Securing Telehealth Applications in a Web-Based e-Health Portal

Qian Liu

A Thesis
in
The Department
of
Computer Science

Presented in Partial Fullfilment of the Requirements
for the Degree of Master of Computer Science at
Concordia University
Montreal, Quebec, Canada

March 2008

Your file Votre référence
ISBN: 978-0-494-40945-9
Our file Notre référence
ISBN: 978-0-494-40945-9

ABSTRACT

Securing Telehealth Applications in a Web-Based e-Health Portal

Qian Liu

Telehealth applications can deliver medical services to patients at remote locations using telecommunications technologies, such as the Internet. At the same time, such applications also pose unique security challenges. First, the trust issue becomes more severe due to the lack of visual proofs in telehealth applications. The public key infrastructure (PKI) is insufficient for providing the same kind of trust a patient may attain during a face-to-face service. Second, telehealth services, such as tele-monitoring or tele-consultant, naturally demand a systematic organization of users, roles, resources, and flows of information. Existing access control mechanisms in an e-health system are usually incapable of dealing with such workflow-based services. This paper provides cost-efficient solutions to those issues in the context of a Web-based e-health portal system. First, we propose a PKI-like infrastructure for establishing trust between users using biometrics-based authentication and hierarchies of trust. Second, we develop an access control method for workflow-based telehealth services using a rule-based module already available in the portal system.

ACKNOWLEDGEMENTS

I would like to thank lots of people who provide help for this thesis.

First of all, I would express my deep appreciation to my supervisor Dr.Dssouli who is one of the nicest ladies I have ever met. Without her help, I am not able to come to Canada pursuing my master of degree.

In addition, gratitude to my co-supervisor Dr.wang for his extreme patience to my slow progress and his guidance during my working on this thesis. I would also like to thank to my two other colleagues Shuo Lu and Yuan Hong, and they gave me a lot of invaluable suggestion on my work.

Finally I thank my wife and my parents to give me unconceivable support during my most difficult time in Canada.

To My Wife, With Love

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Telehealth applications are gaining momentum due to the increased popularity of Web-based e-health systems and a demand for remote and more convenient accesses to medical services. Through leveraging modern telecommunication technologies, such as the Internet, telehealth applications can provide much-needed medical services to patients at remote locations or even in different countries. At the same time, such applications also pose many unique challenges to their design and implementation. In particular, security is crucial to telehealth applications due to the fact that medical services may be critical to patients health or even life.

In this thesis, I study two security issues in telehealth applications in the context of a Web-based e-health portal system. First, a unique trust issue arises due to the lack of visual proofs in telehealth applications. For example, a patient may have doubts in identity of a doctor at the other end of a telehealth service provided via the Internet. The public key infrastructure (PKI) can enable a patient in establishing trust in the organizations website or telehealth applications, which is the very purpose of PKI by design. However, PKI is insufficient for providing the same kind of trust a patient may attain during a face-to-face service. Second, telehealth services, such as tele-monitoring or tele-consultant, usually involve a complex process that naturally demands a systematic organization of multiple

users playing different roles in accessing shared resources and flows of information. Since most commercial e-health systems are built upon existing software components or platforms, the existing access control features are usually incapable of dealing with such workflow-based services.

This thesis provides solutions to the above issues in the context of a Web-based e-health portal system. First, I propose a PKI-like infrastructure for establishing trust between users using biometrics-based authentication and hierarchies of trust. By employing multimedia and biometric features, such as face recognition, the infrastructure can provide an increased degree of trust to users of telehealth applications. Second, to regulate accesses to workflow-based telehealth services in a cost-efficient way, I adopt an approach of re-using the rule-based access control module already available in the portal system. Specifically, the temporal dependency between events is expressed as partial orders and then enforced with a special *done* rule in the logic-based access control engine. In contrast to deploying a full-fledged workflow management system, our approach provides a light-weight and effective solution to existing telehealth applications.

The following elaborates on the two main issues addressed in this thesis.

Trust Management Using PKI and Biometrics With today's ubiquitious accesses to internet, patients may be exposed to many resources that are deceiving and harmful. In the absence of a face-to-face contact, it becomes a challenging issue to ensure patients that the telehealth services he/she visits are indeed trustworthy. Two layers of trust are needed, that for the telehealth websites and that of the medical staff providing the services. First, through phising, patients may be deceived into accessing a fake website, which may cause the patient's private information to be stolen. I adopt public key infrastructure (PKI) for establishing

trust between patients and the telehealth website. Digital certificates are issued by the initially trusted Certificate Authorities (CA). Mutual authentication can be achieved using participants' digital certificates and certificate servers linked to root CA servers. Validity of information in digital certificate leads to the trust in personal identity or service provider. Second, without an in-person communication, patients' identities become more difficult to verify, and to allow patients to trust a medical staff claiming to be an expert may also face difficulties, especially when patients have never met the staff before. In this thesis, I propose a solution based on enhancing PKI with biometrics measures, so sufficient amount of trust can be established in telehealth applications between remote users.

Securing Workflow-Based Telehealth Applications Telehealth applications implemented for business processes at an enterprise-scale can easily involve tens of thousands of participants, including patients, doctors, and other medical staff. In a general hospital, after a patient walks into hospital, medical staff will provide patient a series of registration, examination, consultant, and diagnosis services. How can such a series of inter-dependent services be efficiently and accurately supported in a virtual environment based on software is a challenging issue. Workflow systems naturally fit in this scenario. The basic idea of a workflow system is to separate the business policy from computing applications to enforce the flexibility and maintainability of changes in business processes, so workflow tasks designed according to organizational logic can be applied to different applications. Resource allocation and dynamic adjustment to task changes are also the inherent advantages embodied in workflow systems. With these benefits, a workflow system will provide a natural solution to complex telehealth applications. In this thesis, I first show how several telehealth applications can be implemented as workflows. I then address the access control issue of

such workflow-based applications. Participants in the workflow system are assigned to different tasks in a workflow. If participants mistakenly or maliciously abuse their privileges to execute other participants' tasks, or to execute tasks in a wrong order, then the workflow's logic may be adversely affected, which may lead to serious consequences in a telehealth application. I enhance existing Role-Based Access Control (RBAC) capabilities with a rule-based access control engine, and use *done* rule to enforce the correct execution of tasks in a workflow-based telehealth application.

Chapter 2

Related Work

Telehealth A hospital information system (HIS) is introduced as a subsystem within a hospital dealing with complete information processing and information storage of the hospital organization. Workflow systems are used as a new tool in the design of HIS whose advantage includes enhancement of automation, flexibility of adaptation to change of conventional HIS, and the integration or migration of legacy system in a heterogeneous application perspective [Gra99]. As an expansion of HIS, telehealth refers to the delivery of health-related services and information via telecommunications technologies [Nac02]. Internet introduces a simple way for connecting all participating entities, including individuals and electronic equipments, and also makes it feasible to share information regardless of time and location. Telehealth applications usually involve doctors, nurses, coordinators, other medical staff, and patients. Those participants carry various tasks either independently, or in a cooperative manner according to a well-defined process. Telehealth services typically require a set of coordinated activities for achieving a common business objective [Wsc10]. Such services are thus naturally workflows, which separate various works of a specific process into a group of well-defined steps where each work contains many tasks as different logic steps [Kfska99]. The tasks may be executed manually by human or automatically by applications relevant to the process represented by a workflow.

Security in Telehealth Applications Security is one unique challenge to the design and implementation of telehealth applications [Askr00]. A telehealth work flow system may manipulate information regarding to confidential or private patient records. How to avoid leaking or tempering sensitive information is a growing concern in telehealth work flow systems [Hk03]. Telehealth required authentication mechanism to guarantee that no unauthorized participants can get access to data or task in work flow system. The mutual or self-encryption authentication can provide a reliable way to verify the participants' identities [Jlss05]. Role based access control (RBAC) provides greater productivity to security administrators of work flow systems [Fck95]. The number of participants involved in a telehealth work flow system can easily exceed tens of thousands so managing participants is a challenging issue. This requires managing several categories of roles assigned to participants, which are defined by activities or task executions. Granting authorization to roles instead of to participants, RBAC greatly simplies security administration [Bfa99].

In general purpose workflow systems, security policies are represented as rules or constraints on users or groups involved in a workflow. Such constraints can be expressed with logic-based languages in three categories: static, dynamic, and hybrid, depending on the temporal order of their evaluation in comparison to the initiation of workflow execution or runtime of workflow [Lar04]. The Workflow Authorization Model (WAM) specifies authorizations in such a way that the workflow execution goes in parallel with granting or revoking privilege on users or roles. Synchronizing authorization flows with workflow execution allows WAM to support dynamic constraints to ensure consistency of tasks at run time [Scfy96]. Another model for authorization constraint management in workflow systems is to use active rules implemented as triggers corresponding to workflow events in active databases [As04]. Flexible Authorization Framework (FAF) based on a language that developer can establish

security policies is used to enforce on special accesses. The language permits the specification of common constraints on authorizations and on the derivation or conflict resolved process[Jsss97]. Flexible Authorization Manager (FAM) can enhance rule-based access control policies within a single computing system. FAM is also expressed as a language through which developers can specify authorization constraints and access control policies to control the execution of given tasks. Do or done-rule in the language can be described as predicate symbols to represent the access execution[Jsss01]. The emergence of internet and globalized organizations make it possible and desirable to have operations and task executions go beyond the border of organizations or countries. This requires organization and task-specific access control models for collaboratively enforcing work flow security policies [Kpf01].

By employing unique features of human characteristics, biometrics technologies provide an alternative way over password or digital certificate-based authentication for verifying user identities. Web service has been used for the extraction and verification of bio-metrics across different organizations [Maj04]. How to integrate biometrics with PKI system is a growing concern in fields like e-commerce, e-banking, and e-health, whereas it is particularly relevant to telehealth applications. Using biometrics features is a feasible way to establish private keys [Gmw05]. Two-step authentications can be archived through smart card authentication based on PKI and biometrics measures like fingerprint verification stored in an identical card, and such a combination of PKI and biometrics is believed as double protection for personal authentication [Sy01].

Chapter 3

Architecture Design and Trust Management

Figure 1 illustrates the architecture for e-Health portal systems in which telehealth services are provided [Llhwd08]. The e-Health portal is a web-based application that integrates various medical services provided by multiple hospitals and other medical organizations. An end user, such as a patient or doctor, directs a web browser to the portal server. The portal server displays a webpage, namely, portal interface to the user. The portlets inside each portal interface correspond to a collection of correlated services provided by medical organizations. The user may trigger various actions of a service by clicking on corresponding buttons encapsulated in a portlet (real-time applications, such as tele-consultant service, will bypass the portal server due to a more rigid performance constraint). Our design provides a uniform and easy-to-use interface to users by hiding implementation details of services and their providers. It also enables single sign-on (SSO) for backend and remote services. Moreover, the design also simplifies the administration and maintenance of services at medical organizations, because the presentation layer (that is, the portal server) is separated from the implementation layer (that is, medical organizations). Next, we address the architecture design of the telehealth subsystems, and the trust management issue.

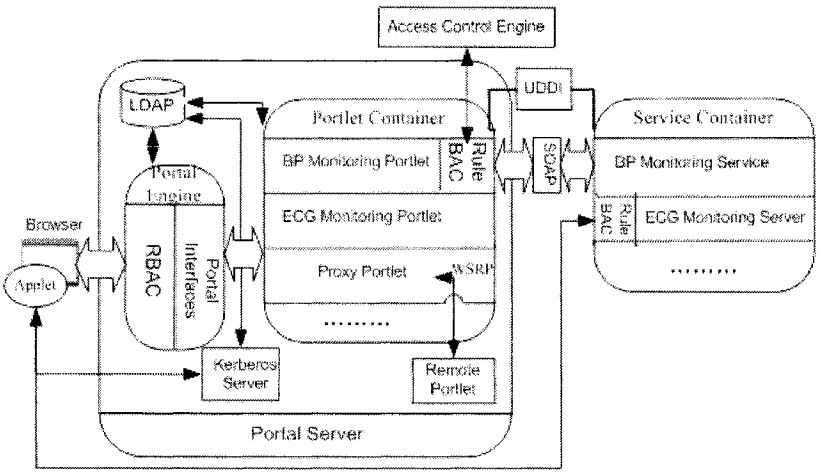

Figure 3.1: Architecture of e-Health Portal

3.1 Architecture Design of Telehealth Subsystem

Figure 2 shows the architecture of the telehealth subsystem with a focus on its security. The responsibility of the biometrics server is to provide doctor's identify information including biometrics features to patients. Behind the portal server are application servers, named E-health server cluster, whose responsibilities are to define and manage workflows, to control and monitor multimedia streams, and to store data in databases. Not shown in the figure, the Certificate Authority (CA) server will issue digital certificate to every hospital and other members of the portal. Since our implementation is completely based on web service, patients client-end application is simply a Web browser and Java applet downloaded from the portal server.

