MACQUARIE UNIVERSITY
SYDNEY ~ AUSTRALIA

Framework for Evaluating the Trustworthiness of E-Health Applications

by

Bienvenida Pagdanganan

A thesis submitted in fulfilment
of the requirements for the degree of
Master of Research
in the
Department of Computing
Faculty of Science
Macquarie University

Supervisor: Dr Rajan Shankaran
Associate Supervisor: Prof Mehmet A. Orgun

10 November 2014

Statement of Candidate

I certify that the work in this thesis entitled "**Framework for Evaluating the Trustworthiness of E-Health Applications**" has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree to any other university or institution other than Macquarie University.

I also certify that the thesis is an original piece of research and it has been written by me. Any help and assistance that I have received in my research work and the preparation of the thesis itself have been appropriately acknowledged.

In addition, I certify that all information sources and literature used are indicated in the thesis.

Mrs Bienvenida Pagdanganan
10 November 2014

TO MY FAMILY

Abstract

The 'lack of trust' is a major inhibitor in the success of e-health applications. Fears about security are an important aspect of this lack of trust. Concerns about privacy, confidentiality and security have to be addressed quite strongly to attract wide participation and use of e-health applications. The security and privacy for e-health applications must be enhanced to encourage and develop this notion of trust.

The main contribution of this thesis is an evaluation framework for assessing the trustworthiness of e-health applications. The thesis also serves as a guide for the developers to help them to integrate trust in a systematic way into e-health applications, thereby enhancing the security of e-health sites and systems. The study achieves in gathering the requirements of the propose framework by examining:

- Security and privacy requirements of e-health applications;
- Existing security technologies and mechanisms for e-health; and
- The notion of trust in e-health, and how the notion of trust can enhance security in e-health applications.

The framework presents various attributes and parameters that influence trust in e-health application. Derived primarily from the security and privacy requirements, and the existing security technologies and mechanisms for e-health, the study achieves in modelling scenarios where trust level needs to be inferred.

Acknowledgments

I most gratefully acknowledge the assistance, professional guidance, direction and supervision of Dr Rajan Shankaran and Professor Mehmet Orgun. They have been very inspiring and encouraging throughout the completion of this thesis.

I would like to thank the Faculty of the Department of Computing, especially Prof Diego Molla-Aliod, and the administrative staff, especially Sylvian Chow, for this wonderful opportunity to be able to conduct research studies at Macquarie University.

I would like to acknowledge the works of the HDR Operations (MRes) Team in providing me administrative support.

I also would like to acknowledge the St Mary's Singers Choir; this is my avenue for relaxation and spiritual inspiration.

To my friends at the Australian Computer Society, NSW Branch Executive Committee; my friends at the St Vincent de Paul Society, Punchbowl Conference and at the St Jerome's Parish community; thank you for your support.

To the healthcare professionals of Royal Prince Alfred hospital, thank you for the excellent care for my husband while I was completing this work.

To my cousin Nico who has been be inspired and achieved in completing his dissertation.

Most of all, I am very grateful for the love and support of my husband, Reynaldo; my son, Raian; my daughter, Raissa; Tess (rip), my sister who passed away here in Australia; my brother-in-law, Allan; my nephews, Alvin and Jeremy; and my extended family members, Emily and Rommel.

Table of Contents

List of Figures and Tables

Chapter 1

1 Introduction

1.1 E-Health and E-Health Applications

Innovations in health management have led to healthcare being personalised and digitised. E-health has surfaced as the most acceptable term and widely used by healthcare individuals, providers, and organisations including governments. As defined by the (World Health Organisation, 2014), e-health is the transfer of health resources and healthcare by electronic means. It encompasses three main areas: a) the diversity of health information, for health professionals and health consumers, through the Internet and telecommunications, b) using the power of IT and e-commerce to improve public health services, e.g., through education and training of health workers, and c) the use of e-commerce and e-business practices in health systems management. As such e-health refers more to services and systems that provision health related services rather than the health of people.

In (Detmer, 2001), the domains of healthcare computing are classified to include consumer informatics, medical or clinical informatics, and bio informatics. Consumer informatics is referred to as e-health and focuses on communications to patients and the public about health topics. Medical or clinical informatics relates directly to healthcare delivery. Clinical informatics encompasses three related types of computer based health records, namely: (1) a personal health record that an individual will keep to track his or her own health, (2) a patient health record that healthcare provider such as general practitioner will keep equivalent to or replacing the paper-based medical record, and (3) computer-based population or community health records that are available through several health related websites.

Consumer informatics and medical or clinical informatics are exemplified in the two projects for consumers in Tasmania (Humphries, 2005-2006). The first project is the Electronic Notification of Hospital Events (ENHE) in which notifications are sent by hospitals to general practitioners that their patients have been admitted to and discharged from hospital. The other project replaces the paper records used by ambulance staff with electronic records that will interface with emergency departments. Consumers are able to see direct relevance of the systems in place and they can visualise how these e-health systems will work and the benefits these will bring.

Another application is a computer-based personal eHealth record by (Australian Government Department of Health, 2014). There can be several subcategories of the main application like records being linked to knowledge-oriented systems or other computer based personal records of healthcare providers, e.g., therapists, clinicians and others.

A study by (Alvarez, 2002) on the promise of e-Health – a Canadian perspective, is laid in the manner and degree to which it can mitigate or resolve challenges to the health system and build on advancements in ICTs supporting the development of a health infostructure. Among the challenges highlighted in this review pertains to providing solutions to privacy and confidentiality in e-health applications.

In China, an EHR system based on cloud computing architecture has been developed and deployed in Xilingol county of Inner Mongolia using various computer resources (hardware and software) to deliver services over the health network using Internet when available (Lin, et al., 2014). An analysis done on 291,087 EHRs created from November 2008 to June 2011 evaluated the impact the EHR system has on preventive medicine and chronic disease management programs in rural China. The cloud-based EHR approach improved the care provision for village doctors in rural China and increased the efficiency of the healthcare system to monitor the health status of the population and to manage preventative care efforts. Security mechanisms are also put in place in the system using strong user authentication (user name and password), antivirus and anti-spyware software, regular operating system updates, verified browser identities and secure

connection with TLS1.0 encryption. Software checks for vulnerabilities were put in place to avoid problems such as SQL injection.

This research considers e-health applications pertaining to consumer and medical or clinical informatics. This area encompasses thousands of health-oriented websites where adequate standards and quality control may or may not be in place. Some of the e-health applications through Internet and mobile technologies include remote health monitoring, online consultation, e-prescription, e-clinical trials, patient information access and asset tracking. Studies on the information structures and processes that empower consumers to manage their own health are surveyed. The security of e-health applications related to trust would be particularly researched.

EHR or electronic health record and PHR or personal health record are used in this thesis as synonymous with e-health record.

1.2 The Research Gap

In this study we focus on the trustworthiness of e-health applications, the gap in lack of trust in the context of security of e-health applications. The 'lack of trust' is a major inhibitor in the success of e-health applications. Fears about security are an important aspect of this lack of trust. For e-health applications to be effective, each of the components that combine to make up the system must be trustworthy. Any breach of security and privacy at any one level will add to the feeling of distrust that patients have towards patient record in e-health application. E-Health systems must be viewed as accessible, safe, secure, and trusted entity.

Trust in e-health applications is a critical factor and an important precondition for people's adoption of e-health applications. The success of e-health depends upon the trust and participation of people who harbour fears about identity theft and inadvertent disclosure of health records (Hill & Powell, 2009). The lack of trust among stakeholders is a significant risk for health IT projects with a societal impact and so must be fostered (Yamamoto, et al., 2011).

Trust can depend largely on perception of reputation but is loosely used as a general term for security and privacy. The reputation of an entity is the aggregated opinion of a community towards that entity. A comprehensive score reflecting the overall opinion typically represents reputation, or a small number of scores on several major aspects of performance may represent reputation (Huang & Nicol, 2013).

The study of (Grandison & Sloman, 2000) considered a form of service trust relating to the reliability or integrity of the trustee. Trust is specified in terms of a relationship between a *trustor*, the subject that trusts a target entity, which is known as the *trustee*, i.e., the entity that is trusted. Trust forms the basis for allowing a trustee to use or manipulate resources owned by a trustor or may influence a trustor's decision to use a service provided by a trustee.

The research explores on the critical aspects in the notion of security of e-health applications, including: (1) confidentiality- the prevention of unauthorised or improper disclosure of e-health record, (2) integrity- the prevention of unauthorised modification of data, and (3) availability- the accessibility of information and data when and where they are needed. Concerns about privacy, confidentiality and security have to be addressed quite strongly to attract wide participation and use of e-health systems.

Security in e-health applications includes the challenge to provide trusted processes. The fear that personal details will be misused is a major concern, which needs to be alleviated. There should be found ways to give the patients and medical practitioners the 'same' protection in the digital clinic that they now have at the medical practitioners' health clinics. Information security is ensuring data integrity in addition to confidentiality and availability. The security and privacy for e-health applications must be enhanced to encourage and develop the trust.

Privacy is a key governing principle of the patient-physician relationship (Appari & Johnson, 2010). In (Australian Government Department of Health, 2014), the Privacy Statement explains in detail the terms of relationship between the individual owner of e-health record and the PCEHR system.

A patient or medical practitioner may have to communicate with an e-health application platform with which they have no previous contact. In this case, the belief that contacting the correct stakeholder entity and the certainty and stability of the behaviour of the entity's platform must be deemed appropriate. For instance, how can you at a minimum, ensure that your local personal computer remains trustworthy, because it may be accessed by remote software during the service?

Trust among stakeholders can be strengthened through consensual formalisation of rules into specific law (Geissbuhler, 2013). In this study a framework for evaluating the trustworthiness of e-health applications is proposed.

1.3 The Research Scope

Subsection 1.3.1 presents the research methodology, 1.3.2 presents the contributions of this thesis, and 1.3.3 gives an outline of the thesis.

1.3.1 Research Methodology

The two methods used in this research are the framework design methodology and a literature survey conducted primarily for the purpose of gathering the requirements of the propose framework.

The framework design methodology lays the courses of action considered in the framework development. These are (1) establishing requirements, (2) determining scope, (3) abstract design, and (4) modeling.

An extensive literature survey is carried out as part of this research in Chapter 2 and Chapter 3, and in sections 4.1 and 4.2 in Chapter 4, in an integrated way with a view to developing a novel framework that evaluates the trustworthiness of e-health applications. This study builds on an investigation of the security and privacy requirements of e-health applications, and on the survey of existing security technologies and mechanisms employed in e-health applications to gather the requirements of the propose framework.

1.3.2 Contributions

The main contribution of this thesis is an evaluation framework for assessing the trustworthiness of e-health applications. The thesis also serves as a guide for the developers to help them to integrate trust in a systematic way into e-health applications, thereby enhancing the security of e-health sites and systems. The study achieves in gathering the requirements of the propose framework by examining:

- Security and privacy requirements of e-health applications;
- Existing security technologies and mechanisms for e-health; and
- The notion of trust in e-health, and how the notion of trust can enhance security in e-health applications.

The framework presents various attributes and parameters that influence trust in e-health application. Derived primarily from the security and privacy requirements, and the existing security technologies and mechanisms for e-health, the study achieves in modelling scenarios where trust level needs to be inferred. An abstract design that introduces *'e-health trust metrics'* gauges trust level in terms of integrity of assessed attributes. The *E-Health Trust Metrics Manager Model* and the Framework Model are highlights of the propose framework.

1.3.3 Thesis Structure

In order to achieve the courses of action considered in the framework design, the rest of this thesis is structured as follows. Chapter 2 gathers an understanding of the security and privacy requirements for e-health applications through literature surveys. A summary gathers an understanding of the security threats and breaches. Chapter 3 presents a review of existing security technologies and mechanisms for e-health with the goal to identify the trust based security and privacy attributes and parameters that are considered in the framework. Chapter 4 presents the notion of trust in the context of security, the framework-related studies and the propose framework for evaluating trustworthiness in e-

health applications. The sections in this chapter present the requirements as use cases (scenarios) where trust has to be established, and the identified attributes for each of the scenarios. The approach for trust evaluation is discussed and the model of the framework is presented. Chapter 5 presents concluding remarks and recommendations for further research.

Chapter 2

2 Security and Privacy Requirements of E-Health Applications

Given that E-health as a discipline is rapidly evolving, one may be tempted to assume that security aspects must have been addressed, and that the resulting environment is a trusted one. Unfortunately, however, the evidence suggests that very limited research has been conducted on the area of information security risks in the healthcare sector in a holistic way. The three fundamental e-health security goals are confidentiality, integrity and availability. The requirement in ensuring data integrity in addition to confidentiality and availability is one of the key concepts in e-health information security. E-health security also involves accountability, which refers to people's right to criticise or ask why something has occurred, and non-repudiation.

This chapter identifies and examines the security and privacy requirements of e-health applications, and security threats and breaches in e-health environment though literature survey. The security and privacy requirements outlined in the chapter will be used to extract key e-health security related attributes to be used in building the trust-based evaluation framework. There are four sections; Section 2.1 presents a state of the art review of the literature in the area of e-health application security and privacy, Section 2.2 presents the e-health security and privacy requirements gathered from the review, Section 2.3 presents a summary of gathered e-health security threats and breaches, and Section 2.4 presents concluding remarks.

2.1 Literature Survey

In this section, we survey state of the art literature on security/privacy requirements and deficiencies in e-health applications. The focus of the survey is twofold: (1) to identify the

features that refer to security and privacy requirements for e-health applications, a requirement in the framework development, and (2) to identify vulnerabilities, threats, and breaches in security and privacy of e-health applications.

(1.) Security requirements for e-health records that are discussed in (Mat Kiah, Nabi, & Zaidan, 2013) involve authentication, authorisation, integrity, non-repudiation, privacy and confidentiality. The security solution proposed is a hybrid technique that combines simple object access protocol/extensible markup language (*SOAP/XML*) and cryptography techniques, such as advanced encryption standard (AES); Rivest, Shamir, and Adleman (RSA); and secure hash algorithm version 1 (SHA-1)), to improve the security of electronic medical records (EMR). XML enhancements to improve its security and privacy features are made through XML encryption, XML signature, and XML key management specification (XKMS). A database is also used for storing electronic medical records (EMRs).

(2.) A study about security issues involved in data storage and sharing of medical images through cloud is presented in (Shini.S.G., Thomas, & Chithraranjan.K, 2012). This study indicates reliability and security as main concerns. The main data security components that are considered are privacy, confidentiality, integrity and availability. The main security threats that are discussed were distributed denial of service attacks (DDoS), confidential data leakage, unauthorised access, spam, injection of malicious codes and server intrusion. Some mechanisms considered are encryption, access control, data ownership and zero tolerance using watermarking techniques.

(3.) A critically surveyed literature on information security and privacy research in healthcare is presented in the study of (Appari & Johnson, 2010). An understanding of privacy threats categorised in two broad areas of organisational threats and systemic threats is given. Systemic threats are outcomes of legal privileges to access patients' information by insiders that arise from an agent in the information flow chain exploring the disclosed data beyond its intended use. Organisational threats arise from inappropriate access of patient data by either internal agents abusing their privileges or external agents exploiting a vulnerability of the information systems. The broad spectrum of organisational threats is at the level of a) accidental disclosure, b) insider curiosity, c)

data breach by insider, d) data breach by outsider, and e) unauthorised intrusion of network systems.

(4.) Security and privacy issues in the context of e-health especially considering e-health portals that provide patients access to Electronic Health Record (EHR) has been investigated by (Stingl & Slamanig, 2008). Besides the traditional security properties, the study has focused on additional threats, namely, the disclosure attack; the anonymity set attack and statistical analysis of metadata. The study has proposed a series of methods including pseudonymisation of e-health portals, multiple identities, obfuscation of metadata and anonymous authentication to prevent attacks on patient's privacy especially from what could be considered insiders, and has made statistical analysis difficult. The proposed privacy-enhancing methods do not rely on application-layer mechanisms that can be easily bypassed by insiders, but are based on cryptographic primitives that are the state of the art.

(5.) The most complex set of risks in EHR adoption is to patient privacy and security. Medical identity theft (MIT) is identified by (Hiller, McMullen, Chumney, & Baumer, 2011) as the prime threat in EHRs. Defined as the theft of personally identifiable health information, MIT can be a type of theft where an internal employee steals a patient's information for ill-defined purposes or where an individual uses another's identity to receive medical services or goods. MIT can result in life threatening damage if the medical records of an individual are changed, stolen, or made erroneous as a result of the theft.

2.2 Gathered Security and Privacy Requirements

This section gathers the security and privacy requirements of e-health applications that are given in the studies and that will be considered in the propose framework. As a summary, the security requirements for e-health in (Mat Kiah, Nabi, & Zaidan, 2013), involve authentication, authorisation, integrity, non-repudiation, privacy and confidentiality. The main data security components considered in the study of (Shini.S.G., Thomas, & Chithraranjan.K, 2012) on the reliability and security in data

storage and sharing of medical images includes privacy, confidentiality, integrity and availability. The requirements are discussed as follows.

