national health network known as Rede Telemática da Saúde (RTS) is described in (Burgsteiner Harald & Dietmar 2008).

An authorization and authentication architecture for e-health services system that integrates the role-based method (Al-Nayadi & Abawajy 2007b) and the attribute certificate (or privilege)
based method (Song et al. 2006) into the electronic health service system is discussed in (Hitchens & Varadharajan 2000). A fingerprint-based model suitable for medical images privacy protection against unauthorized release of images by an authorized recipient is discussed in (Holt et al. 2003). In E-HP2 (Al-Nayadi & Abawajy 2007a), a number of health care organisations (e.g., physicians, pathology labs, pharmacies and hospitals) willingly collaborate by virtually integrating their information systems. E-HP2 enables health providers to share patient information in a seamless, fault-tolerant and scalable manner. It is important to note that the provision of infrastructure services is an enabling mechanism. The infrastructure itself will deliver some benefits, but the main outcomes will be achieved by the provision of additional applications and services.

Existing approaches are based on technical solutions that are well known in distributed system with a single centralized node controlling the authentication process. The common denominators of these previous approaches are generally strongly biased toward a single individual interacting with a single application. Moreover, those based on digital certificate and public key infrastructures to build and operate authentication or authorization infrastructure is only adopted the identity certificate. An identity certificate is an electronic document certificate that provides generally recognized proof of identity just like a passport, or other personal IDs. Identity certificates are issued by Certificate Authorities (CAs) in much the same way as government agencies issue passports after verifying an individual's identity. CAs can be either independent third parties or organizations running their own certificate-issuing server software.

Hitchens and Varadharajan (Hitchens & Varadharajan 2000) proposed an authorization and authentication scheme for e-health services system that incorporates the role-based approach. Authentication design for E-Health was established to endorse E-Health Professionals accessing RTS, a regional platform for sharing clinical data among a set of connected health organisations. The architecture had to adapt detailed RTS needs, namely the security of professionals’
credentials, the mobility of professionals, and the scalability to accommodate new health institutions. The adopted solution uses short-lived certificates and cross-certification agreements between RTS and E-Health institutions for endorsing professionals retrieving the RTS. (Hitchens & Varadharajan 2000).

2.8 Information Access Control

Present health care systems are huge networked systems, which manage patient data with several users retrieving health data for different reasons within and across organisational limits.

Role Based Access Control (RBAC) is one of the novel system which is designed and developed to have control and get important information from a large computer networks (Ferraiolo, Barkley & Kuhn 1999; Sandhu et al. 1996). On the whole, it is showcased as an proficient tool to handle data access in health care industry due to its ability to execute and administer a wide range of access control procedures based on composite role hierarchies normally established in health care organizations (Gallaher 2002). This research mainly stresses on creating algorithms and delineate role based information access (Li & Tripunitara 2006; Motta & Furuie 2003), and appropriate access control (Covington 2000); Motta & Furuie (2003). Later, Schwartmann (2004)extends the above research and proposed an enhanced RBAC scheme which covers attributable roles and authorizations. This enhanced system is intended to lessen the burden of managing access privileges by reducing remarkably huge number of authorizations and roles to a feasible dimension and therefore intend to reduce administrative costs.

Security of EHR is the critical aspects of e health solutions. Different solution develops in year whether the data is secured enough. Privacy and security in electronic health record system help in growing the e health. The development in the policies and satisfying the privacy and security of different stakeholders has proven difficult in health care. The requirement to meet the system to develop is to succeed in achieving the desired goals. Access control is the fundamental barrier
security use for securing data in health care security systems. In this system a paper is present to access control, in the model for electronic health record (Nozaki, Kashiwase and Saito, 2014). Many health portal systems are implemented using the shelf software component. The feature of security provides by the component is quite insufficient. The paper addresses the issues from perspective of access control. Role based access control is the approach to existing supplements with a rule to access control based on flexible authorization framework. Proper accessing control is necessary for EHR system information. Health care information makes the access requirement to different type of industry. The data access is required to provide information system to the health care. Proper access control is necessary for any EHR system operation. Health care is the information dependent industry. It accesses the requirement from different type of industry. The health care provider accesses the data requirement and privacy of the patient data. Requirement in fulfilling the complex task is to be overcome to gain confidence. Access control is required for defining security policy of the organization. It provides access to the relevant information in timely and non-restrictive manner (Organization, 2014). Health care providers have the capacity to patient health information and other health specialist to make decision. Health care authority should have the power in providing patient security.

Furthermore, enhancement is being done in several fronts, which include the usage of autonomous agents to create privacy-aware health care functions (Tentori, Favela & Rodriguez 2006), authorization policy structure for P2P knowledge based disseminated health care system (Al-Naydi, Abbawajy & Ders 2007), encrypted bar code technique for electronic transfer of instruction(Ball, Chadwick & Mundy 2003), pseudonymous linkage (Riedl et al. 2007), and electronic consent models that permits patients to delineate which section of a medical record could be shared to whom (Nepal et al. 2006; O’Keefe 2005).

Despite major technological developments in information access control, operating or using them appropriately is remains a major challenge (Lovis et al. 2007). Because of the complex nature of
data and its access, health care businesses often have larger access rights and take up “Break the Glass (BTG)” strategy to facilitate timely and effective care. For example, Rostad & Edsberg (2006), reported that in most of the instances 99% of physicians were given patient data overriding rights while only 52% required overriding rights on regular basis, the security mechanisms of health information systems were overridden to access 54% of patients’ records. Another common drawback of BTG policy is that employees could misuse such sophisticated privileges. In order to deal with the above mentioned problems (Bhatti & Grandison 2007), proposed a “privacy management architecture (PRIMA)” model that influences artefacts such as audit logs arising from the actual clinical workflow to infer and construct new privacy protection rules. In particular, PRIMA uses policy enhancement modules that occasionally scrutinize the access logs and identifies new policy regulations using refined data-mining procedures. These audit information could be used by privacy administrators to control privacy infringements, which in itself is a complex procedure and regularly necessitates merging data from distinct sources (Ferreira et al. 2006). Unfortunately, such data merging may reveal patients sensitive information to the third parties against the patients’ consents. In a similar research study by Malin and Arioldi (Malin 2007b) established a “Confidential Audits of Medical Record Access (CAMRA)” procedure to guarantee privacy of patient’s identity during such linking of distinct databases for complete audit purpose without revealing any sensitive information. In summary, there are lot of research has been established in the area of information access control providing solutions to achieve data access opportunities in health care establishments. Nevertheless, researchers (Ferreira et al. 2006) acknowledge that “access control management” is not just a technical solution but demands deliberation of work practices, organizational structure and culture to deliver efficient information security. Effectiveness of access control system, for example, with data overriding privileges would very much depend on how the users act together with the system. In order to increase the transparency of “access control management”, hospital
systems are even implementing the policy of sharing audit logs with patients, hence permitting them to constantly update access rights on their health records to health care providers (Lovis et al. 2007).

The Trusted Interoperation of Healthcare Information (TIHI) project deals with security matters that result from when some information is being distributed among collaborating organisations. It assumes that protection exists to prevent infringement by adversaries via secure transmission and firewalls. The TIHI system design provides an opportunity for the system administrator to initiate queries and responses in secured manner. The latter information is usually broadcasted by means of the Internet. The enterprise policy is determined by regulations presented to the negotiator. In this research report, we demonstrate examples of standard rules (Wiederhold G 1996). Even though, the problem and our solution developed mainly focussed in a health care context, but it is equally valid among collaborating enterprises.

### 2.9 Authenticity of the Shared Data

When sharing health data while maintaining the autonomy and independence of the health care providers, the question of shared data authenticity is raised. For instance, it may be sensible to have faith in a single centralized facility, but apparently risky to rely on several anonymous health care providers in the whole distributed network. Hence, it is essential to recognise the legitimacy of the resources given by other health care providers. Due to the shortage of guaranteed legitimacy of the resources to be exchanged, the overall performance of data sharing systems worsens severely for much time and bandwidth is wasted in downloading unwanted data files (Graffi et al. 2009; Lingli, Yeping & Ziyao 2008).

The development and evolution of information technology have facilitated the greater sharing of data and knowledge management used for the collection of information from the data such as corporation, individual and government. It has created huge opportunity in information retrieval
and knowledge management (Zhang, Zhang and Zhang, 2013). Developments have helped in improving decision making in the field of research, public health organization, and medical information and in research committee. Approaches have been proposed to publish different data in different fields. Integration is required in management of data information such as patient identification. Sharing of data and management in different field may lead to misuse of information. Therefore, there is a need to build and design certain logarithm to manage the sharing data efficiently and avoid the misuse of the information (Pace et al., 2010). The goal is for authentication of data system. Summarizing and evaluating different approaches in controlling the different data to control the sharing of management and knowledge to ensure systematic integration. Health information affects the quality of individual employability, insurance and health care. Health information increases the scope of organizational scope in maintaining the integrity and health data. Patient identifies the integrity in quality, accuracy and completeness in demographic data associated or attached with individual patient. This includes quality and accuracy of data that relates to information correctness of matching and linking of existing record of individual with across information system (Pant et al., n.d.). The tremendous cost saving and potential benefits with the health care industry accurate patient interoperability and identification.

Due to the lack of assured authenticity of the resources to be exchanged, the overall performance of the system degrades severely for much time and bandwidth is wasted in downloading unwanted files. The reliability of the information to be exchanged could be critical, and cannot always be judged simply by reading it (Ahmad & Ewe 2005; Wei, Yang & Liu 2007). Moreover, some people, like representative of drug companies, may have vested interest to provide false treatment advice to promote their drug. Trust is essential if the health information collected is to serve as a complete and accurate foundation not only for patient health information but also for
clinical care, research, payment, and health care policymaking (Balfe, Lakhani & Paterson 2005). Therefore, it is important to identify the authenticity of the resources offered by other peers.

### 2.10 Authorized Data Disclosure

In health care division, hospitals often share data across organisational limitations to support the main interests of multiple investors together with agencies involved with public health. Nevertheless, revealing patient’s sensitive medical data and personal information could breach confidentiality as well instigate socioeconomic consequences for patient. However, such data, when concealed for recognising and sensitive information, must sustain the analytic properties to guarantee statistical implications, particularly when released for epidemiological research data (Truta & Vinay 2006).

The privacy rule defines the rules of disclosure of Protected Health Information (PHI) that cover the entity that make without individual authorization. According to the United State department of health and human services PHI is the protected health information, which is created, stored and transmitted electronically. Use, collection and disclosure limitation in principle the rule defines disclosure based and permission based, and attaches the condition accordingly. Privacy rules permit the use and disclosure of number of additional public policies and benefits such as public health or research without the individual authorization. Limitation and specific condition applied to use and disclosure by cover entity of the purposes there should be balance between the public interest need for the information and the individual privacy interest. In electronic health information, the environment exchange and covers an entity disclosure of PHI. Other purposes for which the privacy rule permits that cover the entity to disclose PHI (Park, 2012). Uses and disclosure of privacy rule covers entities in engaging in the electronic health information exchanges that need to contingent of states that leads to privacy law as well federal law that affects the exchange of electronic health information. HIPAA is federal health insurance
portability and accountability Act, which is formed at 1996. HIO refers to the Health Information Organizations, which are non-profit health organization leading by U.S. government. The scope and the purpose of electronic health information is the disclosure by HIPPAA covered through entity that participates in HIO should be according to the privacy rule. Entities participating in HIO have business agreement with HIO that defines the disclosure and uses of the HIO that permits to make with PHI on a covered entity on behalf (Premack, 2001). The privacy rule disclosure and uses entities covers engage in electronic health information system.

Recent advances in technology have helped to consolidate multiple source data into single research database, which supports researchers who are involved in improvement of public health, health services and also clinical methods. An important and emerging research and building on the theory of statistical methods offers variety of data masking practices and frameworks to minimise or control the disclosure risk of patient data. Some of them include:

- “Global and local recoding of patient data (Samarati 2001)
- Micro-aggregation(Domingo-Ferrer et al. 2006; Domingo-Ferrer & Mateo-Sanz 2002),
- Data perturbation (Muralidhar & Sarathy 2005),
- Swapping of sensitive data(Reiss 1984), and
- Data encryption (Hui-Mei, Chin-Ming & Shaou-Gang 2002) among others”.

Promoters of public health debate that privacy interests need to be strongest and communal interests should be boosted where they are likely to attain the greatest public benefits (Hodge 2003). In the recent past, researcher has focused only on developing theoretical answers for secure data disclosure (Gorawski & Bularz 2007; Mishra et al. 2009). Nevertheless, each health care supplier may not employ state-of-the-art technology, incorporated with modern algorithms, to reveal data for secondary reasons. By understanding the operational efficiency of data disclosure, it may assist hospital management in refining data disclosure policies, as well as selecting suitable data disclosure technology solutions.
2.11 Privacy and Security Issues

While personal health information is digitized, communicated and mined for efficient patient care provisioning, fresh forms of risk to security and privacy of the patient information are becoming evident (Sulaiman & Sharma 2011; Thuraisingham 2009). In domains such as health care, there is a need to share privacy-sensitive data among autonomous but cooperating organisations. Shared health care systems are prone to potentially serious privacy and security risks that may come from their use or misuse. These systems make it possible, and in some cases too easy, for people to share personal data (i.e., inadvertent sharing of sensitive information) (Sulaiman & Sharma 2011). Although security is a paramount concern in any networked systems, the need for privacy, confidentiality and security protection takes on new meanings in health care information systems. Also, health care information systems operate within a strict regulatory framework that is enforced to ensure the protection of personal data against processing and outlines conditions and rules in which processing is allowed. Therefore, middleware systems that facilitate clinical data sharing must abide by the strictest conditions of confidentiality that not only meet but also often exceed approved privacy standards and regulations. Securely transferring data between different parts of a health care system is one of the biggest single problems in health care information systems (Al-Nayadi & Abawajy 2007b; Gail-Joon et al. 2003).

In medical practices patient shares sensitive information so they need trust and have honour their confidentiality. Patient trust their health information to keep secure and private and will discuss on more on conditions, symptoms and present and past behaviour. Trust is the business asset and help the patient to request to business records, carefully handling health information to protect the privacy and keep the patient information as accurate as possible (Park, 2012). Facilitate the electronic exchange of patient information and generating electronic records for patient request. The health accountability and health insurance portability is important for storing information. It
ensures the security and privacy of health information including information in EHR it is the key to build trust and requires to realize the potential benefit of EHR. The individual and participants in network lack trust in the exchange of electronic information. Security risk is identified by examining and identifying the potential vulnerabilities and potential threats to protect health information in medical practices. Implement changes to make the patient health information more secure and monitoring the results.

Securing data sharing applications is challenging due to their open and autonomous nature. Unreliable evidences from recent years advocate lack of satisfactory security procedures has caused in various data violations. Due to this, the patients are exposed to economic threats, and mental distress (HealthPrivacyProject 2007). A recent study conducted in the USA implies that 75% of patients are worried about health related websites sharing their personal information without their consent (Raman 2007). Perhaps this is considered as the second highest reported breach since medical data disclosure (Hasan & Yurcik 2006).

Informational privacy is troubled with the restrictions on access to personal information, which include; “confidentiality, anonymity and confidentiality” are branches of it (Brown & Kosa 2008; Thatcher & Clemons 2000). Confidentiality denotes “trust in private and in professional relationships between individuals”. Privacy or secrecy “refers to a state of blocked or limited access to data that identifies persons”. The protection of privacy by professionals is very important to the faith in the profession, for instance, to the public who trust in physicians, lawyers or members of the clergy (Lunshof et al. 2008).

In general, confidentiality can be violated by several reasons that are beyond either individual or institutional control, for example “accidental data release, data release that is required by authorities, or by criminal offences, including burglary, hacking, and hardware and/or data theft”. Privacy violation can produce substantial material and irrelevant harm to social position and opportunities, to individual and family status, and to self-image and insight by others.
Nevertheless, one should not relate privacy infringement to moral failure. Subjective evidence suggests that internal factors, but not the external ones are major threats to patients privacy (Rubenstein 2008).

Policy-related management for combined health care systems have recently become popular because of stringent privacy and disclosure rules. Although the work on privacy rules and implementation tools, such as Hippocratic databases, has improved our perception of designing privacy-preserving strategies for health care databases and the requirement to combine these strategies in practical health care structure is becoming significant. Furthermore, though most work in this extent has been organization-oriented, dealing with transfer of information in personal health care information management have so far not been satisfactorily adopted. These deficiencies occur due to the following:

- Integration of privacy and disclosure policies with well-known health care standards used in the industry, and
- Establishment of global health care services to patients using the same infrastructure that permits united health care management for organizations.

For effective health care delivery, privacy plays a significant role between patients – physician relationship. Patients are needed to share information with their physicians to ease correct diagnosis of treatment, particularly to circumvent hostile drug interactions. However, in many cases patients may refuse to reveal significant information in terms of severe health problems such as Human Immunodeficiency Virus (HIV) and psychiatric behaviour. They also feel that the disclosure of information might lead to social humiliation and perception (Applebaum 2002).

Over the period, a patient’s medical record adds significant personal information including “personal identification, history of medical diagnosis, medical images, treatment received, medication history, sexual preference, genetic information, employment and income details, and physicians particular evaluations of personal information” (Mercuri 2004).
Therefore, sharing highly confidential information and privacy-sensitive data is extremely challenging. Mechanisms by which a patient's right to confidentiality and privacy are maintained and respected are an important component of the health care information systems. There is a growing body of research is focused on developing mechanisms to address privacy and security concerns related to health care applications (Hung 2004; Peyton et al. 2007; Raman 2007; Yi, Yongming & Hung 2007). For example, Choudhury and Ray (Chowdhury & Ray 2007) designed a joint management technique for privacy assurance of various stakeholders interacting through internet based functions in the health care service sector. In a more recent study on health care confidentiality, Sankar et al. (Sankar 2003) make four key inferences. They are:

- "Patients strongly believe that their personal information should be shared only with people who are involved in their health care.