The certificate server in this architecture is a X.509 certificate server acting as a middle-level Certificate Authority (CA), which is authorized by a root CA or superior CA publish digital certificates to participants. The certificates will contain the holder's information regarding organization name, server name, personal name, e-mail address, and mailing address,

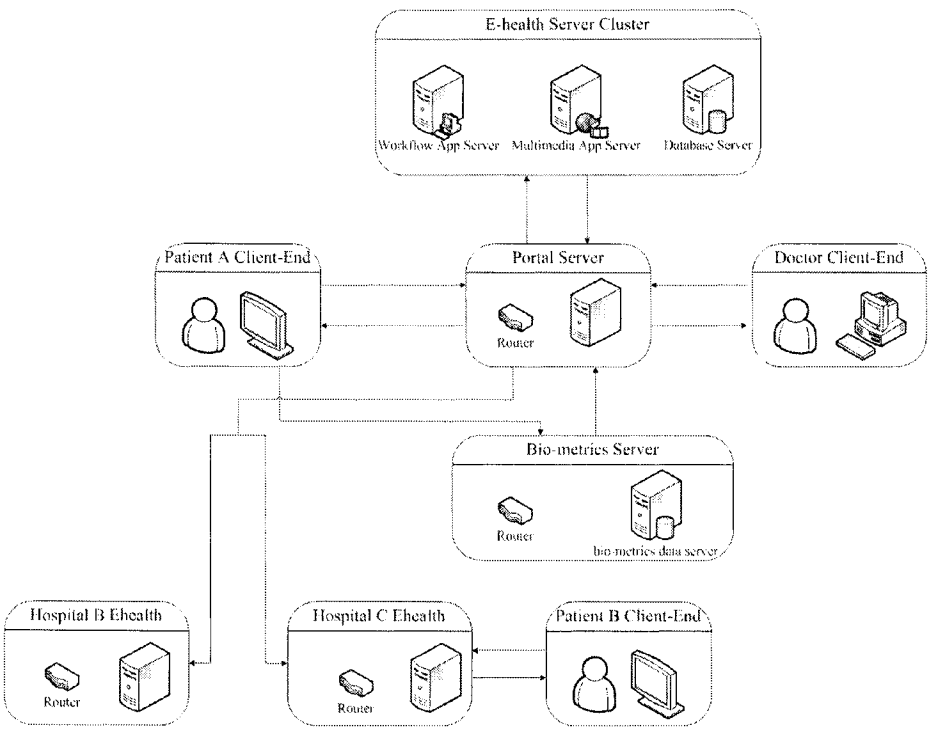

Figure 3.2: Architecture of Telehealth Subsystem

etc. In a X.509 system, every qualified digital certificate also contains a signature signed by a trust CA, and this indicates the CA has verified the certificate holder's information. In telehealth applications, a health organization will be composed by several hospitals. So this organization can be a superior certificate authority that signs digital certificates for its supervised hospitals' CAs. If a patient under hospital A wants to visit hospital B within the same organization, the patient can get a certificate of hospital B and then by verifying the digital certificate, the patient can trust the hospital B, therefore inter-hospital trust can be established by digital certificate chains.

The main responsibility of the biometrics data server is to collect and store participants' unique bio-characteristics in a secure way. The verification of users' identities based on biometrics is used as an enhancement to password and PKI-based authentication in telehealth applications. A doctor must register his personal information, such as a recent picture or other biometrics characteristics, at a specific location under the supervision of special personnel. Like in PKI, the fingerprint of the doctors' biometrics information is also stored in a database within a higher authority, such as Canada health agency (the courterpart of a root CA). This authority ensures the doctor's biometics information is genuine and up to date. The authority can also put a digital seal, such as a visible watermark, inside the biometrics characteristic. The content of visible watermarking can be the URL of the authority, which enables the patient to visit this address to query the information of doctor for verification purposes.

The architecture supports telehealth applications running over various multimedia streams, such as video and audio. To ensure the integrity and efficiently of such streams, the architecture is built upon standard protocols including RTP (Real time protocol), SIP (Session

initiation protocol), which are both responsible for multimedia stream transmission and multimedia playback control. RTP protocol is specifically targeted for multimedia data transmission data such as video and audio over internet, and provides a common way to transfer data in multicast or unicast communications. RTP (Real time protocols) is especially suitable for applications with real-time constraints. These include videoconferencing applications, video on demand, and continuous monitoring data applications. Videoconferencing is necessary for various telehealth applications, such as tele-consultant and tele-education. Video on demand is needed for tele-monitoring. SIP (Session Initiation Protocol) is an application-layer control protocol that can establish, adjust and terminate multimedia sessions or calls. These multimedia sessions can support multimedia conferences, distance learning, and similar applications. SIP can invite participants to both end-to-end and multicast sessions. Participants can be added to an ongoing session. SIP also is a signaling protocol for initiation, merging, or splitting of sessions, which is used for tasks in telehealth workflow applications.

3.2 Trust Management

Trust is a challenging issue in Telehealth applications due to the lack of a visual contact between users. Our solution integrates PKI infrastructure, biometrics, and visible watermark for establishing sufficient trust.

First, for users of a telehealth application to establish trust in the application running in the Web-based portal, I employ digital certificates and the PKI infrastructure in a standard way. More specifically, each provider of telehealth services holds a digital certificate issued by authorities, which can be trusted by a user's browser through trust chains. The certificates give users of the telehealth services a sense of trust when they connect to the services through SSL protocol. It is worth noting that such trust only indicates to the user that he/she is

connected to a trusted service from a trusted organization, and the encrypted communication is secured from snooping. While such trust is typically regarded as enough for e-commerce applications, it is insufficient for telehealth services since a patient may still be wondering who is at the other end of the service. We can certainly extrapolate the PKI-based solution to user-level authentication by issuing a digital certificate to each user. This approach, however, may not be feasible in practice due to the implied cost (of issuing and maintaining a large number of certificates) and the fact that many users of a telehealth application may not possess the knowledge or skills required for using PKI. Moreover, unlike a digitally signed document or email, a real-time telehealth service requires continuous authentication. For example, a doctor may present his/her digital certificate at the beginning of a service and then ask someone else to replace him/her. By authenticating the doctor only once when the service begins, the patient will never detect such a change of identity.

Traditional walk-in medical services, such as consultant and diagnosis, are either within a hospital or in a very limited geographic range, so the uniqueness of facial character acts as the best evidence for a doctor's identity. Trust between patient and doctor can be easily established through implicit referrals and can be trivially achieved during face-to-face services. Although the geographical distance in a telehealth application renders direct visual contact between users infeasible, multimedia components of telehealth applications can provide a similar capability. Most telehealth applications have multimedia components for video capturing and transmission. Integrating such components with telehealth services will give patients an opportunity to see the doctor as if during a face-to-face visit to the organization. In the scenario of a tele-consultant, a patient can interact with a doctor via multimedia communication channels with both video and audio. The doctor's real-time video streams provide a constant authentication of his/her identity to the patient.

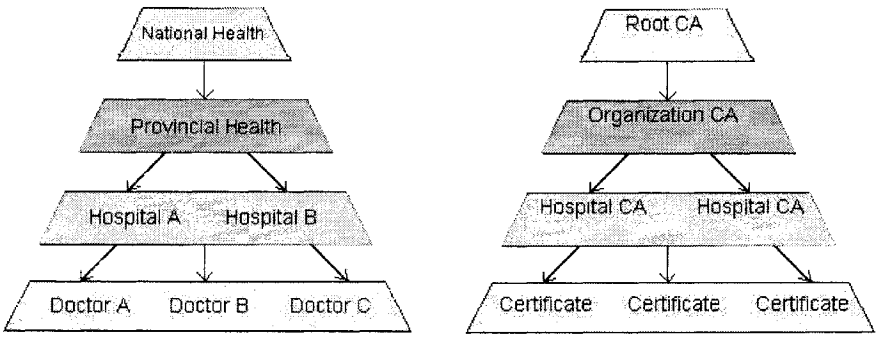

Figure 3.3: Trust Hierarchy in Organizations and PKI

However, a challenging issue is to establish initial trust when the implicit authority in a physical organization is absent. For example, when a patient visits a hospital, he/she implicitly trusts each person during the whole process from registration to the interview with a doctor. Such trust is reasonably reliable in a physical organization, but it becomes suspicious when the organization only virtually exists at the other end of an Internet connection. For example, the trust established with PKI may allow a patient to believe that the service he/she is accessing is indeed from that medical organization. However, this does not mean that organization and everything on its website can be trusted. In particular, if a picture of the doctor posted on a clinics website is used to establish initial trust in that doctor, then the patient will have to trust that clinic and its webmaster. Assuming such trust across the Internet for a clinic that only virtually exists is problematic considering abundant real-world examples of online frauds.

I propose to establish initial trust through hierarchies of trust, which is similar to PKI but applied to biometrics features. More specifically, biometrics features, such as facial characters, are provided by each organization for users to establish trust. Such biometric features

act as digital certificates in PKI. Similar to chains of certificates in PKI, the biometrics features are certified by the organization that issues them, and the organization is certified by higher authorities, such as state or national medical associations, and so on. Like the built-in CAs in a Web browser, the client-side applet of telehealth applications includes a collection of authorities that are trusted. Upon connecting to a telehealth service provided by an organization, the doctors biometrics feature is delivered together with a chain of trust whose root is a higher authority. The patients applet transparently verifies the root against its built-in collection of authorities, and then verifies the chain of trust attempting to establish trust in the biometrics feature. The applet presents the feature to the patient if the trust can be successfully established; it warns the patient about potential fraud and terminates the connection, otherwise. Figure 3.3 shows an example of such hierarchies of trust for medical organizations. The trust in a doctors biometrics feature, such as picture, can be established if it is issued by a hospital that is certified by a provincial health organization, which is in turn certified by the national health organization built into the patients applet.

A complementary mechanism for increasing trust is to embed visible watermarks (which is different from invisible watermarks used for protecting digital copyright) into biometrics features in the form of an image. For example, if a doctor's picture is used as the biometrics feature, then a higher authority such as the national health organization can assert the validity of this biometric feature by embedding its URLs or seals in the doctor's picture, as shown in Figure 3.4. The URL embedded in the doctor's picture is a word-form visible watermark indicating the issuer of the picture. The URL allows patients to visit the higher authority's website to verify the validity of the picture. It is worth noting that this mechanism is helpful only when the patient already trusts the authority appearing in the visible watermark. A malicious organization can certainly put up fake pictures embedding a

URL that leads to itself or its alliances, and in this case the patient will distrust the picture together with the authority that issues it. This fact proves the needs for hierarchies of trust through authorities that patients initially trust (the counterpart of a root CA) and chains of authorities originating from those trusted ones.

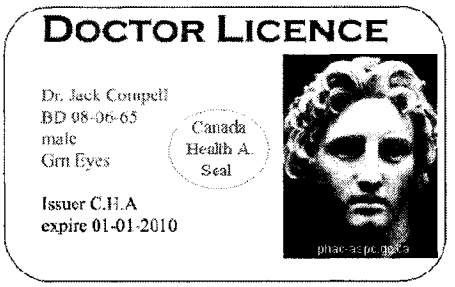

Figure 3.4: An Example of Visible Watermarks

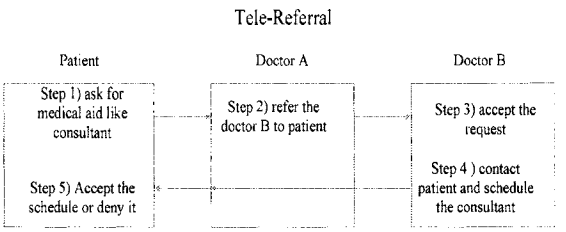

Figure 3.5: Tele-Referral

Similar to revocation of digital certificates, the biometrics features of users are not permanent, either. Biometrics features may change over time so they should have validity duration and will be revoked once they expire. Another issue is to establish trust using a model different from the hierarchical approach of PKI, that is, the web of trust. In traditional

organizations, referrals between users such as doctors are a common way for establishing trust. A similar approach is possible in telehealth applications with the help of multimedia components. For example, a patient may be introduced to a new doctor by someone with whom he/she is familiar via a tele-referral service, as depicted in Figure 3.5.

