
©2007 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.
This is the authors final peer reviewed version of the item published as:


Copyright : 2007, IEEE
An Authorization Policy Management Framework for Dynamic Medical Data Sharing
Fahed Al-Nayadi and J. H. Abawajy
Deakin University
School of Engineering and Information Technology
Melbourne, Vic. Australia

Abstract
To offer the best possible care for their patients, family physicians need coordinated data obtained from the physician’s own patient database, from other physicians database, pharmacies, and drug reference databases. P2P-based sharing systems have been actively researched to enable resource sharing between multiple heterogeneous healthcare enterprises. Unfortunately, P2P system introduces a whole new class of privacy and security threats and in order to enable resource sharing between multiple heterogeneous healthcare enterprises, a policy management framework is required. To solve these problems in a loose-coupling way, we propose a dynamic, distributed and heterogeneous policy management framework for sharing medical information among autonomous and disparate healthcare information systems.

Keywords: Healthcare system, privacy, security, authorization, authentication, policy, P2P.

1 Introduction
Although, healthcare is one of the few domains where sharing information is the norm rather than the exception [4], the localization and access to electronic patient records across healthcare enterprise boundaries have remained an important and challenging problem. The recent advent of middleware technologies such as peer-to-peer (P2P) systems are capable of enabling sharing electronic health record across autonomously managed heterogeneous healthcare information systems across different healthcare enterprises despite the fact that they may be dispersed throughout the world, and that they may not know each other personally. As a result, a flurry of peer-to-peer (P2P) based systems for distributed healthcare data sharing have been emerging recently. For example, under the assumption that the healthcare providers form a Gnutella-like P2P community, an ontology-based P2P approach for facilitating heterogeneous medical information sharing between healthcare providers is proposed in [5]. Also, an approach that loosely couples multi-agent and peer-to-peer technologies for facilitating patient and clinical data sharing between healthcare providers have been discussed in [8]. Although there is a merit for easy accessibility of individual’s health information by qualified and authorized individuals, this could vastly increase the potential for abuse of that information. In general, health and medical information are highly confidential and sensitive. Therefore, privacy, confidentiality and security are essential components of the health record and of fostering trust between healthcare consumers and providers. However, increasing automation of the electronic medical record presents, among others, significant patient privacy and confidentiality issues that could expose the healthcare providers and users to liability. Therefore, in addition to being confidential, such systems must maintain a certain level of safety and security. While it is important that a way to allow authorized individuals have access to the necessary information to do their job the best way, we must also examine potential security threats and how to prevent and protect the confidential information and privacy-sensitive data.

To enable resource sharing between multiple heterogeneous healthcare enterprises, an authorization policy management framework is required. To solve these problems in a loose-coupling way, we propose a dynamic, distributed and heterogeneous authorization policy management framework for sharing medical information among autonomous and disparate healthcare information systems. An approach for mediating
between security and privacy policies is also described.

The rest of the paper is organized as follows: In Section 2, we outline a number of security issues that are characteristic of P2P data sharing systems with emphases on healthcare information systems. The proposed framework is then presented in Section 3. The conclusion and future work is discussed in Section 4.

2 Privacy and Security Issues

P2P systems allow any user to share resources while maintaining the autonomy and independence from the centralized servers. Thus they usually have better availability and fault tolerance than the traditional client-server based systems. However, P2P systems are prone to potentially serious privacy and security risks that may come from their use or misuse. P2P systems make it possible, and in some cases too easy, for people to share personal data (i.e., inadvertent sharing of sensitive information); (2) Data trading introduces risks similar to those faced by Internet users generally (i.e., Security concerns); and (3) File traders who violate copyright laws face obvious legal risks (i.e., Legal risks). Although security is a paramount concern in any networked systems, the need for privacy, confidentiality and security protection takes on new meanings in healthcare information systems. Also, healthcare information systems operate within a strict regulatory framework that is enforced to ensure the protection of personal data against processing and outlines conditions and rules in which processing is allowed. Therefore, middleware systems that facilitate clinical data sharing must abide by the strictest conditions of confidentiality that not only meet but also often exceed approved privacy standards and regulations. Therefore, sharing highly confidential information and privacy-sensitive data in P2P fashion is extremely challenging. In P2P environment, mechanisms by which a patient's right to confidentiality and privacy is maintained and respected is an important component of the healthcare information systems.