- Patients do agree with the necessity of information being shared among physicians; however, HIV patients are less likely to agree for sharing of their health information to others.

- Many patients who agree to information sharing among physicians reject the idea of releasing their personal information to third parties including employers and their family members.

- Finally, the majority of patients who have undergone genetic testing believe that patients should take the accountability of revealing their medical test results family members(Sankar 2003).

The broad research assessed in Sankar et al. (Sankar 2003) mainly contemplated the use of recognisable or potentially recognisable information to other relevant bodies including employers, families, and third parties. Conversely, so far only a little research has assessed patients’ perception on sharing of anonymised health records (Bansal, Zahedi & Gefen 2010; Campbell et al. 2007). Lately some research studies reported that user’s current health status,
personal behaviours, culture, and prior experience with websites and online privacy invasions play a major role in user's trust in the health website and their degree of privacy fears. On the other hand, in a mail based survey study conducted with adult patients in UK, Campbell, et al (Campbell et al. 2007), found that about 28% to 35% of patients are neutral to their health information – “for example age, gender, ethnicity, reason for treatment, medical history, personal habits impacting health, type of treatment obtained, side effects of treatment – being used by physicians for other purpose”. Among them, only around 5–21% of patients, nevertheless, expected their physicians to take their permission to use their information. Likewise, only about 10% of the patients expected to be asked for permission if their physicians use their health data for a wide variety of reasons, which comprise merging data with other patients’ data to put forward better information to future patients, sharing how the treatment is working with other physicians in the hospital, training medical professionals, and writing research articles about diseases and treatments. In another study conducted by Angst, et al. (Angst 2006), investigated difference of insight among patients toward different types of personal health record systems, containing “paper based, personal computer based, memory devices, portal and networked PHR”, which are in the increasing order of technological innovation. The study highlighted that patient’s relative insight of judgment and safety fear improved with the level of technology and educated people also favour PHR systems as compared to the other similar systems.

2.12 Chapter Summary

In this chapter we reviewed the literature in data sharing within of health care domain. New E-health applications mainly rely on Internet and Websites for any important information. However, the preserving the security of Web architecture that can ensure the privacy and security of sensitive health care data is still an open question. Current solutions to this problem mostly
use static RBAC models for solution, which is mainly an application-dependent and do not address the intricate security requirements of health care applications. Health care identifies the consequences and strategies that maximise the health care information. The continuous focus on patient information with the health care provider is the main aim of the e-health care system (Rau, 2013). The privacy and security of the information of the patient through EHR is the best new technology nowadays. Health information is characterized by the information with significant barrier to effective sharing the information in between health care participants. The e-health strategy is commended as the useful guide to next steps in e-health. The e-health is pragmatic; it balances different priority and help to delivery safer, improved sustainable health care system. The ultimate advantage achieved from the e-health strategy is safer and sustainable health system that are equipped to responds to rising health sector costs and demand pressure. The strategy provides sufficient elasticity to individual jurisdictions, and private and public health sectors, determine how they would go about e-health functioning within the common framework and sets of priorities that to maximise efficiencies and benefits. E-health initiatives and patient action introduce portal to access information in EHR and for non-urgent communications with maintaining personal health records, journal of health, clinicians, using monitoring device to manage personal health, telephone, written communication in electronic communication and use of internet based methods such as information, advice, health education and peer support. Number of studies are performed for the purpose of enhancing the expected benefits of improving collaboration such as better decision makings, greater patients knowledge of the conditions and treatments, superior communication, more effective self-care, reduced health care cost, and better health outcome (Smith and Thorner, 2012). Health care provider promotes the use of e-health resources with the increase in the engagement of families and individual collaborating with health care provider to provide the health care system.
The health care industry necessitates flexible, on-demand certification, extensible context-aware access control, and dynamic authorization enforcement. With on-demand certification, users are validated according to their task-specific circumstances. Extensible context-aware access control allows administrators to identify more detailed and clear authorization policies for any application. Dynamic authorization implementation makes authorization judgements based upon runtime factors rather than simply the role of the user (Hu & Weaver 2004a). The literature shows that there is a need for a framework that allows the health care providers to share data for efficient provision of care to their patients and improve the health care management. Although there are many approaches, we identified that several important issues remain open. Specifically, there is still a need to answer:

- How to dynamically exchange electronic health record (EHR) information among disparate health care service providers
- How to ensure that access to the patient records is provided to the authorized person only? We will address some of the answers related to this in Chapter 3 and 4, and
- How to ensure data privacy concerns when data is shared between multiple health care organizations? We will address some of the answers related to this in Chapter 3 and 4.

The authentication framework and authorization policy management will be discussed into later chapters.
Chapter 3

Conceptual Framework for Dynamic Data Sharing

3.1 Introduction

The incorporation of information sources detained by distinct parties, either for security or efficiency reasons, is becoming of great interest. An important issue in this setting is the definition of mechanisms for the integration that correctly fulfill the commercial and corporate policies of the organization, which own the information. Since communication between physicians becomes more important and the reaction to the clinical inquest is becoming the important matter, the usage of information anywhere at any time in a clinical setting is regarded as an important phase health care quality. Hence, there is a need for an effective and ubiquitous health care system, which improves quality of life of patients and also makes it feasible for physicians to treat their patients, is essential.

This thesis proposes a typical conceptual model for search and access to clinical data across health care organizations. The proposed model uses three major technologies. They are: “peer-to-peer (P2P), mobile agents and ontology”. The main objective of this framework is to deliver a universal and collaborative medical care scheme to support medical physicians’ in best decision making, hence refining the medical system’s accessibility to the community. Hence, we propose a novel ontology based software agent and P2P networking prototype to deliver an adaptable and vigorous collection of data across any arrangement of the contributing heterogeneous data sources to increase knowledge sharing. Following sections explains the conceptual model using P2P system. Apart from this, the concept of virtual health care system, mobile agents, and data sharing policy and Ontological systems will be investigated. Finally,
the developed prototype for the proposed conceptual framework is demonstrated, analyzed and tested into chapter 8, the sampled databases were provided for two clinical and one-hospital databases.

3.2 Virtual Healthcare System

In this section, we present the theoretical outline of the virtual medical information systems. In typical client–server architecture, clients share only their demands with the system, but not their resources. Hence, as more clients join the system, fewer resources are available to serve each client, and if the central server fails, the entire network is taken down. One of the solution for this could be using the decentralized P2P networks, which increases robustness because it removes the single point of failure that can be inherent in a client-server based system (Buchegger & Datta 2009; Koutsopoulos, Tassiulas & Gkatzikis 2009). Securing P2P data sharing applications is challenging due to their open and autonomous nature (Deen 2005; Watanabe & Numao 2002). Compared to a client-server system in which servers can be relied upon or trusted to always follow protocols, peers in a P2P system may provide no such guarantee. The environment in which a peer must function is a hostile one in which any peer is welcome to join the network; these peers cannot necessarily be trusted to route queries or responses correctly, store documents when asked to, or serve documents when requested (Byeong-Thaek, Sang-Bong & Park 2008; Xi & Shiguo 2009). In P2P network, it is wise to trust a single centralized service, rather than to trust any multitude of anonymous resource-providers in the whole P2P network. Hence, it is essential to identify the authenticity of the resources offered by other peers. (Campadello 2004; Johnson, McGuire & Willey 2008; Schafer, Malinka & Hanacek 2008).
Figure 3.1 shows the conceptual design of virtual medical information system architecture. The goal is to provide a solution for patient information search on a community of autonomous health care units and provide ubiquitous information access to physicians and health care professionals in a variety of situations. Towards this objective, the proposed virtual health care framework decisively marries ontology-based agent paradigm and P2P network technologies for the retrieval of information residing in health care information systems.

There are $P = [P_1, P_2, \ldots, P_N]$ data sources called peers, which participate in data sharing by clustering themselves into interest groups and establishing pair-wise associates between them. Peer-to-peer (P2P) architectures allow for loosely coupled integration of information services while agents will enable sharing of information transparently. Moreover, P2P communication architecture provides scalability and facilitates the discovery of other mediators.

Since peer’s databases have numerous database designs and implementation structures, thus to simulate the reality, we assume that, there are differences in the way patients’ information is represented both at the schema and at the data instance level for the peer
databases. Each health care provider operates autonomously within peer group. Peers can join or leave the network at their own discretion. Moreover, a peer may form an associate with another peer, for data sharing purposes. When peers become acquainted, local ontologies necessary to allow data sharing are exchanged automatically. Note that each health care provider containing medical information is autonomous and controls entirely its data. This model preserves the independence of the different health care providers while at the same time creates the possibility for sharing of medical information.

In this thesis, we use an agent for each data set maintained by a given peer. The agents reside on the doctor’s computer (desktop or portable computer) and are empowered to search for information, retrieving data from the underlying data repository as well as presents the data to the overall system for merging, and provide the ability to dynamically form composite ontologies from the metadata sources. In this way, the cost of developing these ontologies is reduced while providing the broadest possible access to available data sources. All the interaction between the peers in the system occurs through agents. Agents are programs that can migrate from host to host in a network, at times and to places of their own choosing. Mobile agents have the advantages on reducing network load and overcoming network latency. Also, they can encapsulate protocols, work remotely, asynchronously and even disconnected from a network. Also, a great number of agent platforms are deployed for accessing databases (Amin, Kamal & Ahmed 2007). Sharing medical information between different health care providers has the potential to work because both sides of the partnership benefit. However, since these providers handle extremely important private data (e.g. a patient’s health data) they may be reluctant to share their problems, data, etc. Using certificates to request and encrypt messages between the agents mitigates this panic. Certificate Authority (CA) issues a certificate to subjects and provides system validation and authentication functions to users and devices.
3.2.1 Medical Data Ontology

Since medical information systems today store clinical information about patients in all kinds of proprietary formats, this leads to the interoperability problem. Figure 3.2, shows a sample of differences in the way patients’ information is represented both at the schema and at the data instance level in the databases. This representational discrepancy raises the need for some way of mapping one schema to another. To address this problem, ontologies are used. Ontology is conceptualized as a domain of interest and it stipulates a set of limitations that declare what should essentially hold in any possible world.(Wang & Zhao 2007). In general, Ontologies are used to identify what “is” or “can be” in the world and is representation of the semantics of information exchange. Ontology can be composed in two ways, domain dependent and generic way. Particularly in the area of artificial intelligence, ontologies are being used to simplify knowledge sharing and reuse. Ontology is a specification of an abstract, simplified view of the world that we wish to represent for some purpose. Hence, ontology defines a set of representational terms that we call concepts. Inter-relationships among these concepts describe a target world. (Wang & Zhao 2007).

![Figure 3.2: Agents used to build ontologies](image-url)
We use two types of ontologies: Local ontology and Composite ontology. Local ontology indexes data concepts with their contextual aspects in form of properties according to their domain of application. It is assumed that data owners create local ontology (i.e., health providers). Local ontology is composed of local data concepts and master data concepts as shown in Figure 3.2. We used a simple system that specifies data concepts by defining the equivalence relations between a data owner’s local data concepts and other participating data concepts. For example, as shown in Figure 3.2, the data set of the Dire Clinic provides a simple list of data elements. The first column is labelled Local and the second column is labelled Master. Together they represent a simple ontology, i.e., a specification of the data concepts represented by a mapping from the Local to the Master data concept list. Next, we incorporate data from Wassim clinic in the same manner as just described.

In contrast, the composite ontology is a union of the data concepts across all participating data sets, and a given data set’s ontology is a mapping specifying the relationships between the intersection of that data set’s local data concepts and the master data concepts. In order to construct composite ontologies for Wassim Clinic data set, the data agent looked at Dire Clinic’s ontology mapping. Each data concept in a local data list was mapped to the same concept in the Master. If Wassim Clinic had data that was not in the Master, a new entry was added to the Master. Conversely, if a data concept in the Master was not present in the local ontology then there was no mapping established from Wassim Clinic’s Local to the Master. In the end, the system consists of three ontologies: (1) composite, (2) Dire Clinic Local Ontology, and (3) Wassim Clinic Local Ontology. This process continues for each new data set. Each new data owner uses the previous work to help determine their ontology as a specification of the mapping from their Local to the Master data concepts list (Al-Nayadi & Abawajy 2007b; Al-Naydi, Abbawajy & Ders 2007). Relationships among a selection of the local data sets’ ontologies can be determined using the composite ontology as a point of common reference. It is interesting to
note that ontology for the entire system is distributed across the ontology mappings of the individual data sets and the Master. For example, Dire Clinic data set “Last Name” specifies the same concept as Wassim Clinic data set “Surname” but this cannot be directly determined at one centralized point; rather it is determined via the data set ontologies and the composite ontology.

In the conceptual model shown in Figure 3.1, every health information system is represented as an autonomous peer. Peers belong to interest groups, such as physicians or medical laboratories. When peers become acquainted, logical metadata necessary to allow data sharing are exchanged automatically. These metadata take the form of mappings, both at the data level and schema level, and they help to bridge semantic and syntactic heterogeneities between peers. Note that peers are not obliged to adhere strictly to a globally agreed ontology provided by a central mediator (the bottleneck of the centralized integration systems); rather they could develop their own local ontologies. The only requirement is that they must relate their local ontologies’ concepts to those belonging to their neighbors. Data sharing is achieved by initiating a request for the data through the local agent. The agents’ use distributed local ontology and composite ontology to provide the functionality of a centralized ontology along with the ability to be flexible in meeting the varied needs of the users.

To use the system, a doctor first brings up the graphical user interface (GUI) and invokes the local data agent (LDA) for a list of available agents in the peer group. The LDA then checks the list of agents that are registered, and verifies the availability of each. This agent then reports the availability to the GUI Agent, who displays the available data sources to the user. The user then selects the desired data sources and the software agents dynamically create a merged ontology for the selected data sources. To create this merged ontology, the agent sequentially distributes the Master concepts to the LDA chosen by the user. The first LDA compares this concept list to his local ontology, and deletes from this list the data concepts that are not found (i.e., the data concepts that are not in the local ontology). The LDAs then hands the reduced
data concept list back to the requesting LDA who then passes the reduced list to the next LDA selected by the user. This process continues for each of the user-selected agents until all have seen the list. The final reduced data concepts list, in conjunction with each participating data agent’s ontology, constitutes a shared ontology across the participating data sets. This ontology is dynamically generated based on a request from a user, and is evaluated against the latest information from each local data source. Participating agents can each understand and provide information about all the data concepts that are shared across the participating systems, which significantly increase the capability of current ontologies producing results in much the same way a group of collaborating humans would have done, but significantly faster, and with far greater accuracy (Al-Nayadi & Abawajy 2007a; Al-Nayadi & Abawajy 2007b). The proposed system architecture is declared thoroughly in Appendix A.

3.2.2 User Authentication Framework

The proposed protocol supports the issuing and management of digital certificates which identify and authenticate authorized each user using (CA1 & CA2). When a certificate authority issues an identity certificate, it binds a particular assigned certificate to the name of the entity identified in the certificate (name of entity & name of a doctor). Since the certificate has an expiration date, then the validation date should be checked periodically. The certificate always includes the digital signature of the issuing certificate authority (Name of Certificate, signed by whom, date and time of signature). The proposed framework uses an Attribute Certificate (AC). Attribute Certificates are able to support and implement a significant part of the authorization process. For example, information about a user's current role (e.g. physician) or a client's ability to pay for a resource access may be more important than the client's identity. ACA issues attribute certificate that contains authorized person’s attribute and binds to one of key certificate. It also
verifies the validity of attribute certificate as well as revokes attribute certificate in case of the
attribute is changed or is lost.

Figure 3.3: Authentication protocol

Figure 3.3 shows the authentication protocol. A doctor first brings up the GUI and invokes
the local data agent (LDA) for a list of available agents in the peer group. The LDA then checks
the list of agents that are registered, and verifies the availability of each. This agent then reports
the availability to the GUI Agent, who displays the available data sources to the user. The user
then selects the desired data sources and the software agents dynamically create a merged
ontology for the selected data sources. To create this merged ontology, the agent sequentially
distributes the Master concepts to the LDA chosen by the user. The first LDA compares this
concept list to his local ontology, and deletes from this list the data concepts that are not found
(i.e., the data concepts that are not in the local ontology). The LDAs then hands the reduced data
concept list back to the requesting LDA who then passes the reduced list to the next LDA selected
by the user. This process continues for each of the user-selected agents until all have seen the
list. The final reduced data concepts list, in conjunction with each participating data agent’s
ontology, constitutes a shared ontology across the participating data sets. This ontology is
dynamically generated based on a request from a user, and is evaluated against the latest information from each local data source. Participating agents can each understand and provide information about all the data concepts that are shared across the participating systems, which significantly increase the capability of current ontologies producing results in much the same way a group of collaborating humans would have done, but significantly faster, and with far greater accuracy.

3.3 Conceptual Framework Implementation

Developing a sophisticated interface for the proposed system is beyond the scope of this study. Therefore, a simple graphical user interface was developed to allow the user to interact with the system and retrieve sampled patient data from one or more agent(s). The developed prototype has two operational modules: user and administrator. User module is developed mainly for the inquirer agents while the administrator module designed to taking care for all central meta-data catalogue details.