Chapter 4

Workflow-Based Telehealth Applications and Access Conrol

This chapter studies workflow-based telehealth applications and the access control issue in such applications. Section 4.1 studies several scenarios of workflow-based telehealth applications. Section 4.2 then shows that partial orders can be obtained from workflow tasks based on the dependence relationship among adjoining tasks in those applications. Section 4.3 addresses the access control in workflow-based telehealth applications by studying a specific case, that is, tele-consultant. Existing RBAC (role based access control) capabilities are shown to be insufficient for enforcing the partial orders between tasks, and extensions based on rules are proposed to enforce such partial orders. Finally, Section 4.4 demonstrates in details the tele-consultant scenario.

4.1 Workflow-Based Telehealth Applications

This section studies several scenarios of workflow-based telehealth applications, namely, Tele-Monitoring, Tele-Consultant, Tele-Education, and Tele-Lecture. I first describe the workflow of those applications, and then analyze the workflow tasks in each application.

4.1.1 Tele-Monitoring

The purpose of Tele-monitoring is to transfer a patient's medical data to doctors in real-time so doctors can monitor and analyze the patient's health condition and medical data in his or her office, without the presence of patient.

Although being effective and convenient, patients need to be authenticated by doctors in telehealth work flow systems.Tele-monitoring is different from traditional monitoring where doctor can do medical examinations and analyses face to face with patients. Without a unique identity like the humans face, it is difficult to verity a patient's identity. On the other hand, patients need to make sure a qualified doctor is on the other end.

Online Tele-Monitoring At the beginning, the patient needs to be connected to the monitoring device for analyses or treatments. The patient then makes an appointment. The coordinator censors the appointment and checks the patients record for verifying his identity. If the patient is eligible, the coordinator forwards the appointment to the doctor who is responsible for the patients treatment. The doctor not only receives the appointment but also schedules the exact time for monitoring. Before the exact scheduled time, the patient can make some preparation for the monitoring, such as device preparation. When the schedule time has arrived and before the patient joins the tele-monitoring, the doctor needs to identify the patient due to the absence of the patient's facial characteristic. It is possible that with the intention for deception, the patient asks somebody else to replace himself when tele-monitoring begins. The solution is that after connecting to monitoring devices like BP monitoring but before the medical data transmission, the patient needs to be authenticated by the aid of biometrics, such as facial recognition even iris match. After the patient is authenticated, the process of tele-monitoring begins and monitoring data is

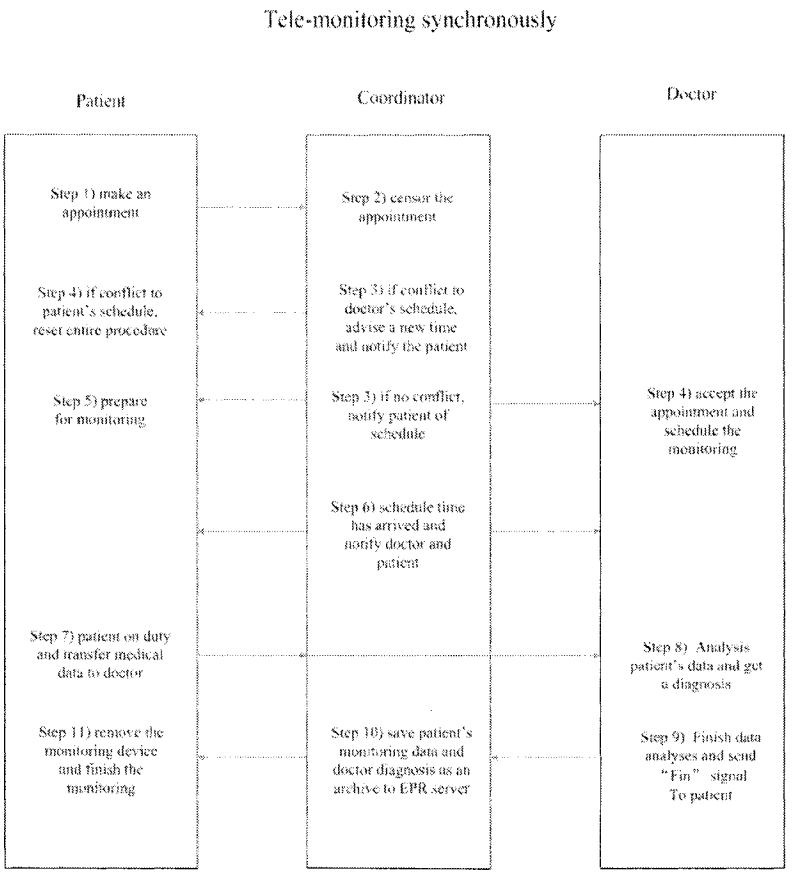

Figure 4.1: Scenario for Online Tele-Monitoring

transferred to the doctor for analyses. During the procedure, if successive data is interrupted for whatever reason, biometrics based authentication must be repeated. The whole process may take a couple of hours or even longer time. When the process is over, the doctor notifies the patient that tele-monitoring is done, and the patient removes the device. Finally, the patient's medical data and doctor's analyses and diagnoses will be stored in the EPR server.

Offline Tele-Monitoring According to the different requirements of patients, the procedure of Tele-monitoring may last only a couple of minutes, like in a BP testing, or a couple of days, like in postoperative monitoring. It is impossible for doctors to take days on a

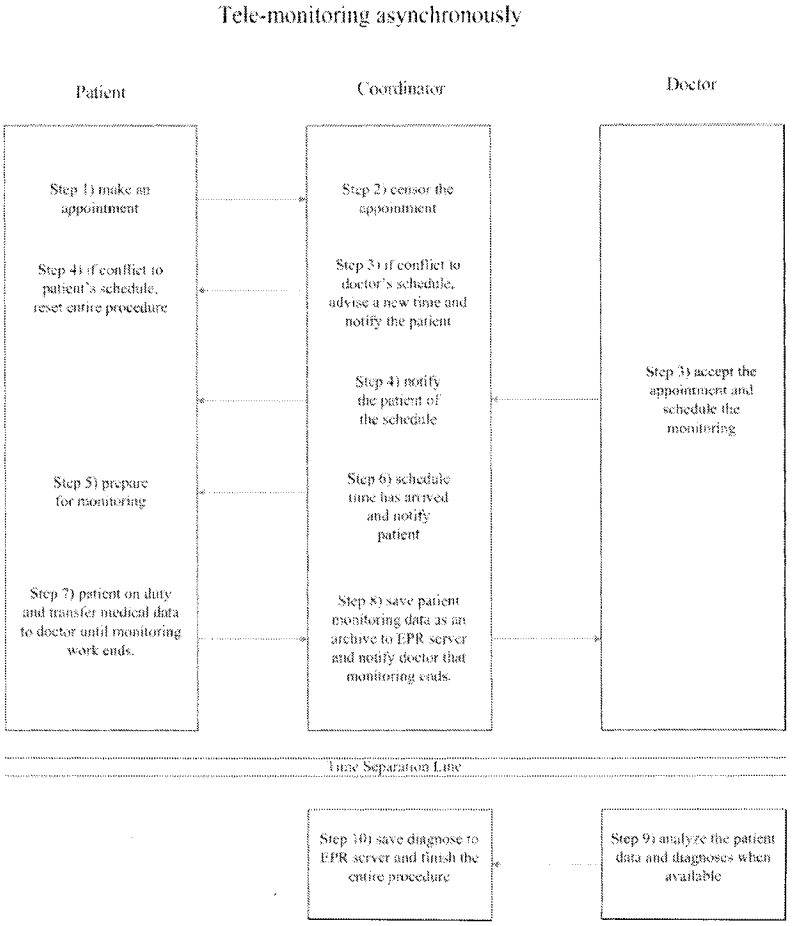

Figure 4.2: Scenario for Offline Tele-Monitoring

single job like tele-monitoring. Tele-monitoring must be initiated and done automatically without doctor's intervention. Although the doctor is absent during medical data transmission, patients authentication is still necessary. The doctor can analyze monitoring data during the procedure, or at the end. However patients should be notified that the process of tele-monitoring is over in both cases.

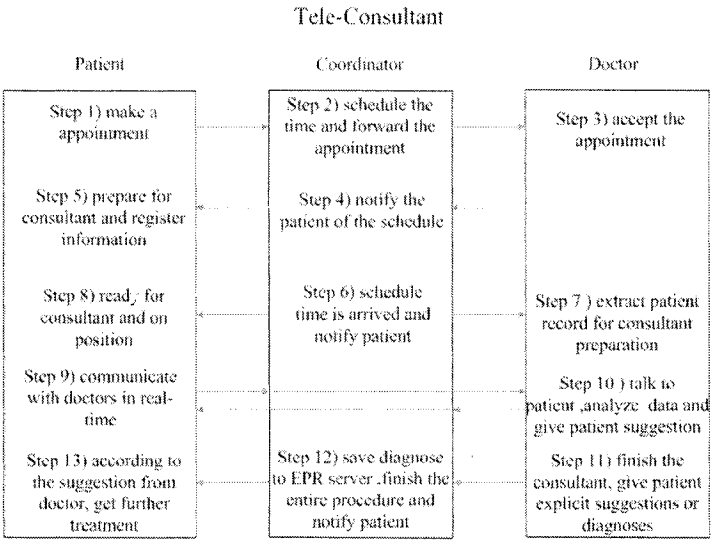

Figure 4.3: Scenario of Tele-Consultant

4.1.2 Tele-Consultant

Tele-Consultant overcomes the geographical distribution of doctors and patients and provides wider used medical services. Regardless of the doctor's and the patient's locations, tele-consultant makes it possible for doctors to communicate with patients, provide consultant services, and help patient get a medical diagnosis and treatment.

Although tele consultant can provide more effective services, patients will encounter new issues, such as how to trust a doctor whom he has never met before. In a face-to-face consultant at the hospital, the patient has no such concerns. Access control is an apparent solution for preventing unauthorized users, but the patient does not know exactly what happens when the doctor joins the tele-consultant. I borrow the idea of public key infrastructure, which establishes trust between strangers through certificate chains.

First of all, a patient who needs a doctor to help him for medical analyses or treatments

makes an appointment for consultant under the supervisor of his clinical doctor. A coordinator censors the appointment and checks the patient's record for verifying his identity. If the patient is registered in the hospital, the coordinator forwards the appointment to the doctor who is responsible for the patient's consultant. The doctor not only receives the appointment, but also schedules the exact time for tele-consultant. Because tele-consultant can provide face to face conversation between doctors and patients with the aid of videoconferencing, the patient's identity can be identified after the session begins. Although the patient may want to ask someone else to replace him/her, the patients face cannot be easily forged . Meanwhile, the patient needs to verify the doctor's identity by comparing the doctor's face seen during the tele-consultant to the picture obtained from an authority organization, either with naked-eyes or using the measure of biometrics. The entire process will last several hours, so the doctor is supposed to be online and to interact with the patient during that time. Once the process is ending, the doctor notifies the patient and stores the analysis and diagnosis data to the EPR server. The patient may further his treatment according to suggestions or diagnoses from the doctor. Another case is that when the patient's consultant doctor is not available at the scheduled time, so the doctor can refer the patient to another doctor to help the patient.

4.1.3 Tele-Education and Tele-Lecture

Tele-education and tele-lecture is a convenient way to spread professional knowledge to patients or medical staff. Participants are not restricted to classrooms or conference centers, and anywhere of the world can be location of a student or lecturer.

