

# Privacy Based Information Brokering for Cooperative Distributed e-Health Systems

AbdulMusalib Masaud-Wahaishi

College of Information Technology, United Arab Emirates University, Al Ain, UAEU  
Email: amasaud@uaeu.ac.ae

Hamada Ghenniwa

University of Western Ontario, London, Canada  
Email: hghenniwa@eng.uwo.ca

**Abstract**— Healthcare services and systems become very complex and encompass a vast number of entities (software systems, doctors, patients, etc.) that are characterized by shared, distributed and heterogeneous information sources with varieties of clinical and medical settings. A major challenge of brokering in open environments is to support privacy. Within the context of brokering, we model privacy in terms of the entities' ability to hide or reveal information related to its identities, requests, and/or capabilities. In this work we present a privacy-based multi-agent information brokering architecture that supports different privacy degrees. Unlike traditional approaches, the brokering is viewed as a set of services in which the brokering role is further classified into several sub-roles each with a specific architecture and interaction protocol that is appropriate to support a required privacy degree. The proposed architecture has been implemented using coordinated intelligent, rational agent (CIR-agent) model for cooperative distributed information e-health prototype using (JADE), FIPA-complaint platform.

**Index Terms**— Agent Technology, Brokering, Cooperative Distributed Systems, Privacy

## I. INTRODUCTION

Healthcare systems become very complex and are characterized by shared, distributed and heterogeneous information sources with varieties of clinical and medical settings. The new vision of building intelligent systems and infrastructure to enable self management of health-oriented concern at homes by the individuals and their families have attracted many architects, developers and researchers to adopt and invent new alternatives that can improve the healthcare sector.

Technologies such as wireless medical sensors, digital home technologies, cognitive assistance, advanced robotics for care support, context aware applications and services, and intelligent proactive computing technologies are some of the enabling tools to fulfill this vision.

e-health<sup>1</sup> systems is to be viewed as an augmented environment that has the ability to consolidate embedded computers, information resources, distributed systems, and multi-modal sensors to offer people unprecedented levels of access to information and assistance. This diversity will make the most of the information and communication technology to provide health services, expertise guidelines and medical relevant-information and hence will radically transform the way health-related services are conceived and delivered.

These proactive health systems have the potential to improve healthcare access and management which significantly lower the associated incurred costs through efficient controlled information flow between various physicians, patients and medical personnel, yet threaten to facilitate data sharing beyond any privacy concerns.

The privacy concerns over inappropriate use of the information make it hard to successfully exploit and achieve the gains from sharing such information. Online identity theft, fraud, and privacy concerns are on the rise. And increasingly sophisticated practices such as "phishing" are invented. In response, a multitude of systems designed to protect privacy have been devised.

The root of these problems is that the e-health systems were designed without taking into consideration the privacy protection of the vast and numerous participants in such environments. Consequently, users and individuals become very reluctant and unwilling to disseminate or publicize information that might lead to adverse outcomes.

The high degree of collaborative work needed in e-health environments implies that developers and researchers should think of other venues that can manage and automate this collaboration efficiently. A cooperative distributed systems (CDS) approach is an ideal and appropriate design paradigm which allows the various e-health entities to exercise some degree of authority in sharing their information and capabilities.

<sup>1</sup> e-health refers to the electronic delivery of healthcare service to users

This paper presents an agent privacy-based information brokering architecture that supports the privacy of various users in cooperative e-health systems. Here, privacy is treated in terms of three attributes: entity's identity, capability and goals. In this architecture, the e-health entities are viewed in terms of three main roles: a service provider, a service requester and a brokering entity.

## II. RELATED WORK

Privacy concerns are key barriers to the growth of health based systems. Legislation to protect personal medical information were proposed and put in effect to help building a mutual confidence between various participants in the healthcare domain. A survey [19] of physicians found that concerns about privacy can compromise quality care. For example, 87% reported that a patient had asked that information be kept out of his/her record, 78% reported withholding information from a record at a patient's request due to privacy concerns, 19% admitted to lying to protect a patient's privacy.