3.3.1 Healthcare Database Peering

Figure 3.4 and Figure 3.5 show the interface for enabling healthcare database peering. In Figure 3.4, we show how a new peer is registered whereas peer management is shown in Figure 3.5.
3.3.2 Ontologies

Figure 3.6 shows the data store for the global and local ontologies. These databases store the master ontology and local ontologies schemas, below is the database diagram for the ontologies.
database. The following Assumption have been considered in designing and development of ontology. Peers are not obliged to adhere strictly to a globally agreed ontology provided by a central mediator; rather they could develop their own local ontologies. The only requirement is that they must relate their local ontologies’ concepts to those belonging to their neighbors. Peers belong to interest groups, such as physicians or medical laboratories. Logical metadata necessary to allow data sharing are exchanged automatically. These metadata take the form of mappings, both at the data level and schema level, and they help to bridge semantic and syntactic heterogeneities between peers. If a clinic had data that was not in the Master, a new entry was added to the Master. Conversely, if a data concept in the Master was not present in the local ontology then there was no mapping established from that clinic’s Local to the Master. Use two types of ontologies: Local ontology and Composite ontology. Local ontology indexes data concepts with their contextual aspects in form of properties according to their domain of application. It is assumed that local ontology is built by the data owners (i.e., health providers). Local ontology is composed of local data concepts and master data concepts. Using a simple system that specifies data concepts by defining the equivalence relations between a data owner’s local data concepts and other participating data concepts.

The composite ontology is a union of the data concepts across all participating data sets, and a given data set’s ontology is a mapping specifying the relationships between the intersection of that data set’s local data concepts and the master data concepts. In order to construct composite ontologies for X Clinic data set, the data agent looked at Y Clinic’s ontology mapping. Each data concept in a local data list was mapped to the same concept in the Master. If X Clinic had data that was not in the Master, a new entry was added to the Master. Conversely, if a data concept in the Master was not present in the local ontology then there was no mapping established from Y Clinic’s Local to the Master. In the end, the system consists of three
ontologies: (1) composite, (2) Y Clinic Local Ontology, and (3) X Clinic Local Ontology. This process continues for each new data set.

Each new data owner uses the previous work to help determine their ontology as a specification of the mapping from their Local to the Master data concepts list. Relationships among a selection of the local data sets’ ontologies can be determined using the composite ontology as a point of common reference. It is interesting to note that ontology for the entire system is distributed across the ontology mappings of the individual data sets and the Master. For example, X Clinic data set “Last Name” specifies the same concept as Y Hospital data set “Surname” but this cannot be directly determined at one centralized point; rather it is determined via the data set ontologies and the composite ontology. When peers become acquainted, logical metadata necessary to allow data sharing are exchanged automatically. These metadata take the form of mappings, both at the data level and schema level, and they help to bridge semantic and syntactic heterogeneities between peers.

Master ontology in this application is the main map for any query translation in the system. This system uses the master ontology to describe the patient information schema and to map it between the different peer’s schemas. The master ontology builder page in the application allows

![Peers table columns](image-url)
the admin to define the master ontology for the patient details. From this page we can define the master tables, master fields, master fields values. Below figure 3.7 shows the full master page we used while testing our application.

The admin can add a master table shown below in Figure 3.8. Admin will add the master columns for added table shown below in Figures 3.9 and 3.10. If a column has possible value, the admin can define those possible values.
Local ontology builder is the app page where we admin can map any peer local schema with master schema through the user interface. Figure 3.11 explains how mapping can be done using the user interface.
For each connected peer (clinic or hospital) in the system, the admin will map the local schema to the master ontology through an editor. Below step by step demo will show how the application will be configured with multiple data sources, then queries will be performed and result will be drilled from those different data sources in a satisfactory way.

**Sample local schemas**

In this demo our application will have 3 peers connected with 3 different schemas and data values as below
Data Source 1: Al Noor Hospital

Sample of the Patient table data

Blood Test Table

X-ray Table
Data Source 2: Dire Clinic

Sample of the Patient table data

<table>
<thead>
<tr>
<th>Reg_No</th>
<th>Reg_Date</th>
<th>Patient_Name</th>
<th>Patient_Address</th>
<th>Patient_Gender</th>
<th>Patient_DOB</th>
<th>Patient_M_Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10/25/2015 19:12</td>
<td>ISSA MOHAMMAD T NASSAR</td>
<td>Dubai</td>
<td>M</td>
<td>2/16/1960</td>
<td>Married</td>
</tr>
<tr>
<td>2</td>
<td>1/26/2014 9:58</td>
<td>SHAA ALAM</td>
<td>Dubai</td>
<td>M</td>
<td>4/2/1960</td>
<td>Married</td>
</tr>
<tr>
<td>3</td>
<td>10/8/2015 21:40</td>
<td>MUHAMMAD NOOR</td>
<td>Dubai</td>
<td>M</td>
<td>5/20/1960</td>
<td>Married</td>
</tr>
<tr>
<td>4</td>
<td>1/12/2016 9:24</td>
<td>ZAYNAB SHODEYA</td>
<td>Dubai</td>
<td>F</td>
<td>7/6/1960</td>
<td>Married</td>
</tr>
<tr>
<td>5</td>
<td>10/10/2015 13:44</td>
<td>ABDULLAH NUR</td>
<td>Al Ain</td>
<td>M</td>
<td>8/24/1960</td>
<td>Married</td>
</tr>
<tr>
<td>7</td>
<td>9/27/2015 7:13</td>
<td>AHMED ALI ANDUAN</td>
<td>Al Ain</td>
<td>F</td>
<td>8/26/1960</td>
<td>Married</td>
</tr>
<tr>
<td>8</td>
<td>10/14/2015 8:52</td>
<td>FERNANDO JR BERNARDO BAUTISTA</td>
<td>Al Ain</td>
<td>M</td>
<td>8/27/1960</td>
<td>Married</td>
</tr>
<tr>
<td>9</td>
<td>10/13/2015 6:40</td>
<td>BABBAR AFTAB</td>
<td>Al Ain</td>
<td>M</td>
<td>8/28/1960</td>
<td>Married</td>
</tr>
<tr>
<td>10</td>
<td>12/12/2015 9:39</td>
<td>LOVE LEON CASTILLD ESPRITU</td>
<td>Al Ain</td>
<td>F</td>
<td>9/29/1960</td>
<td>Married</td>
</tr>
<tr>
<td>11</td>
<td>10/15/2015 19:00</td>
<td>NORMAN DOGILLO</td>
<td>Al Ain</td>
<td>F</td>
<td>9/30/1960</td>
<td>Married</td>
</tr>
</tbody>
</table>

Sample of the Blood test table data

<table>
<thead>
<tr>
<th>Reg_No</th>
<th>Dag_No</th>
<th>Rx_Reg_No</th>
<th>Test_Name</th>
<th>Results</th>
<th>Abnormal</th>
<th>Blood_Group</th>
<th>Plasma_Rheingilin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>D072</td>
<td>B072141</td>
<td>low</td>
<td>high</td>
<td>normal</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>2</td>
<td>D0192</td>
<td>B002717</td>
<td>low</td>
<td>normal</td>
<td>normal</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>3</td>
<td>D01942</td>
<td>B002214</td>
<td>high</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
</tr>
<tr>
<td>4</td>
<td>D00133</td>
<td>B003311</td>
<td>low</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
</tr>
<tr>
<td>5</td>
<td>D00140</td>
<td>B000411</td>
<td>low</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
</tr>
<tr>
<td>6</td>
<td>D00159</td>
<td>B005511</td>
<td>low</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
</tr>
<tr>
<td>7</td>
<td>D001225</td>
<td>B005321</td>
<td>low</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
</tr>
<tr>
<td>8</td>
<td>D002325</td>
<td>B0022321</td>
<td>low</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
</tr>
<tr>
<td>9</td>
<td>D002413</td>
<td>B002214</td>
<td>low</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
</tr>
<tr>
<td>10</td>
<td>D003542</td>
<td>B0033145</td>
<td>low</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
</tr>
</tbody>
</table>

Urine test table

<table>
<thead>
<tr>
<th>Reg_No</th>
<th>Dag_No</th>
<th>Rx_Reg_No</th>
<th>Test_Name</th>
<th>Appearance</th>
<th>SP_Gravity</th>
<th>Reaction</th>
<th>Albumin</th>
<th>Sugar</th>
<th>URINE_JC_DESCRIP</th>
<th>ICD_CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-16-0911572</td>
<td>CKD (chronic kidney disease)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-15-0917400</td>
<td>AP (pancreatic atrophy)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-15-0918100</td>
<td>ACUTE RESPIRATORY FAILURE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-15-0918200</td>
<td>Strees syndrome</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-15-0918300</td>
<td>ARF (acute kidney injury)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-15-0918400</td>
<td>Chronic kidney disease (CKD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-15-0918500</td>
<td>Chronic kidney disease (CKD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-15-0918600</td>
<td>Chronic kidney disease (CKD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-15-0918700</td>
<td>Chronic kidney disease (CKD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>D00041</td>
<td>Reg47</td>
<td>Light-Yellow</td>
<td>1.00</td>
<td>Negative</td>
<td>02-MU-15-0918800</td>
<td>Chronic kidney disease (CKD)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Data Source 3: Wassim Clinic

Patient table

<table>
<thead>
<tr>
<th>PIDNo</th>
<th>PName</th>
<th>PSurname</th>
<th>PDOB</th>
<th>PAddress</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MARK</td>
<td>GELBOLINGORECONOSE</td>
<td>23/03/1971</td>
<td>Dubai</td>
</tr>
<tr>
<td>2</td>
<td>AHMED</td>
<td>SHAABANELSAYED</td>
<td>27/10/1990</td>
<td>Abu Dhabi</td>
</tr>
<tr>
<td>3</td>
<td>ISSA</td>
<td>MOHAMMADT NASSAR</td>
<td>06/01/1990</td>
<td>Abu Dhabi</td>
</tr>
<tr>
<td>4</td>
<td>MUHAMMAD</td>
<td>SAGHIRKHAN</td>
<td>08/09/1987</td>
<td>Abu Dhabi</td>
</tr>
<tr>
<td>5</td>
<td>SALVADOR</td>
<td>JRD EANO</td>
<td>12/06/1990</td>
<td>Abu Dhabi</td>
</tr>
<tr>
<td>7</td>
<td>ABOOBACKER</td>
<td>A. CHERUTHU</td>
<td>21/10/1989</td>
<td>Abu Dhabi</td>
</tr>
<tr>
<td>8</td>
<td>MAHESH</td>
<td>KCBIRBAHADUR</td>
<td>08/12/1968</td>
<td>Abu Dhabi</td>
</tr>
<tr>
<td>9</td>
<td>MARY</td>
<td>ROSEELEAZARGALVAI</td>
<td>09/11/1992</td>
<td>Abu Dhabi</td>
</tr>
<tr>
<td>10</td>
<td>RENE</td>
<td>LAPIZZAMOR</td>
<td>25/12/1984</td>
<td>Abu Dhabi</td>
</tr>
<tr>
<td>11</td>
<td>SULAIMAN</td>
<td>ABDULMUTHALIF</td>
<td>03/01/1986</td>
<td>Abu Dhabi</td>
</tr>
</tbody>
</table>

Urine Table

<table>
<thead>
<tr>
<th>REG_NO</th>
<th>ACCESSION</th>
<th>NAME</th>
<th>DATE</th>
<th>APPEARANCE</th>
<th>GRAVITY</th>
<th>SUGAR</th>
<th>ICD</th>
<th>URINE_ICD_DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7/1/15776</td>
<td>Do0001</td>
<td>Reg01</td>
<td>2015-11-20</td>
<td>11:00:00.00</td>
<td>Smow</td>
<td>1.01</td>
<td>NULL</td>
</tr>
<tr>
<td>2</td>
<td>98035865</td>
<td>Do0002</td>
<td>Reg02</td>
<td>2015-03-02</td>
<td>08:30:00.00</td>
<td>Light-Yellow</td>
<td>1.04</td>
<td>NULL</td>
</tr>
<tr>
<td>3</td>
<td>98464305</td>
<td>Do0003</td>
<td>Reg03</td>
<td>2015-04-08</td>
<td>08:34:00.00</td>
<td>Dark-Yellow</td>
<td>1.02</td>
<td>Negative</td>
</tr>
<tr>
<td>4</td>
<td>98323486</td>
<td>Do0004</td>
<td>Reg04</td>
<td>2015-04-01</td>
<td>11:10:00.00</td>
<td>Yellow</td>
<td>1.01</td>
<td>Negative</td>
</tr>
<tr>
<td>5</td>
<td>98067081</td>
<td>Do0005</td>
<td>Reg05</td>
<td>2015-03-27</td>
<td>10:30:00.00</td>
<td>Yellow</td>
<td>1.02</td>
<td>Negative</td>
</tr>
<tr>
<td>6</td>
<td>98404195</td>
<td>Do0006</td>
<td>Reg06</td>
<td>2015-03-10</td>
<td>16:20:00.00</td>
<td>Yellow</td>
<td>1.02</td>
<td>Negative</td>
</tr>
<tr>
<td>7</td>
<td>98494830</td>
<td>Do0007</td>
<td>Reg07</td>
<td>2015-08-11</td>
<td>18:29:00.00</td>
<td>Colorless</td>
<td>1</td>
<td>Negative</td>
</tr>
<tr>
<td>8</td>
<td>98954908</td>
<td>Do0008</td>
<td>Reg08</td>
<td>2015-04-31</td>
<td>13:01:00.00</td>
<td>Smow</td>
<td>1</td>
<td>Negative</td>
</tr>
<tr>
<td>9</td>
<td>98677001</td>
<td>Do0009</td>
<td>Reg09</td>
<td>2015-04-18</td>
<td>13:20:00.00</td>
<td>Smow</td>
<td>1</td>
<td>NULL</td>
</tr>
<tr>
<td>10</td>
<td>98770767</td>
<td>Do0010</td>
<td>Reg10</td>
<td>2015-04-15</td>
<td>14:41:00.00</td>
<td>Light-Yellow</td>
<td>1.01</td>
<td>Negative</td>
</tr>
<tr>
<td>11</td>
<td>98847444</td>
<td>Do0011</td>
<td>Reg11</td>
<td>2015-10-31</td>
<td>21:57:00.00</td>
<td>NULL</td>
<td>1.02</td>
<td>Negative</td>
</tr>
</tbody>
</table>

Nabil Hospital Patient table name is Person and data columns are as below

Local mapping for (Nabil Hospital)

<table>
<thead>
<tr>
<th>SSN</th>
<th>Person_F_Name</th>
<th>Person_M_Name</th>
<th>Person_Sure_Name</th>
<th>Sex</th>
<th>Dats_of_Birth</th>
<th>Address</th>
<th>Contact_Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>MOHAMMAD</td>
<td>MIAH</td>
<td></td>
<td>Male</td>
<td>9/6/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>SRINIVAS</td>
<td>ADRUTHI</td>
<td></td>
<td>Female</td>
<td>9/7/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>BERNADETH</td>
<td>LAPUIZ</td>
<td></td>
<td>Male</td>
<td>9/6/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>HANA</td>
<td>ABERA</td>
<td></td>
<td>Female</td>
<td>9/9/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>AMELITA</td>
<td>BURAY</td>
<td></td>
<td>Mofo</td>
<td>9/10/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>SAINUDEEN</td>
<td>KVEETIL</td>
<td></td>
<td>Male</td>
<td>9/11/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>AHMED</td>
<td>ELSAYED</td>
<td>MOHAMMED</td>
<td>Male</td>
<td>9/12/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>GLENDA</td>
<td>SAING</td>
<td></td>
<td>Male</td>
<td>9/13/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>RAFAAQ</td>
<td>RAHMAT</td>
<td>DIN</td>
<td>Female</td>
<td>9/14/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>SAID</td>
<td>YABRAC</td>
<td></td>
<td>Mofo</td>
<td>9/15/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>ABUDUL</td>
<td>KADAR</td>
<td></td>
<td>Female</td>
<td>9/16/1960</td>
<td>Al Ain</td>
<td></td>
</tr>
</tbody>
</table>
Note: as below mapping screen shows some of the fields are left empty because they are not in local schema, this system will accept this mapping even with missing fields.