Tele-education and tele-lecture can accommodate more participants than tele-monitoring and tele-consultant, so how to identify participant and how to avoid malevolent intruders

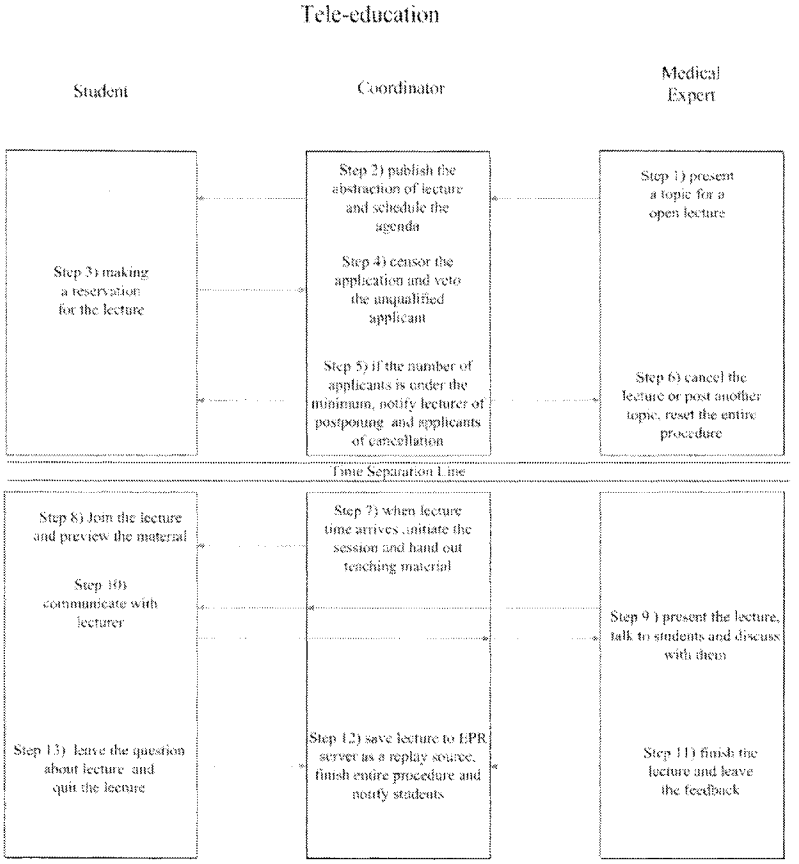

Figure 4.4: Scenario of Tele-Education

are of conerns.

Tele-Education The first step of tele-education is that medical expert posts a topic for the lecture, which should include title, abstraction, and the lecturer's introduction. Then a coordinator publishes the topic with the lecturer's personal information, like his biography, recent picture, and schedules. The coordinator censors the application and filters unqualified participants for security or capability reasons. He/she then distributes the lecture before it begins. If the number of entitled participants is too few to reach a minimum standard, then the coordinator has the right to postpone or even cancel the lecture, and notifies the

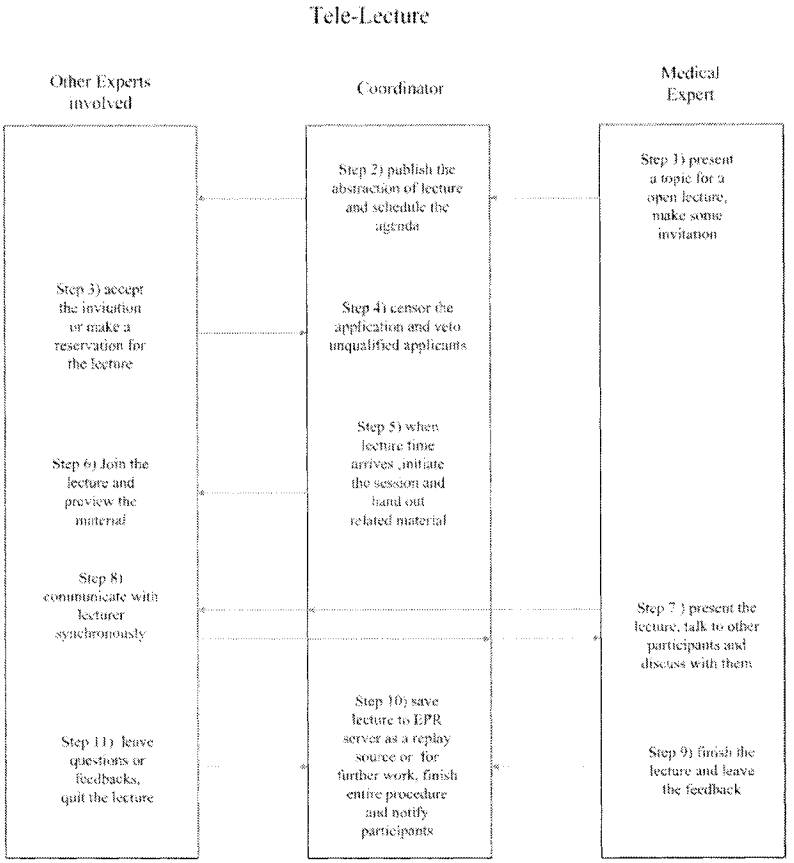

Figure 4.5: Scenario of Tele-Lecture

lecturer and participants. The lecturer must re-select the topic and schedule until capability requirement of the lecture is satisfied. When lecture time arrives, the lecturer should be in position, and participants can join on time or be allowed to join during the session. Before joining the lecture, the participants need to be authenticated to avoid unauthorized participants, which is similar to tele-monitoring described in section 5.1. If participants are suspicious of the lecturer's identity, they can compare the picture posted by the coordinator. During the lecture, the lecturer can talk to participants in real-time. Once the lecture is over, the presentation will be stored into the media server for the purpose of future playback, and participants can leave questions or feedbacks to the lecturer.

Tele-Lecture The main difference between tele-education and tele-lecture is that the latter one strictly restricts the membership of participants and only invites specific participants to the lecture. Because participants involved in a tele-lecture are more specific than in tele-education, the requirement of authentication is also more stringent. In order to communicate more efficiently among participants in a tele-lecture, the voice from participating experts except the lecturer will be a necessary part of the lecture.

4.2 Dependency Between Workflow Tasks

From previous discussions, participants can be categorized into five groups: patient, doctor, coordinator, student, and medical expert. According to their different roles or groups, participants may have different tasks assigned in a workflow. But in most circunmstances, tasks should only be executed by certain roles. Appropriate privileges should be assigned to roles for participants to execute tasks in the workflow. To prevent maliciously privilege escalation in Telehealth applications, we leverage the role-privilege relationship to describe each role's duties. With the use of such relationships, we can guarantee that no unauthorized participants can get accesses to data or resources or to execute a task assigned to others. However referring to previous workflow scenarios, we can see that in a workflow system, RBAC is insufficient to limit the execution of some tasks that is against the pre-defined logic in workflows. We need extra measures to enforce such special role-based access control policies. First, we add task-checking mechanisms into RBAC. In the scenario of Tele-Monitoring above, the role of patient can reset the whole procedure if the recommend time set by the coordinator conflicts with the patient's schedule. However, by RBAC policies, even when conflict has not happened, the patient can still reset the procedure and even cancel the monitoring appointment without notifying the coordinator and doctor. This may result in

task exceptions in some steps of the workflow. We must add additional measures to RBAC to avoid such exceptions. RBAC can only restrict participants assigned to certain roles to execute certain task in a workflow, but those tasks may have pre-conditions, which have to be fulfilled before proceeding to the next task. Task checking mechanism is not adaptive to every steps in a workflow and is also not specific to certain roles in the workflow, but it is still necessary for authorization enforcement in RBAC.

Now we define all the pre-conditions for tasks in aforementioned scenarios. Those conditions will be used to implement the checking mechanisms at the application level according to the workflow logic. Table 1 through table 4 demonstrate the role and privilege, privilege and pre-condition relationship. We use the first character of role name to represent it in the table such as C for coordinator, P for patient, and D for doctor. Task code also indicates the sequence number of tasks executed by specific roles. P1 in tele-monitoring is the task described as that a patient makes an appointment for monitoring. I introduce a digraph structure to represent the relationship between tasks and pre-conditions, as shown in Figure 13 through figure 16. For example, in tele-education, task S1(students making a reservation) is shown as a pre-condition for four tasks involved in the workflow application, C2, C3, C4, meaning that the coordinator censors the reservation, defers lecture, and handouts teaching material. L2 means that if the number of reservation is below the quota, the lecturer can cancel or post another topic for lecture.

4.3 Enforcing Task Dependency in Access Control

I will illustrate the approach through a case study of the tele-consultant scenario. Recall that in tele-consultant, as demonstrated in Figure 4.4, a patient needs to consult a doctor for helps on treatments. The patient first makes an appointment through a coordinator. The

Role	Task Code	Privilege	Pre-condition
Tele-monitoring			
Patient	P1	Make a appointment	No
	P2	Reset, if conflict	Reschedule (C3)
	P3	Transfer to doctor	Notify others time arrive (C4)
Coordinator	C1	Censor the appointment	Make a appointment (P1)
	C2	Schedule the time	Make a appointment (P1)
	C3	Reschedule if conflict	Make a appointment (P1)
	C4	Notify others	Make (P1) accept (D1)
	C5	Save to EPR server	End the monitoring (D3)
Doctor	D1	Accept the appointment	Make(P1),schedule(C2)or reschedule (C3)
	D2	Analysis and diagnosis	Notify others time arrive (C4)
	D3	End the monitoring	Notify others time arrive (C4)

Table 4.1: Tasks within Tele-Monitoring

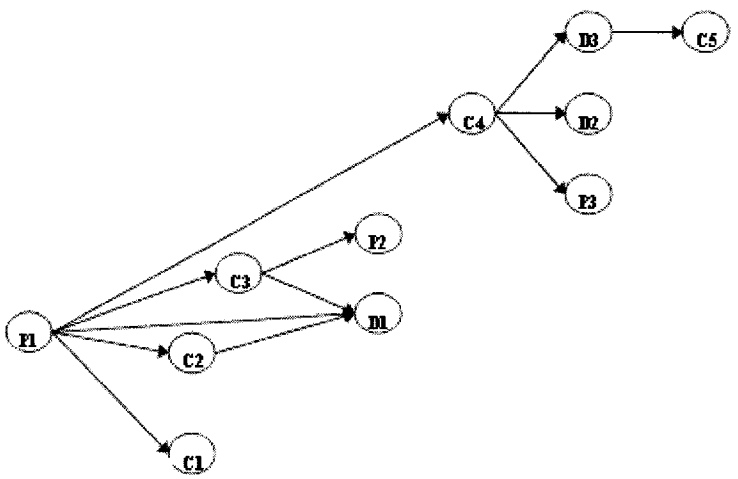

Figure 4.6: Partial Order of Tele-Monitoring Task

Role	Task Code	Privilege	Pre-condition
Tele-consultant			
Patient	P1	Make a appointment	No
	P2	Reset, if conflict	Reschedule (C3)
	P3	Talk to doctor	Notify others time arrive (C4)
Coordinator	C1	Censor the appointment	Make a appointment (P1)
	C2	Schedule the time	Make a appointment (P1)
	C3	Reschedule if conflict	Make a appointment (P1)
	C4	Notify others	Make (P1) accept (D1)
	C5	Save to EPR server	End the monitoring (D3)
Doctor	D1	Accept the appointment	Make(P1),schedule(C2)or reschedule (C3)
	D2	communicate with patient analyse and diagnose	Notify others time arrive (C4)
	D3	End the consultant	Notify others time arrive (C4)

Table 4.2: Tasks within Tele-Consultant

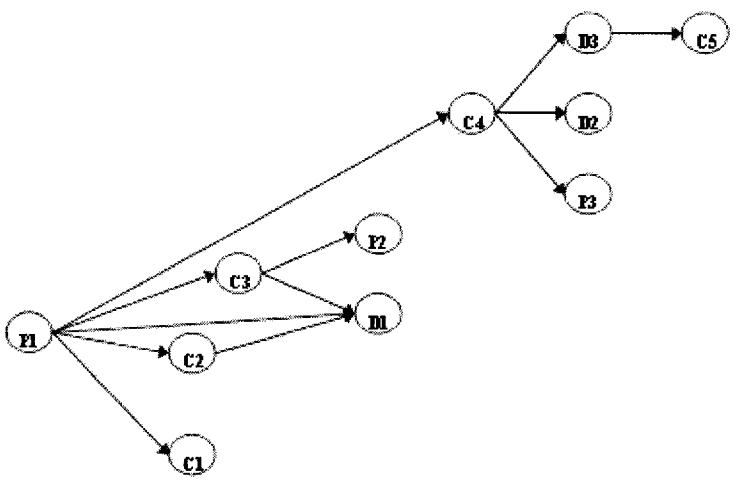

Figure 4.7: Partial Order of Tele-Consultant Task

Role	Code	Privilege	Pre-condition
Tele-education			
Student	S1	Make a reservation	Publish abstract and agenda (C1)
	S2	Join and preview material	Initiate lecture (C4)
	S3	Communicate with lecturer	Initiate (C4)and Present lecture (L1)
	S4	Leave question and quit	Finish lecture (L4)
Coordinator	C1	Publish abstract and agenda	Select a topic (L1)
	C2	Censor reservation	Make a appointment (S1)
	C3	Postpond	Make reservation (S1),select topic (L1)
	C4	Handout teaching material	Reservations(S1), Censor reservation (C2)
	C5	Save lecture to EPR	Finish the lecture (L4)
	C6	Notify student of ending	Finish the lecture (L4)
Lecturer	L1	Present a topic	No
	L2	Cancel and post another topic	Postpond lecture if minimum (S1) not reach (C3) make reservation (S1)
	L3	Present lectures and talk with students	Join the lecture (S2), initiate the session (C4)
	L4	Leave the feedback	Initiate session(C4),Present lecture(L3)