Securely transferring data between different parts of a healthcare system is one of the biggest single problems in healthcare information systems. Securing P2P data sharing applications is challenging due to their open and autonomous nature. Compared to a client-server system in which servers can be relied upon or trusted to always follow protocols, peers in a P2P system may provide no such guarantee. The environment in which a peer must function is a hostile one in which any peer is welcome to join the network; these peers cannot necessarily be trusted to route queries or responses correctly, store documents when asked to, or serve documents when requested.

Unless proper protection is in place, the possibility of introducing and spreading a Trojan horse or virus becomes as easy as sending an e-mail. It may be reasonable to trust a single centralized service, but obviously unwise to trust any multitude of anonymous resource-providers in the whole P2P network. Therefore, it is important to identify the authenticity of the resources offered by other peers. For example, P2P systems can be exploited to distribute malicious software, such as viruses and Trojan horses, even bypassing the protections of firewalls. Therefore, a malicious peer can easily deceive other peers, and hackers as well as worm virus can use spoofed identity to damage the whole P2P system.

Even if not taking the security threats into count, due to the lack of assured authenticity of the resources to be exchanged, the overall performance of P2P systems degrades severely for much time and bandwidth is wasted in downloading unwanted files. The main difference between this case and music sharing is that the reliability of the information to be exchanged could be critical, and cannot always be judged simply by reading it. Moreover, some people, like representative of drug companies, may have vested interest to provide false treatment advice to promote their drug. Trust is essential if the health
information collected is to serve as a complete and accurate foundation not only for patient health information but also for clinical care, research, payment, and healthcare policymaking.

3 Policy Framework

Architecture

In this section, we propose a policy for governing medical data sharing in decentralized P2P environments. Generally speaking, the purpose of such a policy is (a) to provide for effective coordination between members of the community, and (b) to ensure the security of community members, and of the information they share with each other. To achieve these purposes, the policy might impose constraints on both the membership of the community and on the behavior of its members when they are interacting with each other—all these in a highly application dependent manner. We now describe the main component of the system shown in Fig. 1 in more detail. Due to space limitation, we will elaborate on the exact mechanism for maintaining this reputation later in the extended version of the paper.

3.1 System Architecture

Fig. 1 shows a network of peer database systems of family doctors, hospitals, medical laboratories, and pharmacists that are willing to share patient information about diagnosis, treatments and medications. We refer to this infrastructure as healthcare provider community (HPC). Each healthcare provider operates autonomously within distinct domain and has different healthcare information systems to support local patient care. The connection between peers must be secure, which requires at least the capability of each peer to identify the other participant in the connection. Secondly, the sensitive data managed or exchanged via applications must be protected. The trust and security properties are established by using various techniques such as authentication of peers communicating with each other or with any other entity involved in the P2P application, authorization of certain entities to do some action or access some information, encryption of sensitive information flowing between peers over an unsecured network.

3.2 Certification Process

Sophisticated security mechanisms rely on the use of credentials (also called certificates, tokens, or assertions). In order to properly utilize credentials, mechanisms must be in place to issue, validate, and revoke them. In a service-oriented setting, these mechanisms are provided by specialized services.

There are several certification authorities (e.g., CA_i) in the system providing credentials (also known as certificate, tokens, or assertions) to the peers for the purpose of correctly authenticating themselves with. We assume that the CAs also store detailed information on each peer in the community including the address, phone number business
registration number. This information could be used, if need be, to establish the identity of the caller (such as by calling back to a number in the CAs), and to always notify the patient. The CAs also ensures proper utilization of the credentials by regularly validating and revoking credentials them.