Local mapping for (Wassim Clinic)
### Local mapping for (Dire Clinic)

<table>
<thead>
<tr>
<th>Reg_No</th>
<th>Reg_Date</th>
<th>Patient_Name</th>
<th>Patient_Address</th>
<th>Patient_Contact</th>
<th>Patient_Gender</th>
<th>Patient_DOB</th>
<th>Patient_M_Sate</th>
</tr>
</thead>
<tbody>
<tr>
<td>101911701</td>
<td>10/25/2015 19-12</td>
<td>ISSA MOHAMMAD T. NASSAR</td>
<td>Dubai</td>
<td>5261117</td>
<td>M</td>
<td>2/16/1960</td>
<td>Married</td>
</tr>
<tr>
<td>106494448</td>
<td>1/20/2016 9-58</td>
<td>SHAH ALAM</td>
<td>Dubai</td>
<td>5261203</td>
<td>M</td>
<td>4/2/1960</td>
<td>Married</td>
</tr>
<tr>
<td>105943542</td>
<td>12/1/2016 8-24</td>
<td>ZAYYAD SHODIEVA</td>
<td>Dubai</td>
<td>5261298</td>
<td>M</td>
<td>7/6/1960</td>
<td>Married</td>
</tr>
<tr>
<td>101483411</td>
<td>10/10/2015 12-44</td>
<td>ABU DUN NUR</td>
<td>N/A</td>
<td>5261347</td>
<td>M</td>
<td>8/24/1960</td>
<td>Married</td>
</tr>
<tr>
<td>101115747</td>
<td>10/7/2015 22:25</td>
<td>DEBENDRA NEUPANEY</td>
<td>N/A</td>
<td>5261349</td>
<td>M</td>
<td>8/28/1960</td>
<td>Married</td>
</tr>
<tr>
<td>100474536</td>
<td>10/7/2015 7:13</td>
<td>AHMED AU ANDUMIN</td>
<td>N/A</td>
<td>5261349</td>
<td>F</td>
<td>8/28/1960</td>
<td>Married</td>
</tr>
<tr>
<td>101335349</td>
<td>10/14/2015 9:52</td>
<td>FERNANDO JR BERNARDO Bautista</td>
<td>N/A</td>
<td>5261350</td>
<td>M</td>
<td>8/27/1960</td>
<td>Married</td>
</tr>
<tr>
<td>101356937</td>
<td>10/13/2015 5:40</td>
<td>BABER ANDAB</td>
<td>N/A</td>
<td>5261351</td>
<td>M</td>
<td>8/28/1960</td>
<td>Married</td>
</tr>
<tr>
<td>101471384</td>
<td>10/12/2015 9:39</td>
<td>LOVE LEAH CASTILLO ESPRITU</td>
<td>N/A</td>
<td>5261352</td>
<td>F</td>
<td>8/28/1960</td>
<td>Married</td>
</tr>
<tr>
<td>101714140</td>
<td>10/19/2015 19:08</td>
<td>NORMAN DOGILLO</td>
<td>N/A</td>
<td>5261353</td>
<td>F</td>
<td>8/28/1960</td>
<td>Married</td>
</tr>
</tbody>
</table>
Local mapping for (Al Noor Hospital)

<table>
<thead>
<tr>
<th>Reg</th>
<th>Reg_Date</th>
<th>Name</th>
<th>Gender</th>
<th>Patient_DOB</th>
<th>Patient_Motirol_State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/9/2016 7:00</td>
<td>Patient 518</td>
<td>Male</td>
<td>6/1/1971</td>
<td>Married</td>
</tr>
<tr>
<td>2</td>
<td>1/9/2016 16:13</td>
<td>Patient 519</td>
<td>Male</td>
<td>6/2/1971</td>
<td>Mamod</td>
</tr>
<tr>
<td>3</td>
<td>1/10/2016 11:48</td>
<td>Patient 520</td>
<td>Male</td>
<td>6/3/1971</td>
<td>Married</td>
</tr>
<tr>
<td>4</td>
<td>1/10/2016 10:15</td>
<td>Patient 521</td>
<td>Female</td>
<td>6/4/1971</td>
<td>Mamod</td>
</tr>
<tr>
<td>5</td>
<td>1/14/2016 21:18</td>
<td>Patient 522</td>
<td>Male</td>
<td>6/5/1971</td>
<td>Married</td>
</tr>
<tr>
<td>6</td>
<td>1/14/2016 11:25</td>
<td>Patient 523</td>
<td>Male</td>
<td>6/6/1971</td>
<td>Married</td>
</tr>
<tr>
<td>7</td>
<td>1/21/2016 10:15</td>
<td>Patient 524</td>
<td>Male</td>
<td>6/7/1971</td>
<td>Momod</td>
</tr>
<tr>
<td>8</td>
<td>1/12/2016 1:19</td>
<td>Patient 525</td>
<td>Male</td>
<td>6/8/1971</td>
<td>Married</td>
</tr>
<tr>
<td>10</td>
<td>1/19/2016 8:33</td>
<td>Patient 527</td>
<td>Male</td>
<td>6/10/1971</td>
<td>Married</td>
</tr>
<tr>
<td>11</td>
<td>1/19/2016 11:38</td>
<td>Patient 528</td>
<td>Male</td>
<td>6/11/1971</td>
<td>Mamod</td>
</tr>
</tbody>
</table>
3.3.2 Authentication

The interaction of health providers with the system are secured through a complex process of authentication and authorization. Each healthcare professional (HP) is assigned a set of specific rights (roles) that governs the permissions needed to accomplish his/her tasks. The use of remote and local user roles with each requiring different authentication mechanisms. Consider that a pathologist has the right to read and write the pathology reports of a patient, but if he/she only asks to read the patient pathology report then the pathologist is only given a read permission.

A pathologist can log on to the system with any identification technology available on his system. An authentication token including the user details and the authentication trust level of identification technology is send to the Authorization module of the system. If the pathologist uses a username and password to log on to the system then he is given a permission only to read, if there exists a policy specification that “a pathologist should need an authentication level of a password to read data and an authentication trust level of a fingerprint to write data”. To write data the pathologist will again have to log on to the system using a fingerprint as the identification technology.

A service provider maintains information about its customers in some internal database with a proprietary schema. Also, we do not consider the use of known identifying information such as a social security number or a combination of name and age, to be a privacy threat in this context because it is typically already known by the types of organizations targeted by our work. Each service provider maintains a private metadata, which is a set of privacy views. Each privacy view defines a set of private attributes, its owner, the tables, and conditional expression. Providers have public keys K and private keys k respectively.

Using certificates to request and encrypt messages between the agents. Certificate Authority (CA) issues a certificate to subjects and provides system validation and authentication functions to users and devices. The CAs ensures proper utilization of the credentials by regularly validating
and revoking them. These CAs ensure that there are no ways for peers to request certificates for other people or multiple certificates for the same peer. There are four certification authorities

- **CA1**: for controlling and certifying membership to the Data sharing community by providing credentials (certificate) to the peers for the purpose of correctly authenticating themselves (peer level). Certificate Authority (CA1) also store detailed information on each peer in the community including the address, phone number business registration number. This information could be used, if need be, to establish the identity of the caller (such as by calling back to a number in the CAs), and to always notify the patient. Below figure 3.12 shows the peers management page in the application

<table>
<thead>
<tr>
<th>PeerID</th>
<th>PeerName</th>
<th>Token</th>
<th>IssueDate</th>
<th>ValidUntil</th>
<th>Automatic Renew</th>
<th>Is Active</th>
<th>Renew</th>
<th>Revoke</th>
<th>Auto</th>
<th>Manual</th>
<th>Edit Attribute Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Al Noor Hospital</td>
<td>56c6a0b-ccdf-46b3-8c3a-7679f3ae7e2</td>
<td>3/20/2016 10:24:49 AM</td>
<td>4/19/2016 10:24:49 AM</td>
<td>no</td>
<td>yes</td>
<td>Renew</td>
<td>Revoke</td>
<td>Auto</td>
<td>Manual</td>
<td>Advanced</td>
</tr>
</tbody>
</table>

Figure 3.12: Peers certificate management

Form this management page the system allows to perform the below actions:

a. Issuing /Renewing peer certificate: a new certificate will be issued to the selected peer with 1-month validity from the issuing date.

b. Revoking peer certificate: current peer certificate will be revoked and peer will have no valid certificates
c. Changing certificate mode between automatic and manual. When peer certificate is configured with manual mode if the certificate expires peer users will not be able to login to the system and they will receive invalid certificate message.

When peer certificate is configured with automatic mode if the certificate expires peer users will be able to login to the system and system will automatically issue them a new certificate.

- **CA2**: for representing medical board and responsible for certifying medical doctors (health staff level) in good standing. Below figure 3.13 shows the users (medical board) management page in the application

<table>
<thead>
<tr>
<th>User</th>
<th>Peer</th>
<th>Token</th>
<th>IssueDate</th>
<th>ValidUntil</th>
<th>Automatic Renew</th>
<th>Is Active</th>
<th>Renew</th>
<th>Revoke</th>
<th>Auto</th>
<th>Manual</th>
<th>Edit Attribute Certificate</th>
</tr>
</thead>
</table>

**Figure 3.13: User's certificate management page**

Form this management page the system allows to perform the below actions:

d. Issuing /Renewing user certificate: a new certificate will be issued to the selected peer with 1-month validity from the issuing date.

e. Revoking user certificate: current employee certificate will be revoked and user will have no valid certificates

f. Changing certificate mode between automatic and manual

When user certificate is configured with manual mode if the certificate expires user will not be able to login to the system and they will receive invalid certificate message. When user certificate is configured with automatic mode if the certificate expires user will be able to login to the system and system will automatically issue him a new certificate.
**ACA**: Attribute Certificate Authority - which has a data structure comparable to an identity certificate. Attribute Certificate (AC) contains attributes that specify access control information associated with the AC holder (such as group membership, role, and security clearance. ACA can be assigned to both peers and users, at the end the user Attribute certificate will be the join of both his ACA and his peer ACA as shown in figure 3.14.

Below is screen shot for editing attribute certificate of a user or a peer. Form the above page admin can configure the user/peer ACA by granting him access to only specific tables from the master schema. Admin clicks on advanced button for a specific table to grant access only to specific attributes in the selected table.
<table>
<thead>
<tr>
<th>Table</th>
<th>Allow</th>
<th>Has access</th>
<th>Advanced</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master_Patient_Details</td>
<td>Grant Access</td>
<td>true</td>
<td>Advanced</td>
<td>Filter</td>
</tr>
<tr>
<td>Master_Blood_Test</td>
<td>Grant Access</td>
<td>true</td>
<td>Advanced</td>
<td>Filter</td>
</tr>
<tr>
<td>Master_Diagnosis_Details</td>
<td>Grant Access</td>
<td>true</td>
<td>Advanced</td>
<td>Filter</td>
</tr>
<tr>
<td>Master_X-Ray_Table</td>
<td>Grant Access</td>
<td>true</td>
<td>Advanced</td>
<td>Filter</td>
</tr>
<tr>
<td>Master_Urine_Test</td>
<td>Grant Access</td>
<td>true</td>
<td>Advanced</td>
<td>Filter</td>
</tr>
</tbody>
</table>

Table Advanced Options for Master_Patient_Details:
- **Reg_No**: Grant Access, Has access: true
- **Reg_Date**: Grant Access, Has access: true
- **Patient_Name**: Grant Access, Has access: true
- **Patient_Address**: Grant Access, Has access: true
- **Patient_Contact**: Grant Access, Has access: true
- **Patient_Gender**: Grant Access, Has access: true
- **PatientDOB**: Grant Access, Has access: true
- **Patient_M_Stat**: Grant Access, Has access: true

Save
CCA: Consent Certificate Authority to control access to information content based on personal consent, the role of the information-accessing entity, and the type of information use (for individual). From the table ACA certificate edit page, the admin clicks on the filter button to edit the user CCA certificate for the selected table. The update CCA page allows the admin to build a conditions list to describe the data to be excluded as below screen shot shows: admin can compose a conditions list limiting the user to not see any records which meets the conditions defined by the admin, admin can add as many conditions as needed.

### Update Filter

<table>
<thead>
<tr>
<th>Column</th>
<th>Check</th>
<th>Value</th>
<th>Operand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient_Address</td>
<td>NotEqual to</td>
<td>Dubai</td>
<td>And</td>
</tr>
<tr>
<td>Patient_Gender</td>
<td>NotEqual to</td>
<td>Female</td>
<td>And</td>
</tr>
</tbody>
</table>

[Add] [Save] [Delete and start again]
We now illustrate the login process to use the application as demonstrated in figure 3.15.

When password and user name are correct, the user will be directed to the application home page.

Figure 3.15 login process
However, when user name enters wrong user name or password, a message will appear to the user informing him that the user name or password he typed are wrong as shown in figure 3.16 below. In the case where the user name and password are correct but the user certificate is expired or disabled, the user will receive a message that she/he don’t have a valid certificate. Finally, in the case where the user name and password entered successfully but user peer certificate is expired, the user will receive a message that her/his peer don’t have a valid certificate.

Figure 3.16 Wrong user name or password
3.4 Chapter Summary

In this chapter, we proposed a novel ontology-based software agent and peer-to-peer (P2P) networking paradigm to provide a flexible and dynamic conglomeration of data across any combination of the participating heterogeneous data sources to maximize knowledge sharing. For example, this will allow a family physician to find the results of any lab tests stored in the database of any acquainted specialist physician, pharmacy or medical laboratory. The proposed approach provides a more flexible solution for scalable data sharing, where every plant design management system (PDMS) peer can join easily the sharing environment and contribute new data, then relate them to existing neighbors’ local ontologies, define itself a new local ontology that others can use as a glue to relate their own ontologies to the rest of the network. P2P platform is very risky, because it makes you very susceptible to infection, attack, exposure of personal or company information. Therefore, security and authentication framework is required to address these risks. The next chapter discusses these issues and illustrate an authorization policy management framework for dynamic medical data sharing.
Chapter 4

An Authorization Policy Management

4.1 Introduction

Increasingly, patient care is provided by a team of health professionals from different healthcare organisations. In order to provide better patient experiences when patients are cared for by multiple health professional from different healthcare providers, cross-organisational healthcare data sharing is important. All available information resources should be integrated into a system that will deliver precise information to the proper clinicians at the appropriate time so they can make suitable selections that increase the quality of patient’s care (Staroselsky et al. 2008). Medical data is usually managed by networked computer systems thus, generally speaking, the speed in which electronic health records (EHR) adopted by healthcare organisations is phenomenal. In general, EHR flexibility and functionality can facilitate access of the patient data can be accessed independent of location and time. This fits well with distributed organizations since data can be easily transmitted within and across health businesses electronically.

Patient data protection is driven by a wide variety of concerns such as legal, regulatory, reputation, financial and other requirements. Generally patient data are required to be protected by law or statute (e.g., HIPAA) and if released to unauthorized individuals could expose the healthcare providers to legal or financial obligations. Therefore, access request authorization management is a fundamental problem in multi-domain collaborative environments. Although, the need for sharing patient data by authorized healthcare providers is evident, issues such as complexity involved in setting up collaborative health data sharing, the security and the
necessity to protect privacy of the patients have been the main barriers for cross-organisational patient data sharing.

Generally, a healthcare domain is very complex environment and integrating many autonomous healthcare systems for the purpose of sharing patient data further complicates the system. However, recent advances in information technology and networking has greatly facilitated efforts in developing technologies that can possibly integrate these disparate systems to enable seamless and dynamic collaborations among the healthcare providers. With advances in technology come advanced cybersecurity attacks. As a result, security concerns become another chief barrier that prevent widespread adoption of medical data sharing. Also, regulatory requirements from organisations such as HIPAA emphasis privacy and security concerns on patients’ medical records and breach can lead to hefty fines as well as erosion of reputations. Therefore, much attention of confidentiality and security of the electronic health records (EHR) systems.

In this chapter, we address the problem of authorization policy for inter-domain collaboration purposes with emphases on healthcare environment. This problem is important since authorization policy is a central component of the access control mechanism. Although, authorization policies in cooperative settings have started attracting the attention of the research community, it has generally remained “an area that has not seen many developments (Daiqin-He and Yang, 2009).” This thesis contributes towards these efforts by proposing a policy-based collaborative authorization management (PCAM) framework to facilitate dynamic patient data sharing between different healthcare providers in a secure manner. The proposed framework is based on logical integration of the cooperating partners’ authorization policies to enables the collaborating healthcare providers manage authorization control.
4.2 Distributed Healthcare Provider Community Framework

In this thesis, we address the problem of dynamic healthcare data sharing in a distributed setup. In this setup, the data sharing partners (e.g., family physicians, hospitals, medical laboratories, and pharmacists) form peer-to-peer collaboration to share patient information about diagnosis, treatments and medications.

Figure 4.1 depicts the conceptual framework of the proposed distributed data sharing framework in which various healthcare providers that are willing to share patient information. We refer to this infrastructure as distributed health care provider community (DHPC). Each health care provider in DHPC operates autonomously within distinct domain and has different health care
information systems to support local patient care. Basic characteristics of the DHPC consists of the following layers:

a. users layer that grants access to patient data through a secure physical network;

b. middleware service layer that verifies users access privileges; and

c. authentication policy layer that specify the rules of engagement.

In DHPC, each health care system maintains a patient database along with policy, reputation on other peers and credential information. The patient database maintains patient personal data (i.e., about diagnosis, treatments, medications, etc.). As the custodian of patient information, each health care provider is responsible for protecting patient information in patient database against unauthorized use. Although the P2P research area might appear promising and exciting, series of measures based on trust and security must be implemented to each peer to establish a secure connection and computing for each distributed network setting. In order to implement those measures, first of all, the connection between peers must be safe and secure, which need at least the capability of each peer to recognise the other participant in the network connection. Secondly, the sensitive information, which is exchanged or managed via network, must be protected. The security and trust properties are established and managed by various methods such as authentication of peers communicating with each other or with any other individuals involved in the P2P application. Also, authorization of certain individuals to carry out certain tasks or access some data, encryption of sensitive information flowing between peers over an unsecured network (Guo Xiao, Zhao Zhi & Guo 2010; Li & ZhaoJian 2009). In order to maintain consistence with standard security practices, we assume a “closed” policy, where data can be made available to only to individuals explicitly authorized for that. Hence, data items in all related systems may be authorized to view part of the contents of sharable health care data. We consider authorizations in a simple, yet authoritative form, stipulating visibility of data sharing permissions for subjects
to view certain schema sections. The healthcare provider that collected the data from the patients is considered the data custodian. Therefore, the data custodian is responsible to ensure the following:

1) protect patient data from unauthorized access,

2) observe and check the legitimate use of the patient data, and

3) make sure that legitimate users observe the community rules and agreements.

In order to address these problems, we have proposed a data sharing brokerage and policy as shown in Figure 4.1. Since our focus in this thesis is on facilitating access to already existing patient data, we do not address issues related to the standardization. For example, we assume that the healthcare providers use standardized data exchange messaging protocol to support communications among themselves. Many standards such as HL7 have been developed for data and message exchange between different healthcare providers. We also assume that when a healthcare provider accesses data from another healthcare provider, the receiving healthcare provider of the patient data is ultimately accountable for maintaining the confidentiality, integrity and availability of the shared data. To this end, we assume that all the healthcare providers understand their responsibilities and have in place appropriate information security controls.