Table 4.3: Tasks within Tele-Education

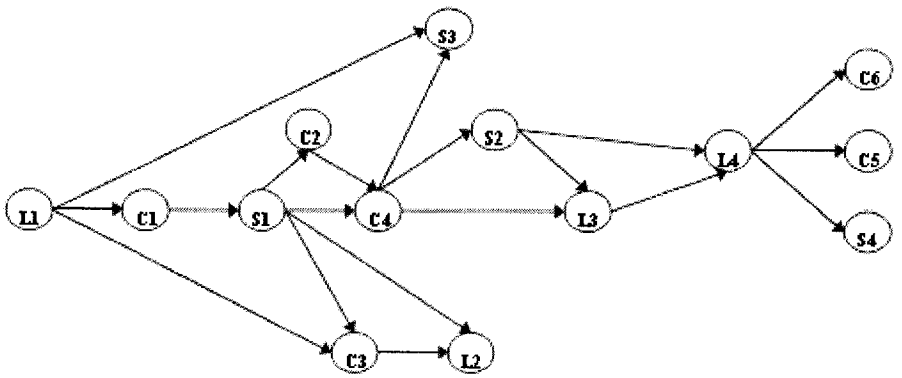

Figure 4.8: Partial Order of Tele-Education Task

Role	Task Code	Privilege	Pre-condition
Tele-lecture with other experts			
Other Experts	O1	Make a reservation or accept invitation	Publish the abstraction (C1), make invitation (L1)
	O2	Preview material and join	nitiate session hand out material (C3)
	O3	Discuss with lecturer	Join the session (O2)
	O4	Leave question and quit	Save lecture into ERP and notify participants lecture's ending(C4)
Coordinator	C1	Publish the abstract and schedule agenda	Select a topic (L1)
	C2	Censor reservation	Make reservation (S1)
	C3	Initiate lecture and distribute material	Censor and at least one participant accept invitation (C2)
	C4	Save lecture into EPR	Lecture ending(L3)
	C5	Notify participants of lecture's ending	Lecture ending(L3)
Lecturer	L1	Present a topic make some invitation	No
	L2	Present lecture, discuss with other experts	Join the lecture (O3), nitiate the session (C3)
	L3	Leave the feedback , finish the session	Initiate session(C3), Present the lecture (L2)

Table 4.4: Tasks within Tele-Lecture

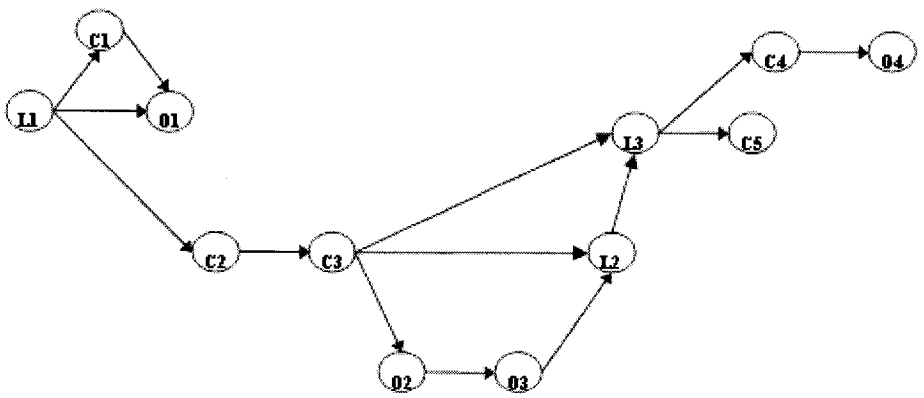

Figure 4.9: Partial Order of Tele-Lecture Task

coordinator checks the patients record for verifying his eligibility for making such a request. If the patient is registered with the medical organization and has appropriate privileges, the coordinator will send the appointment information to the corresponding doctor who is assigned to the patient. The doctor sets up a schedule for the consulting service and notifies the coordinator who in turn notifies the patient about the schedule. When scheduled time arrives, the coordinator notifies both the patient and doctor to start consulting service. The patient and doctor both need to authenticate to each other before the service starts, using techniques outlined in the previous section. After the service completes, the doctor notifies the patient with results and recommendations and stores the analyses and diagnoses data to the EPR server. The patient can then obtain further treatments according to the suggestion or diagnose results.

In the scenario, dependencies between different tasks clearly exist. Table 4.2 summarizes the tasks and their relationships in terms of pre-conditions. The dependency between tasks should be enforced by access control mechanisms in order to prevent users from either mistakenly or deliberately executing tasks in a wrong order. To enforce the partial order, we leverage the existing rule-based access control engine in the Web-based portal system. This access control engine is based on the classical Flexible Authorization Framework (FAF), which utilizes a logic-based language for authorization derivation, conflict resolution, and other advanced access control features. For our purpose, the done rule is sufficient for enforcing the partial order between different tasks. Each done rule specifies a past event, which can be a precondition of one or more other tasks. In Figure 16, the preconditions of the task D1 can be expressed as below:

$$cando(o, s, +make\_apt) \leftarrow in(s, patient), typeof(o, appointment)$$

$$do(o, s, +make\_apt) \leftarrow cando(o, s, +make\_apt)$$

$do(o, s, -make\_apt) \leftarrow \neg do(o, s, +make\_apt)$

$cando(o, s, +schedule\_apt) \leftarrow done(o, s, +make\_apt), in(s, coordinator), in(s, patient),$

$typeof(o, appointment)$

$do(o, s, +schedule\_apt) \leftarrow cando(o, s, +schedule\_apt)$

$do(o, s, -schedule\_apt) \leftarrow \neg do(o, s, +schedule\_apt)$

$cando(o, s, +reschedule\_apt) \leftarrow done(o, s, +make\_apt), in(s, coordinator), in(s, patient),$

$typeof(o, appointment)$

$do(o, s, +reschedule\_apt) \leftarrow cando(o, s, +reschedule\_apt)$

$do(o, s, -reschedule\_apt) \leftarrow \neg do(o, s, +reschedule\_apt)$

$cando(o, d, +accept) \leftarrow done(consultant, c, +schedule), done(consultant, c, +reschedule),$

$done(appointment, p, +make), in(c, coordinator), in(p, patient), in(d, doctor), typeof(o, appointment$

$do(o, s, +accept) \leftarrow cando(o, s, +accept)$

$do(o, s, -accept) \leftarrow \neg do(o, s, +accept)$

These expressions indicate that a doctor can only execute the accepting appointment task if a patient has already made that appointment via the coordinator, and the coordinator has sent over a schedule for the appointment. In this case, a task has more than one pre-condition. As another example, a task may be a pre-condition to other multiple tasks. The following shows that only after the coordinator sends a notification can other three tasks be executed:

$cando(o, s, +initiate\_con) \leftarrow in(s, coordinator), typeof(o, consultant)$

$do(o, s, +initiate\_con) \leftarrow cando(o, s, +initiate\_con)$

$do(o, s, -initiate\_con) \leftarrow \neg do(o, s, +initiate\_cont)$

$cando(o, s, +give\_con) \leftarrow done(o, s, +initiate\_con), in(s, doctor), in(s, coordinator),$

$typeof(o, consultant)$

$do(o, s, +give\_con) \leftarrow cando(o, s, +give\_con)$

$do(o, s, -give\_con) \leftarrow \neg do(o, s, +give\_con)$

$cando(o, s, +end\_con) \leftarrow done(o, s, +initiate\_con), in(s, doctor), in(s, coordinator),$

$typeof(o, consultant)$

$do(o, s, +end\_con) \leftarrow cando(o, s, +end\_con)$

$do(o, s, -end\_con) \leftarrow \neg do(o, s, +end\_con)$

$cando(o, s, +receive\_con) \leftarrow done(o, s, +initiate\_con), in(s, patient), in(s, coordinator),$

$typeof(o, consultant)$

$do(o, s, +receive\_con) \leftarrow cando(o, s, +receive\_con)$

$do(o, s, -receive\_con) \leftarrow \neg do(o, s, +receive\_con)$

4.4 Demonstration of the Tele-Consultant Scenario

I will give each task or step in the tele-consultant scenario a detailed description based on the implementation.

User Logon Logon interface is identical for every user whose role can be doctor, patient, or coordinator. Username and password are mandatory for the basic security reason. Incorrect password input will deny the user's access to tele health system.

Patient Making Appointment At the begining of a tele-consultant, patients logon to the system and make an appointment for their treatments or consultant services. The patient need to provide some information about his or her health condition, and pick an appropriate time for this appointment. Once this is done, the appointment will be displayed on the same page for review.

A doctor's information is displayed at this step, and the doctor's digital certificate can be

Figure 4.10: Snapshot of Logon

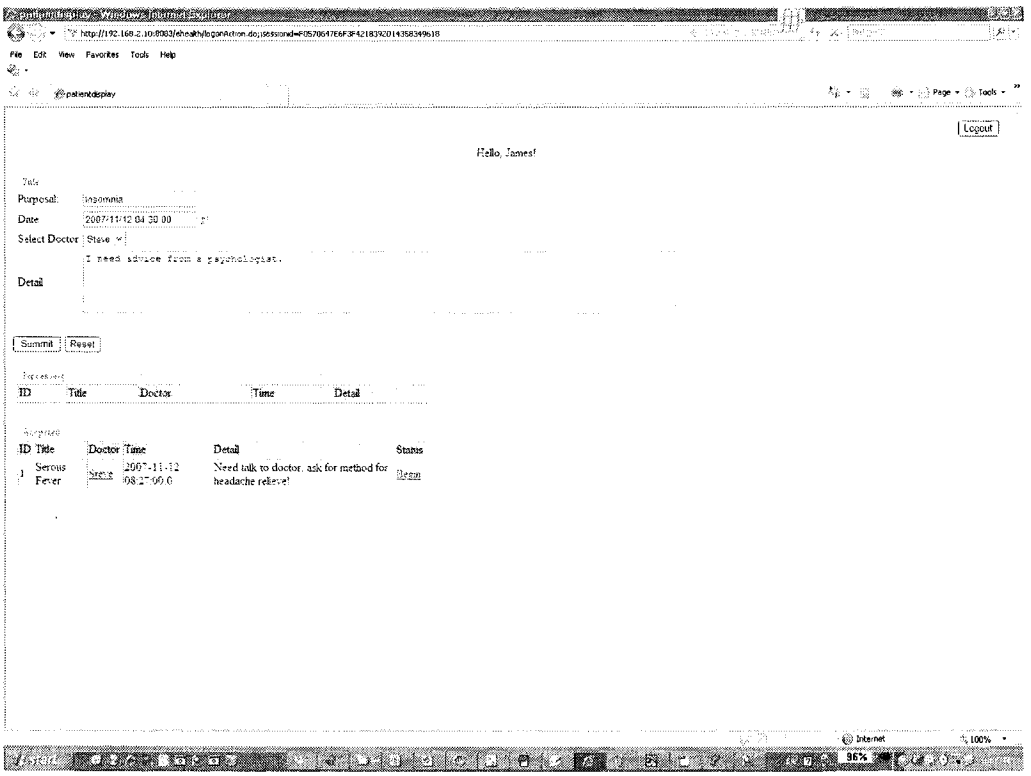

Figure 4.11: Snapshot of Patient Making Appointment

Figure 4.12: Snapshot of Doctor's E-licence

verified by a higher authority. Doctor's latest picture is displayed to patients and patients can click the doctor's picture and be redirected to the website of the higher authority, such as Canada health agency. Visible watermark on the edge of the doctor's picture is the address of the higher authority website's which can provide patients with the doctor's detailed information including the doctor's current picture, so patients can compare the two pictures to verify the doctor's identity.

Coordinator Forward Appointment to Doctor As described in the previous sections, one of the coordinator's duties is to forward a patient's requests to a doctor and censor the feasibility of the appointment. Coordinator can list all appointments and review the status of each appointment.