The healthcare providers (i.e., peer) join HPC community with the objectives to be able to share and have access to remote data obtained from other physicians’ database, pharmacies, and drug reference databases to offer the best possible care for their patients. Membership to the HPC data sharing community is controlled and certified by CA1 certification authority. In our system, membership to the data sharing community is controlled and certified by CA1 certification authority while the second certification authority (CA2) represents the medical board and responsible for certifying medical doctors in good standing. We assume that these CAs ensure that there are no ways for peers to request certificates for other people or multiple certificates for the same peer.

Once a submitted certificate is verified, its validity is to be monitored as follows: certificates issued by CA1 are to be checked for validity every day, while certificates issued by CA2 should be checked every 30 days. This difference in frequencies reflects different expectation about the stability of the certificates issued by the two authorities.

### 3.3 Membership Maintenance

One way to enhance the trustworthiness of the information exchanged is to limit the membership in the community to trustworthy people, however this may be defined. While the set of criteria for admission and removal can be arbitrarily complex, the sensitive nature of the information to be shared dictates three fundamental concerns for HPC community: (i) members should be doctors, (ii) members should have some level of trust in each other, and (iii) if a member misbehaves, it must be possible to revoke peers membership.

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

We attempt to discourage inappropriate use of the system, by punishing users who misbehave as well as by placing limit on the number of queries individual peer will submit per day. A regular member is removed from this community if three different members vote for the peers’ removal. We regulate the rate of queries in such a way that every query has a cost, which must be paid for from the budget of the peer presenting it.

### 3.4 Reputation Management

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

We use a simple yet general reputation system to help members in assessing the reliability of information provided by each others. Each peer must maintain a
reputation value that summarizes other members’ feedback on the quality of their responses to posted queries. Further, this reputation must be presented along with every response to a query. Each member of a HPC has a numeric reputation in the range of $MIN$ to $MAX$, which is attached to every query-hit message so that the querier can decide whether to trust the answer or not. In the framework, larger numeric reputation values imply greater trust.

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

3.5 Policy Management

Typically, a healthcare provider implements the legislation by authoring a security policy that mandates working practices and security technology requirements. A security policy is a set of rules for authorization, access control, and trust in a certain domain; it can also contain information about some users’ roles and the abilities associated with those roles. For example, healthcare providers could define privacy policies that state which healthcare professionals are able to access specific medical data. Fig. 2 shows the components of security policy in the proposed framework.

The physician-patient relationship is confidential and typically, healthcare providers have different security policies that state a diverse set of security requirements and capabilities. Also, in practice, peers may have different security requirements and capabilities. Similarly, authentication and authorization mechanisms for healthcare professions may also be different. To address this issue, we use security agents (i.e., security brokers) as depicted in Fig. 2. Each domain has security agents that enforce the policy. Security agents’ reason about these signed assertions and the appropriate security policies to provide access control to services in their domain.

In addition to specifying security policies, healthcare providers need to restrict access to medical data to only authorized healthcare professionals. In addition to specifying security policies, healthcare providers need to restrict access to medical data to only authorized healthcare professionals. The commonly used approach, role-based authorization, is insufficient to model access restrictions in all but simple healthcare scenarios. We use workflow context access control, where authorization decisions are based on the healthcare professional and the context in which they are accessing data.

4 Conclusion and Future Directions

Although there is a merit for using P2P to ease accessibility of individual’s health information by qualified and authorized individuals, this could vastly increase the potential for abuse of that information. To address this problem, we proposed a dynamic, distributed and heterogeneous policy management framework for sharing medical information among autonomous and disparate healthcare information systems in P2P environments.

We are currently in a process of implementing and studying its performance. We are also looking into an approach that allows a healthcare provider to develop role ontology that defines the clinical occupations for healthcare professionals within their organization. These roles are then attached to concepts.
in the clinical concept ontology. As medical data is described using the clinical concepts, authorization is enforced based on the role of the healthcare professional and the clinical concept being accessed. We are also exploring WS-SecurityPolicy [12] based approaches.

3 References
2. Gruber, T., A Translation Approach to Portable Ontology Specifications, Knowledge Acquisition, 5(2), 199-220, 1993