### 4.2.1 Access Credentials

A data sharing request is accompanied by the requester’s credentials. According to Bakker (2004), in a request to an information system that possibly holds data for a certain patient; the following elements should be indicated:

- “**The identity of the patient.**

- **The date and time when the data are requested.**

- **The identity and qualifications of the health professional who is asking for the data.**
The role of the health care professional.

In order to properly utilize credentials, mechanisms must be in place to issue, validate, and revoke them. In a service-oriented setting, these mechanisms are provided by specialized services (Kai & Qianni 2006; Li & ZhaoJian 2009). The proposed framework considers use of several certification authorities for the purpose of facilitating credentials (e.g., CA1) in the system (also known as certificate, tokens, or assertions) to the peers for the purpose of correctly authenticating themselves with. We assume that the CAs also store detailed information on each peer in the community including the address, phone number business registration number etc. This information could be used, if need be, to establish the identity of the caller (such as by calling back to a number in the CAs), and to always notify the patient. The CAs also ensures proper utilization of the credentials by regularly validating and revoking them.

4.2.2 Membership Maintenance

Note that the peer-to-peer architecture used to realize the distributed healthcare provider community implies that all parties in the community have equal since all parties are potential providers and consumers of the patient data. As none of the community member possesses dominating position in the community, one possible way to increase the trustworthiness of the collaboration environment is to limit the membership in the distributed health care provider community (DHPC) to trustworthy people. While the set of criteria for admission and removal can be arbitrarily complex, the sensitive nature of the information to be shared dictates three fundamental concerns for DHPC community (Blobel 2001; Istepanian 2005; Weiwei et al. 2007):

(i) members should be physicians,

(ii) members should have some level of trust in each other, and

(iii) if a member misbehaves, it must be possible to revoke its membership.
There has been support for healthcare data sharing by authorized individuals from various sectors including healthcare regulatory bodies and public (Daiqin-He and Yang, 2009). However, medical data contains very sensitive and confidential personal data, thus it is important that sharing medical data should be extremely secure and reliable. Due to the sensitive nature of medical information, it is hence important that such data is safeguarded from disclosure except when medical experts need to access patient medical records in order to provide medical care to patients. Hence, privacy, confidentiality and security are considered as essential parameters of the health record and nurturing trust between health care providers and consumers (Acharya 2010; Meingast, Roosta & Sastry 2006b). One of the important issues in this context concerns suitable establishment (i.e., authorization) of EHR access. Also, one of the major criteria for this should be genuineness, meaning that only medical professional going to deliver care to a particular patient should only be permitted to access to the essential medical data of the concerning patient they will be providing care. Another major security issue would be securing, managing and handling transport and storage of personal medical information (Serour 2006).

Since everyone has one or more personal and sensitive medical information, preserving security and privacy of medical data has been major concerns for authorities for the last few decades. Moreover, in the recent past, the manual record keeping systems lacked automatic administration of medical data and medical experts would essentially not be prevented to access random patient information. Hence, the privacy of patients was depending mainly on the decision of each individual medical practitioner and legal administration.

Therefore, DHPC membership is controlled such that a peer will be allowed to join the DHPC community if the peer is a medical doctor as certified by CA2 and the peer either is one of the founders of this community as certified by CA1 or is recommended by at least two current members of HPC community in good standing. Note that certification from CA1 will only be
given to a peer provided that the health care providers system meets or exceeds the state and federal regulations governing the health care industry.

Inappropriate use of the system will be discouraged; by punishing users who misbehave as well as by placing limit on the number of queries individual peer will submit per day. A regular member is removed from this community if three different members vote for the peers’ removal.

We regulate the rate of queries in such a way that every query has a cost, which must be paid for from the budget of the peer presenting it (Blobel 2001; Istepanian 2005; Weiwei et al. 2007).

Each healthcare provider maintains digitally signed membership application that details condition of the membership and regulations for access to health data. We assume that such membership application form is available and we will postpone the format and structure for the future work.

Usually the health care providers don’t have any pre-existing relationship and may reside in different security domains. Therefore, trust is essential if the health information collected is to serve as a complete and accurate foundation. In this context, the reliability of the information to be exchanged is typically critical. However, the reliability of the information cannot always be judged simply by reading it. Moreover, the system could be abused, like representative of drug companies, may have vested interest to provide false treatment advice to promote their drug.

Therefore, building trust relationship between health care providers in a large-scale distributed system is a fundamental and challenging research topic (Alhaqabani & Fidge 2009; Zia 2008).

We used a simple yet general reputation system measure to help members in assessing the reliability of information provided by each other’s. Each peer must maintain a reputation value that summarizes other members’ feedback on the quality of their responses to posted queries.

Further, this reputation must be presented along with every response to a query. Each member of a HPC has a numeric reputation in the range of $MIN$ to $MAX$, which is attached to every query-
hit message so that the person who is making queries can decide whether to trust the answer or not. In the framework, larger numeric reputation values imply greater trust.

The protocol is as follows: (1) each member starts with a reputation of 0 when it first joins the community; (2) whenever a member receives a query-hit message from a peer, it is allowed to rate the quality of the answer given by that peer; (3) this rating can range from -1 to 1 and is simply added to the peer’s reputation; (4) a member is allowed to make only one rating per answering peer per query. Further, this reputation must be presented along with every response to a query.

4.2.3 Authorization Policy

Note that each healthcare provider has its own set of authorization control policies for specific data access requests within and outside the organisation. We assume that request for access to the patient data that originate from the inside is dealt with differently from the requests coming from partner healthcare providers. In this thesis, we will focus on the latter case. Therefore, when a request for a patient data arrives from a partner healthcare provider, the authorization system makes authorization decision based on its own authorization policy and the requester’s access credentials. We assume that the collaborating partner organisations have prior knowledge about each other authorization policies and submit data request in compliance of the data owner’s policy. Typically, a health care provider implements the legislation by authoring a security policy that mandates working practices and security technology requirements. A security policy is a set of rules for authorization, access control, and trust in a certain domain; it can also contain information about some users’ roles and the abilities associated with those roles (Liang et al. 2009; Randeree, Kishore & Rao 2005). For example, health care providers could define privacy policies that state which health care professionals are able to access specific medical data. Figure 4.2 shows the components of security policy in the proposed framework. The policy
captures information such as who can access patient data, for what purpose and how the patient data can be accessed. For example, patient data can only be accessed by healthcare providers (e.g., doctors, nurses, technicians) who are treating the patients.

Controlling the way in which patient data is exchanged between the collaborating healthcare providers is central to the DHPC framework. This is accomplished by the authorization policies, which dictate the conditions under which the collaborating organizations are able to share the patient data. In addition, the policies enable genuine collaborators to have access to the patient data and filter out others who deemed to be not authorized collaborators even if they have appropriate credentials. The policy must ensure compliance to the laws and regulations governing health data protection. Note that each healthcare provider autonomously maintains its authorization policy based on what is important to it. We will not address the challenges of how authorization policies are specified, compared and integrated for the inter-domain collaboration here. This is left for the future work.

### 4.2.3.1 Consent control mechanisms

Continuation-of-care is the main reason that the healthcare providers share patient data among themselves. Thus, an example of authorization policy is the patient consent, which could be used in authorization control and policy evaluation to permit or deny access to the patient data. To this end, the patient consent form one of the main elements in arriving at a decision to permit or deny access to the patient data in the proposed framework. Thus, consent serves another level of trust mechanisms needed to achieve patient data sharing in the proposed framework. Generally speaking, consent can be expressed as an assertion. Patients' consent can be obtained by different ways including informed consent, implied consent, general consent, General denial with specific consent and express consent.
- **Informed consent** means, informed, competent and voluntary consent (Kluge 2004). It is said to obtain when the patient has been given all information that the objective reasonable person in the patient's position would want to know before making a choice. In addition, the patient must have understood the information at a subjective level, must also have understood the likely consequences of any choice that could be made, and must have made the choice in an authentic fashion. The electronic patient record should be treated never as a mere thing but always as a person-analogue in information and decision space”(Kluge 2004).

- **Implied consent** is where agreement may reasonably be informed from the action or inaction of the individual and there is good reason to believe that the patient has knowledge relevant to this agreement”(Win 2005).

- **Express consent** is the consent given explicitly, either orally or in writing. Express consent is equivocal and does not require any influence on the part of provider seeking consent”(Win 2005).

- **General consent** with specific denials refers to an instance in which a patient attaches specific exclusion conditions to the general approval of access to the record for future accesses”(Coiera & Clarke 2004).

- **General denial with specific consent** refers to an instance in which a patient issues a blanket block on all future accesses, but allows the inclusion of future use under specified conditions”(Coiera & Clarke 2004).

Informed consent denotes that patients are completely well versed of the consequences of their health condition, and give voluntary agreement to disclose and authorize access to collect their information (Win 2005). Efficient notice and accurately informed consent necessitates that people know and realize the matters that are mentioned in the record (Win & Fulcher 2007). In some cases, healthcare providers may release data without an explicit consent from the patient. In this cases, the consent is implied unless the patients specifically withdraw their
consent. It is immoral to use implicit consensus when the patient is not completely understood or aware of data disclosure. According to Win (2005), health record should not be managed in the absence of explicit agreement unless they are needed for medical purposes or undertaken by a professional who, in the circumstances, owes a duty of privacy. The above information assumes the patient is knowledgeable; however, not all patients belong to this class. Some are ineffectual, and even there are many sub-categories, for example children, and the patients who previously were skilled, etc. A principled security structure should contain tests for proficiency in its protocols and it should involve suitable auxiliary consensus or agreement (Kluge 2004).

4.2.4 Authorization Brokerages

The realization of the DHPC depends on the availability of the middleware mechanisms with the capability to provide integrated access to the required patient data on demand. In this thesis, we propose a policy driven authorization brokerage for governing medical data sharing in decentralized manners. Generally speaking, the purpose of such a policy driven authorization brokerage is

(a) to provide an effective coordination between members of the community, and

(b) to ensure the security of community members, and information they share with each other. To achieve these purposes, the authorization brokerage might impose constraints on both the membership of the community and on the behaviour of its members when they are interacting with each other—all these in a highly application dependent manner. When a healthcare provider receives a request for patient data from another healthcare provider, the request is passed to the security brokerage first, where the request is analysed to determine its validity. Note that the normal access request within the same organization does not involve the authorization brokerage. Only inter-domain access requests will be passed to the authorization brokerage for
processing it according to the authorization policy. The authorization brokerage has a number of components discussed in the following subsections.

4.2.4.1 Access control

The health care providers (i.e., peer) join DHPC community with the objectives to be able to share and have access to remote data obtained from other physicians’ database, pharmacies, and drug reference databases to offer the best possible care for their patients. For instance, in Figure 4.1 above, membership to the DHPC data sharing community is controlled and certified by CA1 certification authority. In designed system, membership to the data sharing community is controlled and certified by CA1 certification authority while the second certification authority (CA2) represents the medical board and responsible for certifying medical physicians in good standing. By using multiple CAs we could ensure that there are no ways for peers to request certificates for unauthorized people or multiple certificates for the same peer. Once a submitted certificate is verified, its validity is to be monitored as follows: certificates issued by CA1 are to be checked for validity every day, while certificates issued by CA2 (basing on user role) should be checked every 30 days. This difference in frequencies reflects different expectation about the stability of the certificates issued by the two authorities.

4.2.4.2 Reputation Management

In accordance with general medical rules, ethics and due to the private nature of medical data, access to the medical information should depend on the basis of need to know and legality. In other words, the medical data of patients should only need to be disclosed to medical expert, who has genuine need to access the medical information of a particular patient, in order to offer proper medical support to that patient. Hence, proper measured need to take to restrict the accessibility of data in accordance with the “need- to know”-principle. The large amounts of
medical data are universally reachable due to computerized data management and networking foster important requirements concerning the well-being and confidentiality of medical data and privacy of patients. This chapter discusses pertinent security and privacy features that are examined in this thesis, and also presenting a proposed authorization policy management framework to enable resource sharing between multiple heterogeneous health care enterprises via P2P communication environment.

4.3 Policy-based Collaborative Authorization Management

Framework

In this section, we will describe the functionality provided by the DHPC to enable the collaborating healthcare providers how to share their patient data with each other. Healthcare is by nature a dynamic environment and any collaborative efforts by autonomous healthcare entities such as data sharing is fully distributed. Also, the participating healthcare providers maintain their resources exclusively. They also have specific authorization policies that is tailed to its own needs. Moreover, the participating healthcare providers can join and leave the collaboration community at any time. These characteristics of healthcare environment makes the realization of the DHPC to depend on the availability of the middleware mechanisms with the capability to provide integrated access to the required patient data on demand. In this section, we discuss the various components of the authorization policy and brokerage middleware for governing medical data sharing in decentralized environments.
Figure 4.2 shows a scenario in which two healthcare providers collaborate in data exchange process. In the scenario, the Dire Clinic wants to access a patient data that is provided by Nabil Hospital. There are two possible ways for Dire Clinic (i.e. client) to find a partner that provides required data. The first approach is to ask the patient about where the patient has been treated before. The second option is to push the request to the community and obtain the list of the healthcare providers that maintain data on the patient. In this case, the receiver of the request may also send the request to another group on behave of the requester provided that it is belong to several communities. The third approach is to use centralised entities such as a trust third party that maintains visiting records of the patients. Patient history discovery is another area that has been adjourned for future work. The data is sent to the requesting partner through secure protocols, such as WS-Security and WS-SecureConversation.

Note that each healthcare provider is restricted to make certain number of queries per day to a specific partner. This is mainly to avoid denial of service attack problem. If the request receiving healthcare provider maintains the required data, it checks to see the requester's credentials are
valid before making the authorization decision according to its own authorization policy. Therefore, an authorization control requires determining:

1. the requester is a member of the DHPC community,
2. How many queries have been posted by this requester?

Even though Figure 4.2 is a simplified version of collaborative environment among the healthcare provider, we note that such collaborations involve complex relationships and communications among the collaborating healthcare providers. Therefore, security considerations on the relationships between collaborating partners are extremely important. To ensure this requirement, we propose an approach composed of two level authorization control mechanism prior to granting the access right to the data requester. In the proposed mechanism, the first step is to ascertain that the data requester is a member of the DHPC and the second step is to determine the collaborability of the healthcare provider for the patient data requested. Note that as discussed in the previous section, the membership application describes the standard and rules for collaboration, and all members must observe the rules.

In the proposed framework, each healthcare provider maintains an authorization policy and an authorization brokerage associate with the policy. The authorization brokerage manages the first stage of the authorization control whereas the authorization policy is used to control the way in which data is shared between the collaborating healthcare providers. The physician-patient relationship is confidential and typically, health care providers have different security policies that state a diverse set of security requirements and capabilities. Also, in practice, peers may have different security requirements and capabilities. Similarly, authentication and authorization mechanisms for health care professions may also be different. To address these issues, we use security agents (i.e., security brokers) as depicted in Figure 4.2 Each domain has security agents that enforce the policy. Security agents’ reason about these signed assertions and the appropriate
security policies to provide access control to services in their domain. In addition to specifying security policies, health care providers need to restrict access to medical data to only authorized health care professionals. The commonly used approach, role-based authorization, is insufficient to model access restrictions in all but simple health care scenarios. We use workflow context access control, where authorization decisions are based on the health care professional and the context in which they are accessing data.

4.4 Security Analysis

In this section, we validate our proposed model using a network of healthcare providers that collaborate to deliver a wide-ranging healthcare services. The healthcare providers are assumed to maintain a medical report for each patient that has received services from them as well as payment and some sensitive personal information. As noted earlier, each healthcare provider maintains its local security policy to manage its local user access control privileges. Similarly, each healthcare provider in the sharing community defines its own interoperability access control security policy that controls access to the patient data when interacting with other healthcare providers. In the experiment, we set up CA using OpenSSL tool and sign a certificate and Java Keytool. We used the Java programming language to implement and test the authorization policy.

4.4.1 Secure Interaction

In the first experiment, we tested how secure the interactions between the healthcare providers. We used various forms of the man-in-the-middle attacks such as reply attack to test the resilience of the proposed authentication policy. In the experiment, we submitted 1000 authentication request from a healthcare provider to another healthcare provider. We varied the
number of false authentication request by 5%, 10%, 20%, 30% and 40%. Figure 4.3 shows the result of the experiment.

![Figure 4.3: Analysis of secure interaction between the healthcare providers](image)

Our aim in this experiment is to understand whether the collaboration among the healthcare providers can be achieved securely. As results show, all false authentication request are rejected while all genuine authentication requests are accepted and processed. The experiment confirms that the security policy and the authentication brokerage perform as expected.