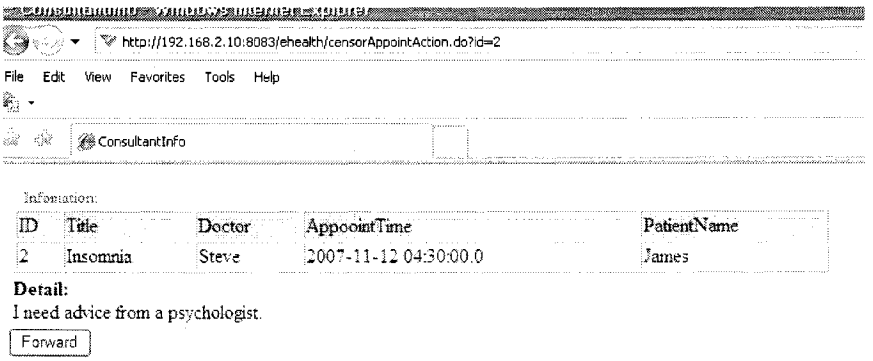

Figure 4.13: Snapshot of Coordinator Forwarding Appointment

Doctor Accept Appointment Forwarded from Coordinator Doctor receives the request for consultant appointment from coordinator, then he can accept it and follow the appointment time scheduled by the patient. If the doctor cannot resolve time conflict, he can change the appointment time before accepting this appointment. The doctor can preview the patient's medical information and other health data from the EPR server provided by other modules of the e-health system. Once the doctor accepts the patient's appointment, he can modify or cancel the appointment piror to the initiation of this consultant.

Waiting or Begining the Consultant The appointment is divided into two groups within the user's web page, while processing means that the appointment is pending and not forwarded by the coordinator nor accepted by the doctor. Another group, means these appointments are already accepted by the doctor and are waiting for the appointment time. For the patient, after the doctor accepts the appointment for consultant, the patient can review the status of the appointment. If the appoinment time has not arrived, the status will be waiting. For the doctor, the suituation is similar, that is the status of consultant is either begin or waiting.

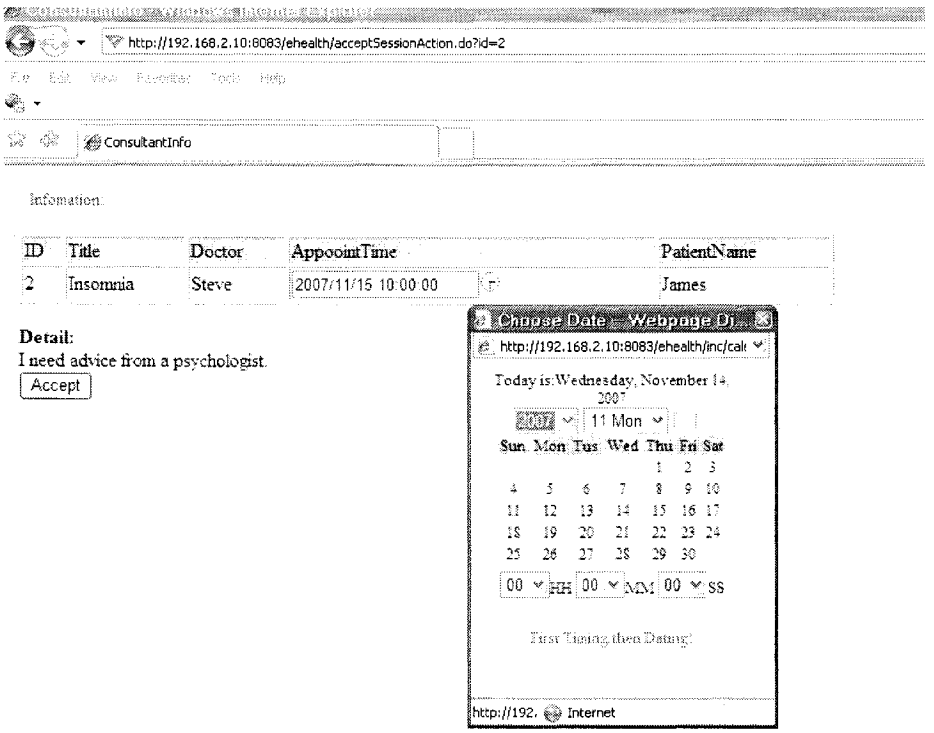

Figure 4.14: Snapshot of Doctor Accepting Appointment

Processing:

ID	Title	Doctor	Time	Detail
3	Back pain	Grey	2007-11-22 00:00:00.0	Back pain, which method can relieve extreme pain faster.

Accpeted:

ID	Title	Doctor	Time	Detail	Status
1	Serous Fever	Steve	2007-11-16 08:27:00.0	Need talk to doctor, ask for method for headache relieve!	Waiting
2	Insomnia	Steve	2007-11-12 04:30:00.0	I need advice from a psychologist.	Begin

Figure 4.15: Snapshot of Reviewing the Appointments

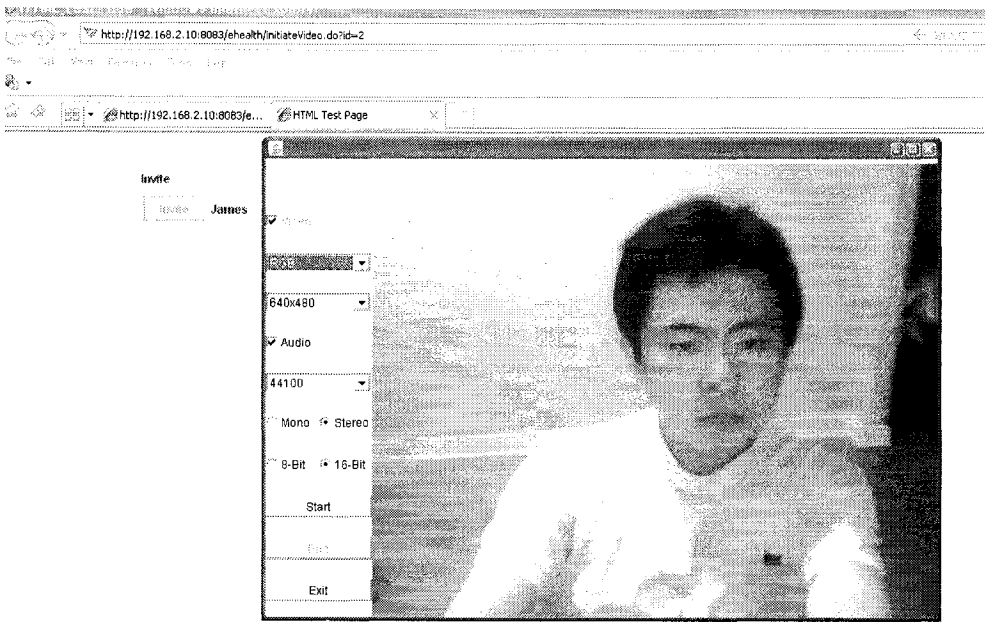

Figure 4.16: Snapshot of Tele Consultant Conversation

Tele Consultant Conversation When the appointment time arrives, the patient and doctor must logon the system punctually. The doctor and patient can click the link to begin the consultant, then the applet program for multimedia capture and transmission will be launched. The doctor clicks the invite button to send out an invitation message to the patient's reception program. Once the patient receives the invitation message, real time multimedia communications start. The patient and doctor can talk to each other just like in a face-to-face conversation. This procedure is not based on portal service,instead in a peer-to-peer mode due to a more rigid performance requirement. Once the conversation is over, the patient and doctor can shut down their applet programmes and quit the tele-consultant system.

Accepted:

ID	Title	Patient	Time	Detail	Status
1	Serous Fever	James	2007-11-16 08:27:00.0	Need talk to doctor, ask for method for headache relieve!	Waiting
2	Insomnia	James	2007-11-12 04:30:00.0	I need advice from a psychologist.	Finish

Figure 4.17: Snapshot of Session's Status From Doctor

Processing:

ID	Title	Doctor	Time	Detail	Status
3	Back pain	Grey	2007-11-22 00:00:00.0	Back pain, which method can relieve extreme pain faster.	Forward

Accepted:

ID	Title	Doctor	Time	Patient	Detail	Status
1	Serous Fever	Steve	2007-11-16 08:27:00.0	James	Need talk to doctor, ask for method for headache relieve!	Accept
2	Insomnia	Steve	2007-11-12 04:30:00.0	James	I need advice from a psychologist.	Finish

Figure 4.18: Snapshot of Session's Status From Coordinator

The End of Tele Consultant The doctor is a supervising entity in a tele-consultant session and has the responsibility for reviewing each completed consultant session. One duty of the coordinator is to manage all consultant sessions. The doctor and coordinator both have the capability to check the status of a tele-consultant session. The difference is that the doctor can only check a session involving himself.

Chapter 5

Implementation

This chapter gives more detailed descriptions of implementation based on the architecture of telehealth subsystem introduced in chapter 4. I will demostrate all components involved this architecture, which includes servers and applications. I will divide the discussion of the architecture into two parts according to the communication mode, namely, is client-server and peer-to-peer.

5.1 Implementation Environment

We choose Java as the main language for the implementation, so it can be platform independent. Client-server mode means the web browser is used to access services. The Windows platform is our choice for the server's deployment. The peer-to-peer mode is implemented using communications through java applets. The integration of the two difference modes is thus easy.

5.2 Client-Server Mode

The client-server mode is a centralized architecture in which the server represents computing services, software servers or hardware computing systems. Generally, database servers, web servers and application servers are in client-server mode. In our design, the majority of

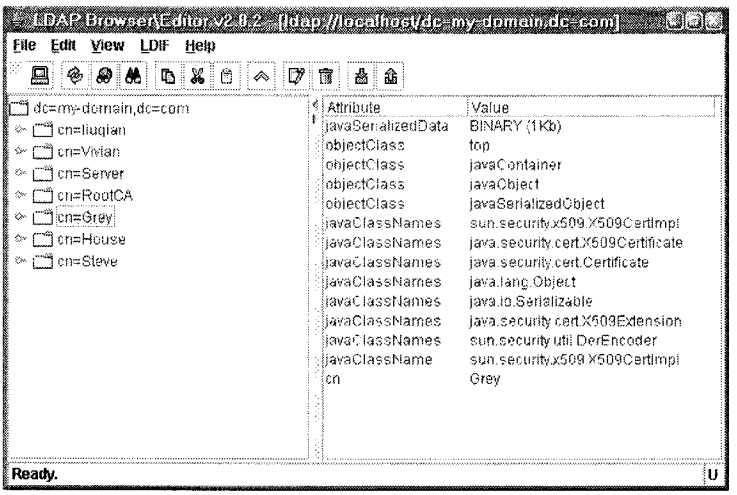

Figure 5.1: Digital Certificate in OpenLDAP Server

deployed services runs in client-server mode. These services are directory service, website service and database service. For implementation these are OpenLDAP server, Tomcat server and Mysql database server. The following explains the functionality of each server.

5.2.1 OpenLDAP server

LDAP (Lightweight Directory Access Protocol) is based on X.500 standard protocal, which is composed of a series of protocols. Directory service is a special database optimized for the purpose of querying, browsering, and searching. It is also a computing system created from a set of accessing protocols. The aim of our OpenLDAP server is to store digital certificates and health organizations certificates, which is treated as a higher authority and to issue certificates under the supervision of the health organization. The digital certificate and organization's certificate are of X.509 certificate type. We can check the certificate in OpenLDAP through a browser tool called LDAPBrowser.

5.2.2 Tomcat web server

We choose light-weight Tomcat server. Tomcat can provide full support for struts framework whose MVC (Model-View-Control) model is used to control workflow tasks. The MVC model of struts provides charateristics especially suitable for workflows. The entity Model makes it possible to reuse java classes within different function modules. In the testing environment, this can also be deployed on JBoss or Weblogic platform based on JDK run time environment due to Java's platform independence.

5.2.3 Mysql database server

The main functionality of the database server in our implementation is to interact with the Prolog server to achieve rule-based access control, and to save necessary data of tele-consultant which includes appointment details and all SIP communication records. Due to less rigor performance requirement, we choose Mysql database server that is eligible enough to provide data research, extract and storage. Rule-based access control is a introduced for satisfying the security requirement of the workflow system and Prolog is used to support the do and done rules expressed in the FAF language [22] to represent constraints in workflow systems. These constraints can be used to enforce partial orders on tasks during run-time of workflows. The data and parameter used to instantiate the constraints are stored in the Mysql server to create the rule's predicate.