(1.) Authentication is the process of establishing, verifying, or proving the validity of a claimed identity of a user, process, or system. It is a design feature that permits the claimed identity of a user, process, or system to be proven to and confirmed by a second party. In order to safely share and manage access to information in the healthcare system, it is essential to be able to authenticate users, processes, or systems.

(2.) Authorisation is defined as a process ensuring that correctly authenticated users can access only those resources for which the owner has given them approval. It is the function of specifying access rights to resources related to e-health information security and computer security in general and to access control in particular. In e-health "to authorise" is to define an access policy. For example, hospital staffs are normally authorised to access patient records and this policy is usually formalised as access control rules in a computer system. During operations, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected). Resources include individual files or an item's data, computer programs, computer devices and functionality provided by computer applications. Examples of consumers are computer users, computer programs and other devices on the computer (Wikimedia Foundation, 2014). For instance, authorization, in the context of eHealth information security, may refer to rights a particular user (e.g., health professional) has with regards to eHealth service systems.

(3.) Integrity service ensures that information is accurate and is not modified in an unauthorised fashion. Integrity refers to the correctness of data; it guarantees that the data is exactly as originally generated and that it has not been changed, either intentionally or by error. In e-health the integrity of information must be protected to ensure patient safety. A system protects the integrity of data if it prevents unauthorised modification as opposed to protecting confidentiality of data, which prevents unauthorised disclosure. One important component of this protection is ensuring that the information’s entire life cycle is fully auditable.

(4.) Non-Repudiation service deals with the situation where an entity cannot deny having performed an action after it has been committed. As an example, a sender cannot deny sending a record to the electronic health register or to another person. Normally non-repudiation requires the proof of integrity of data and the proof of the origin in an irrefutable relation that can be verified by an authorised third party. Audit trails and logs and evidence of actions must be provided for legal and fairness purposes if a conflict occurs subsequently. For instance, if a physician refuses to accept false diagnosis and treatment for a patient, the log server can provide the transaction records as proof.

(5.) Privacy means protection from unauthorised disclosure of data. It refers to the claim of individuals, groups, or institution to determine for themselves when, how, and to what extent information about them is communicated to others. In e-health scenario, privacy may involve the control on the access to medical data in electronic records and in general practitioners' document records as an essential safeguard to patients' privacy.

Privacy is distinctly different from confidentiality from a legal standpoint. While confidentiality is an ethical duty, privacy is a right rooted in common law. Confidentiality refers to personal information shared with a physician, therapist, or other individual that generally cannot be divulged to third parties without the express consent of the patient. On the other hand, privacy refers to the freedom from intrusion into one's personal matters, and personal information.

(6.) Confidentiality refers to the process that ensures information is accessible only to those authorised to have access to it, and not being divulged to unauthorised parties. Health information is regarded as being among the most confidential of all types of personal information. For instance, in the context of the doctor-patient confidentially, it is crucial that healthcare providers can only consult health data if this is necessary for the treatment of a specific patient. Patients are required to share information with their physicians to facilitate correct diagnosis and treatment, and to avoid adverse drug interactions. Patient's record accumulate over time that may include significant personal information including identification, history of medical diagnosis, digital renderings of medical images, treatments, medication history, dietary habits, sexual preferences,

genetic information, psychological profile, employment history, income and physician's subjective assessments of personality and mental state. Patient's e-health record serves a range of purposes apart from diagnosis and treatment, which may include the use of information to improve efficiency within the healthcare system, drive public policy development and administration, the conduct of medical research, the sharing of information with payer organisation to justify payment of services rendered. In this context, data protection and security is a key aspect in order to increase users' acceptance of these new technologies, given the highly sensitive nature of personal health data to be transmitted to and from e health systems. As such, confidentiality is a key requirement in e-health applications.

(7.) Availability refers to the property of being accessible and usable upon demand by an authorised entity. The availability of health information is also critical to effective healthcare delivery. E-health systems must remain operational in the face of natural disasters, system failures and denial-of –service attacks.

(8.) Reliability represents the ability of a service to function correctly and consistently and provide the same service quality despite system or network failures. Reliability may be expressed in terms of number of transactional failures per month or year. Patients expect an electronic healthcare system that is totally reliable. The e-health system preserves the care and to provide the errors free service to its users requires innovative methods that can lead to qualitative improvements.

(9.) Accountability refers to processes or mechanisms whereby the performance of tasks or functions carried out by an individual or institution are subject to oversight or scrutiny by appropriate authorities and relevant stakeholders. Accountability has become a major issue in healthcare. Accountability entails the procedures and processes by which one party justifies and takes responsibility for its activities.

The work in (Gajanayake, Iannella, & Sahama, 2011) identifies four general sets of participants in a basic e-health scenario as follows.

- Health professionals (e.g. doctors, nurses, etc.)
- Non-health professionals (e.g. financial officers, laboratory technicians, etc.)
- Consumers (e.g. patients)
- Organisations (e.g. hospital, laboratory, pharmacy, health authority, etc.)

The domains these participants play a role in - or what they do to be considered to have misused patient information - have to be defined according to how information can be used in the healthcare domain. The authors argue that the underlying mechanisms of holding any of these participants accountable - or how to hold them accountable for playing a given role in a healthcare domain which consist of misusing patient information - have to be rigorously and fully defined after investigation into a specific healthcare scenario.

2.3 Security Threats and Breaches

This section identifies the security threats and breaches by entities in e-health applications highlighted in the studies investigated in this chapter. The main security threats discussed in (Shini.S.G., Thomas, & Chithraranjan.K, 2012) were distributed denial of service attacks (DDoS), confidential data leakage, unauthorised access, spam, injection of malicious codes and server intrusion. The threats are categorised by (Appari & Johnson, 2010) in two broad areas of organisational threats and systemic threats, where organisational threats include accidental disclosure, insider curiosity, data breach by insider, data breach by outsider, and unauthorised intrusion of network systems. The study of (Stingl & Slamanig, 2008) focused on additional threats namely the disclosure attack; the anonymity set attack and statistical analysis of metadata. Medical identity theft (MIT) is identified in the study of (Hiller, McMullen, Chumney, & Baumer, 2011).

The summary lists and explains each of the security incidents, breaches, threats, and entities that can launch potential threat to the security and privacy of e-health applications.

(1.) Distributed Denial of Service Attacks (DDoS) – A denial-of-service attack is one in which an attacker prevents authorised e-health users from accessing a service, but does not enable unauthorised access to any services. Distributed denial-of-service attack is a form where the attacker breaks into a lot of machines, and installs software on them to have them all attack the victim machine. These compromised machines are called zombies or drones. With enough zombies, any machine can be made inaccessible, since even if the machine itself can process packets as fast as they can possibly arrive, the link or routers in front of that machine can be overwhelmed. Since the packets are coming from hundreds or thousands of compromised machines, it is hard to distinguish these packets from packets coming from legitimate users. The DoS attack may be caused due to the large groups of legitimate users who access the e-Healthcare service provider at the same time, or the attacker continuously launches false traffic with a high data rate. The system should ensure acceptable QoS level to resist the DoS attack.

(2.) Confidential data leakage can take the form of accidental disclosure or insider curiosity. In accidental disclosure, healthcare personnel unintentionally disclose patient information to others (e.g., a mail message sent to the wrong address or inadvertent web posting of sensitive data). In insider curiosity, an insider with data access privileges pries upon a patient's record out of curiosity or for their own purpose (e.g., nurse accessing information about a fellow employee to determine the possibility of a sexually transmitted disease or medical personnel accessing potentially embarrassing health information about a celebrity and transmitting it to the media).

(3.) Unauthorised access can take the form of data breach by insider or data breach by outsider with physical intrusion. Data breach by insider happens when insiders access patient information and transmit it to outsiders for profit or revenge. Data breach by outsider with physical intrusion happens when an outsider enters the physical facility either by coercion or forced entry and then has access to patient information and transmits it to outsiders for profit or revenge.

(4.) Spam is most often considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. Real spam is generally email advertising for some product sent to a mailing list or newsgroup. E-health is rapidly shaping up as one of the key killer applications on the truly high-speed

broadband networks. Judging from the amount of health-related SPAM, it is apparent that e health applications are very vulnerable to such spamming attacks.

(5.) Injection of malicious codes such as viruses or worms. Viruses are malicious software that is a set of instructions, which when executed, inserts copies of itself into other programs. In email messages, these instructions when executed cause the malicious code to be sent in email to other users. Worms are malicious software, e.g., programs that replicates itself by installing copies of itself on other machines across a network. Consider the case where a Patient is likely to visit the doctor when he/she has an infection, but what if the e-health records in the doctor's office were infected themselves -- with viruses, worms and other malware? That could not only be detrimental to patient's health but also change the course of patient's life.

(6.) Server intrusion can take the form of unauthorised intrusion of an e-health network system that happens when an outsider, including former employees, patients, or hackers, intrudes into an organisation's network from the outside to gain access to patient information or render the system inoperable. It can also be in the form of electronic monitoring, e.g., listening to network traffic in order to capture information, i.e., capturing username and password.

(7.) A disclosure attack takes place if a person 'motivates' or even forces another one to present her EHR.

(8.) Anonymity Set Attack – In the context of anonymous authentication, anonymity is the ability to send a message so that the recipient cannot find out the identity of the sender (Stingl & Slamanig, 2008). Anonymization (Neubauer & Heurix, 2011), the removal of the identifier from the medical data, cannot be reversed and therefore prevents primary use of the records by healthcare providers who obviously need to know the corresponding patient.

(9.) Statistical Analysis of Metadata – Metadata refers to the physical representation of meta-information (meta-knowledge) – much as data are representations of information

(knowledge). Information in medical tests must be arranged as metadata using some data structure (Rubio, Alesanco, & Garcia, 2013).

E-health metadata provides information on data and about processes of producing and using data. Metadata are needed for proper production and use of the data they inform about. Metadata are analysed through a statistical meta-information system, a system which uses and produces statistical metadata, informing about statistical data, and which fulfills its tasks by means of functions like "statistical metadata collection", "statistical metadata processing", "statistical metadata storage", and "statistical metadata dissemination". Like other meta-information systems, a statistical meta-information system may be active or passive, as defined above. A user of an active e-health meta-information system, who has identified some potentially interesting data, can immediately proceed to retrieve the data from the same system. Such a system is an integrated information/meta-information system. In contrast, a user of an e-health passive meta-information system, who has identified some potentially interesting data, will have to retrieve these data from another system.

(10.) Medical Identity Theft (MIT) is defined as the theft of personally identifiable health information, MIT can be a type of theft where an internal employee steals a patient's information for ill-defined purposes or where an individual uses another's identity to receive medical services or goods.

2.4 Summary

This section presented a review of literature that reveals the security and privacy requirements for e-health applications and the security threats and breaches that are of concern in e-health systems. Several security-related attributes will be extracted from these studies, which will then be used to develop an evaluation framework for e-health applications.

Chapter 3

3 Existing Security Technologies and Mechanisms for E-Health Applications

E-Health capabilities are essentially a broad collection of IT applications, each addressing a different healthcare problem and impacting different stakeholders. The following diagram provides an illustration of the major E-Health applications under their appropriate R&D, clinical, administrative or public health classification. This framework provides a view of the scope of the technology referred to generally as E-Health.

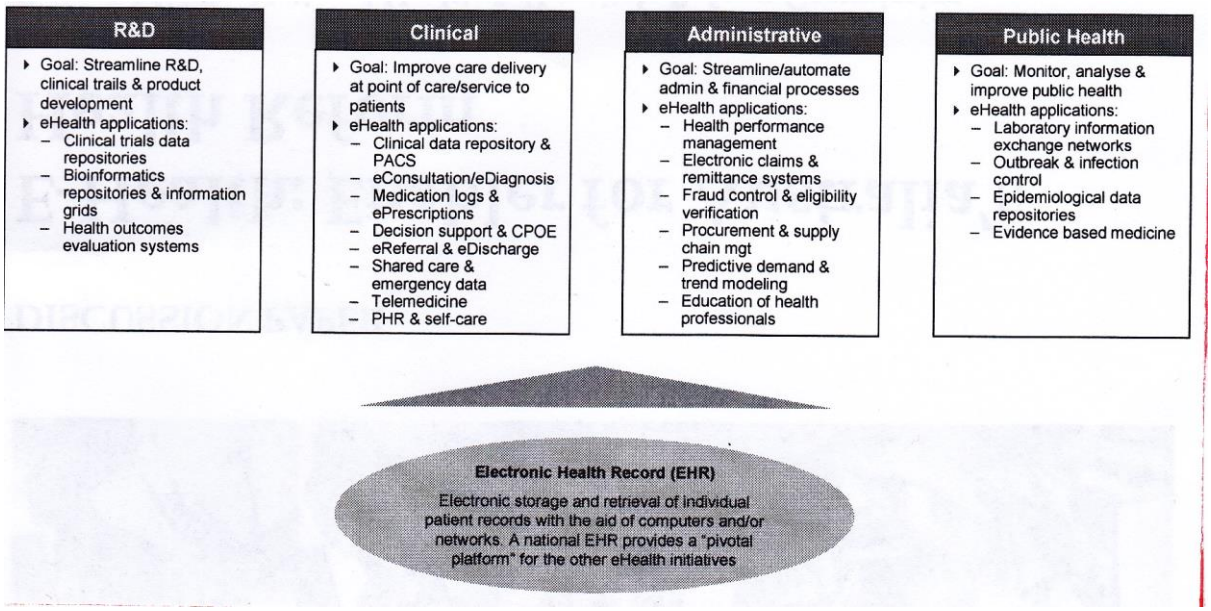

Figure 1 Classification of E-Health Applications (Bartlett, Boehncke, & Haikerwal, 2008)

Figure 1 illustrates the importance for an EHR as infrastructure that effectively supports other types of E-health applications and the potential benefits they bring. Thus, the

importance of the adoption of e-health records cannot be ignored. Despite the benefits of widespread EHR adoption, its acceptance and implementation will not be achieved unless the risks are mitigated with security technologies and mechanisms. The most complex set of risks is to patient privacy and security.

This chapter discusses security technologies, solutions, systems and services that reduce impact, or prevent or deter threats from being realised in e-health applications. This discussion is undertaken to explore key e-health systems and other approaches with a view to identify technologies and mechanisms, which could be considered attributes and entities that could be included in the propose framework for e-health applications.

This chapter has four sections. Section 3.1 presents a literature survey on existing security technology, solutions and mechanisms for e-Health applications. Section 3.2 discusses the e-health technologies and mechanisms identified in the studies, which are to be considered in the propose framework. Section 3.3 presents key e-health application systems, regulatory compliance and other approaches. Section 3.4 presents a chapter summary.

3.1 Literature Survey

The following literature survey gathers an understanding of the existing security technologies and mechanisms for e-health. The objective is to identify key e-health systems and security components, i.e., the technologies and mechanisms that are used in e health applications, which are to be considered in the propose framework.

(1.) The study of (Blobel & Roger-France, A systematic approach for analysis and design of secure health information systems, 2001) has presented an e-health security services-mechanisms relationship. The relationship is illustrated below.

Security services	**Security mechanisms**
Identification/authentication (peer and data origin)	Digital signature

Authorisation and access control	Digital signature, encryption, access control lists
Integrity	Digital signature, check values
Confidentiality	Encryption
Accountability	Audit trails, logs, receipts
Availability	Access control lists, digital signature, key escrow or key recovery
Non-repudiation	Digital signature

(2.) A study by (Narayan, Gagne, & Safavi-Naini, 2010) has explored the techniques which guarantee security and privacy of medical data stored in the cloud. The study has shown how new primitives in attribute based cryptography (*attribute-based encryption* ABE) can be used to construct a secure and privacy-enhancing EHR system that enable patients to share their data among healthcare providers in a flexible, dynamic and scalable manner. Such an ABE is known as ciphertext-policy ABE (*cp- ABE*). The user/subject attributes consist of type identifier (e.g., patient, doctor, pharmacy), and attributes that define the identity and characteristics of the subject such as name, ID, location, specialisation, etc. Access policies consist of monotone Boolean formulas on the attributes; that is - Boolean formulas that use only the logical 'or' and logical 'and' gates. For example, the policy 'doctor ∧ ID1234' states that only a user who possess the attributes **doctor** and ID1234 is allowed access. Considerations about data stored in the cloud include dispersed geographical locations by those who have access and hence can see data in transit and in their stored form.