### 4.4.2 Authentication Policy Behavior

In the second experiment, we aim to verify whether the policy behaves as required by the original security requirements. Note that the authentication policy postulates a set of rules that expresses the privileges of those people who has access to the patient data from another healthcare provider.
In this experiment, we formulated 1000 queries with varying number of illegal requests such as missing patient consent, incorrect credentials and the number of allowed query per day. Figure 4.4 shows the result of the experiment. About 600 queries were positively responded to by the system while the remaining 400 queries were reject for various reasons. About 120 queries have some issues with the patient consent and thus they were rejected as being potential queries that can violate patient rights. About 130 queries were sent by a doctor who has been evicted or by doctors’ assistant such as a nurse from a member healthcare provider. Again the system rejected these queries as queries violating the policy that clearly indicates the requesting party must have appropriate credentials form the medical board. The final category tested queries from legitimate members that exceeded their daily maximum number of request for data. The system has been able to detect such queries and reject them.
4.4.3 Verification of Security Attributes

In this section, we use a tool to verify the correctness of authentication policies. We used a Scyther tool (Cremers, 2008) to verify the security attributes of the proposed protocol. Although there are many formal verification approaches capable to analyze the proposed approach, the shortcomings associated with formal verification models such as error proneness make them unfit for our purpose. The good aspect of Scyther is that it has many attack scenarios relevant to our case. Also, it allows for checking claims such as confidentiality of a certain value or certain properties such as authentication between communication partners should hold. The input to the Scyther consists of the authentication rules, adversary model and the protocol’s claim description. Security Protocol Description Language (SPDL) is used to represent the input (i.e., the protocol description and claims, adversary model). The output is a report summarizing the failure provided that there are security failures. Otherwise, the status of each claim is displayed. The outcome of the simulation is as follows: it is verified that the local security objectives of a healthcare provider is maintained while exchanging and sharing patient data with other healthcare providers.

4.5 Conclusion

Real world health care systems are generally large and overly complex systems. Designing privacy-friendly protocols for such systems is a challenging task. In this chapter we proposed an authorization policy management framework and interface specification for health care distributed processing environments. The policy enables complex access decisions to be defined, managed, and enforced. The policy base controls and manages how, when and who will access the data automatically. We consider patient data sharing in autonomous and distributed healthcare settings, evaluate the authorization policy effectiveness and show that it could preserve patient data privacy. The evaluation also shown that the authorization policy decreases
security breach against the patient data. Next chapter discuss how a certificate-based e-Health authentication and authorization architecture shall be utilized into the proposed framework.
Chapter 5

An Authentication Framework for E-Health Systems

As a result of increasing patient requirements for high quality healthcare delivery coupled with the growing mobility of patients, large—scale networked healthcare systems composed of healthcare sectors such as clinics, hospitals and pharmacies are becoming a norm. In such interconnected distributed healthcare systems, sharing of dynamic medical data among a wide spectrum of geographically distributed healthcare providers is gaining traction as well. Efficient and secure authentication protocol is an important and a significant challenge in such large-scale Internet-connected healthcare systems. In this chapter, we address this problem and propose a new efficient and secure authentication protocol that enable healthcare providers to securely and efficiently share medical data.

5.1 Introduction

In order to share information and perform distributed computations, increasingly emerging scenarios necessitate different parties, each withholding large amounts of independently managed information, and to cooperate with other parties in a larger distributed system. Such situations vary from traditional distributed database systems, where a centrally planned database design is distributed to different locations such as to federated systems, where independently developed databases are merged together. The system is also extended to dynamic coalitions and virtual communities, where independent parties may need to selectively share part of their knowledge towards the completion of common goals. Irrespective of the specific situation, a common point of such a merging and sharing process is selective and there is a need to share some data and cooperate. Moreover, there is a need for protecting those data that, for various reasons, should not be revealed.
In E-health infrastructure (E-HP2), a number of health care organizations (e.g., physicians, pathology labs, pharmacies and hospitals) willingly collaborate by virtually integrating their information systems. Hence, consumers can receive safer, better-coordinated and more reachable care as a result of the improved accuracy, completeness and availability of personal health information and the ability to gain remote access to care delivery facilities. They can also be better supported to stay healthy through access to consistent health information sources, tailored care plans and automated care provider monitoring of personal health status. It is important to note that the provision of infrastructure services is an enabling mechanism. The infrastructure itself will deliver some benefits, but the main outcomes will be achieved by the provision of additional applications and services.

The high-level sensitivity of medical information mandates stronger authentication and authorization mechanisms to be used in e-Health systems. To accomplish a secure authentication of a person (health professional or patient) it is essential to have a unique identifier. The person must then be registered in a database together with a certificate issued by a trusted body. In order to authorize a person to access applications or information, the liaising organizations have to agree on a certain type of rules. Authentication is the process where a networked resource user establishes a right to an identity. A substitute to general authorization is to individually describe how access should be permitted for each specific application. Authorization can also be given by invitation for a particular application or occasion. Authorization and authentication framework is a necessary tool for deploying and using a reliable, secure and trustworthy e-health system.

A large number of techniques may be used to authenticate a user: passwords, biometric techniques, smart cards, and digital certificates. Generally, the authentication methods used should match the value of the data being accessed. It should also correspond to the type and level of access the user is providing. Moreover, a method of user authentication is needed that
imposes a minimum additional workload on the user (Elmufti et al. 2006; Elmufti et al. 2008; Slamanig & Stingl 2008).

This chapter describes the design and implementation of certificate-based e-Health authentication and authorization architecture. A proposed authorization policy management framework to enable resource sharing between multiple heterogeneous health care enterprises via P2P communication environment has been provided. Furthermore, architecture was designed to authenticate e-Health professionals accessing shared clinical data among a set of affiliated health institutions based on peer-to-peer networks described in the previous chapter. The authentication architecture had to accommodate specific medical data sharing and handling requirements, namely the security of professionals’ credentials.

5.2 Credential-based Authentication Protocol

We propose an authentication framework for distributed and multidisciplinary team e-health systems with multilevel administrative domains. The major goal of this system is to produce a usable authorization system for an environment consisting of distributed resources used by geographically and administratively distributed users. The proposed authentication protocol is based on digital certificates that convey identity, use-constraints, and attributes. The proposed protocol offers a number of advantages such as user-friendly access to remotely managed patient data and related information, it does not require a huge amount of ongoing maintenance, provides strong authentication and gives confidence that systems are secure. Moreover, it is suitable for fine-grained access control and guarantees user privacy and confidentiality. It also addresses user accountability, with administrators able to investigate if improper use is discovered.

Although there is a merit for easy accessibility of individual's health information by qualified and authorized individuals using P2P network, this could immensely increase the potential for
This chapter we add an authentication protocol to achieve sharing of patient data and related information in a seamless and secure way. However, authentication protocol is more difficult to achieve in a pure P2P network architecture than in a centralized environment. This is because no central server is used to verify a peer’s identity.

The protocol is based on a Public-Key Infrastructure (PKI) that supports the issuing and management of digital certificates, which identify and authenticate authorized users. When a certificate authority issues an identity certificate, it binds a particular public key to the name of the entity identified in the certificate (such as the name of a doctor). The certificate also has an expiration date, the name of the certificate authority that issued the certificate and other information. Most importantly, a certificate always includes the digital signature of the issuing certificate authority. We also use an attribute certificate (AC) which has a data structure comparable to an identity certificate (Farrel & Housley 2002).

However, a major difference is that an attribute certificate does not contain a public key. It contains attributes that specify access control information associated with the AC holder (such as group membership, role, and security clearance). Attribute certificates are able to support and implement a significant part of the authorization process. For example, information about a user's current role (e.g. physician) or a client's ability to pay for a resource access may be more important than the client's identity.

5.2.1 Authentication Architecture

The interaction of health providers with the system has to be secured through a complex process of authentication and authorization. These protocols provide secure and flexible communication between user and health care systems. The proposed system offers several advantages including...
a user-friendly strong authentication and authorization system, which gives that confidence that the data are secure.

![Networked electronic health care system](image)

Figure 5.1: Networked electronic health care system

Figure 5.1 shows the proposed overall operational architecture. We assume that each health care professional (HP) is assigned a set of specific rights (roles) that governs the permissions needed to accomplish his/her tasks. We propose the use of remote and local user roles with each requiring different authentication mechanisms. First, the health care professionals (HP) must be authenticated to the local e-health system. At the second level, there should be a remote access authentication system. These are achieved through two distinct phases.

Initially, every user obtains an identity certificate. We assume that each autonomous domain has its own Identity Certificate Authority (ICA). We also assume that the ICAs in the P2P trust each other. The ICAs are responsible for the creation, digitally signing and distribution of the identity certificates to users registered in that domain. In a multi-team environment, the issue of managing patient consent to the use and disclosure of personal information is paramount. In this thesis, it is assumed that when a patient visits a hospital, the patient provides his/her consent on the use of
her medical data and digitally signs the consent form and the consent form is sent to the local data repository. For remote authentication, attribute and consent certificates are used to assign attributes and patient data use constraints to HP respectively in a verifiable way. Therefore, the second phase consists of obtaining the consent and attribute certificates. The consent certificate will impose use-conditions on the patient data. All of the use-conditions must be met simultaneously in order to satisfy the requirements for patient data access. An attribute certificate certifies that the user possesses a value for a given attribute. An attribute describes a property associated with an individual such as information that describes the qualifications and authorities granted to the target entity. Each attribute certificate may use only the information that is absolutely necessary to obtain the needed services. Attribute certificate validity period must be within the validity period of the identity certificate. A HP may possess different attribute certificates related to different validity intervals or even different purposes. It must be noted that, generally speaking, attributes are subject to change according to each situation. For example, the rights of HPs usually consist of both static and very dynamic permissions. As a result, the content of attribute certificates varies from case to case. Basically, health authorities issue static permissions and dynamic permissions may be issued even by hospitals and clinics. Static qualification and authorization attributes can also be connected with dynamic permissions and admission, for example by a supervisor or administrator within the IT environment of a hospital.

The system uses the attribute certificate authority (ACA) and the individual consent certificate authority (CCA) to control access to information content based on personal consent, the role of the information-accessing entity, and the type of information use. ACA issues attribute certificate that contains authorized people attributed and binds to one’s public key certificate. It also verifies the validity of attribute certificate as well as revokes attribute certificate in case of the attribute is changed or is lost.
The CCA maintains and serves information about the consent given by individuals about the use of their personal health information. It is assumed that patients are able to review and adjust consent information through a web-based interface. The gateway (GW) node at each participating health care providers runs the policy engine that determines, based on the roles assigned to HP, the users’ rights with respect to the requested access to health care data and resources. Since our focus is on remote exchange of health care data between different health care providers, we will not discuss the local authentication protocol in this thesis. We assume that the CAs ensures proper utilization of the credentials by regularly validating and revoking them. These CAs ensure that there are no ways for peers to request certificates for other people or multiple certificates for the same peer.

5.2.2 Authentication Protocol

E-health remote monitoring system generally deals with sensitive information. Therefore, the security of the system and the privacy of the data are vital issues that must be contemplated for such applications. Some of the important features, that are used while developing such a system includes:

- Authentication of the patient to the Health Care Authentication Server (HAS).
- Protecting the privacy of data during transmission and during storage.
- Protecting the reliability of data during transmission and
- Preventing replay attacks

One of the main features in deciding the meaning of a message in authentication protocol is the “time varying factors”. These parameters may be used in authentication protocols to prevent to reply and incorporating attacks. In this thesis we propose an authentication protocol, which does similar function, which is described above.
Figure 5.2 shows the steps performed in the proposed authentication mechanism. Specifically, when HP initiates a new session for remote data request; he/she must first identify and authenticate himself or herself, with the local gateway one (LGW) server, by using their IC and password. The validated IC of the user is then used by the GW to gather up all the relevant certificates, depending on the responsibility/authority of the HP roles activated by the request.

The GW also ensures that the HP has the need for the information sought. The remote gateway and the local gateway exchange a random number (RN) to be used in the authentication protocol. This random number is generated as follows:

\[
Hello \leftarrow (\text{RN})^{\text{sig}^{-1}_{\text{LGW}}}K^+_{\text{LGW}}
\]  \hspace{1cm} (1)

\[
Hello \leftarrow (\text{RN})^{\text{sig}^{-1}_{\text{RGW}}}K^+_{\text{RGW}}
\]  \hspace{1cm} (2)
Where the remote gateway signs the random number using its private key $\text{Sig}^{-1}_R$ and then encrypts it with its public key and send it to the requesting gateway. Finally, the local gateway produces a short-lived attribute certificate with a subset of HP roles from a set of initially assigned roles, which are needed to accomplish specific tasks.

The HP will then will create a request by concatenating the attribute certificate (AC) and the consent certificate (CC), signs it using its private key ($\text{Sig}^{-1}_R$) and then encrypts it with the public key of the remote gateway (RGW) ($K^+_R$) as follows:

$$\text{Request} \leftarrow \left( \left( (AC)|||CC)\right) \cdot \text{Sig}_R^{-1} \cdot K^+_R \right)$$

The HP will then send it to the remote gateway. When the RGW receives the access request from the health professionals, it sends the attribute certificate and the consent certificate to the local attribute certificate authorities (ACA) and consent certificate authorities (CCA) for verification respectively. These certificate authorities generally use published verification procedures to ensure that an entity requesting the data is in fact who it claims to be. Attribute verification is the process of establishing an understood level of confidence that an attribute applies to a specific individual. If the attributes are verified to be authentic, the HP is authenticated. Otherwise the request is rejected.

### 5.2.3 Communication overhead

An efficient protocol with low communication and computation overhead is necessary in the authentication process. The communication cost of the protocol is represented by:

$$T_{\text{overall}} = \left( T_{\text{local}} + T_{\text{veryfy}} \right) + \left( T_{\text{remote}} + T_{\text{veryfy}} \right)$$

Where $T_{\text{local}}$ is the communication cost due to local steps while $T_{\text{remote}}$ is the communication cost due remote steps. The $T_{\text{veryfy}}$ is the time taken to verify the validity of the authentication request both locally and remotely. Linking the consent form to the healthcare provider is an
example of the extra time taken. If we assume that $T_{\text{veryfy}}$ is the same for both local and remote verifications, we can reduce the above equation as follows:

$$T_{\text{overall}} = T_{\text{local}} + T_{\text{remote}} + 2 \cdot T_{\text{veryfy}}$$ (5)

5.3 Context-Aware Access Control Model

Future large-scale health care systems will engage many diverse businesses collaborating in patient care, including physicians, private physicians, private clinics, hospitals, dentists, pharmacies, drug and insurance companies. A context-based access control technique offers the security given by both the user-based and role-based access control and takes it one step further by including the context for making access control decisions. Context-based access control takes into account the person attempting to access the data, the type of data being accessed and the context of the transaction in which the access attempt is made. In this section, we present a framework for context-aware authorization for e-Health environments. We present an architecture consisting of authorization infrastructure and context infrastructure.

5.3.1 Contextual Model

We adapt the terminologies of (Fudzee & Abawajy 2008) to describe the context model presented in this chapter. We assume a finite set of data objects $D$, that require protection in the domain of a health care provider.

$$D = \{d_1, d_2, ..., d_n\}$$

Examples of the data objects maintained by the system resources include a prescription, a clinical note, a radiological report, a laboratory test result, a diagnostic image, etc. There is a set of users, $U$, in the system that will access the data objects in the data set of an application.
A user is an entity (a person who uses the system or an application program in the system) whose access is being controlled. Examples of users are physicians, nurses, administrative staff, etc. At any given time, each user is associated with a set of attributes, \( C \), that represents the set of context information such as location, health care unit, date/time, etc.

\[
C = \{c_1, c_2, \ldots, c_n\}
\]

Every application has its own context set based on the context type. An application designer decides which context types will be used to denote access by analysing the security requirements. Also, the system administrators can add new ones dynamically when required.

The system also maintains a set of roles, \( R \), and a set of permissions, \( P \), that govern access to the system. Roles are used to grant users access to specific resources. The set of the roles that describe a set of functional responsibilities within the health care organization are defined as follows:

\[
R = \{r_1, r_2, \ldots, r_n\}
\]

A user (e.g., a doctor) is assigned a subset of roles from the entire role set during a session. Example of the roles include, “attending physician”, “attending nurse”. The potential role of a doctor can include prescribing medications, recommending treatments, and interpreting the results of an imaging test. The role of a nurse can include providing care for patients, measuring vital signs, and monitoring drug administration. The role of a medical assistant may include taking health histories, and performing laboratory tests. Roles have role activation, role revocation, and role hierarchies.

A request in traditional RBAC comes from a certain user who has a set of roles associated with his/her. This association is achieved via the definition what roles \( U \) is allowed to take on based on the responsibilities and functions of \( U \) and that the set of roles are transferred to \( U \) and can
subsequently be used during access requests. This is called role activation in RBAC. Roles can be hierarchical, mutually exclusive, collaborative, or overlapping. For example, in a hospital some roles are hierarchical. The doctor role may include all privileges granted to the nurse role, which in turn includes all privileges granted to the medical assistant role. Role hierarchies are a natural generalization of organizing roles for granting responsibilities and privileges within an organization.

Each user is assigned one or more roles, and each role is assigned one or more privilege. Thus, every role that has privilege to access the resource is assigned a subset of permissions from the entire permission set, $P$, maintained by the system:

$$P = \{p_1, r_{p_2}, ..., p_n\}$$

A role $r_m \in R$ can perform an operation $o_i \in O$ on an object $d_j \in D$, if there is a permission $p_k \in P$ that authorizes the role to perform the operation on the object. Permission is an approval to perform an operation $O$, on one or more protected e-health data objects:

$$O = \{o_1, o_{p_2}, ..., o_n\}$$

Example of the operations includes reading, writing, deleting, inserting, etc.

### 5.3.2 Conceptual Framework

Figure 5.3 below shows the context-based access control method architecture for the e-health system. Service request is specified in the form of $(u_i, d_k, o, l)$, where $l$ is the authentication trust level of user $u_i \in U$ that is allowed to access or manipulate an object $d_k \in D$ through an operation $o \in O$ such as read, write or execute.
In the proposed scheme, the authentication tokens are issued to the users by the authentication module and thus create an authentication trust level for that token. Based on the service access request, the system decides the appropriate access policy for the demanded service. A set of constraints on the role and service name will be the foundation for this policy, and evaluated in combination with the on hand contextual information to implement fine-grained access control.

An access policy comprises of a compilation of access conditions.