5.2.4 Prolog server

The access control engine receives the authorization request from external applications and then forwards it to the validator module of the Prolog server. The predicates from FAF language's do or done rule can be invoked by predicate API, which can extract data or parameters from the database to execute the implementation of predicates. The Prolog

server can return the rule's decision to applications or web page interfaces to show the result of these constraints described by the do rules.

5.3 Peer to Peer Mode

Different from client-server mode, the peer-to-peer model is a decentralized structure, and every peer is equivalent within the communication environment. Unlike a web-based service, a user sends a request to the server for a service, like logon to a system or sumbit data. Upon receiving the request, the server needs to respond to the request. The peer-to-peer mode allows one user to send a request to another user. Between users there does not exists any server whose responsibility is to route the request to the correct destination. Within peer to peer mode, there is no explicit servers or clients, every peer node can be a server or client to other peers. One important goal of the peer-to-peer mode is that all peer nodes can provide their resources including bandwidth and computing capability to increase the total capacity of the system. Pure peer-to-peer mode is decentralized. However in our implementaion, conversation between doctor and patient during tele-consultant can be throught as a peer-to-peer communication, we also need a non-peer element called as central index service for routing messages which works like the DNS server in internet.

5.3.1 Jiplet container

Jiplet container is a set of Java class, which is developed as a container deployed as service-side SIP [Hssr99] application. Jiplet container provide developer many efficient and convinient Java APIs to support SIP message formatting, parsing, thread-pooling, authentication, and authorization. Jiplet container creates the realm concept. It can be used for the enforcement of authenticaiton and authorization. There are two approaches to deploy

the Jiplet container, one of which is standalone which means we can set up and run Jiplet container as a common Java application. Another is to deploy the Jiplet container as a JBOSS service. We choose to run Jiplet in a standalone mode, because Jiplet container is supposed to occupy less momery resources and run smoothly on a smaller computer. More specifically, the jiplet container is just a container for jiplet application(s). According to our requirement for real time tele-consultant, we only need to implement some fundamental functions with Jiplet, such as user registering user's contact information, receiving incoming message from other users, routing message to correct destination, and terminating message exchange session between users. We will give more detailed explanations of how SIP work in the next section implementation.

5.3.2 Real-time Transport Protocol

Real-time Transfer Protocol (RTP)[Sccf03] provides end-to-end delivery services for data (such as interactive audio and video) with real-time characteristics. RTP works in a pure peer-to-peer mode. In our implementation, during the conversation between doctor and patient, after doctor or patient logon onto the Realm created by Jiplet container, Jiplet container is able to route the message accurately to which it is supposed to send, so sip session is established sucessfully. Doctor can connect his video camera to the computer and turn on microphone to capture video and audio stream, and send these data packet to patients. Upon receiving the multimedia data packet, the patient's decoding program will reconstruct the data packets into video and audio streams for presentation. All operations of multimeida such as capturing, transferring and presenting video or audio streams have been prefectly implemented by JMF API (java medial framework) introduced by SUN. Our work imposes these APIs to make possible Java applet as a SIP agent within the communication

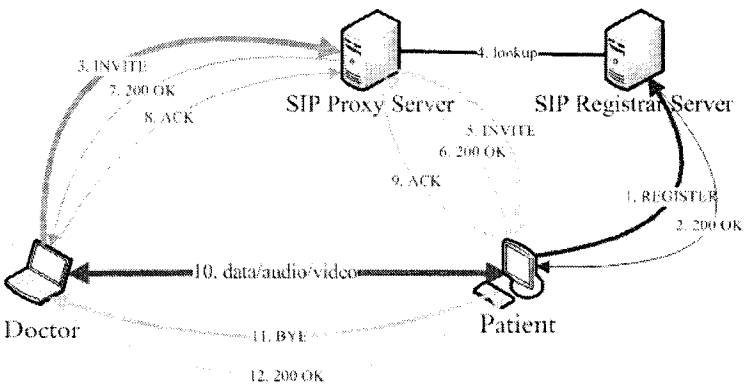

Figure 5.2: SIP RTP and Jiplet Cooperation for Tele-Consultant

environment. The figure 27 describes the whole process and working mechanism of SIP, Jiplet container and RTP during Tele-consultant session.

1. Patient registers himself to the registrar server by sending a REGISTER request.

2. The registrar server accepts the registration, which contains the patient's name, IP address, port and other contact information, and respond with a 200 OK status code.

3. Doctor requests to establish a communication session with Patient by sending an INVITE request to the proxy server. The INVITE message's content typically contains the description of the communication session the caller wants to establish, such as media type, doctor's IP address and port.

4. The proxy server looks up the registrar server to find out the patient's current IP address and port.

5. The proxy server forwards the INVITE request from doctor to patient based on their current registered IP address.

6. Patient accepts the invitation request by responding back a 200 OK status code.

7. The proxy server forwards a 200 OK response from patient to doctor.

8. Doctor confirms the session establishment by sending an ACK message to the proxy server.

9. The proxy server forwards the ACK to the patient. Thus, the three-way handshake is completed by the aid of the proxy server, and eventually a session is established.

10. Now the conversation for tele consultant between doctor and patient happens. Mixture of video and audio conversations are transmitted over RTP directly between doctor and patient and it is not necessary to bypass the proxy server.

11. Now, Patient finishes the conversation and wishes to terminate the session by sending a BYE request.

12. Doctor responds with a 200 OK status code to accept session termination.

I demostrate and explain two SIP messge INVITE and its response messge ACK. $INVITEsip:James@cafesip.orgSIP/2.0$

$Call-ID: d8307ab1270ee6b15998005f9da435c2@192.168.2.10$

$CSeq: 1INVITE$

$From :< sip: Steve@cafesip.org >; tag = 1024367196$

$To :< sip: James@cafesip.org >$

$Via: SIP/2.0/UDP192.168.2.10: 9091; branch = z9hG4bKb272c00bd00e5b936c530f8fffffebf$

$Max-Forwards: 70$

$Contact :< sip: Steve@192.168.2.10: 9091; transport = udp >; expires = 3600$

$Route :< sip: 192.168.2.10: 5060; lr; transport = udp >$

$Content-Length: 0$

The goal of this SIP message is that doctor Steve invites patient James to join the session and provide him with contact information like IPAddress 192.168.2.10 and port 9091, when James answers message , he can response back to this address.

$ACKsip : James@192.168.2.11 : 9091; transport = udpSIP/2.0$

$Via : SIP/2.0/UDP192.168.2.10 : 9091; branch = z9hG4bK8562645685eecead2bd17ad1b244b724$

$CSeq : 1ACK$

$Call - ID : d8307ab1270ee6b15998005f9da435c2@192.168.2.10$

$From :< sip : Steve@cafesip.org >; tag = 1024367196$

$To :< sip : James@cafesip.org >; tag = 1585117505$

$Expires : 0$

$Max - Forwards : 70$

$Route :< sip : 192.168.2.10 : 5060; lr >$

$Content - Length : 0$

We notice that the call-ID of two message is identical, so two message is relative INVITE and ACK message. One is request and other is response to confirm message for INVITE.

5.4 Security Enhancement Implementation

In this thesis, our cardinal goal is to enforce the security of telehealth with two distinct measures which are Biometrics authentication and do rules-based access control. The implementaion of these measures is a comprehensive work involved many technologies and computing services.

Figure 5.3: Doctor's E-Licence

5.4.1 Biometrics-based Authentication and Hierarchies of Trust

In our implementation, we provide patients with a specific visual card, which is called e-licence and it works like a doctor's ID card adorned on the doctor's uniform. Within traditional hospitals, doctor's identitiy can be verified by his uniform or his ID card. Because the hospital's specific environment, doctor's uniform can represent himself. Patient can compare the doctor's facial character with picture on his ID card within hospital, this leads to the most fundamental biometrics authentication. The below picture is e-licence implementation based on java applet.

The doctor's information shown on the applet is read directly from the doctor's digital certificate saved in the OpenLDAP server whose main function is as introduced in previous chapters. Java API and java.security.cert.X509Certificate class provide all operations on X509 Certificate such as extracting cerficate's holder's name, Issuer, expiration time and

how to use higher authority's public key to verify the authenticity of the doctor's digital certificate. The steps of which e-licence applet connects to OpenLDAP server, extracts doctor's certificate, read all information from digital certificate, and how to verify it are described below:

1. Java Naming and Directory Interface (JNDI) provides a feasible method lookup() to extract certificates stored in the remote OpenLDAP server.

```
Properties env = new Properties();
env.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.LdapCtxFactory");
env.put(Context.PROVIDER_URL, "ldap://192.168.2.10:389/");
DirContext ctx = new InitialDirContext(env);
o = (Object) ctx.lookup("cn=Steve,dc=my-domain,dc=com");
X509Certificate cer=(X509Certificate) o;
```

   Java Object o actually is doctor Steve's digital certificate and ldap://192.168.2.10:389/ is the Address where OpenLDAP server deploys.

2. java.security.cert.X509Certificate class provides many methods to operate the digital certificate, like getSubjectDN() to get certificate holder Steve's personal information on her digital certificate, getIssuerDN() to get Steve's certificate Issuer, higher authority 's detail information and getNotAfter() to get this digital certificate's expire time.

3. Verifying digital certificate authenticity is an important step in this E-Licence Applet. This step can demostrate to patient that the information from this licence is genuine. This information is verified by authoritative organiztion like Canada Health Agency, so the information can be totally trusted. We can extract the issuer's higher authority's certificate from keystore, which is like a collection of authorities that are trusted, and then get the public key of this higher authority with method getPublicKey()

from java.security.cert.X509Certificate class. Below is some java code for verifying the Steve's digital certificate.

```
KeyStore ks = KeyStore.getInstance("JKS");
ks.load(keystoreInput, passWord.toCharArray());
java.security.cert.Certificate rootCACertificate =
ks.getCertificate("rootca");
//the public key of RootCA
PublicKey pbk = rootCACertificate.getPublicKey();
//vertify the user's Certificate
clientcr.verify(pbk);
```

It is worth noting that rootca in previous code is the alias name for higher authority stored in the Keystore, all of these codes is implemented with standard X509 Certificate API motheds.

4. The E-licence shows the doctor's recent picture on the right part of the applet, and we can compare this picture to the people in the video present during the conversation of Tele consultant. So biometrics can work in this way and we still need to prove the picture's authenticity to patient. In implementation, we put a visiable watermarking on doctor's picture, on this picture is "www.phac-aspc.gc.ca", while it is a address of website from some organization one of whose duties is to supervise and manage doctor's qualification. In order to implement biometrics authentication for patients, the doctor's picutre on applet can be clicked to open a new browser redirecting page to the website address of supervising organization like Canada Health agency offical website, and so the patient is able to authenticate the doctor's biometrics. Below is some code to demostrate how to open a browser within applet.

```
URL authorizationURL = new URL("http://www.phac-aspc.gc.ca");
getAppletContext().showDocument(authorizationURL, "_blank");
```

5.4.2 Rule-base Access Control Enforcing Workflow Execution

Do rules are already expressed by FAF language which is introduced in the chapter 3 and chapter 4. What concerns our implementation most is how to translate these rules into constraints for access control and apply these constraints to avoid workflow tasks conflict. Actually Prolog server is a middleware connecting the workflow runtime envirommment to constraints and rules saved in the MySql database. Prolog provides source code file whose extensions is .pl for several purposes on implementaion of rule-based access control. The first one is to bind external request interface to do- or done-rules validator. Actually external interface can be java class method or .net function. The below is some code segment.

$register\_query(validate(O, S, A), do(O, S, A))$

The second is to judge predicates from rules or constraints based on workflow access control policy. This part in source code of Prolog is quite similiar with FAF language's do- or done-rule.

$cando(o, s, +receive\_con) \leftarrow done(o, s, +initiate\_con), in(s, patient), in(s, coordinator)$

The third purpose is to instantiate predicates from external data source like role's information or workflow status saved in the MySql database.

$foreign\_resource(recollector, [init(recollector\_init)])$

The third purpose needs some support from external application recollector.cpp to read data and information from MySql server and provide predicate judge binding with funcation of external application. C++ code segment is below.