Some assumptions were considered here in (Narayan, Gagne, & Safavi-Naini, 2010) in presenting the methodology of the research. These include the following:

a) There is a trusted authority (TA) who generates keys for the users of the system. There is also a public directory that is used by the TA to publish the system public values (such as public keys) and parameters that are needed for cryptographic operations.

b) A user is associated with (i) a unique identifier (ID), and (ii) a set of attributes (*w*). Each user has a public key and a private key. The private key is generated and issued by the TA after verifying the user's attributes.

c) The health record database is hosted on cloud storage. The cloud server is trusted for performing the requested operations but should not be able to do other unspecified operations such as reading patients' data. The health information on the storage must be kept in secured form.

(3.) The study of (Haas, Wohlgemuth, Echizen, Sonehara, & Muller, 2011) on aspects of privacy for electronic health records (EHR), has considered the enterprises that store EHRs in a centralised database system and maintain these services (e.g., Microsoft Health Vault). This scenario shifts the ownership of the EHR to the patient who becomes in charge of his/her personal health record (PHR). The PHR lose the protection of the implied trusted domain of medical institutions due to their maintenance by non-medical staff. Enabling access to an increased number of users of the PHR poses threats to security and privacy. Patients should be able to express and enforce obligations regarding a disclosure of health data to third parties.

An organisation providing EHRs should neither be able to gain access to these health data nor establish a profile about patients. (Haas, Wohlgemuth, Echizen, Sonehara, & Muller, 2011) has proposed a privacy management system that offers informational self-determination to the patients including usage control with implicit possibility to trace data flows after sensitive data has been legitimately disclosed. There are two parts in the proposal, 1) a trustworthy central EHR system and 2) a modified digital watermarking scheme to control and observe data flows after disclosure. The requirements for a privacy-preserving EHR are tied into a binding privacy policy that consists of access rules and obligations, and audit capabilities on the use and disclosure of health data. The system is divided into two subsystems namely a) data service and b) patient service. Patient service is divided into three components namely, 1) policy management, 2) logging service and 3) verification service.

(4.) A healthcare system that provides real-time data collection for the health status of patients has been developed by (Nikolidakis, Georgakakis, Giotsas, Vergados, &

Douligeris, 2010). The system simultaneously supports mobility of the patients and security for the clinical data that are transmitted between the patient and the medical personnel. Security and privacy are ensured using AES encryption and digital certificates. The study leverages the flexibility of the IP (Internet Protocol) Multimedia Subsystem (IMS) to provide seamless mobility (See also (Nikolidakis, Giotsas, Vergados, & Douligeris, 2009)).

The standardised encoding adopted used by (Nikolidakis, Georgakakis, Giotsas, Vergados, & Douligeris, 2010) is the Health Level Seven (HL7) framework by HL7 which is a non-profit, ANSI-accredited organisation dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services. The HL7 standard sends information as a collection of one or more messages, each of which transmits one record or item of health-related information. The HL7 has published the Clinical Document Architecture (CDA), which is a document markup standard that specifies the structure and semantics of a clinical document. CDA documents are encoded in Extensible Markup Language (XML) and are used for exchanging documents in heterogeneous environments. The CDA documents can be exchanged in HL7 messages, or can be exchanged using other transport solutions.

(5.) A study has been conducted by (Peyton, Hu, Doshi, & Seguin, 2007) leveraging the Liberty Alliance project that has been established in 2001 as a consortium of technology vendors and consumer-facing enterprises and which develop an open standard and set of specifications for identity management. The federated identity management in a simple scenario based on an ePrescription service is used in the study to look at the potential impact of privacy compliance on the ownership responsibilities and architecture associated with three existing components of the Liberty Alliance federated identity management framework. These components are Discovery Service, Identity Mapping Service, and Interaction Service. A fourth component (Audit Service) has been proposed to address the potential privacy breaches in Liberty Alliance.

A key concept in the Liberty Alliance Project is a "Circle of Trust" (CoT), in which federated identity management is used to create a business-to-business (B2B) network of cooperating enterprises that provide integrated services to users. These cooperating enterprises have trust relationships and operational agreements establish among them. The ePrescription scenario is one, which is used by doctors who write prescriptions, and patients who receive the prescription drugs. In the CoT, prescriptions are sent to the patient's pharmacy, ePharmacy, for fulfilment and the pharmacy is able to bill the patient's insurance company, eInsurance.

Throughout the scenario, the Identity Provider provides a single sign on (SSO) service for the CoT so that users need to authenticate or 'log in' only once. After that, each service (ePrescription, ePharmacy, and eInsurance) recognises the patient by a different pseudonym (called 'opaque identifier' in the Liberty Alliance literature) known only to them, which is provided by the Identity Provider through an Identity Mapping Service (IMS).

When a service wishes to access data about a patient from another service, it first discovers the service, which has the patient's data, using a Discovery Service (DS) within the Identity Provider to obtain an end point reference (EPR). The EPR contains security and identity tokens that allow the invoked service to extract their pseudonym or 'opaque identifier' for the patient without revealing it to the calling service. The patient must have granted permission for the two services to share the data. If not, the Identity Provider can invoke an Interaction Service, which can be used to contact the patient to obtain their permission.

From the scenario described by (Peyton, Hu, Doshi, & Seguin, 2007) above, it is gathered that the Liberty Alliance Federated Identity Management Framework is able to protect identity through a federated system of pseudonyms supported by the Identity Management Service. It is also able to control the sharing of data and protect identity using an end point reference (EPR) provided by a discovery service, as well as obtain permission from the patient by the invocation of an Interaction Service. In addition an Audit Service provides deterring functionalities on privacy breaches with audit trails providing verifiable evidence in case breaches happen. The Audit Service can be

implemented as a standard Attribute Provider data service based on the relevant ID-WSF 2.0 specifications and templates.

(6.) The HIPAA Security Rule (Walsh, 2013) has provisioned that healthcare organisations are required to perform security audits. These provisions include 1) information system activity review that requires an organisation implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports, and 2) audit controls that require the organisation implement hardware, software and procedural mechanisms that record and examine various activities in information systems that contain or use electronically protected health information.

(7.) (Fernandez-Aleman, Senor, Lozoya, & Toval, 2013) has conducted a systematic literature review (SLR) related to security and privacy of e-health applications. The article analyses security and privacy based on the ISO 27799 standard which has been specifically tailored to healthcare and defines guidelines to support the interpretation and implementation of health informatics of ISO/IEC 27002. ISO/IEC 27002 standard addresses the information security management needs of the health sector.

Of the 49 articles selected, 29 use standards or regulations related to the privacy and security of EHR data. The most widely use regulations are the Health Insurance Portability and Accountability Act (HIPAA) and the European Data Protection Directive 95/46/EC. In these reviews, 23 use symmetric key and/or asymmetric key schemes while 13 employ pseudo anonymity technique in EHR systems; 11 articles propose the use of a digital signature scheme based on PKI (Public Key Infrastructure) while 13 propose a login/password for authentication with 7 of them combine with a digital certificate or PIN. The preferred access control model appears to be the Role Based Access Control (RBAC), since it has been used in 27 studies. Of the studies, 10 discuss who should define EHR system's roles while 11 studies discuss who should provide access to EHR data: patients or health entities. Overall 16 articles indicated that it is necessary to override defined access policies in the case of emergency. In 25 articles an audit log of the system is produced. Only 4 studies mention that system users and/or health staff should be trained in security and privacy.

The SLR by (Fernandez-Aleman, Senor, Lozoya, & Toval, 2013) concludes that while in recent years the design of standards and the promulgation of directives concerning security and privacy in EHR systems have been witnessed, more work should be done to adopt these regulations and to deploy secure EHR systems.

(8.) The study of (Blobel, Intelligent security and privacy solutions for enabling personalized telepathology, 2011) presents among others, a Generic Component Model (GCM) shown in Figure 2 (see Page 37); an architectural approach to the security and privacy domain based on the GCM shown in Figure 3 (see Page 38); and the HL7 Common Security and Privacy Domain Analysis Model shown in Figure 4 (see Page 39).

GCM has been deployed as an abstract architectural representation framework for any eSystem, thereby describing the components' composition/decomposition, the representation of the domains involved, and the unified ICT development process for analysing, designing, specifying, implementing and deploying of the intended domain solution.

The architectural approach to the security and privacy presented in Figure 3 is highly specific for health due to the social impact of personal health information. In the layered security services model comprising communication security and application security, the challenge dealt with in the study pertains to the application security that covers safety, security and privacy of health-related services and personal health information.

Technical specifications that include the identification and authentication of identities are managed depending on the distinguishing features used such as knowledge, tokens, and properties. Privacy-related services such as privilege management, authorisation, access control, etc. are summarised as policies and are defined in legislation, regulation, rules, consent statements or documents, codes of ethics, etc.

A layered system of ontologies has been introduced that reflects the different granularity levels of the GCM. Application ontology describes the system with its domain and has been derived from domain ontologies. Aggregations of components within and between

different domains are restricted to the same level of granularity, presented as neighbourhood components, if the relation can be logically/ontologically proven.

The generic reference model for the informational representation of privilege management and access control in a business context standardised in the HL7 Common Security and Privacy Domain Analysis Model, shown in Figure 4 is provided as a Draft Standard for Trial Use. It is the first international standard, which took up the challenge of combining the very advanced definitions of several standards to one harmonised and comprehensive view. The offered model provides a combination of the composition/decomposition schema of policy base classes, of informational references, the actor schema as well as the action defined.

(9.) In (Blobel, Comparing approaches for advanced e-health security infrastructures, 2007), the study concludes that policies determine processes and systems. Policies define and distinguish constraints for communication and collaboration. Therefore modelling policies and performing policy bridging are the main challenges to be met.

The requirements for policy-controlled entities (actors and objects) and activities, as covered by the Access Control Model defined in ISO 22600-2 is given in Figure 5 (see Page 40). This policy by that way defines rules, conditions, and contexts related to entities and processes as required.

The Organisation for the Advancement of Structured Information Standards (OASIS) has developed the Security Assertion Markup Language (SAML) and the Extensible Access Control Markup Language (XACML) for expressing security policy statements.

(10.) In (Blobel & Roger-France, A systematic approach for analysis and design of secure health information systems, 2001), a systematic approach used in the study presents a general conceptual security model that employs methodologies such as the Unified Modelling Language and that distinguishes between communication security and application security issues.

Communication security pertains to secure messaging (secure objects, example HL7, XML) or secure connections (secure channels, example SSL/TLS). Application security deals with improvement of, e.g., authorisation and access control including the definition of roles and decision support.

In integrating security into e-health application architectures, a unified process as well as design-related meta-languages and appropriate constraint languages, such as Object Management Group's Unified Modelling Language (UML) and its Object Constraint Language (OCL), both allowing for the transfer to the XML standard set, could be used.

In the analysis of the architecture and functionalities of the system, the basic components, types and classes has been derived. Security-related use cases (scenarios) are specified where sets of security services are selected and sets of security mechanisms are identified. Figure 6 (see Page 41) presents the layered security model based on the concepts – services – mechanisms – algorithms view with different levels of granularity containing possible elements for each level.

The list of abstract security-related use cases defined in the study include the following:

- User management specifying roles and rules,
- User authentication,
- Patient consent,
- Communication initialisation,
- Information request,
- Access control,
- Information provision,
- Information transfer, and
- Audit.

An example of use case is given in Figure 7 (see Page 42), which is an abstract basic use case 'Information Transfer'.

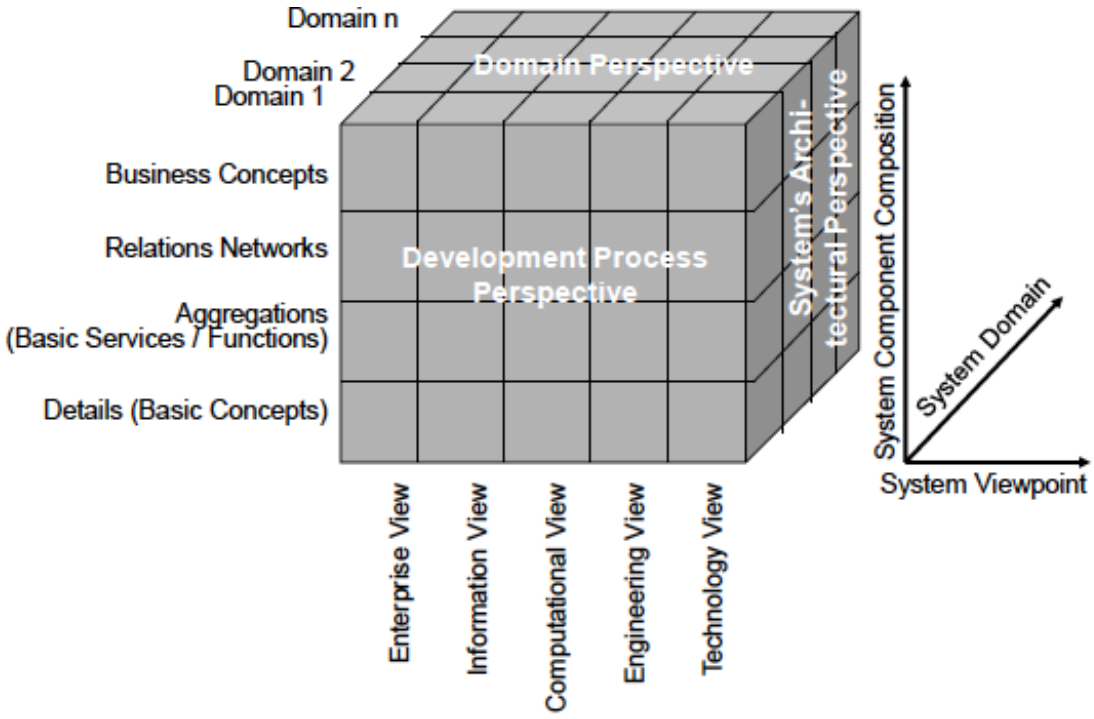

Figure 2 The Generic Component Model

(Blobel, Intelligent security and privacy solutions for enabling personalized telepathology, 2011)

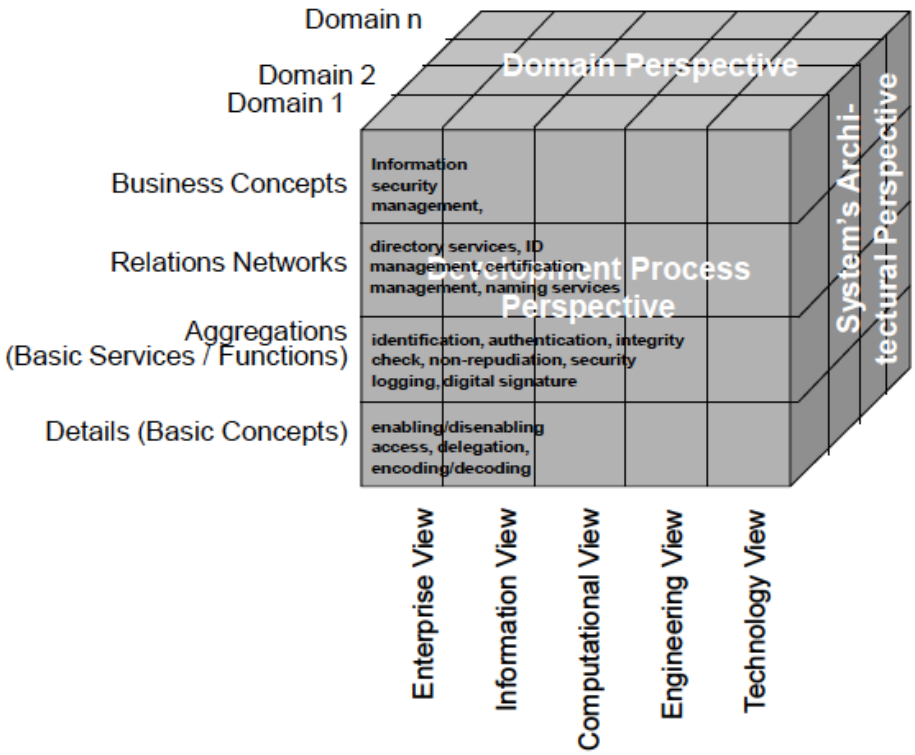

Figure 3 An architectural approach to the security and privacy domain using the GCM (Blobel, Intelligent security and privacy solutions for enabling personalized telepathology, 2011)