The job of the authorization module is to monitor all service requests from the users and evaluate the information provided by the user to access the service that he/she wants. The authorization module evaluates a request based on the authorization rules and the contextual information provided by the user for a particular service. If the information satisfies the prerequisites of a service, then the user is granted permission for that service. The Document composition module

![Figure 5.3: Context-based access control system architecture](image-url)
(DCM) compiles the policy documents and contains the XML-policy base, which has the policy information. The XML-Policy sheets have the information, which is used to implement the authorization constraints. The XML-policies of an enterprise are permitted by the GTRBAC framework to be specified and imposed through a Java-based GUI-enabled application whose code is already integrated in a Web browser by a mechanism provided by Java. More explicitly, the users are granted or denied permission depending on the roles, which they are assigned to as per the XURAS (XML User-to-Role Assignment Sheet) policy sheet and the related permissions per the XPRAS (XML Permission-to-Role Assignment Sheet). The XML-Parser and the GTRBAC processor are the two main parts of the system. The XML parser forwards the DOM instance of the parsed XML documents to the GTRBAC processor. The GTRBAC processor has the GTRBAC module, which controls and implements the policy according to the policy sheets supplied by the XML policy base (Bhatti et al. 2007).

We now give an example to show how the system works. Consider that a pathologist has the right to read and write the pathology reports of a patient, but if he/she only asks to read the patient pathology report then the pathologist is only given a read permission. A pathologist can log on to the system with any identification technology available on his system. An authentication token including the user details and the authentication trust level of identification technology is sending to the Authorization module of the system. If the pathologist uses a username and password to log on to the system then he is given a permission only to read, if there exists a policy specification that “a pathologist should need an authentication level of a password to read data and an authentication trust level of a fingerprint to write data”. To write data the pathologist will again have to log on to the system using a fingerprint as the identification technology.
5.3.3 Authorization Framework

Contextual authorizations can be included into the existing RBAC models, which will increase the expressive power to classify access control policies. At the time of access request the contextual information that is provided by the user, such as nurse/patient relationship can influence the decision of authorising a user to perform a particular task. This facilitates a new flexible and specific authorization policy design, where authorization is approved or deprived of in accordance with the right of the user and his/her needs at the current situation.

As an illustration, we now present a scenario of access control mechanism in e-health based on our Context-based Access control model. Let us consider that there is a Doctor A who has a patient B. Suppose we have a context set defined as follows:

\[ CS = [T, L, AL, AR] \]

where T=time, L=location, AL=authentication level, and AR=attending relation. Let hospital (H) and emergency department (ED) is a valid value of the contextual attribute location:

\[ L = [H, ED] \]

A valid value of the authentication level (AL) can be expressed as follows:

\[ AL = [PW, FP, SC] \]

where PW=password, FP=finger print and SC=smart card.

Suppose we have a partial security rule such as “patient data can only be accessed by attending physician who is Doctor A from within the hospital between 9am and 4pm or from within the emergency department at any time with a trust level of a “password”. If in is a user-defined operator, then context constraint (CC) for this rule can be expressed as:
This is a simple scenario where the patient B and the doctor A have an attending relation. But if doctor A is not present in the hospital and patient B is in the emergency department and needs immediate medical attention, then the present doctor in the emergency department will need to view the medical records of the patient to check for any allergies, blood pressure etc. before starting the treatment. To solve such complex scenarios, the system administrators can add one more clause with the existing context constraint such as “patient data can only be accessed by attending physician who is doctor A from within the hospital between 9am and 4pm or from within the emergency department at any time with a trust level of a password; otherwise a higher level of trust such as a finger print of the doctor present at the emergency department is required to view the patient records”. If “in” is a user defined operator and “emergency department” is a valid value of the contextual attribute space, then this rule can be expressed as follows:

\[
CC = (AR = A \cap 9:00 \leq T \leq 16:00 \cap L = "H" \cap AL \geq "PW") \cup \\
(AR = A \cap L = "ED" \cap AL \geq "PW") \cup \\
(AR = Doctor \cap L = "ED" \cap AL = "FP")
\]

5.3.4 Policy Specification for Access to Services

An access policy specification in our context-based access control framework indicates which role can access which types of services under some context conditions. In e-health systems, it is not only a hospital that access medical information but there are other participants as well such as insurance companies, pharmacies, private clinics who access patient information to do their business.

Although the authorization engine uses the access policies for access control decisions but these policy specifications are also needs to be exchanged to other domains specified above. For this
reason, we chose to specify our policies in an XML format as it can be easily integrated into the present XML-based architectures for Web Services and will be understandable to other domains. Figure 5.4 shows an example of the access control rule. In this example, a pathologist can only view a patient’s pathology report when he/she logs in from the pathology lab in the hospital and provides an authentication level of a password.” The authorization policy for this access rule is given in Figure 5.4.

```
<wsp:Policy>
  <wsp:AppliesTo>
    <wsa:EndpointReference>
      <wsa:DataType>PatientPathologyReport
      </wsa:DataType>
      <wsa:OperationType>View
      </wsa:OperationType>
      <wsa:ServiceType>ViewPatientPathologyReport
      </wsa:ServiceType>
    </wsa:EndpointReference>
  </wsp:AppliesTo>
  <wsse:SubjectToken wsp:Usage="wsp:Required">
    <wsse:TokenType>Pathologist
    </wsse:TokenType>
  </wsse:SubjectToken>
  <wsp:OneOrMore wsp:Usage="wsp:Required">
    <wsp:All>
      <wsse:ContextToken wsp:Usage="wsp:PathologyLab">
        <wsse:ContextType>Location
      </wsse:ContextType>
    </wsse:ContextToken>
    <wsse:ContextToken Constraint>
      <wsse:ContextType>Authentication Level
    </wsse:ContextType>
  </wsp:All>
  </wsp:OneOrMore>
</wsp:Policy>
```

Figure 5.4: Policy specification for access to services
5.4 Protocol Analysis

E-health system with capability that enables healthcare providers to deliver medical service over the Internet has been growing rapidly. Since the electronic health information maintained by the healthcare providers are highly sensitive and distributed over a wide area, it is paramount important that the system is guarded by a strong authentication mechanism that guarantees performance and security to healthcare professionals, consumers and providers and clients.

In this chapter, we proposed a new authentication protocol. As a proof of concept, we implemented the proposed authentication framework and studied several properties of the protocol ranging from its susceptibility to security attacks such as impersonation and replay attacks as well as performance in terms of the communication overhead using a discrete-event network simulator. In the experiments, the authentication protocol was exposed to various scrutiny to analyse the security based on the most common authentication attacks.

5.4.1 Authentication request analysis

The aim of the experiment is to see if illegal authentication requests can be accepted or not. One aspect of the proposed authentication protocol is that it imposes use-conditions on the patient data. All of the use-conditions must be met simultaneously in order to satisfy the requirements for patient data access. In the test data, we created several authentication requests that violate the use conditions and investigate the capability of the proposed protocol. We also created invalid requests from various combinations. An example of invalid authentication request is an authentication request with missing patient consent form.
In order to test the capability of the authentication protocol, we created a batch of 5000 authentication requests. We submitted the authentication requests while varying the number of invalid authentication requests. Fig. 5.5 shows the performance (y-axis) of the protocol when the number of invalid authorization request varies (x-axis). We observe that the request authenticator is able to detect and reject all illegal requests while permitting all valid authentication requests.
5.4.2 Impersonation attacks

An impersonation attack occurs when a dishonest entity within the hospital successfully assumes the identity of a genuine entity and access the patient data. The proposed protocol appears to be susceptible to impersonation attacks. This is because, there are many actors in the healthcare environment that could pretend to be an authentic user. Note that the system uses the attribute certificate authority (ACA) and the individual consent certificate authority (CCA) to control access to information content based on personal consent, the role of the information-accessing entity, and the type of information use. Thus the test data also included requests that violate the above. For example, a nurse requesting patient payment data.

Fig. 5.6 shows the performance (y-axis) of the protocol when the number of invalid authorization request varies (x-axis). The result shows that the protocol is immune to impersonation attacks. This is because the proposed framework uses an Attribute Certificate that contains information about a user's current role (e.g. physician) and is able to support and implement a significant part of the authorization process. ACA issues attribute certificate that contains authorized...
person’s attribute and binds to one of key certificate. Also, the proposed protocol cryptographically links an entity to a claimed identity and thus an entity within the hospital cannot pretend to be another entity. This result offers the confidence level required for entity authentication in critical healthcare environment.

5.4.3 Replay attacks

A replay attack is a form of a security attack in which an adversary captures the authentication information from the sender to the receiver while it is in transmission and then contact the authenticator server and presents to it the hijacked authentication information as the proof of his/her identity and authenticity to receive the patient data. The aim of the experiment described in this section is to expose the authentication protocol to a reply attack and check its resistance to it.

![Replay attacks graph](image-url)

Figure 5.7: Authorization request with replay attacks
Fig. 5.7 shows the result of several replay attack injections (x-axis) as a function of the number of requests (y-axis). In the experiments, we assumed that the adversary submits the captured authentication information after the decision to the original request has been completed. This is in fact the situation in real life scenarios.

From the figure, we can see that the protocol is resistant to reply attacks. Note that the attacker cannot modify the request since the request is encrypted with the public key of the remote gateway and the private key of the remote gateway is needed to decrypt it. Therefore, the attacker must send the request as is to the remote gateway to perform the replay attack. The adversary fails for two reasons. First the attribute certificate is short-lived as discussed above. Second, both the remote gateway and the local gateway include random values in their opening handshake messages which are used in subsequent authentication process. This is able to prevent the unmodified reuse of previously captured authentication request. Therefore, the proposed protocol maintains strong user privacy with respect to the authentication message.

### 5.4.4 Timing Analysis

In the previous sections, we have shown that the proposed protocol maintains strong security with respect to the authentication messages. In this section, we investigate the efficiency of the proposed protocol in terms of communication overhead. We compare the proposed protocol with the slightly modified protocol proposed in (Mantas, et. al., 2010). In particular, we submitted a batch of well-formed authentication requests starting with small number but progressively increase the batch size.
Fig. 5.8 shows the relative performance of the two approaches for a set of authentication requests (x-axis) relative to the communication overhead (y-axis). We refer to the baseline protocol as PKI protocol since the protocol is designed based on a PKI infrastructure to enable exchange of data among healthcare providers spread over a wide area. In contrast, we refer to our protocol as an attribute protocol in the graph. The experiment indicates that the two protocols are more or less have the same overhead at low load while the proposed protocol substantially outperforms the PKI protocol as the number of authentication requests increase. This shows that the proposed protocol is highly scalable.

5.5 Chapter Summary

In the recent past, E-health system has been used as communication system that allows distributing medical service over the Internet. The medical data, which is accessible in E-health systems, is extremely sensitive and circulated that stresses strong authentication and
authorization mechanisms for communication between the health care providers and consumers. In this chapter we demonstrated an authentication protocol system for E-health applications. Medical data security is an important issue that poses technical, organizational and ethical challenges. In this chapter we proposed an authorization policy management framework and interface specification for health care distributed processing environments. The policy enables complex access decisions to be defined, managed, and enforced. The policy base controls and manages how, when and who will access the data automatically.

Furthermore, we introduced a two-level authentication protocol for P2P-based e-health system that provides integrated services to health care providers. The authentication framework is based on identity, attribute and consent certificates that together uniquely identify the HP as well as the roles and accesses associated and constraints imposed on the health care data usage. The protocol offers a number of advantages including a user-friendly and strong authentication and gives confidence that systems are secure. In the next chapter we will introduce a context-based access control mechanism to extend the standard role-based access control. The context-based access control inspects not only network layer and transport layer information but also examines the application-layer protocol information. It intelligently filters TCP and UDP packets based on application-layer protocol session information and can be used for intranets, extranets and Internets. Through extensive experimentation, we evaluated the feasibility of the proposed framework and its resistance to various common attacks such as impersonation and reply attacks.
Chapter 6

Privacy-Preserving Queryable E-Health Systems

6.1 Introduction

In many domains, data integration from multiple autonomous data sources has emerged as an important practical problem (Hu 2009). For example, in order to offer the best possible care for their patients, physicians need coordinated data obtained from the physicians own patient database, from other physicians database, pharmacies, drug reference databases and labs each of which gather and maintain data for the purpose of health care delivery. However, security concerns and legal implications that require privacy compliance make privacy-preserving data management for querying data residing at different organisations a must. Privacy preservation means that the data owners are only willing to share the minimum information required for processing queries correctly.

In this chapter, we address the problem of data sharing with privacy preserving among a diverse set of autonomous but cooperating organisations with emphases on health care domain. The fundamental question addressed here is how can organisations share data to meet their needs to support decision making or to promote social benefits while at the same time protect personal data from being released. In the health care domain, the data required to support health care comes from several organisations such as physicians, hospitals, pharmacies and labs each of which gather and maintain data for the purpose of health care delivery.

Much of the data in the health care domain is considered private and confidential. Clearly, preservation of privacy when sharing data in a dynamic environment is very challenging. This is due to various reasons such as competition among data owners or possible legal implications requiring confidentiality of the data. There are few works that addresses privacy concerns when
data is exchanged between multiple organisations in a dynamic environment. In such environments, the approaches that enable sharing of data in a secure manner have lagged far behind the ability to store such data locally (Nan 2007; Siegenthaler & Birman 2009). Therefore, there is a need for approaches that offer some level of control on data manipulation procedures that can respond to those privacy considerations.

In this chapter, we propose a framework for data sharing with privacy preserving in dynamic environments such as health care domains. The proposed framework enables the exchange of data while revealing only the minimum amount of information that is necessary to accomplish a particular task. We wish to note that the proposed framework is not domain specific, though it is perhaps most compelling for the health care industry because in that area there is both a desire to openly share information with anyone who needs it and a high expectation that data will not be exposed to public view or otherwise fall into the wrong hands.

### 6.2 Developing a Privacy Preserving Query Processing Solution

The research challenge in developing a privacy-preserving query processing solution is that the answers to the queries need to be provided while preserving the privacy of the data sources. When sharing personal information for analysis and research, health care providers need to ensure that individual’s sensitive information should not be revealed. Specifically, the problem of query processing across multiple private databases is defined as follows (Emekci et al. 2006):

> **Given a set of autonomous data sources** \( D = \{D_1, D_2, ..., D_n\} \), **and a query** \( Q \) **that multiple parties collaborate to answer**, **the problem is to compute the answer of** \( Q \) **without revealing any additional information to any of the data sources.**

Three important properties that any privacy preserving system should provide include (Nan 2007; Siegenthaler & Birman 2009):
a) Data privacy: The service customer learns only the answer to the query, and not any of the data used to compute it.

b) Query privacy: The service provider does not learn the query, only that a query was performed against a particular user’s information.

c) Anonymous communication: Service customers and service providers do not know who the opposite party is.

Anonymous communication is important because either the query asker or the data owner might be a specialist, for example an AIDS clinic, where merely revealing that the patient is in some way associated with an organisation of that nature would constitute a privacy violation (Nan 2007; Siegenthaler & Birman 2009).

Similarly, a query might contain information about a specific condition of the patient that some of the data owners do not already know about. In this chapter, we make a point about the patients’ privacy and emphasise that once a person (user) has authorized an organisation to pose queries, only minimum disclosure information and requirements need to be applied so that the user should not be denied proper medical care because a legitimacy query could indirectly lead to a privacy violation.

### 6.3 Layered System Architecture Model

Several techniques have been proposed to preserve the privacy of data sources in the areas of databases and cryptography. Our work complements this work as we address both the query execution as well as the decision of determining which queries should be permitted for execution.
Figure 6.1 shows the high-level architecture of the system model used in this chapter. The system is divided into three functional layers: Client, broker and Service, the client layer represents several sites $S = \{S_1, S_2, ..., S_n\}$, each site represents an autonomous health care organisation. Each site, $S_i \in S$, has its own data stores including all health-related patient information comprising demographic data, diagnostic data, prescription data, treatment data, financial and insurance data. In summary, the associations among these entities can be reviewed as follows. The health care organisations act as sources (applications) that supply the patient data. The data collector collects this data from the health care organisations (sources), and makes it available to data analysts, which carry out the required data analysis. The system guarantees that personal (individual) categorizing data is substituted with aliases once it leaves the sources, and that only the reclamation authority is proficient of linking aliases to its respective identity. Here, we assume that patient data is distributed through the system. For this whole chapter, we refer to the data clients (requesters) as service customers while to data benefactors (providers) as service...
providers. The broker layer is accountable for formulating the dynamic query for exchanging requested patient information between service providers and customers. The functional descriptions for each designed model’s layer are provided into the following sections.

6.3.1 Service Provider

Service providers are accountable for guaranteeing the availability and perseverance of any data that they control. Such institutes could be for instance hospitals, or insurance companies. We assume that every institute delivers its data to its analogous source application as a set of data records. A service provider maintains information about its customers in some internal database with a proprietary schema. As in (Siegenthaler & Birman 2009), the cases of erroneous identifiers or persons with multiple aliases are outside the scope of this chapter.

Also, we do not consider the use of known identifying information such as a social security number or a combination of name and age, to be a privacy threat in this context because it is typically already known by the types of organisations targeted by our work. Each service provider maintains a private metadata, which is a set of privacy views. Each privacy view defines a set of private attributes, its owner, the tables, and conditional expression.

Providers have public keys K and private keys k respectively. A provider A communicating with a provider B is able to sign messages it sends and verify the signature on messages that it receives using the following functions;

\[
\text{Sign (kA, msg)}
\]

\[
\text{Verify (KB, msg)}
\]

It may also encrypt and decrypt messages using functions

\[
\text{Encrypt (KB, msg)}
\]

\[
\text{Decrypt (kA, msg)}
\]
Additionally, providers must be able to verify that any other providers with which they communicate are authorized to participate in the system. This is accomplished by having the public keys signed by a trusted accreditation agency.