$voidrecollector\_init(intwhen)$

$SP\_define\_c\_predicate("typeof", 2, "user", typeof, NULL);$

$SP\_define\_c\_predicate("hasAppointed", 2, "user", hasAppointed, NULL);$

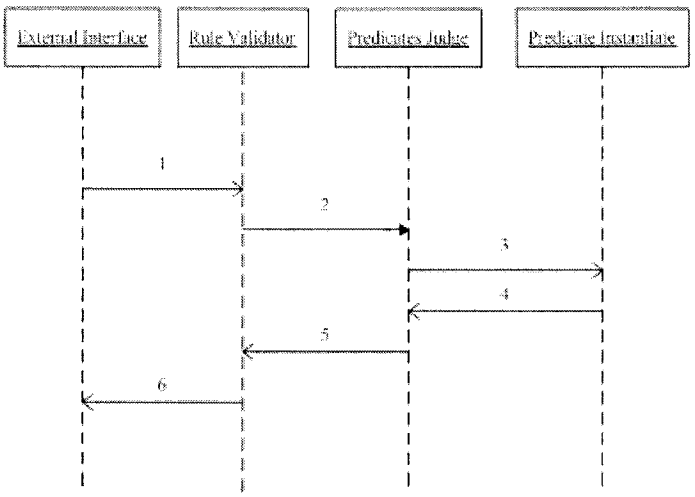

Figure 5.4: Sequence Diagram of Prolog Working Mechanism

$SP\_define\_c\_predicate("status", 2, "user", status, NULL)$;

We demostrate how Prolog acts as a middleware and works with other external application cooperatively to enforce the rule-based access control following this figure.

1 . Web interface sumbits rule's validation request to Prolog server, and Prolog receives and forwards it to corresponding rules.

2 . Validated rules contains several predicates like do rules from FAF language and invokes their implementation through predicate API provided by external applicatoin recollector.cpp.

3 . 4 External applications connect to database and then extracts role information and workflow status to instantiate predicate.

5 . External application executes predicate judging function and return predicate's execution results to rule validator.

6 . Rule validator returns rule validation result as a response to web interface according

to predicate's execution result.

Chapter 6

Conclusion

6.1 Conclusion

We have studied two security issues of telehealth applications in the context of a Web-based e-health portal. First, for establishing trust in the lack of visual contacts, we proposed a PKI-like hierarchical approach to provide users with biometrics authentication. The established trust can be verified during a telehealth service using multimedia components. Second, for telehealth services that involve workflow-like complex processes, we proposed a method for representing the dependency between tasks as partial orders, and then enforcing such partial orders using logic rules. This approach was cost-efficient since it reused the existing rule-based access control engine in the Web-based e-health portal.

6.2 Future Work

With those implements, I accomplished this thesis. What's more in the future, we can do some extra work on a few aspects that has been mentioned in this thesis.

1. First, we can apply the automatic facial recognizer from commercial productions instead of relying on human eyes and we could collect the human voice or other biological characters as template within the biometrics process.

2. Secondly, we can apply the enhanced RBAC into more complex workflow based health

service involved many more users and add flow control mechanism into the execution of multi-task.

3. Finally, we need to improve and guarantee the quality of service of videoconferencing particularly in the broadcasting mode lile tele education service.

Bibliography

[As04] Mohammad A Al-Kahtani, Ravi S. Sandhu. Rule-base RBAC with negative authorization. 20th Annual Computer Security Applications Conference, 2004.

[Askr00] Gail-Joon Ahn, Ravi Sandhu, Myong Kang and Joon Park. Injecting RBAC to secure a Web-based WorkFlow System. Proceedings of the fifth ACM workshop on Role-based access control,2000.

[Atl01] Vijar Atluri. Security for Workflow systems. Information Security Technical Report,2001.

[Bfa99] Elisa Bertino,Elena Ferrari,Vijay Atluri. The Specification and Enforcement of Authorization Constraints in Workflow Management Systems. ACM Transactions on Information and System Security (TISSEC),1999.

[Bmncn04] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman. RFC 3711 The Secure Real-time Transport Protocol (SRTP). RFC 3711, 2004.

[Brus94] Brussels. Workflow reference model. Technical report, Workflow Management Coalition, 1994.

[Fck95] David F. Ferraiolo, Janet A. Cugini, D. Richard Kuhn. Role-Based Access Control (RBAC): Features and Motivations. Computer Security Applications Conference, 1995.

[Fwub02] Geoffrey Fox, Wenjun Wu, Ahmet Uyar, Hasan Bulut. A Web Services Framework for Collaboration and Audio/Videoconferencing. proceedings of 2002 International Conference on Internet Computing, 2002.

[Ghs95] Diimitrios Georgakopoulos, Mark Hornick, Amit Sheth. An overview of workflow management: From process modeling to workflow automation infrastructure. Journal Distributed and Parallel Databases, 1995.

[Gmw05] Mark Gasson, Martin Meints and Kevin Warwick. A study on PKI and biometrics. the FIDIS NoE Technical Report, 2005.

[Gra99] S. Graeber. The Impact of Workflow Management Systems on the Design of Hospital Information Systems. Joint European Conference on Artificial Intelligence in Medicine and Medical Decision Making,, 1999.

[Ha99] W-K Huang and V.Atluri. SecureFlow: A Secure Web-enable Workflow Management System. 4th ACM Workshop on Role-based Access Control,1999.

[Hc03] K.-F. Hwang and C-C Chang. A self-encryption mechanism for authentication of roaming and teleconference service. IEEE Trans. On wireless Community. vol.2,2003.

[Hk03] Patrick C.K. Hung, Kamalakar Karlapalem. A Secure Workflow Model. Proceedings of the Australasian information security workshop conference on ACSW frontiers, 2003 .

[Hllwd07] Yuan Hong, Shuo Lu, Qian Liu, Lingyu Wang and Rachida Dssouli. A Hierarchical Approach to the Specification of Privacy Preferences . Proc. 4th International Conference on Innovations in Information Technology (Innovations 2007), IEEE.

[Hssr99] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg. RFC 2543 SIP: Session Initiation Protocol . RFC 2543, 1999.

[Jlss05] Yixin Jiang and Chuang Lin, Minghui Shi and Xuemin (Sherman) Shen. A Self-Encryption Authentication Protocol with Identity Anonymity for Teleconference Services. PGlobal Telecommunications Conference,2005.

[Jsss97] Sushil Jajodia, Pierangela Samarati, Maria Lusia Sapino, V. S. Subrahmanian. A Unified Framework for Enforcing Multiple Access Control Policies. Proceedings of the 1997 ACM SIGMOD international conference on Management of data , 1997.

[Jsss01] Sushil Jajodia, Pierangela Samarati, Maria Lusia Sapino, V. S. Subrahmanian. Flexible Support for Multiple Access Control Policies. Volume 26, Issue 2, ACM Transactions on Database Systems (TODS) , 2001.

[Ka95] N,Krishenakumar and A.Aheth. Management heterogeneous multi-system tasks to support enterprise-wide operations. Distributed and Parallel Databases, 1995.

[Kfska99] Myong H. Kang, Judith N. Froscher, Amit P. Sheth, Krys J. Kochut, and John A.Miller. A multilevel secure workflow management system. Proceedings of the 11th Conference on Advanced Information Systems Engineering , 1999.

[Kpf01] Myong H. Kang, Joon S. Park and Judith N. Froscher. Access Control mechanisms for Inter-organizational Workflow. Proceedingof the 6th ACM symposium on Access Control. Methods and Technologies, 2001.

[Lar04] Ravi S. Sandhu. Role-based access control. Addison-Wesley, 2004.

[Lar04] C. Larman. *Applying UML and patterns.* Addison-Wesley, 2004.

[Llhwd08] Qian Liu, Shuo Lu, Yuan Hong, Lingyu Wang and Rachida Dssouli. Securing Telehealth Applications in a Web-Based e-Health Portal . Proc. 3rd International Conference on Availability, Reliability and Security (ARES 2008), IEEE.

[Lhlwd07] Shuo Lu, Yuan Hong, Qian Liu, Lingyu Wang and Rachida Dssouli. Access control for e-Health system portal . Proc. 4th International Conference on Innovations in Information Technology (Innovations 2007), IEEE.

[Lrs02] F.Leymann, D.Roller, M.-T. Schmidt. Web service and business process management. IBM system journal, 2002.

[Maj04] Andrew Joseph Marshall. A Comparative Study of Biometrics and Their Application In A Web Based Healthcare Environment. Technical Report, 2004.

[Mskw96] J.A. Miller, A.P.Sheth, K,J, Kochut and X Wang. Corba-base Real-time architecture for Workflow management systems. Journal of Systems and Software, 1996.

[Nac02] A.C. Norris. Essentials of Telemedicine and Telecare. ISBN 0-471-53151-0, John Wiley Sons, West Sussex, England, 2002.

[Sccf03] H. Schulzrinne, S. Casner, S. Casner, R. Frederick. RFC 3550 RTP: A Transport Protocol for Real-Time Applications. RFC 3550 , 2003.

[Scfy96] Ravi S. Sandhu, Edward G coyne, Hal L ,Feistein, Charles, E ,Youman. Role-based acess control Models. IEEE Computer, 1996.

[Sy01] Youchi Seto. Development of Personal Authentication System using Fingerprint with Smart card and Digital signature technologies. Proceedings of the 34th Annual Hawaii International Conference on System Sciences, ISBN: 0-7695-0981-9, 2001.

[Wphshs97] Michael Webber, Gerhard Partsch, Siegfried Hock, Geoge Schneider, Astrid Scheller Houy, Jean Schweitzer. Integrate synchronous multimedia collaboration into workflow management. Proceedings of the international ACM SIGGROUP conference , 1997.

[Wsc10] Workflow Management Coalition (WfMC). Workflow Security Considerations C White Paper. Document Number WFMC-TC-1019, Document Status-Issue 1.0.

[Vas97] Rohit Valia, Yahya AI-Salqan Secure Workflow Environment. Proceedings of the 6th Workshop on Enabling Technologies on Infrastructure for Collaborative Enterprises ,1997.

Glossary

BCS	Bio Medical Cognitive Science
BPM	Business Process Management: An merging field of knowledge and research at the intersection between managment and IT
CIM	Clinical Information Management
CHI	Consumer Health Informatics
CORBA	Common Object Request Broker Architecture: A standard enables software components written in multiple computer languages and computers to work together (Defined by Object Management Group)
Closed Policy	Authorizations specify permissions for an access
E-Health	Healthcare practices supported by electronic processes and communication, such as Electronic Patient Records, Telemedicine .etc
EPR	Electronic Patient Record: The patients' digital records, including personal information, diagnosis, prescription .etc
FAF	Flexible authorization framework

FGAC	Fine-Grained Access Control: Implement access control with security policies or functions in a fine-grained level
HIPAA	Health Insurance Portability and Accountability Act: was enacted by the US Congress in 1996
HTML	Hypertext Markup Language: a markup language for web pages
JMF	Java multimedia framework
JPF	Java Page Flow: A feature set built upon a Struts-based Web application programming model
JRC	European Union's Joint Research Center
JSP	Java Server Pages: A Java technology that enables to dynamically generate HTML, XML or other file types for response upon the Web client request
MVC	Model-View-Controller: A multi-tier architecture pattern used in software engineering
MLP	Medical Language Processing
OLAP	Online Analytical Processing: An advanced for of data analysis for data warehousing environments
Open Policy	Authorizations specify denials for an access
RBAC	Role base access control

REST	Representational State Transfer: A style of software architecture for distributed hypermedia systems
RPC	Remote Procedure Call: A technology that enables a computer program to make a procedure execute in another address space without explicitly coding the details
RLS	Row-Level Security: Another term for Oracle's implementation of Fine-Grained Access Control, besides VPD
RTP	Real-time transfer protocol
SIP	Session initiate protocol
SQL	Structured Query Language: A database computer language designed for data retrieval, database schema creation, modification or access control mechanisms
SOA	Service-Oriented Architecture: a software architecture that uses loosely coupled software services to support the requirements of business processes and software users
SOAP	Simple Object Access Protocol: A protocol for exchanging XML-based messages over computer networks, which is the basis of web services

TEL	Telemedicine: A developing technology for clinical medicine where medical information is transferred via telephone, Internet for remote medical diagnosis or examination
VPD	Virtual Private Database: Oracle's implementation of Fine-Grained Access Control
W3C	World Wide Web Consortium: The main international standards organization for the World Wide Web
WSDL	Web Services Description Language: An XML-based language which provides standard format to define web services
WSRP	Web Services for Remote Portlets: A network protocol standard designed for communications with remote portlets (defined by OASIS)
XML	Extensible Markup Language: A general purpose standardized markup language, which can be defined in many platforms and various systems