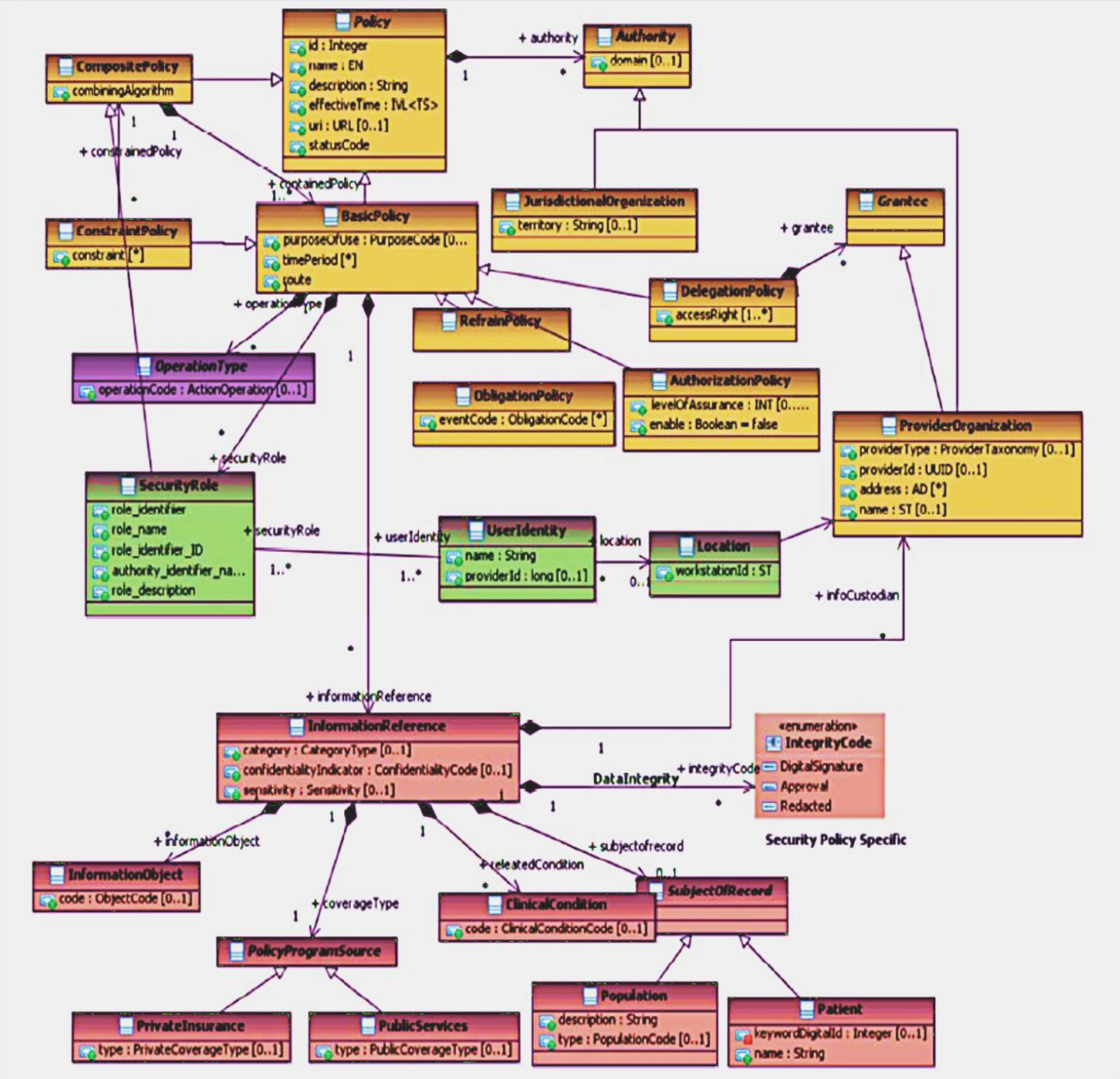

Figure 4 The HL7 Common Security and Privacy Domain Analysis Model

(Blobel, Intelligent security and privacy solutions for enabling personalized telepathology, 2011)

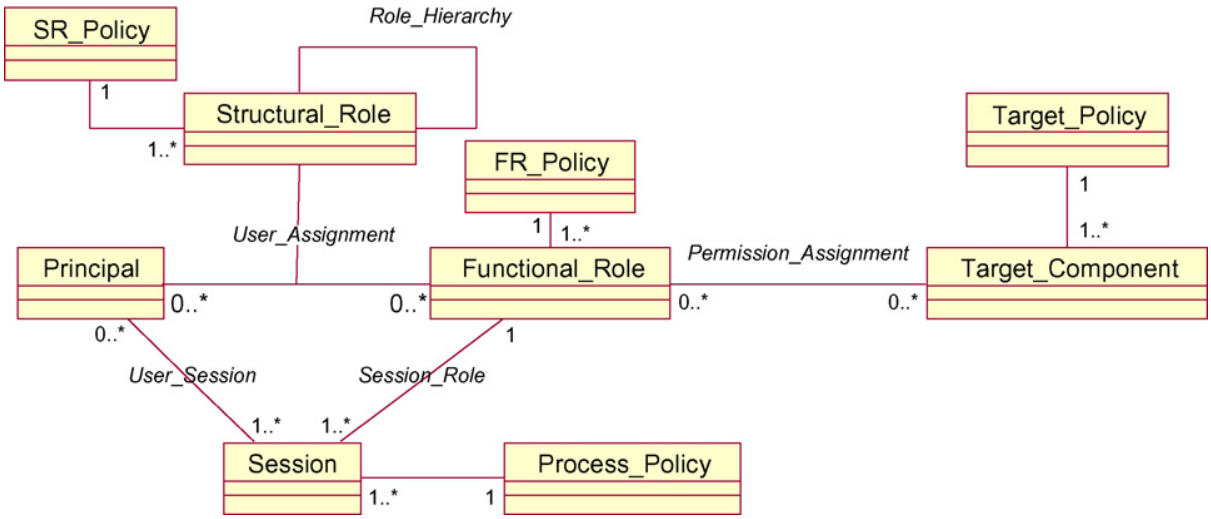

Figure 5 Policies in the context of role based access control

(Blobel, Comparing approaches for advanced e-health security infrastructures, 2007)

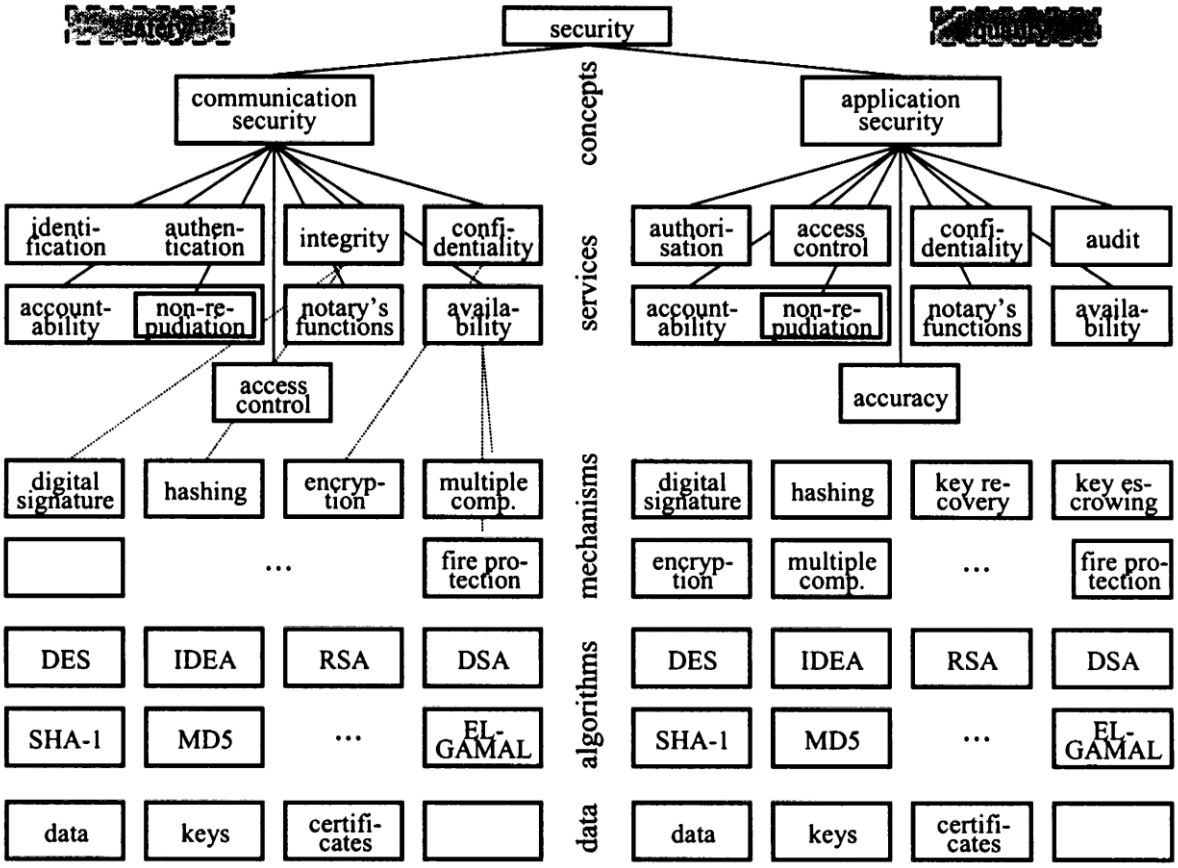

Figure 6 Layered security model based on a concepts-services-mechanisms-algorithms view

By ((Blobel & Roger-France, A systematic approach for analysis and design of secure health information systems, 2001)

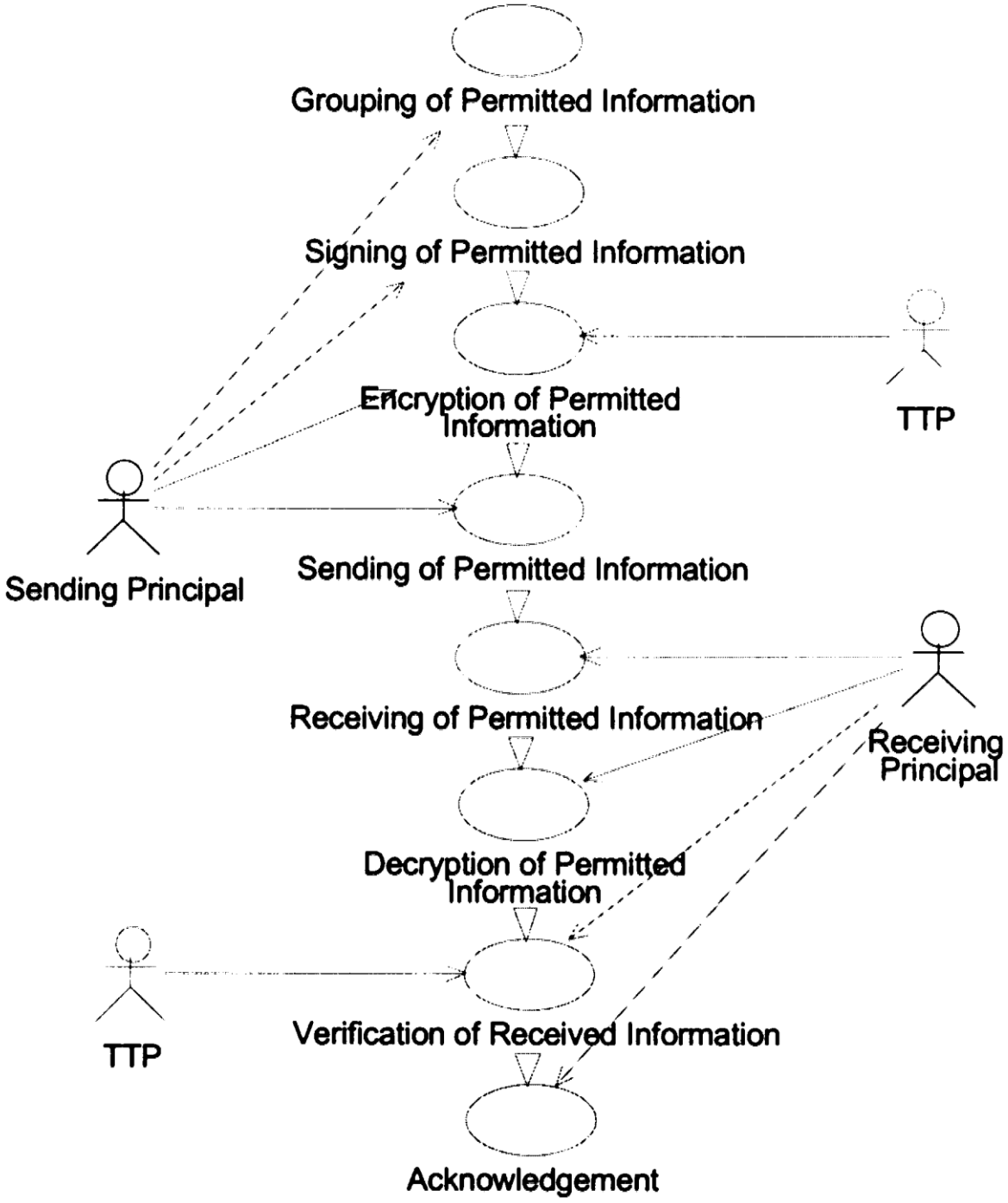

Figure 7 Abstract basic use case 'Information Transfer'

By (Blobel & Roger-France, A systematic approach for analysis and design of secure health information systems, 2001)

3.2 Gathered Technologies and Mechanisms

This section gathers the existing security technologies and mechanisms in e-health applications that are given in the literature review. These mechanisms will be considered as attributes for the propose framework for evaluating trustworthiness of e-health applications.

3.2.1 Cryptographic Based Techniques

Cryptography, considered in the study of (Narayan, Gagne, & Safavi-Naini, 2010), is the science of secret writing. It is the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling. The goal of cryptography is to design cryptosystems. In a cryptosystem, the original message is called plaintext. The mangled information is known as ciphertext. Cryptographic algorithm is a set of mathematical rules to determine transformation process. A key or keys are pieces of data that control the behaviour of a cryptographic algorithm.

3.2.1.1 Data Encryption

The process for producing ciphertext from plaintext is known as encryption, considered in the study of (Blobel & Roger-France, A systematic approach for analysis and design of secure health information systems, 2001). The reverse of encryption is called decryption. A cryptosystem consists of at least four fundamental parts: plaintext, ciphertext, encryption/decryption algorithm and cryptographic key or keys.

Data encryption increases security. In addition to data, identifiers (pseudonyms), keys and data attributes (metadata) are also encrypted. A key is a quantity used in cryptography to encrypt or decrypt information. There are two generic types of cryptographic techniques: symmetric key and asymmetric key. Symmetric cryptography uses the same key for both encryption and decryption. In an asymmetric key system, different keys are used for encryption and decryption. The asymmetric key system is

more generally referred to as a public key system. In a public key system, the two keys are mathematically related but one key cannot be derived from the other. Normally, one key is made public (for encryption) and the other key is kept secret (for decryption).
Symmetric (or secret) keys and public key (or asymmetric) schemes are used to store encrypted data. Private key or secret key refers to the quantity in public key cryptography that must be kept secret. Public key refers to the quantity in public key cryptography that is safely divulged to as large an extent as is necessary or convenient. The original purpose of cryptography is to protect sensitive data from unauthorised disclosure. However, cryptographic techniques can be used to provide a range of security services such as confidentiality, data integrity, authentication and non-repudiation.

AES (Advanced Encryption Standard) is a symmetric key algorithm adopted by the US government in 2001 as a Federal Information Processing Standard [FIPS01}. AES is a standardisation of an algorithm called *Rijndael*, named after two Belgian cryptographers who developed and submitted it- Dr Joan Daemen of Proton World International and Dr Vincent Rijmen, a postdoctoral researcher in the Electrical Engineering Department (ESAT) of Katholieke Universiteit Leuven [DAE99].

A ciphertext-policy attribute-based encryption (cp-ABE) (Bethencourt, Sahai, & Waters, 2007) is proposed in the Cloud platform to ensure that a Cloud provider cannot see (or copy) EHR data (Narayan, Gagne, & Safavi-Naini, 2010).

3.2.1.2 Public Key Infrastructure (PKI)

A PKI, considered in the study of (Fernandez-Aleman, Senor, Lozoya, & Toval, 2013), consists of the components necessary to securely distribute public keys (Kaufman, Perlman, & Speciner, 2002). Ideally, it consists of certificates, a repository for retrieving certificates, a method of revoking certificates, and a method of evaluating a chain of certificates from public keys that are known and trusted in advance, referred as trust anchors, to the target name. A certificate is a signed message vouching that a particular name goes with a particular public key.

Public key cryptography is also known as asymmetric cryptography, a cryptographic system where encryption and decryption are performed using different keys. The main

idea of public key cryptography is that both the encryption method and its key can be made public. The decryption method should not be symmetric with the encryption method, which means that there is a trapdoor for decryption. The encryption key and decryption key are separated.

The challenge with a public key system is how to make it broadly available and easily accessible to possible users and how to ensure that the correct identity is bound with a given public key. There are several methods for the distribution of public keys, such as public announcement, public directory, public key authority, and public key certificate. With a public key certificate, the responsibility of creating and updating certificates lies with a trusted authority, a Certification Authority. Any party can use the certificate to check the validity of a public key.

A Certification authority is a trusted third party whose signature is well recognised. After the public key certificate is created, the certificate can be read to obtain the identification and the public key of the certificate's owner. The user of the public key can verify that a public key originates from the certificate authority and not another entity. The public key of the certificate authority is originally distributed through some trusted channels and is assumed to be widely available in public so that its authenticity is guaranteed.