### 6.3.2 Service Customer

The Service customers are the entity that gathers anonymized version of the data records that the sources collect. Service customers run queries against data that is distributed through the system. Here, queries are written in a relational algebraic language (which is similar to SQL). Standard select, project, and join operations are accomplished against tables that are fragmented across various service providers and the results may range from binary (yes/no) answers processed(computed) over the data to real values of data found in the databases. Also, results should not comprise any information that the customer is not authorized to discover. This chapter mainly focuses on query execution, leaving the decision of figuring out (determining) which queries should be permitted for future research. All accumulation (aggregation) of data (information) across table fragments at different organizations is carried out at query time. Records are kept separate in the underlying databases and only the links between them are stored. This process guarantees (ensures) that any incorrect connections may be incomplete (undone) without leaving the original data in an unstable state.

### 6.3.3 Service Broker

In chapter six of this thesis we stated that each organisation is responsible for storing and maintaining the data that it generated. We assume that there is a well-defined process on how data analysts can request a set of records from the data collector. Customers interested in certain data submit queries to the broker. The broker is assumed to be secure and fully trusted to safeguard the privacy of organisational data. The service broker is responsible for both the query
execution as well as the decision of determining which queries should be permitted for execution. The broker ensures that results of the query do not contain any information that the asker is not authorized to discover. The broker uses an algorithm called semantic request mediation based on global ontology (Emekci et al. 2006; Mitra et al. 2006) to translate customer queries so that the semantic heterogeneity between organisation A’s schema and N’s schema can be resolved.

6.4 Privacy-preserving Data Sharing Framework

In this section, we will show that the broker provides the three privacy features discussed in the previous section. We will demonstrate how queries can be answered in a distributed manner that preserves the privacy of the original data. The main idea of the proposed framework is to support queries that reveal enough information so that organisations can go about their business, and no more. For the sake of clarity and to permit better optimisation later, we split querying into two phases.

Phase one performs a global search for records pertaining to the person in question and returns a set of data handles, each of which indicates the presence of a record somewhere in the system but does not reveal where that record resides. Phase two uses the data handles to execute a relational algebraic query, while keeping the original data hidden from the customer and keeping the query hidden from the data owners.

Figure 6.2 shows the privacy preserving algorithm protocol in action. Potential customers encrypt the query (sensitive transactions) and send it to the broker. The sensitive transactions are those that fully or partially support the generation of sensitive patterns from a dataset. Service customers are also required to submit their credentials to the broker who then checks (this is performed by the admission control algorithm) to check whether the customer is certified to post query to any of the service provider that are registered with the broker. The main idea can be assessed as follows; firstly, broker finds a set of outlines from the transactional dataset, and then
recognises the complex tasks which include privacy algorithm and admission control. Secondly, it uses a transaction recovery engine to identify all sensitive data submitted by the service customers in the original database and amend them accordingly while directly copying all non-sensitive transactions to create a new, fresh (clean) database.

Queries that are admitted will be sent to the query parser algorithm, which checks, among other things, if the query contains attributes that the customer is not authorized to access. If so, the parser rewrites the query and deletes all private attributes before clearing the query for execution. Queries that are cleared will then be sent to the privacy algorithm for anonymising it before sending it to service provider for processing. When the query from customer or the results of the query from the service provider arrives, the broker invokes the privacy algorithm. Also, the privacy algorithm is responsible for taking the result as input and anonymousness it. This makes the broker able to answer queries without revealing any useful information to the data sources or to the third parties.

The proposed framework enables the exchange of data while revealing only the minimum amount of information that is necessary to accomplish a particular task. The system is divided
into three functional layers: Client, broker and Service. Each site has its own data stores including all health related patient information comprise demographic data, diagnostic data, prescription data, treatment data, financial and insurance data. The health care organizations act as sources (applications) that supply the patient data. The data collector collects this data from the health care organizations (sources), and makes it available to data analysts, which carry out the required data analysis. The system guarantees that personal (individual) categorizing data is substituted with aliases once it leaves the sources, and that only the reclamation authority is proficient of linking aliases to its respective identity. The broker layer is accountable for formulating the dynamic query for exchanging requested patient information between service providers and customers.

The main idea of the proposed framework is to support queries that reveal enough information so that organizations can go about their business. Querying can be split into two phases:

- Phase I performs a global search for records pertaining to the person in question and returns a set of data handles, each of which indicates the presence of a record somewhere in the system but does not reveal where that record resides.
- Phase II uses the data handles to execute a relational algebraic query, while keeping the original data hidden from the customer and keeping the query hidden from the data owners.

Potential customers encrypt the query (sensitive transactions) and send it to the broker. The sensitive transactions are those that fully or partially support the generation of sensitive patterns from a dataset. Service customers are also required to submit their credentials to the broker who then checks to ensure whether the customer is certified to post query to any of the service provider that are registered with the broker.

Queries that are admitted will be sent to the query parser algorithm, which checks, among other things, if the query contains attributes that the customer is not authorized to access. If so, the
parser rewrites the query and deletes all private attributes before clearing the query for execution. Queries that are cleared will then be sent to the privacy algorithm for anonymising it before sending it to service provider for processing. When the query from customer or the results of the query from the service provider arrives, the broker invokes the privacy algorithm. Also, the privacy algorithm is responsible for taking the result as input and anonymousness it. This makes the broker able to answer queries without revealing any useful information to the data sources or to the third parties.

6.5 Implementation and Analysis

The proposed prototype of virtual medical information system was developed using an Oracle Forms Developer that was based on the Oracle Database. Figure A-1 depicts the main building blocks of the system. Later in this chapter, the proposed system functionality and development assumptions have been introduced with an overview of the system architecture for the study, a collection of sampled patient and medical datasets were used in a number of database tables. The concept-based information sharing is based on the idea that unifying the concepts of medical data items according to master meta-data catalogue with utilizing a developed dynamic SQL query generator engine which formulate the query parameters according the inquirer preferences to improve data sharing performance and solves the dissimilarity of database designs across peers electronic health systems.

The projected prototype system utilizes a central and distributed data catalogues, in addition to synchronization mechanisms to propagate altered/added data from central to distributed catalogues and vice versa. Overview of the overall system architecture is shown in Figure 6.3. It is divided into two operational tiers (sides): central and remote (distributed) side, while the later representing the participated clinical entities (peer). Diagram shows several databases, a central database mainly used for holding meta-data dictionaries, peers profiles, communication profiles,
and certification authority serving both peer and roles levels. Each of other databases is represents the local clinical/hospital health care system’s databases.

6.5.1 System functionality
The designed workflow of the developed prototype is consisting of four sequenced functional steps initiated at the inquirer side, process start with check the available/connected agents (health care entity), followed by selecting a specific interested data source agents or all connected agents, then enter the search query words by inquirer user with providing the first and last name of the looked-for patient, at this position the search query is reformulated with a fully dynamic SQL statement after substituting the search parameter with the name of data fields and database tables located into the sourced agent system’s database, the dynamic query engine utilize a sharing and
synchronized data sets sited in all anticipated agents; afterward the selected data source agent will responds with existing patient’s health records categorized according to type of transaction (like operation, x-ray, medicine, lab test, .. etc.) in addition to the reputation of the sourced agent; after that the inquirer agent shall select the chosen data record according to his requirements. Finally, inquirer agent shall assess the retrieved information and update the reputation of sourced agent on all peers in addition to central database. Figure 6.4 shows the sequence diagram for the proposed prototype comprises exchanged data between inquirer and inquired agents.

Figure 6.4: Proposed System Sequence Diagram

The following assumption has been considered in designing the functionality of the prototype application:
1. Data sharing is achieved by initiating a request for the data through the local agent. The agents’ use distributed local ontology and composite ontology to provide the functionality of a centralized ontology along with the ability to be flexible in meeting the varied needs of the users.

2. The agents reside on the doctor’s computer and are empowered to search for information, retrieving data from the underlying data repository as well as presents the data to the overall system for merging, and provide the ability to dynamically form composite ontologies from the metadata sources.

3. When inquirer initiates a new session for remote data request; he/she must first identify and authenticate himself or herself, with the local gateway server, by using their username and password. The validated username is then used by the inquired agent to gathers up all the relevant certificates, depending on the responsibility/authority of the inquirer roles activated by the request. The inquired agent also ensures that the inquirer has the need for the information sought. The inquirer will then send to the remote data source agent a request for data.

4. Service customers run queries against data that is distributed throughout the system. Queries are written in a relational algebraic language similar to SQL. All aggregation of information across table fragments at different organizations is performed at query time.

5. Data sharing is achieved by initiating a request for the data through the inquirer agent. The agent’s use distributed local ontology and composite ontology to provide the functionality of a centralized ontology along with the ability to be flexible in meeting the varied needs of the users.

6. Each member of a data sharing community has a numeric reputation in the range of MIN to MAX, which is attached to every query-hit message so that the inquirer can decide
whether to trust the answer or not where larger numeric reputation values mean greater trust.

7. Customers interested in certain data submit queries to the inquirer agent. The agent is assumed to be secure and fully trusted to safeguard the privacy of organizational data. The inquirer service agent is responsible for both the query execution as well as the decision of determining which queries should be permitted for execution. The inquirer agent ensures that results of the query do not contain any information that the asker is not authorized to discover. The agent uses an algorithm called semantic request mediation based on global ontology to translate customer queries so that the semantic heterogeneity between organization A’s schema and N’s schema can be resolved.

8. For the sake of clarity and to permit better optimization the querying process have been divided into two phases.
   a. Phase one performs a global search for records pertaining to the person in question and returns a set of data handles, each of which indicates the presence of a record somewhere in the system.
   b. Phase two uses the data handles to execute a relational algebraic query, while keeping the original data hidden from the customer and keeping the query hidden from the data owners.
   c. Service customers are also required to submit their credentials to the agent who then checks to see if the customer is authorized to post query to any of the service provider registered with the agent.
   d. Queries that are admitted will be sent to the query parser algorithm, which checks, among other things, if the query contains attributes that the customer is not authorized to access. If so, the parser rewrites the query and deletes all private attributes before clearing the query for execution.
e. Queries will then be sent to the inquired agent service provider for processing. Then the query from customer or the results of the query from the inquired agent arrived

9. Due to complexity of developing a full authentication framework, the Certificate Authority (CA) has been simulated using a peer’s user-based authentication module and verification procedures.

10. Certificate Authority (CA) issues a certificate to peer’s users and provides system validation and authentication functions to recognized users.

11. Membership to the Data sharing community is controlled and certified by a single certification authority, while another certification authority represents the medical board and responsible for certifying medical professionals in good standing.

12. The system uses the attribute certificate authority to control access to information content based on personal consent, the role of the information-accessing entity

6.5.2 Data Query Page

This page as shown in figure 6.5 be used by the clinic doctor to query patient information. Information might be in the local database or can be in a remote data base. From this single page the doctor will retrieve combined result from both local and remote data sources based on the clinic permissions
This page is fully dynamic and connected to the master ontology, whenever a field is added in the master patient table it will be automatically reflected in this page as a query field.

The doctor adds any search inputs and clicks search (e.g. Patient_Name = ISSA MOHAMMAD T. NASSAR)

Figure 6.6: Data query sample
As above screen shot (figure 6.6) shows the patient with name (ISSA MOHAMMAD T. NASSAR) has been found in two data sources (Dire Clinic and Al Noor Hospital). The result header is coming from the master ontology (see light green in the following diagram):

![Data query sample](image)

Figure 6.7: Data query sample

If any new field is added to the master patient details ontology, it will be automatically shown here in the result.

### 6.5.3 Query Translation page

Figure 6.8 shows the test to the query translation algorithm. Translation result is shown in Figure 6.9.
you are Querying Data as: **Dire Clinic**

you have access to the following peers:

- Nabil Hospital
- Wassim Clinic
- Dire Clinic
- Al Noor Hospital

**Input queires to be translated (Each query in Separate line):**

- `select SSN, Address from Person where Sex='Male'`

<table>
<thead>
<tr>
<th>Peer</th>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Master Query</strong></td>
<td><code>Select Patient_Address, Reg_No from Master_Patient_Details where Patient_Gender='Male'</code></td>
</tr>
<tr>
<td>Nabil Hospital</td>
<td><code>Select Address, SSN from Person where Sex='Male'</code></td>
</tr>
<tr>
<td>Wassim Clinic</td>
<td></td>
</tr>
<tr>
<td>Dire Clinic</td>
<td><code>Select Patient_Address, Reg_No from Patient_Details where Patient_Gender='M'</code></td>
</tr>
<tr>
<td>Al Noor Hospital</td>
<td><code>Select Reg from Patient where Gender='Male'</code></td>
</tr>
</tbody>
</table>

Figure 6.8: Query translation
6.6 Conclusion

In this chapter, we addressed the problem of developing a privacy-preserving query processing solution for data sharing in a dynamic environment. It provides a practical balance between privacy preserving and data sharing. The computation cost of this method is mainly associated with construction and modification of the data set. We presented a broker-based solution that provides answers to the legitimate queries while preserving the privacy of the data sources. The basic technology now exists to build an infrastructure that permits sharing of sensitive data across organisation boundaries. System experimental results of developed prototype (storing and querying private electronic health data) have been stated into the next chapter.
Chapter 7

Conclusion and Future Directions

7.1 Introduction

The purpose of this chapter is to summarize the achievement, which has been made by this study. In view of the conceptual model described in Chapter 3, this study introduced an infrastructure to share dynamic medical data amongst heterogeneous health care providers in a secure manner, which could benefit the health care system as a whole. This thesis proposed a framework that enables health care providers share dynamic medical data in a secure manner.

7.2 Thesis Contributions

The thesis has introduced the following:

- An architectural framework that enables a flexible and dynamic conglomeration of data across any combination of the participating heterogeneous data sources to maximize knowledge sharing
- A privacy preserving service broker architecture for data sharing in virtual health care environment
- Context-based e-health system access control mechanism for virtual health care environment. An authentication framework for e-health systems in virtual health care environment and
- Finally, an authorization policy management framework for dynamic medical data sharing in virtual health care environment

The proposed system has enabled health care providers to offer the best possible care for their patients. It emphasises on the following advantages:
– Reduces the volume of redundant medical problem lists, medication lists, allergy lists, notes/reports, labs, and imaging lab tests.
– Data like images and lab results can be communicated fast and thus, guarantee an optimized care process.
– Does not require health care providers to change their internal systems.

Apart from the above, the thesis was able to introduce the sharing of the dynamic data only by creating a conceptual framework for ubiquitously sharing heterogeneous patient information among autonomous health care providers and complementing it with an authorization policy management framework, an authentication framework for e-health systems, context-based e-health system access control mechanism, and privacy-preserving queryable-health systems. Storing and querying of private electronic health data are investigated in this research study. This research study also investigated data privacy, anonymity of communication and query privacy. More work is necessary to investigate the out of scoped areas, especially on the issue of determining which queries are acceptable and which queries are not. However, the simple technology now exists to develop an infrastructure that permits sharing of sensitive information electronically across organization boundaries. A proposed method for processing queries across private databases has been demonstrated while protecting the data providers’ confidentiality. The proposed outline is capable of computing and answering the queries without violating the privacy requirements of the data sources in an authenticate atmosphere. Our proposed method uses a meta-data via a P2P communication protocol.

7.3 Future directions

This thesis has introduced an infrastructure to share dynamic medical data amongst heterogeneous health care providers in a secure way, which could benefit the health care system
as a whole. The study results of the ubiquitously data sharing into a heterogeneous patient information system prototype have motivated the researcher to carry out more work in this area. This involves the extension of the work in a way to fully improve the peer-to-peer communication approach into data sharing community. Another option of future research is that of conducting large sample texts with real health care managing systems to validate the results of the present study. However, there is still lot of work needed to improve the dynamic medical data sharing. Some of them include the following:

- There is a need for sophisticated techniques for safer data transfer and maintaining 100% security in patient data.
- We believe that the technique proposed in this research study might simplify the description of new performance queries for P2P-based patient data sharing applications and may provide a shared method to relate present applications. In reality, there is a need for further investigation in the areas of P2P based file sharing network model.
- Although Cloud computing is capable of solving some of the technical issues faced by dynamic data sharing among healthcare providers, the exiting compliance requirement by various agencies such as Insurance Portability and Privacy Act (HIPPA) as well as security and privacy concerns will dictate that patient data will continue to be maintained by the healthcare providers. In our future work, we plan to investigate the possibility of Cloud Computing systems and mobile technologies in dynamic healthcare data sharing.
References


Ashley, P., Hada, S., Karjoth, G., Powers, C. & Schunter, M. 2003, 'Enterprise privacy authorization language (EPAL 1.2)', Submission to W3C.

Aka, T. 2005, 'Cryptographically generated addresses (CGA)'.


Blankenhorn, D. 2008, 'Microsoft HealthVault is nothing like Google Health'.


Brailer, D.J. 2005, 'Interoperability: The Key to the Future Health Care System', Health Affairs.


Clarke, I., Sandberg, O., Wiley, B. & Hong, T.W. 2001, 'Freenet: a distributed anonymous information storage and retrieval system', paper presented to the International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability, Berkeley, California, United States.


Hall, G.J. 2004, 'Advanced Web services policies & Microsoft WSE: use WS-Policy support in Microsoft WSE to secure you', Web Services Journal.


Thatcher, M.E. & Clemons, E.K. 2000, 'Managing the costs of informational privacy: bundling as a strategy in the individual health insurance market', Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, Hawaii, 4-7 JAN 2000, pp. 10