A public key certificate is a digital document used to identify an entity and the public key. It has a data part and a signature part. The data part is in plaintext and contains the identification of the entity (who has the key), the public key (what is the key), a valid period of the public key (when it is valid), and additional attributes, such as algorithm and intended use, and the signature algorithm of the certificate authority. The identification of an identity must be unique in the system. The signature part is the digital signature of the certification authority on the data part.

A Certificate Revocation List (CRL) is a digitally signed message that lists all the unexpired but revoked certificates issued by a particular Certificate Authority (CA) that signs certificates.

3.2.1.3 Digital Signature

Digital signature, considered in the study of (Blobel & Roger-France, A systematic approach for analysis and design of secure health information systems, 2001), is a digital method for signing a digital document. It is a number associated with a message and its sender that can be verified as authentic by others, but can only be generated by the sender. It has the same property as a handwritten signature in that; only one person can generate it. A digital signature indicates who has signed the message and what is signed. It guarantees that an unauthorised person cannot produce the signature. After a signature has been created, it cannot be altered without detection. Since the digital signature depends on the content of the message, if someone alters the message the signature will no longer be correct and the tampering will be detected.

The separation of public key from private key enables the idea of digital signature without third party involvement. The first international standard for digital signatures, ISO/IEC9796, was adopted in 1991 based on the RSA public key scheme. RSA is a public key cryptographic algorithm named for its inventors (Rivest, Shamir, and Adleman) that does encryption and digital signatures.

With digital signature the signing process and the verifying process can become inefficient. Another issue is that signing a message directly may not guarantee data integrity; this means the signed message can be modified and the result could still be verified successfully. Cryptographic hash function (Quantin, Jacquet-Chiffelle, Coatrieux, Benzenine, & Allaert, 2011) provides a solution to these problems.

A hash function takes a message of arbitrary length and produces a digest with a fixed size. Normally, the signature of a message is to sign the hash digest of the message and not the message directly. Hash function is a one-way function, which is easy to compute but it is computationally difficult to invert the hashing process. The hash digest must depend on the entire message and there is a small possibility for different messages to have the same-hashed digest.

3.2.1.4. Pseudo Anonymity Techniques

De-identification is the process of removing (or modifying) identifiers from the health personal data so that identification is not reasonably possible. This technique is used to prevent misuse of health data.

Pseudo anonymity technique, considered in the study of (Peyton, Hu, Doshi, & Seguin, 2007) allows third parties to access patients' health data without disclosing patients' personal data (for example, an identifier is shown rather than patients' personal data). A patient identifier hash can be used; this is a token, which is derived from applying a hash function to the patient's identifier. Hash is a cryptographic one-way function that takes an arbitrary-sized input and yields a fixed size output (Kaufman, Perlman, & Speciner, 2002). The hash function ensures that it is difficult to compute the patient's identifier from the token.

Another approach for pseudo anonymity is reversible pseudonym generation (Elger, Iavindrasana, Lo Iacono, & Muller, 2010). The standard symmetric encryption algorithm AES (Advanced Encryption Standard) can generate the pseudonym. Integrity protection is incorporated in the pseudonym in order to have the proof that the pseudonym is unaltered before reverting it. To support future inter-clinic patients' mobility, a dual-pass pseudonymisation scheme was developed, signifying that a patient's identity will result in the same pseudonym, regardless of which participating study centre collects the patient's data.

A robust cryptographic hash function to anonymise information related to a patient's identity (Quantin, Jacquet-Chiffelle, Coatrieux, Benzenine, & Allaert, 2011) is a technique that uses reversible pseudonym generation method. A list of pseudonymous partial identifiers for each patient can be generated giving a linkage probability level to each record thereby solving the risk of collision.

Another approach to pseudonymity is sharing of pseudonyms based on the threshold scheme of Shamir (Shamir, 1979) that provides mechanisms to recover lost or destroyed keys. A pseudonym tree for each patient (Alhaqbani & Fidge, 2008) is another approach where each patient can have a different pseudonym in each health provider.

Health data are exchanged between organisations by using the Cloud. The basic premise of data interoperability is to facilitate accurate and seamless data exchange within and between organisations to support timely healthcare. Anonymity is another way to secure patient information security when shared.

3.2.1.5 Authentication

Authentication, considered in the study of (Stingl & Slamanig, 2008), is the process of reliably verifying the identity of someone (or something). There are various forms of authentication including password-based, address-based and cryptographic based.

In the context of e-Health, user authentication can be defined as the way in which users prove their authenticity to the EHR. Username or identity (ID) with an associated password has been the most common user authentication mechanism in EHRs. Other access mechanisms include username/password; login/password combined with a digital certificate; password and PIN; a smart card and its PIN; a smart card, its PIN and a fingerprint; and access policy spaces.

Cryptographic based authentication can be much more secured than either password-based or address-based authentication. The cryptographic operation uses hashes, secret key cryptography, and public key cryptography.

Data authentication is the process used to ensure the origin of a data source. Authentication systems in the healthcare industry use digital signature scheme based on PKI or Digital Rights Management (DRM) (Jafari, Safavi-Naini, Saunders, & Sheppard, 2010) to control access to EHRs by licences. With DRM two certificates are employed: a security processor certificate that contains a key-pair which is used for cryptographic authentication of the machine and is bound to its unique hardware features, and a separate certificate called a rights management account certificate which contains a key-pair used for the authentication of the user and is bound to the user's unique identifier and email address.

A sufficiently secure solution to user authentication is a credential system in which only the user who holds a legitimate credential issued by a trusted authority can gain access to

the EHR (Win, Susilo, & Mu, 2006). A credential system is a system where users obtain credentials from organizations and demonstrate possession of these credentials, either implicitly or explicitly. The user who has obtained a credential can perform cryptographic operations, such as signing or decryption.

Cross-organisation authentication can be addressed by the use of federated identity management (refer to study of (Peyton, Hu, Doshi, & Seguin, 2007)). Federated technologies provide secure methods for a service provider to identify users who are authenticated by an identity provider. The Security Assertion Markup Language (SAML) is a federation standard that defines standardised mechanisms for the communication of security and identity information between business partners.

3.2.2 Access Control

Access control enforces a definition of allowed and disallowed access or use of a resource. It is a mechanism for limiting use of some resource to authorised users. There are varying types of access control, which may include mandatory, discretionary and nondiscretionary access controls.

Mandatory access control (MAC) is a system-controlled policy restricting access to resource objects (such as data files, devices, systems, etc.) based on the level of authorisation or clearance of the accessing entity, be it person, process, or device. MAC is a type of access control in which only the administrator manages the access controls. The administrator defines the usage and access policy, which cannot be modified or changed by users, and the policy will indicate who has access to which programs and files. MAC is most often used in systems where priority is placed on confidentiality.

Discretionary Access Control (DAC) is a type of access control in which a user has complete control over all the programs it owns and executes, and also determines the permissions other users have to those files and programs. Each resource object on a DAC based system has an Access Control List (ACL) associated with it. DAC is typically the default access control mechanism for most desktop operating systems. Because DAC requires permissions to be assigned to those who need access, DAC is commonly

described as a "need-to-know" access model. Discretionary Access Control provides a much more flexible environment than Mandatory Access Control but also increases the risk that data will be made accessible to users that should not necessarily be given access. An access control list (ACL) is a data structure associated with a resource that specifies the authorised users who can access the resource.

Role Based Access Control (RBAC), also known as Non-discretionary Access Control, takes more of a real world approach to structuring access control. Access under RBAC is based on a user's job function within the organization to which the computer system belongs.

3.2.2.1 Access Control Models

Access control models deployed in the healthcare industry include Role-Based Access Control (RBAC) and SitBAC. RBAC is originally developed to manage access to resources in a large computer network. It is generally presented as an effective tool to manage data access because of its ability to implement and manage a wide range of access control policies based on complex role hierarchies commonly found in healthcare organisations. Each user who has access to the system has a role, which defines his permissions and restrictions.

SitBAC is a superset of RBAC that defines scenario in which patient's data access is permitted or denied. The main concept underlying this model is the Situation Schema, which is a pattern consisting of entities along with their properties and relations. Another access control model that regulates access to medical data is based on policies that are modelled as a set of authorisations stating who can or cannot execute which action on which resource.

A unified access control scheme is an access model that supports a patient-centric selective sharing of virtual composite EHRs using different levels of granularity, accommodating data aggregation and privacy protection requirements.
A fine-grained access control and on-demand revocation can be implemented to enhance basic access control provided by the delegation mechanism and the basic revocation mechanism respectively. Policy driven RBAC can be used by health organisations, which

defines a framework to represent, and manage computable policy agreements between parties in order to exchange and use information. The policy agreements specify which information can be exchanged and under which security related circumstances. In this context, the term 'profile' is used as the set of constraints regarding the permissions assigned to users, usually represented through their role and as a corresponding set of policies.

3.2.2.2 Access Policies and Policy Spaces

Access policies are bypassed in the case of emergencies. The four different policy spaces are 1) authorised accesses, 2) denied accesses, 3) planned exceptions, and 4) unplanned exceptions. The planned exceptions space allows the definition of polices which are used to regulate emergency requests that include all the accesses that are necessary to preserve patient's health, and are inherently different from the normal routine.

3.2.2.3 User Roles

There is a need to determine who must define the roles, i.e., patients or health organisations, and what roles are created in an e-health system.

In case of an emergency, when the patient's life is at risk, it is necessary to override defined access controls. A method to ensure the patient's safety and security in case of an emergency is to have a read access open to anyone who is authorised. In majority of cases doctors were given overriding privileges. Employees can misuse broad based privileges. A security committee must verify access properness to ensure that the confidentiality of the personal health data in the e-health application is being respected.

3.2.2.4 User Authorisation

EHR data access can be granted either by the patient or by authorised health professionals. There is a need to define what kind of data is available to what kind of user. Two approaches to user authorisation are by implicit consent and by explicit consent. Implicit consent signifies that the patient consents to predefined rules unless

otherwise indicated. Explicit consent signifies that the patient forbids access unless he/she grants it.

In EHR maintained by e-health data storage enterprises, patients and health providers can grant access to health information.

3.2.3 Communication Protocol

Security in the transport layer provides an end-to-end protection. It provides application-to-application protection, and it can also include user authentication. The paper of (Marti, Delgado, & Perramon) identifies SSL/TLS or HTTPS as examples of transport layer security for mobile e-health services.

The most common communication protocol used to establish a secure connection is secure socket layer (SSLs) (Kaufman, Perlman, & Speciner, 2002). This method guaranties the secure low-cost end-to-end transmission of information over the potentially insecure Internet. Implementing a firewall and antivirus protection through security policies will further provide a more secure Internet connection. SSL allows two parties to authenticate and establish a session key that is used to cryptographically protect the remainder of the session.

3.2.4 Data Masking Methodologies

Data masking is the process of replacing existing sensitive information in store with information that is realistic but not real. Data masking techniques will obscure specific data within a database table ensuring data security is maintained.

Pharmaceutical or healthcare organisations share patient data with medical researchers to assess the efficiency of clinical trials or medical treatments. Data masking methodologies minimise or control the disclosure of patient information with global and local recoding, micro aggregation, data perturbation, data swapping, data encryption, de-identification or removal of data identifiers. Defining and identifying sensitive data to mask is only part of the solution. It is also, important to ensure data integrity to maintain

correct application behaviour after masking. Links are used to control data validity and reduce the cost of data maintenance.

3.2.5 Security Audits

System activities are traced with audit logs. Privacy officials use audit logs to determine privacy violations. These logs contain information on who accesses EHR, with what aim, and the time stamping of actions. Audit trail should comply with regulations and existing laws to prevent possible abuses later and misuse of exception mechanisms, and to define better access policies. Audit trails can serve as proofs when dispute arise regarding serious issues such as abuse of permissions, illegal access attempts, and the improper disclosure of patient's health data. HIPAA requires healthcare organisations to retain access logs for a minimum of six years (Walsh, 2013).

Audit trails can become a fundamental data security tool, as some security breaches have resulted from the misuse of access privileges by unauthorised persons. Audit logs should be accessible and understandable by patients. The current practice of auditing access logs involves identifying suspicious accesses to record base on known and simple patterns.

3.2.6 Policies

Policies define and distinguish constraints for communication and collaboration. Considered in (Blobel, Comparing approaches for advanced e-health security infrastructures, 2007), the study concluded that policies determine processes and systems.

Security policies indicate the security requirements and policies of a service, system or application. A security policy describes security tokens (e.g., identity, entitlements, authorisation), digital signatures, and encryption. An example of a security policy is the requirement that a Web service may expect a requestor to attach a security token when it sends a request to the Web service.

A Quality of Service (QoS) policy (Papazoglou, 2008) describes the functional and non-functional service properties that collectively define a service, system or application. QoS

refers to the ability of the system to respond to expected invocations and to perform them to a level commensurate with the mutual expectations of both its provider and its customers. A QoS policy includes performance requirements, information regarding service reliability, accessibility, integrity, security, scalability, and availability, transactional requirements, change management and notification, and so on. It also includes factors relating to the service-hosting environment. A QoS policy also describes technical service characteristics including response times, tolerated system interruption thresholds, levels of message traffic, bandwidth requirements, dynamic rerouting for fall-over or load balancing. QoS covers a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput, e.g. bits per second), latency (delay), and error rate. A network monitoring system must typically be deployed as part of QoS, to insure that networks are performing at the desired level.

A **Service Level Agreement (SLA)** is basically a QoS guarantee (Papazoglou, 2008) typically backed up by charge-back and other mechanisms designed to compensate users of services and to influence organisations to fulfil SLA commitments. An SLA is a formal agreement (contract) between a provider and a client, formalising the details of a service, system, or application (contents, price, delivery process, acceptance, and quality criteria, penalties, and so on). For instance, in a booking service for doctors' appointment, an SLA is an important instrument in the maintenance of service provision relationships as both service providers and clients alike utilise this. An SLA may contain the information about: (1) purpose, this describes the reasons behind the creation of the SLA; (2) parties, this describes the parties in the SLA and their respective roles, e.g., service provider and service consumer (client); (3) validity period, this describes the period of time that the SLA will cover, delimited by the start time and end time of the agreement term; (4) scope, defines the services covered in the agreement; (5) restrictions, defines the necessary steps to be taken in order for the requested service levels to be provided; (6) service-level objectives, defines the levels of service of both the service customers and the service providers agree on, and usually includes a set of service level indicators, like availability, performance, and reliability that has target levels to achieve; (7) optional services, specifies any services that are not normally required by the user, but might be required in case of an exception; (8) exclusion terms, specifies what is not

covered in the SLA; and (9) administration, describes the processes and the measurable objectives in an SLA and defines the organisational authority for overseeing them.

The paper of (Al Salami & Al Aloussi, 2013) noted that major advances in health services are required in user Quality of Service (QoS) based allocation of resources given competing applications in a shared environment provisioning through secure virtual machines. The paper pointed in addressing the problem of enabling Service Level Agreement (SLA) oriented resources allocation in data centres to satisfy competing applications demand for computing resources. E-Health offers a QoS Health Report designed to compare performance variables to QoS parameters and indicate when threshold has been crossed. E-Health graphs relevant performance metrics on the same axes as thresholds indicative of SLAs or equivalent requirement. The study suggests a methodology that helps in SLA evaluation and comparison.

3.3 E-Health Systems: Security and Regulation Standards

The following discusses some key e-health technologies that offer a range of security services. The regulatory compliance and other approaches are also taken into account to gather understanding of the mechanism.

(1.) Electronic Health Record (EHRs)/Personal Health Record (PHRs) -These e-health records store patient information with full interoperability within the enterprise. EHRs/PHRs connect different medical and technical departments. Security is considered in the creation of EHR/PHR and will give a secure and more integrated interconnection between the departments, (as in a hospital). EHR provides information into several subsystems such as patient management system, pharmacy management system, laboratory management system, radiology information system, billing and insurance system and staff management system.

An example of PHR is the Australian Government's personally controlled electronic health record system (PCEHR) (PCEHR - NETHA, 2014) or eHealth (Australian Government Department of Health, 2014). People can now register for an eHealth record

– a secure electronic summary of their important health information. PCEHR enables better access to important health information held in dispersed records across the country. E-Health brings together the technologies of unique identification, authentication and encryption to provide the foundations and solutions for the safe and secure exchange of healthcare information. PHR users can set own access controls and specify what information can be viewed and by whom. They can add own notes, and allow healthcare professionals to view this information and to also add new information to your record. This increases the ease of sharing health information. PHR users can access PHR whenever at need to, from wherever, using a web-enabled device through the consumer interface portal, even when travelling interstate.

(2.) Smart Card Technology – A smart card is a small card or similar device with an embedded integrated circuit. The chip is a powerful minicomputer that can be programmed for different applications. The chip enables a smart card to store and access data and applications securely and exchange data securely with readers and other systems. Smart card technology can provide high levels of security and privacy protection, making smart cards ideal for handling sensitive information such as identity and personal health information (Smart Card Alliance, 2012).

In Europe and beyond, smart cards are frequently used for enabling communication and application security services for health networks and personal health records (Blobel & Pharow, A model driven approach for German health telematics architectural framework and security infrastructure, 2007). The basic principle consists of a certified binding of a principal (human user, organisation, device, system, application, component, or even a single object) to its electronic unique identifier or assigned properties, rights and duties, also called attributes of that principal. Communication security services concern the identification and authentication of communicating principals.

(3.) Telemedicine is the use of telecommunication and information technologies in order to provide clinical healthcare at a remote location. It helps eliminate distance barriers and can improve access to medical services that would often not be consistently available in distant rural communities. It is also used to save lives in critical care and emergency situations. Telemedicine technologies permit communications between a patient and

medical staff with convenience and fidelity by facilitating secure transmission of medical, imaging and health informatics data from one site to another.

Security has been identified as a determinant for successful telemedicine implementations. Telemedicine requires information security and privacy on issues such as authorization, authentication and accounting. Policy and standards help in building confidence among the consumers and providers regarding the reliability and safety of the telemedicine service.

TeleMedicine Australia (TMA) is the first supplier of telemedicine technology at primary care and aged care levels in Australia. This includes telemedicine solution (AUSTM™), telemedicine peripherals, telemedicine encounter management software, and telemedicine solution for Home care (HiCare) [see www.telemedicineaustralia.com.au]. However, the TMA website has not provided information on security of their products or services.

(4.) Picture archiving and communication systems (PACS) - an integrated management system for archiving and distributing medical image data. Communication of medical images in a PACS environment is usually over the internal hospital network that is protected by a firewall from outside intruders. Medical image security is an important issue when digital images and their pertinent patient information are transmitted across public networks. Mandates for ensuring health data security have been issued for example in the US by the Health Insurance Portability and Accountability Act (HIPAA), where healthcare institutions are obliged to take appropriate measures to ensure that patient information is only provided to people who have a professional need. Guidelines, such as digital imaging and communication (DICOM) standards that deal with security issues, continue to be published by organising bodies. DICOM standard was developed with the purpose of helping the distribution, display and storage of medical images (CT, MRI, US) in mind. DICOM is a universal standard that describes the way digital data used in medicine can be transferred, stored and displayed.

(5.) Electronic Transfer of Prescription (e-prescription) – Electronic prescriptions contain patient information. Information security attributes of confidentiality, integrity

and availability must be established. The security mechanisms include digital signature by the prescribing doctor, encryption with a key when prescription is sent shared by the pharmacy. In Australia, the National E-Health Transition Authority (NETHA) asked Information Integrity Solutions (IIS) to conduct a Privacy Impact Assessment on the new features of the Electronic Transfer of Prescription (ETP) Specification known as Release 1.1. The ETP is being developed as part of NETHA's Electronic Medication Management (eMM) program and is one of the five capabilities that NETHA has identified as being necessary for comprehensive eMM.

(6.) Regulatory Compliance

Bodies of legislation are formulated with the intent to improve the privacy protection offered under existing regulations by creating incentives to de-identify health information, establishing health IT and privacy systems, bringing equity to healthcare provision and increasing private enterprise participation in patient privacy. Standards and regulations are structured to provide clear and concise expectations of efficiency, cost saving and risk avoidance.

Several legislations that provide safeguards to health information privacy and security are mentioned in the study of (Appari & Johnson, 2010); these include the Health Maintenance Organisation Act of 1973, the landmark Health Insurance Portability and Accountability Act (HIPAA) of 1996, and national initiatives such as 'State Alliance for eHealth' started in 2007 by the National Governors Association Centre for Best Practices. Federal regulations being considered by the US Congress include the Health Information Privacy and Security Act, National Health IT and Privacy Advancement Act of 2007 and Technologies for Restoring User's Security and Trust in Health Information Act of 2008.

In the US, The Office for Civil Rights enforces the Health Information Portability and Accountability Act (HIPAA) Privacy Rule, and that protects the privacy of individually identifiable health information. The HIPAA Security Rule sets national standards for the security of electronic protected health information and the confidentiality provisions of the Patient Safety Rule, which protects identifiable information being used to analyse patient safety events and improve patient safety (U.S. Department of Health & Human

Services, 2014). The Health Information Technology for Economic and Clinical Health Act (HITECH) Act of 2009 amended HIPAA.

In the European Union (EU), the Data Protection Directive 95/46/EC is the reference text on the protection of personal data. It sets up a regulatory framework that seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union. The Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the protection of these data (Europa Summaries of EU Legislation).

(7.) Other Approaches

(7.1) Health Bank is a platform for storage and exchange of patient health records patterned after a personal banking system where consumers could deposit and withdraw information. Examples of such health banking system are Microsoft's Health Vault and Google Health. However, this type of e-health application opens up a whole gamut of security risks compounding the privacy concerns such as data theft and unauthorised access.

(7.2) 'Circle of Trust' (CoT) is an emerging technology framework based on federated identity management for cooperating enterprises such as hospitals, pharmacies, labs and insurers thereby enabling them to offer web-based e-health systems to patients. In this framework, personally identifiable information is managed by a designated 'Identity Provider' who provides pseudonymous identities of patients for transactions among partners. In case of pseudonymous identity, one can link events across sessions to an identity without actually knowing the identity or any identity data. An audit service, provided by an independent organisation, logs all transactional requests made by members of CoT enabling a privacy officer or regulatory agency to validate privacy compliance or investigate allegations of privacy breaches, and for individual patients to verify how their data is being used and challenge data accuracy. Support of pseudonymous identity is central to how identity is protected in a Circle of Trust.

(7.3) The OCTAVE approach was developed at the Software Engineering Institute (SEI) at Carnegie Mellon University and was first published for use in 2001. The approach uses asset-based information security assessment, Bayesian network analysis, elicitation of user's privacy valuation using experimental economics and information security insurance contracts. The approach is considered well suited for healthcare organisations as it offers the flexibility to meet the customised needs of an organisation depending on its size and complexity. OCTAVE framework was developed on three core groups of principles – a) information security risk evaluation principles, b) risk management principles, and c) organisational and cultural principles.

(7.4) User Training- Staff training on security and privacy issues are necessary for both health staff and patients. Patients should be provided with a general education in their privacy rights and duties, including clinical data privacy. Healthcare professionals must also receive affordable security guidance. Educational tools that implement security policies and procedures may be offered.

3.4 Summary

Healthcare must invest in many information security measures such as access control systems, intrusion detection systems, policies and personnel. Security technologies and mechanisms must be in place to gain significant benefits in the implementation and utilisation of secured and trusted e-health applications. Other than the associated cost savings as an element in the changing delivery of healthcare, the reduction of care variability by the use of data to define and disseminate the best practices that are helping to deliver more effective care to a broader patient base is a benefit.

The literature survey in this chapter considers technologies, mechanisms and solutions of key e-health systems. The technologies and mechanisms gathered from the studies are discussed and will be considered as candidate attributes to be used in the proposed framework that is presented in the next chapter.

Chapter 4

4 Framework for Evaluating Trustworthiness of E-Health Applications

This chapter has several sections. Section 4.1 presents studies about notion of trust in the context of security of e-health applications. Section 4.2 discusses the framework-related studies that have some relevance to the development of the framework that is proposed. Section 4.3 presents the propose framework for evaluating trustworthiness of e-health applications and is composed of Subsections 4.3.1 and 4.3.2. Section 4.3.1 highlights the framework requirements, as scenarios (use cases) where trust needs to be inferred, and the entities in e-health applications; Subsection 4.3.1.1 reveals the attributes for trust evaluation. Section 4.3.2 highlights the design of the framework; Subsection 4.3.2.1 presents the Framework Model, 4.3.2.2 presents the trust assessment metrics, 4.3.2.3 presents the E-Health Trust Metrics Manager, and 4.3.2.4 presents an e-health trustworthiness assessment. Section 4.4 presents a summary.

4.1 The Notion of Trust in E-Health Applications

Trust may be regarded as a consequence of progress towards security and privacy objectives of application systems. Trust is defined as the security expectation of an entity from a service according to available security evaluation information of that entity (Bahtiyar & Caglayan, Extracting trust information from security system of a service, 2012).

The following studies reveal the notion of trust in e-health applications in the context of security.

(1.) The ethics of *e-trust* and *e-trustworthiness* in the context of healthcare, looking at direct computer-patient interfaces (DCPIs), information systems that provide medical information, diagnosis, advice, consenting and/or treatment directly to patients without clinicians as intermediaries, are examined in the paper of (Nickel, 2011). The claim is that designers, manufacturers and deployers of such system have an ethical obligation to provide evidence of their trustworthiness to users. The argument is based on *evidentialism* about trust and trustworthiness: the idea that trust should be based on sound evidence of trustworthiness.

Evidence of trustworthiness is a broader notion including not just information about the risks and performance of the system, but also interactional and context-based information. The author suggests some sources of evidence in broader sense that make it plausible for designers, manufacturers and deployers of DCPIs to provide evidence to users that the DCPIs is cognitively simple, easy to communicate, yet actually connected with trustworthiness. One of the evidence considered is reputational staking combined with other means of demonstrating trustworthiness.

(2.) Trust in digital data is characterised in terms of confidentiality, authenticity, and integrity (ISO, 1989). Confidentiality is the property that information is not made available or disclosed to unauthorised individuals, entities, or processes. Authenticity is defined as the corroboration that the source of data received is as claimed. Integrity is the property that data has not been altered or destroyed in an unauthorised manner. In the study of (Cao, Huang, & Zhou, 2003) on digital images, two examples in digital mammography and chest CT are illustrated to show how easy it is to change medical digital images.

An image security system based on the Digital Envelope (DE) concept has been proposed to assure data integrity, authenticity and confidentiality in a Picture Archiving and Communications System (PACS). DE has a PACS security server that monitors, as one of its functions, user access log and security events. Access information of clinical information for a specific patient include (1) identification of the person that accessed this data, (2) data and time when data has been accessed, (3) type of access (create, read, modify, delete), (4) status of access (success or failure), and (5) identification of the data.

4.2 Framework-Related Studies

Studies regarding trust and trust frameworks vary in depth and scope. Matters of trust in distributed computing are often discussed in terms of abstract concepts or security features, and it is sometimes difficult to appreciate the impact of issues pertaining to trust on the users of the system. The literatures reviewed in this section are about trust-based frameworks that have some relevance to the propose framework. The focus of the review is to have a basis for reference and comparison, and to explore the methodologies used in the studies to determine differences in approaches towards the development of propose framework for evaluating the trustworthiness of e-health applications.

(1.) In a previous study, (Pagdanganan, 2009) draws a framework for trust management to formalise trust negotiation in Web services. A hybrid trust model has been proposed (see Figure 8 Page 65) for managing trust incorporating hard trust and soft trust. Hard trust is policy-based and soft trust is reputation based. The approach is developed within the context of different environments and targeting different requirements. Hard trust relies on "strong security" mechanisms such as signed certificates and trusted certification authorities in order to regulate the access of users to services. The result is a binary decision – trusted or not. Soft trust relies on a "soft computational" approach, a method of evaluation of soft trust attributes developed in the study and illustrated through a hypothetical example. In this case, trust is typically computed from local experiences and feedback given by other entities in the network and some related classifications. The approach is trust relationships are based on the exchange and brokering of hard trust attributes and on the support of soft trust attributes that have been established by the corresponding security authorities.

Policy-based trust has been developed within the context of structured organisational environments. Reputation-based trust addresses the unstructured user identity involving reputation, experience, and feedback in the community and/or service usage. Different types of attributes are described for hard trust and soft trust. The composition of the types of attributes involving hard trust and soft trust, shown in Figure 8, includes hard trust attributes, and reputation-based soft trust attributes as trust requirements for trust

management in web services-based service oriented architectures. Soft trust attributes are associated with dynamic and human behaviour and computation of soft trust is based on categories of conditions imposed on the provider and requester, for example 'Is Citizen' = 'Y'. The overall weight of these trust attributes is balanced, provider attributes against requester attributes, to determine whether the resulting trust has a positive or negative influence on the relationship.

The study prescribes the creation of a Reputation Authority, which is a soft trust attribute authority body that evaluates reputation-based trust. The Reputation Authority can validate the Reputation Rating of the user for a given role or capability as identity based attributes for the user. The approach to evaluate reputation is by using weighted values, which is then referred as 'Reputation Token', a precondition for the exchange of identities and security tokens that are hard attributes associated with the customer or client. The study provides:

- A framework for a hybrid trust model incorporating hard trust and soft trust, and the attributes in hard trust and soft trust;
- A methodology by example for evaluating reputation-based soft trust attribute;
- A methodology by example for incorporating soft trust attributes in a service policy;
- An institution of Reputation Authority as soft trust authority body; and
- A federation based trust model in Web services incorporating soft trust, Reputation Authority, and soft trust attributes.

Figure 8 shows the Hybrid Trust Model and lists soft trust attributes and hard trust attributes. Some of the claimed attributes for a hard trust or policy-based trust are also listed and include user name and password, secret keys, digital signatures, digital certificates, certificates from trusted authorities, and proof of possession.

In this research, we adapt the trust model of (Pagdanganan, 2009) with variations, and the design methodology is adapted in some ways to develop the propose framework for evaluating trustworthiness in e-health applications.

Trust Management Model – Hybrid Trust Model	
Reputation Based or Soft Trust	**Policy-Based or Hard Trust**
Soft Trust Attributes	Hard Trust Attributes
• Reputation	• Claims – e.g. username and password, secret keys, digital signatures, digital certificates, certificates from trusted authorities, and proof of possession
• Reference	
• Membership	• Security Token
• Experiences	• Policy
• Community Feedback	
• Audit Trails	
• Record of Usage Services	
• Acceptance/Rejection of Services	

Figure 8 Trust Management Framework (Pagdanganan, 2009)

(2.) An entity-oriented model is proposed by (Bahtiyar & Caglayan, Trust assessment of security for e-health systems, 2014) for trust assessment of security of an e-health system. Entities are autonomous agents or software applications that represent patients. An entity can interact with many services and other entities to obtain information for trust assessments. The security system of an e-healthcare service from an entity point of view is represented with atomic units. Each entity generates information about all atomic units of an e-healthcare service by observations and obtaining information from other entities. An entity can observe only security mechanisms of an e-healthcare service as the security system of the service.

The model facilitates an entity to assess the trust using a novel set of trust assessment metrics of all properties of a security system (total metrics) or some properties of the security system (partial metrics) depending on the contextual need. Partial metrics are about a specific security property whereas total metrics are about all security properties of

an e-healthcare service. Trust assessments are carried out in trust assessment systems of entities. Six trust metrics determine the trust of a security system based on the needs of an entity and specific to security context of e-health systems in emerging open environments. These are partial and total metrics definition for trust level; confidence and relative trust assessment metrics.

The propose framework for evaluating trustworthiness has a similar approach with (Bahtiyar & Caglayan, Trust assessment of security for e-health systems, 2014) with regard to using a novel set of trust assessment metrics.

(3.) The study of (Piliouras, et al., 2011) has one of the goals to provide healthcare professionals with tools to make informed decisions on health information technology, so the adoption of EHR is not rejected out of hand based on fear or accepted without appropriate due diligence. A multiple-criteria decision model of trustworthiness is presented in the study that involves the following steps:

1. Define relevant decision factors
2. Collect data related to decision factors
3. Assign a certainty value to the perceived credibility of collected data
4. Use collected data and associated certainty value as inputs to mathematical model for trustworthiness and compute *Trustworthiness* score for EHR.
5. Sort all EHR candidates based on their trustworthiness score, from high to low. The ranking indicates the preference order of one EHR over another.
6. Examine the potential weakness in decision factor hierarchy and identify risk mitigation strategies.

The trustworthiness model is of the following general form:

$F(X) = Operator\ (D_1^{c_1}, D_2^{c_2}, \ldots\ldots, D_n^{c_n})$;

Where:

- D_j represents a decision factor associated with trustworthiness;
- C_j represents a weighing or certainty factor associated with D_j;
- "$Operator$ " represents a general mathematical aggregation procedure for computing a Trustworthiness score based on the weighted decision factors;
- $F(X)$ represents an overall Trustworthiness score.

Key features of the model include:

- Objective and/or subjective criteria used in the evaluation process, for example, system availability expressed as percentage, and reputation that is a subjective factor where standard of measurement may be based on personal preferences and opinions of decision maker.
- Multiple decision factors, (D_j), are used to assess EHR trustworthiness, depicted in the study in a hierarchy, with the most fundamental level – security – representing the foundation of EHR trustworthiness.
- Decision factors include security, governance and regulatory compliance, functionality, system performance, vendor characteristics, and user characteristics. The decision factors are expressed on a scale between one (indicating complete trustworthiness) and zero (indicating completely untrustworthy).
- Each decision factor is associated with a certainty, (C_j), weighting factor that expresses the level of confidence in the evidence used to assess (D_j), and maybe expressed by a single dimension of certainty, or as an aggregate of multiple dimensions of certainty.

Trustworthiness is calculated as the sum over all decision factor hierarchies, (D_j), raised to the power ($^1/_{C_j}$) – where $C_j$is defined as the certainty associated with D_j; hence $\sum(D_j)^{1/C_j} = Trustworthiness$. The trustworthiness model has been adapted in our study.

(4.) We have a similar approach with (Coetzee & Eloff, 2006) in inferring trust level. A framework for trust assessment and computation developed by (Coetzee & Eloff, 2006) considers the dynamic and fluid nature of web services. The trust framework, characterised by information and reasoning, has mechanisms that allow web services entities to manage trust autonomously by activating a trust level and trust types by means of a fuzzy cognitive map (FCM). The framework gives a web service the ability to determine the trustworthiness of others at execution time, instead of determining such trustworthiness manually or by means of cryptographic PKI frameworks. Figure 9 shows the trust manager proposed in the study of (Coetzee & Eloff, 2006).

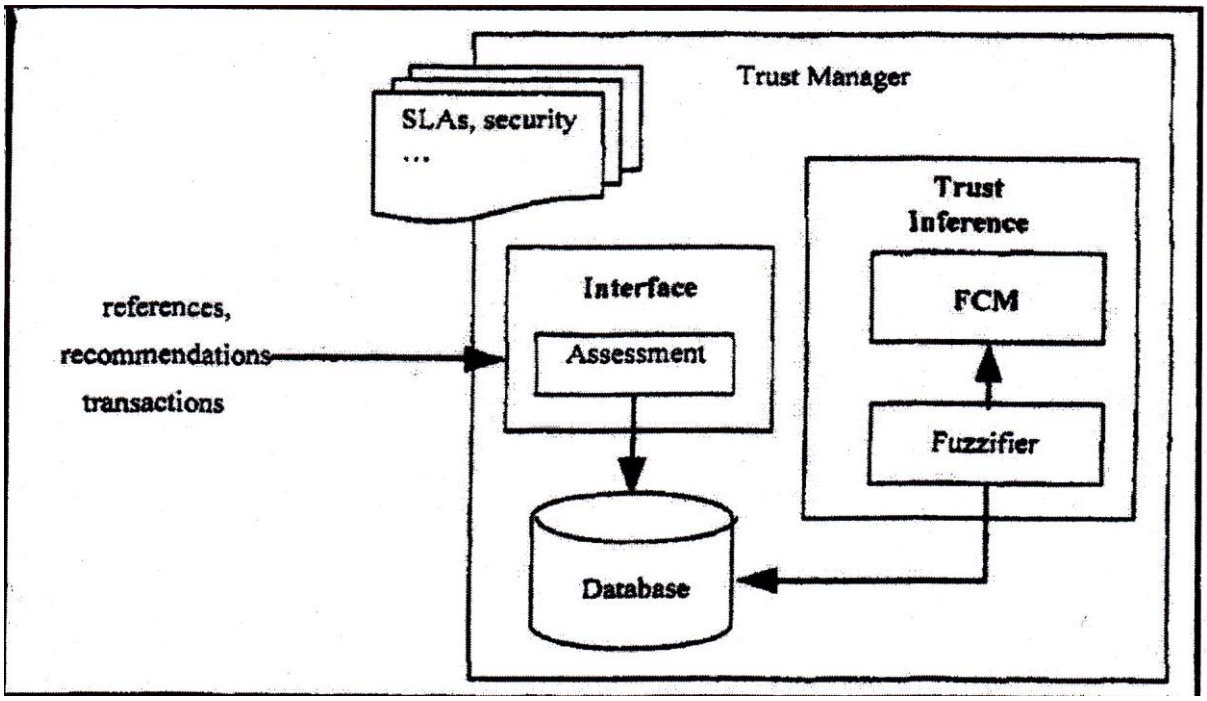

Figure 9 Web services architecture for trust (Coetzee & Eloff, 2006)

The Trust Manager makes explicit the role of security mechanisms and controls in trust assessment, and identifies additional elements such as competence, over which trust can be formed. Nodes of the FCM represent trust concepts that are used to describe the main behavioural characteristics of the system. An Interface component intercepts SOAP messages, applies rules to analyse and categorise the information, and stores information in a database. The Trust Inference component populates nodes of the FCM with values in the fuzzy interval range [0, 1] after information is fuzzified. Finally a trust level is inferred. Trust levels are defined as the set {*ignorance, low, moderate, good, high*} where *ignorance* $\subseteq$ *low* $\subseteq$ *moderate* $\subseteq$ *good* $\subseteq$ *high.*

In our framework we have *'e-health trust metrics'*, that are used as *'expected values'* referring to trust levels and is defined as the set {'*high integrity', 'average integrity', 'low integrity',* '*no integrity*'}. The *'e-health trust metrics'* are stored and managed by an entity called '*e-Health Trust Metrics Manager'* that is similar to the Trust Manager in (Coetzee & Eloff, 2006).

4.3 The Framework

This is a novel framework that is built on the requirements gathered through an exploration of literature in Chapters 2 and 3. The framework components developed include: 1) the requirements, i.e., use cases, entities and attributes where trust needs to be inferred, and 2) the abstract design, scope, and models.

4.3.1 The Requirements

Gathered through literature surveys in Chapters 2 the security and privacy requirements are defined and include: 1) authentication, 2) authorisation, 3) integrity, 4) non-repudiation, 5) privacy, 6) confidentiality, 7) availability, 8) reliability, and 9) accountability. In Chapter 3, User and Application/service are identified as entities in e-health applications.

The requirements are summarised as scenarios where trust needs to be inferred, as cases where User wishes to invoke Application/service, considering the security and privacy requirements and vice versa, i.e., Application/service verifies User. The use cases are as follows.

- On authentication
  - User verifies the identity of the application/service
  - Application/service verifies the identity of user
- On authorisation
  - Authorised user invokes application/service
  - Application/service verifies authorisation level of user
  - Application/service verifies user's access privileges and capabilities through access policy
- On integrity
  - User verifies that the information in the application/service is accurate and not modified in an unauthorised fashion
  - Application/service ensures the integrity of data through unauthorised modification

- On non-repudiation
  - User cannot deny having performed an action after it has been committed
  - Application/service verifies that user has performed an action
- On privacy
  - User verifies unauthorised disclosure of data
  - Application/service ensures unauthorised disclosure of data
- On confidentiality
  - User verifies unauthorised access to data
  - User ensures information is not divulged to unauthorised parties
- On availability
  - Application/service ensures that it is accessible and usable upon demand
  - Application/service verifies authorised user access the system
- On reliability
  - Application/service ensures it function correctly and consistently
  - Application/service ensures it provides the same service quality despite system or network failures
- On accountability
  - User can be monitored by appropriate authorities

4.3.1.1 Attributes For Trust Evaluation

Each of the use cases identified in subsection 4.3.1 requires the attributes that User and Application/service must submit for trust evaluation. These attributes are identified from the gathered technologies and mechanisms discussed in Chapter 3. Table 1 lists the requirements, use cases (scenarios), User attributes, Application/service attributes and source technology/mechanisms where the attribute is derived or obtained.

A similarity can be inferred in this approach of presenting the requirements, scenarios, attributes and source technology/mechanisms with the abstract security-related use cases in the study of (Blobel & Roger-France, A systematic approach for analysis and design of secure health information systems, 2001) (Blobel & Roger-France, A systematic approach for analysis and design of secure health information systems, 2001).

Table 1 Requirement, Scenario, User Attribute, Application/Service Attribute, Source Technology/Mechanism

Requirement	Scenario	User Attribute	Application/Service Attribute	Source Technology/Mechanism
Authentication	- User verifies the identity of the application/service - Application/service verifies the identity of user	- User name - Password	- Public key certificate	- Cryptography - Authentication
Authorisation	-Application/service verifies authorisation level of user - Application/service verifies user's access privileges and capabilities through access policy	- User Role - Access Rights and Privileges	- Access Policy - Resource Access Control Policy	- Cryptography - Access Control
Integrity	- User verifies that the information in the application/service is accurate and not modified in an unauthorised fashion - Application/service ensures the integrity of data through unauthorised modification	-Digital signature		- Cryptography - Data Encryption
Non-repudiation	- User cannot deny having performed an action after it has been committed	- Experience - Reputation	- Audit Trail - Transaction logs	- Cryptography - Authentication
Privacy	- User verifies unauthorised disclosure of data	- Experience - Reputation	- Access Policy	- Access Control
Confidentiality	- User verifies unauthorised access to	- Experience - Reputation	- Access Policy	- Cryptography - Authentication

	data - User ensures information is not divulged to unauthorised parties			- Access Control
Availability	- Application/service ensures that it is accessible and usable upon demand - Application/service verifies authorised user access the system	- Experience - Reputation	- Audit Logs - Record of down time	- Policies - Security Audits
Reliability	- Application/service ensures it function correctly and consistently - Application/service ensures it provides the same service quality despite system or network failures	- Experience - Reputation	- Audit Logs - Record of transactional failures per month or year	- Policies - Security Audits
Accountability	- User can be monitored by appropriate authorities	- Reputation	- Audit Logs	-Cryptography - Security Audits
Accessibility	- User invokes application/service	- User name - Password	- SSL - QoS - SLA	- Cryptography - Authentication - Policies

4.3.2 The Abstract Design, Scope and Models

Our approach is premised on hybrid trust following the study of (Pagdanganan, 2009) that has proposed a hybrid trust model which is composed of hard trust and soft trust and the study of (Habib, Varadharajan, & Muhlhauser, 2013). Other than identifying User attributes and Application/service attributes, each of these attributes is classified as hard trust attribute or soft trust attribute. Hard trust attributes refer to strong security mechanisms and mature technologies. Soft trust attributes relies on behaviour or experience, over time the return value in assessing soft trust attributes may vary. The process of gathering the listed soft trust attributes is not the scope of this study, however, the study of (Nickel, 2011) mentions about evidentialism. A summary of the categorised e-health hybrid trust model is presented in Table 2.

Table 2 Hybrid Trust Model

Hard Trust			Soft Trust	
User Attributes	Application/service Attributes		User Attributes	Application/service Attributes
- User name	- Public key certificate		- User Role	- Access Policy
- Password	- SSL		- Access Rights and Privileges	- Resource Access Control Policy
- Digital signature	- QoS		- Experience	- Audit Trail/Log
- Digital certificate	- SLA		- Reputation	- Transaction Log
- Secret keys				

4.3.2.1 The Framework Trust Model

The propose framework gathers attributes from the security and privacy requirements of e-health applications in Chapter 2 and from the existing technologies and mechanisms for e-health applications in Chapter 3. The attributes are associated to User and Application/service entities. Figure 11, shows the Framework Trust Model.

Framework Trust Model: Attribute Based Hybrid Trust Model			
Hybrid User Trust		Hybrid Application/Service Trust	
Hard Trust	Soft Trust	Hard Trust	Soft Trust
User Attributes		Application/Service Attributes	
Hard trust attributes	Soft trust attributes	Hard trust attributes	Soft trust attributes
- User name	- User Role	- Public key certificate	- Access Policy
- Password	- Access Rights and Privileges	- SSL	- Resource Access Control Policy
- Digital signature	- Experience	- QoS	- Audit Trail/Log
- Digital certificate	- Reputation	- SLA	- Transaction Log
- Secret keys			

Figure 10 Framework Trust Model

4.3.2.2 Trust Assessment Metrics

We introduce '*e-health trust metrics'*, a novel set of trust assessment metrics that gauges trust level in terms of integrity of assessed attributes. Integrity refers to correctness of the assessed attribute. '*E-health trust metrics*', used as '*expected values',* have trust levels that are expressed in the set {'*high integrity', 'average integrity', 'low integrity', 'no integrity'*} *where ('no integrity' < 'low integrity' < 'average integrity' < 'high integrity').* The computational equivalents are *high integrity = 1, no integrity = 0, 0 < low integrity ≤ 0.5, and 0.5 < average integrity < 1*.

Trust in each of the scenarios in Table 1, evaluated through attributes, returns a trust level expected as a value in the '*e-health trust metrics'.*

Hard trust evaluates to '*e-health trust metric*' {'*high integrity'* or *no integrity'*}. Soft trust evaluates to any level in the set {'*high integrity', 'average integrity', 'low integrity' and 'no integrity'*}.

When trust is established in each of the requirements, the gathered security threats and breaches will be mitigated.

4.3.2.3 The E-Health Trust Metrics Manager

We institute an '*e-Health Trust Metrics Manager'* that stores and manages for every User and for any Application/service, the attributes and corresponding attributes' *'e-health trust metrics'.* E-health trust relationship is defined in this study as the characteristic that a User or an e-health Application/service willingly sends its attribute to rely upon the '*e-Health Trust Metrics Manager'* in obtaining its '*e-health trust metrics'.* '*E-Health Trust Metrics Manager'* intercepts the request in order to obtain an assessment of the attribute in the form of an '*e-health trust metric'.* The model is shown in Figure 10. It has some similarity with the model for Web services architecture for trust by (Coetzee & Eloff, 2006).

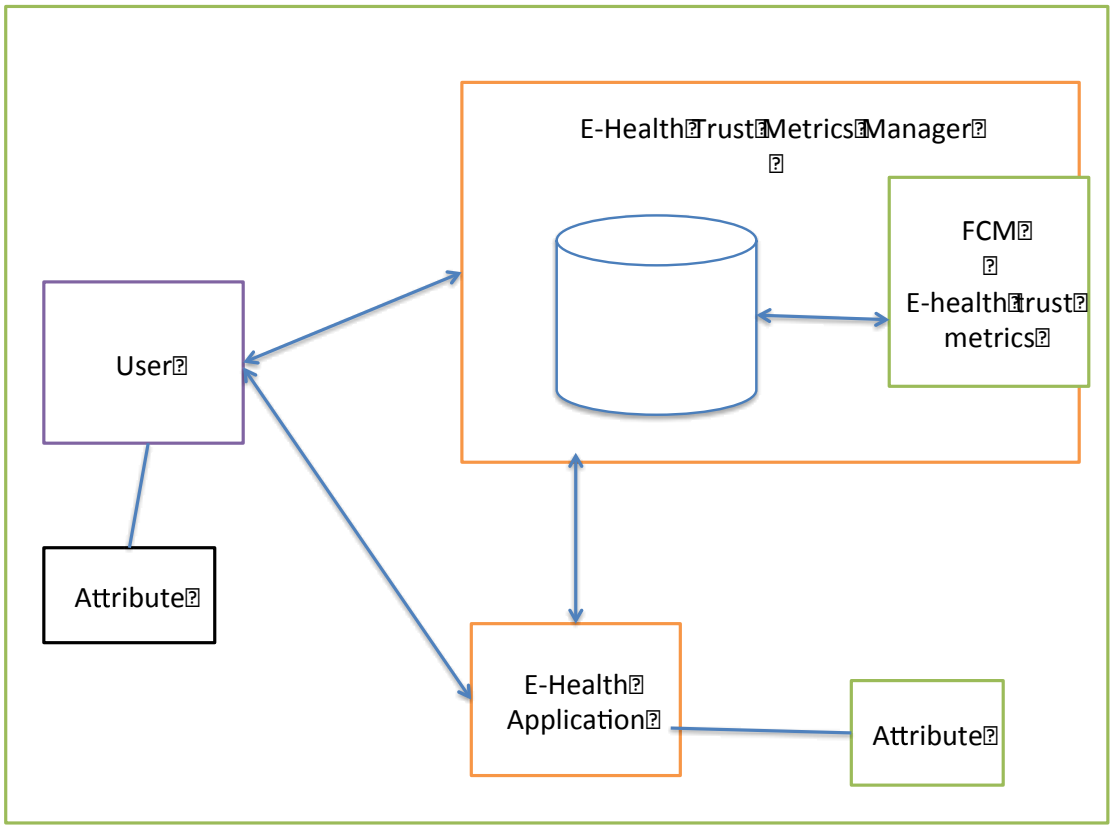

Figure 11 E-Health Trust Metrics Manager Model

For example, when User sends user name and password to invoke an e-health Application/service, '*e-Health Trust Metrics Manager*' verifies that the attributes are authentic and returns either a '*high integrity*' *or* '*no integrity*' result. The interface is a message box that indicates to User about the result of trust evaluation.

We propose that '*e-Health Trust Metrics Manager*' has the task to do E-Health Trust Attribute Certification. The '*e-Health Trust Metrics Manager*' stores attribute assessment trust level expressed as '*e-health trust metric*' contained in the set {'*high integrity*', '*average integrity*', '*low integrity*', '*no integrity*'}.

An e-health trust attribute certificate (EHTAC) is a statement digitally signed by the '*e-Health Trust Metrics Manager*' to certify that the EHTAC holder has a set of specified

attributes. While it is envisioned that '*e-Health Trust Metrics Manager'* is also a database management service, its implementation is not in the scope of this thesis.

4.3.2.4 Trustworthiness Assessment

Trust is inferred in each scenario listed in Table 1. The granularity of established trust in this research is based on the scenarios. Calculated trust on each of the scenarios is determined through the assessment of attributes sent by User or Application/service.

Hard trust attributes are strong security mechanisms and hard trust evaluates to '*e-health trust metric*' {'*high integrity' or 'no integrity'*}.

Soft trust attributes evaluates to any value in the set {'*high integrity', 'average integrity', 'low integrity', 'no integrity'*}.

A fuzzy computational model for soft trust computation that will derive rating or score that can evaluate into expected values of the '*e-health trust metrics*' is not in the scope of this study. Nonetheless a fuzzy computational model for trust and reputation propose by (Bharadwaj & Al-Shamri, 2009) can be integrated in the framework.

In (Bharadwaj & Al-Shamri, 2009), trust and reputation systems are rating systems where each individual is asked to give opinion after completion of each encounter in the form of ratings. The set of all partners (users) is represented as A = $\{a_1, a_2, \ldots\ldots, a_m\}$ where M is the number of partners in the system. Each partner will rate the other after completing the encounter. An encounter $e_k \in$ E is an ordered pair given as follows.

$e_k(a_i, a_j) = (r_{a_i}^{e_k}(a_j), r_{a_j}^{e_k}(a_i))$ where $r_{a_i}^{e_k}(a_j)$, is the rating partner a_i has given rating to partner a_j for encounter e_k. The rating scale Z can take the form Z_{β} = {3, 2, 1, 0} that can be translated into {'*high integrity', 'average integrity', 'low integrity', 'no integrity'*}. The set of ratings partner a_i has given to partner a_j is $S_{a_i}(a_j) = \{r_{a_i}^{e_k}(a_j) \mid e_k \in \text{E}\}$. The whole past history of partner a_i is $H_{a_i} = \{S_{a_i}(a_j) \mid \square\ a_j(\neq a_i) \in \text{A}\}$. An empty set occurs when both partners do not rate each other.

Trustworthiness is a result of the aggregation of the results of computation of each of User and Application/service hybrid trust attributes. The soft trust attributes vary the trustworthiness assessment of e-health applications. The trustworthiness model patterned from the study of (Piliouras, et al., 2011) is propose to be of the following general form:

$F(X) = Operator\ (HT_1^{c_1}, HT_2^{c_2}, \ldots\ldots, HT_n^{c_n})\ (ST_1^{e_1}, ST_2^{e_2}, \ldots\ldots, ST_n^{e_n})$;
Where:

- HT_j represents an assessment associated with trustworthiness of hard trust attributes;
- C_j represents a weighing or certainty factor associated with HT_j;
- ST_j represents an assessment associated with trustworthiness of soft trust attributes;
- E_j represents a weighing or certainty factor associated with ST_j;
- "$Operator$ " represents a general mathematical aggregation procedure for computing a Trustworthiness score based on the weighted assessment factors;
- $F(X)$ represents an overall Trustworthiness score.

The computational value of trustworthiness of e-health application will have the conversion equivalent to the values of the set in the trust assessment metrics.

4.4 Summary

This chapter has revealed a notion of trust in e-health applications from the two studies reviewed. The framework studies are considered with a view to gain a basis of reference and comparison in the development of the presented propose framework.

Chapter 5

5 Conclusions and Recommendations

5.1 Conclusions

This research has been achieved using the two methods employed, namely the framework design methodology and an exploration of literature primarily for the purpose of gathering the requirements of the propose framework. The main contribution of this thesis is a novel framework for evaluating the trustworthiness of e-health applications.

There has been a systematic approach in developing the framework. In Chapter 2 we gather the security and privacy requirements from the literature reviews. In Chapter 3 we gather the technologies and mechanisms for e-health from the literature reviews, and identify the entities and attributes of the entities. In Chapter 4 we present the use cases (scenarios) that are laid as a guide for developers to help them to integrate trust in a systematic way into e-health applications, thereby enhancing security of the sites and systems. We present the various use cases (scenarios) and attributes that require the evaluation of trust in e-health applications. We present our approach to trust evaluation that relied on trust based on the notion of hybrid trust, which is composed of soft trust and hard trust.

We introduced '*e-health trust metrics'* that gauges trust levels in terms of integrity of assessed attributes. '*E-health trust metrics*', used as '*expected values',* have trust levels defined in the set {'*high integrity', 'average integrity', 'low integrity', 'no integrity'*} *where high integrity = 1, no integrity = 0, and ('no integrity' < 'low integrity' < 'average integrity' < 'high integrity').*

We instituted an '*e-Health Trust Metrics Manager'* that stores and manages for every user and for any application/service, the attributes and corresponding attributes' *'e-health trust*

metrics'. We propose that '*e-Health Trust Metrics Manager'* has the task to do E-Health Trust Attribute Certification. The '*e-Health Trust Metrics Manager'* stores attribute assessment value in the set of proposed '*e-health trust metrics'* containing {'*high integrity', 'average integrity', 'low integrity' and 'no integrity'*}. We presented the Framework Model.

The study has faced several challenges in the process; particularly my husband had an open-heart double bypass surgery and recovered during the last two months of completion of the thesis. During this phase my trust in e-health applications, particularly those used in hospitals solidified in the view that e-health systems serve the purpose to assist in providing healthcare to patients.

5.2 Recommendations

This study did not cover in scope the implementation of the framework. The details in the processes of '*e-Health Trust Metrics Manager'* as a database management service, is not in the scope of this thesis. The Fuzzy Computational Model (FCM) is not in the scope of the study. It is recommended that further studies be made to implement the framework and integrate this in an e-health application.

The process of gathering the listed soft attributes is not the scope of this study. We need further studies on the reputation and experience of the user on behaviour related to privacy, confidentiality, availability reliability, accountability and non-repudiation as requirements for e-health application. Studying the behaviour and experience of the user and the application/service that can lead to assessing reputation will be another area of research.

Studies on access roles can be another area of research. For instance, nursing students who are doing on the job training in teaching hospitals could be given the professional nurses' access to patient records. The responsibility that comes with access roles would equate to the accountability requirements in the e-health environment, hence access roles must be given importance.

Further research can be made on security audits, the information system activity review that review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Studies can be made to look at the audit controls on implemented hardware, software and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Bibliography

Al Salami, N., & Al Aloussi, S. (2013). Neural Network Solution for Intelligent Service Level Agreement in E-Health. (G. H. al., Ed.) *HIS LNCS 7798* , 65-77.

Alhaqbani, B., & Fidge, C. (2008). Privacy-preserving electronic health record linkage using pseudonym identifiers. *In: Proceedings 10th International Conference on e-health Networking, Applications and Services*, (pp. 108-17).

Alvarez, R. (2002). Review The promise of e-Health - a Canadian perspective. *EHealth International , 1* (4).

Appari, A., & Johnson, M. (2010). Information security and privacy in healthcare: current state of research. *Int. J. Internet and Enterprise Management , 6* (4).

Australian Government Department of Health. (2014). *Privacy.* Retrieved August 12, 2014 from EHealth: http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/ehealth_privacy

Australian Government Department of Health. (2014). *Welcome to eHealth.gov.au*. Retrieved October 23, 2014 from EHealth.

Australian Government Department of Health. (2014). *Welcome to eHealth.gov.au.* Retrieved August 6, 2014 from EHealth: http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/home

Bahtiyar, S., & Caglayan, M. U. (2012). Extracting trust information from security system of a service. *Journal of Network and Computer Applications , 35* (1), 480-490.

Bahtiyar, S., & Caglayan, M. U. (2014). Trust assessment of security for e-health systems. *Electronic Commerce Research and Applications , 13*, 164-177.

Bartlett, C., Boehncke, K., & Haikerwal, M. (2008). *E-Health: Enabler for Australia's Health Reform.* National Health & Hospitals Reform Commission.

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. *In: Proc IEEE symp security and privacy*, (pp. 321-34).

Bharadwaj, K. K., & Al-Shamri, M. H. (2009). Fuzzy computational models for trust and reputation systems. *Electronic Commerce Research and Applications , 8*, 37-47.

Blobel, B. (2007). Comparing approaches for advanced e-health security infrastructures. *International Journal of Medical Informatics , 76*, 454-459.

Blobel, B. (2011). Intelligent security and privacy solutions for enabling personalized telepathology. *The 10th European Congress on Telepathology and 4th International Congress on Virtual Microscopy Vilnius.* Lithuania.

Blobel, B., & Pharow, P. (2007). A model driven approach for German health telematics architectural framework and security infrastructure. *International Journal of Medical Informatics , 76*, 169-175.

Blobel, B., & Roger-France, F. (2001). A systematic approach for analysis and design of secure health information systems. *International Journal of Medical Informatics , 62*, 51-78.

Cao, F., Huang, H., & Zhou, X. (2003). Medical image security in a HIPAA mandated PACS environment. *Computerised Medical Imaging and Graphics , 27*, 185-196.

Coetzee, M., & Eloff, J. (2006). A Framework for Web Services Trust. (S. Fischer-Hubner, K. Rannenberg, L. Yngstrom, & S. Lindskog, Eds.) *IFIP International Federation for Information Processing , 201*.

Detmer, D. (2001). Transforming Health Care in the Internet Era. *World Hospitals and Health Service , 37* (2).

Elger, B. S., Iavindrasana, J., Lo Iacono, L., & Muller, H. (2010). Strategies for health data exchange for secondary, cross-institutional clinical research. *Computer Methods and Programs in Biomedicine , 99* (3), 230-51.

Europa Summaries of EU Legislation. (n.d.). *Protection of Personal Data*. Retrieved August 9, 2014 from Data protection, copyright and related rights: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm

Fernandez-Aleman, J. L., Senor, I. C., Lozoya, P. O., & Toval, A. (2013). Security and privacy in electronic health records; A systematic literature review. *Journal of Biomedical Informatics , 46*, 541-562.

Gajanayake, R., Iannella, R., & Sahama, T. (2011). Sharing with care: an information accountability perspective. *IEEE Internet Computing , 15* (4), 31-38.

Geissbuhler, A. (2013). Lessons learned in implementing a regional health information exchange in Geneva as a pilot for the Swiss national eHealth strategyhealth. *International Journal of Medical Informatics , 82*, e118-e124.

Grandison, T., & Sloman, M. (2000). A Survey of Trust in Internet Application. *IEEE Communications Surveys and Tutorials* .

Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Muller, G. (2011). Aspects of privacy for electronic health reords. *International Journal of Medical Informatics , 80*, e26-e31.

Habib, S., Varadharajan, V., & Muhlhauser, M. (2013). A Trust-aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces. *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on* (pp. 459-468). IEEE.

Hill, J. W., & Powell, P. (2009). The national healthcare crisis: Is eHealth a key solution? *Business Horizons , 52*, 265-277.

Hiller, J., McMullen, M., Chumney, W., & Baumer, D. (2011). Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): US and EU Compared. *B. U. J. Sci. & Tech. L. , 17*.

Huang, J., & Nicol, D. (2013). Trust Mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications , 2* (9).

Humphries, C. (2005-2006). E-Health HealthConnect - The consumer representative expereince in Tasmania. *The Australian Health Consumer , 3*.

Information Integrity Solutions. (2010, December 15). PIA on the Electronic Transfer of Prescription Release 1.1.

ISO. (1989). *ISO 7498-2:1989, Information processing systems, Open Systems Interconnection, Basic Reference Model- Part 2: Security Architecture.* Retrieved August 30, 2014 from ISO: http://www.iso.org

Jafari, M., Safavi-Naini, R., Saunders, C., & Sheppard, N. (2010). Using digital rights management for securing data in a medical research environment. *In: Proc digital rights management workshop*, (pp. 55-60).

Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security, Private Communication in a Public World.* Upper Saddle River, NJ: Prentice Hall PTR.

Lin, C.-W., Abdul, S. S., Clinciu, D., Scholl, J., Jin, X., Lu, H., et al. (2014). Empowering village doctors and enhancing rural healthcare using cloud computing in a rural area of mainland China. *Computer Methods and Programs in Biomedicine , 113*, 585-592.

Marti, R., Delgado, J., & Perramon, X. (n.d.). Security Specification and Implementation for Mobile e-Health Services.

Mat Kiah, M., Nabi, M. S., & Zaidan, B. B. (2013). An Enhanced Security Solution for Electronic Medical Records Based on AES Hybrid Technique with SOAP/XML. *J Med Syst , 37* (9971).

Narayan, S., Gagne, M., & Safavi-Naini, R. (2010). Privacy Preserving EHR System Using Attribute-based Infrastructure. *Proceedings of the 2010 ACM workshop on Cloud computing security workshop* , 47-52.

Neubauer, T., & Heurix, J. (2011). A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics , 80*, 190-204.

Nickel, P. J. (2011). Ethics in e-trust and e-trustworthiness: the case of direct computer-patient interfaces. *Ethics Inf Technol , 13*, 355-363.

Nikolidakis, S., Georgakakis, E., Giotsas, V., Vergados, D., & Douligeris, C. (2010). A Secure Ubiquitous Healthcare System Based on IMS and the HL7 Standards. *ACM* .

Nikolidakis, S., Giotsas, V., Vergados, D. D., & Douligeris, C. (2009). A Mobile Healthcare System Using IMS and the HL 7 Framework. *ACM/IEEE Symposium on Architectures for Networking and Communications Systems.* USA: Princeton.

Pagdanganan, B. (2009). *An Analysis of Trust Requirements and Design Choices for Trust Management in Web Services Based Service Oriented Architectures.* MIT Report, Macquarie University, Computing.

Papazoglou, M. P. (2008). *Web Services: Principles and Technology.* Prentice Hall.

PCEHR - NETHA. (2014). *PCEHR - NETHA.* Retrieved August 9, 2014 from PCEHR - NETHA: http://www.nehta.gov.au/our-work/pcehr

Peyton, L., Hu, J., Doshi, C., & Seguin, P. (2007). Addressing privacy in a federated identity managment network for e-health. *Proceedings of the 8th World Congress on the Management of eBusiness*, (pp. pp 12-22). Toronto, Canada.

Piliouras, T., Yu, P., Su, Y., Siddaramaiah, V., Sultana, N., Meyer, E., et al. (2011, 11). Trust in a Cloud-Based Healthcare Environment. *IEEE* .

Quantin, C., Jacquet-Chiffelle, D.-O., Coatrieux, G., Benzenine, E., & Allaert, F.-A. (2011). Medical record search engines, using pseudonymised patient identity: An alternative to centralised medical records. *International Journal of Medical Informatics , 80* (2), e6-11.

Rubio, O. J., Alesanco, A., & Garcia, J. (2013). Secure information embedding into 1D biomedical signals based on SPIHT. *Journal of Biomedical Informatics , 46*, 653-664.

Shamir, A. (1979, November). How to share a secret. *Communication of the ACM , 22*(11). From http://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf

Shini.S.G., Thomas, T., & Chithraranjan.K. (2012). Cloud based medical image exchange- security challenges. *Procedia Engineering , 38*, 3454-3461.

Smart Card Alliance. (2012, September). Smart Card Technology in US Healthcare: Frequently Asked Questions.

Stingl, C., & Slamanig, D. (2008). Privacy-enhancing methods for e-health applications: how to prevent statistical analyses and attacks. *International Journal of Business Intelligence and Data Mining , 3* (3), 236-254.

U.S. Department of Health & Human Services. (2014). *Health Information Privacy*. Retrieved August 05, 2014 from HHS.gov: http://www.hhs.gov/ocr/privacy/

Walsh, T. (2013). *Privacy and Security Audits of Electronic Health Information.* Retrieved June 01, 2014 from AHIMA HIM Body of Knowledge: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050599.hcsp?dDocName=bok1_050599

Wikimedia Foundation. (2014, October 16). *Authorization*. Retrieved October 13, 2014 from Wikipedia: http://en.wikipedia.org/wiki/Authorization

Win, K., Susilo, W., & Mu, Y. (2006). Personal health record systems and their security protection. *J Med Syst , 30* (4), 309-15.

World Health Organisation. (2014). *E-Health*. Retrieved February 25, 2014 from WHO: http://www.who.int/trade/glossary/story021/en/

Yamamoto, K., Okuhara, Y., Kluge, E.-H. W., Croll, P. R., France, F., Ruotsalainen, P., et al. (2011). The recommendations from the 2009 SiHIS working conference in Hiroshima- Issues on trustworthiness of health information and patient safety. *International Journal of Medical Informatics , 80*, 75-80.