Several approaches were proposed for integration of distributed information sources in healthcare [20]. In one approach [5], the focus was on providing management assistance to different teams across several hospitals by coordinating their access to distributed information. The brokering architecture is centralized around a mediator agent, which allocates the appropriate medical team to an available operating theatre in which the transplant operation may be performed.

Other approaches attempt to provide agent-based medical appointments scheduling [1][4], in these approaches the architecture provides matchmaking mechanisms for the selection of appropriate recipient candidates whenever organs become available through a matchmaking agent that access a domain specific ontology.

Many approaches proposed the use of privacy policies along with physical access means (such as smartcards), in which the access of private information is granted through the presence of another trusted authority that mediate between information requesters and information providers [18][8].

TelemediaCare, focuses on developing an agent-based framework to support distant care and patients' assistance, the architecture composes two types of agents, namely stationary "static" and mobile agents [6][16].

However, there are few attempts that address privacy as a design aspect. For example, the work in [15] has proposed agent-based mediation approach, in which privacy was treated as a base for classifying various mediation architectures; only for the initial state of the system. In another approach [6], agents' capabilities and preferences are assumed to be common knowledge, which might violate

the privacy requirements of the participants. Various programs and initiatives have proposed set of guidelines for secure collection, transmission and storage of patients' data. Some of these programs include: (IPSE) [11] and (HIPAA) [10].

Another approach [17] provides access control mechanisms and tools for protecting requesters' personal privacy [17][12][7]. Service requesters joining an environment are prompted for the required privacy policies of each service in the environment. A dedicated requester's proxy checks these policies against the user's predefined privacy preferences and accordingly decides upon using or declining the services.

Another approach proposes the usage of MPEG-21 standard as a mechanism to access control to medical [19][7]. However, the approach does not provide an architecture or guidelines for utilizing the standards and hence the author considers it as open future research issue.

Gialelis et al [20] propose a pervasive healthcare architecture into which a wearable health monitoring system is integrated into a broad tele-medical infrastructure allowing high – risk cardiovascular patients to monitor critical changes and get experts feedback.

However, the proposed architecture does not address any privacy considerations, which may lead to serious breaches. Yet, these guidelines need the adoption of new technology for e-health requester /provider interaction.

## III. A COOPERATIVE AGENT-BASED E-HEALTH INFORMATION BROKERING

E-health users and service providers are concerned about their personal privacy from different perspectives. For example, they may wish to protect their identities from being used, or decide by whom it will be revealed, and for what purposes, or retain the choice about whether or not to reveal their personal interests or capabilities. The dynamic nature of the e-health entities participating in different brokering scenarios requires that they be able to change their configuration according to their roles.

The challenge here is how to adopt a technology that provides means and mechanisms by which these entities would be able to interact with each other and determine an appropriate privacy degree. Such interaction is characterized by the non-determinism aspect and the dynamic nature of the environment where these entities exist and operate. These requirements could not be met using traditional ways of manually configuring software.

### A. *The Privacy Model*

Using privacy as a desirable feature, the information brokering architecture composes several roles; each role deals with specific privacy requirements as needed by any

participant in the environment. The concern of the brokering model is to view privacy in terms of three attributes: the entity's identities (*Id*), capabilities (*Cap*) and requests (*Req*). The brokering model permits various e-health service requesters and service providers to participate with different roles and hence be capable of automating their privacy. A requester or a provider is able to choose whether to reveal or hide a particular privacy attribute.

Both service requester and service provider are recognized as roles of any participant's agent in the domain environment.

A service requester is an entity with goals that are either beyond its own capability; or they might be achieved by other entities to maximize its benefits (for example, goals can be achieved with a lower cost or at higher quality).

A service provider is an entity that is able to provide some services in the domain. The following tables (1 and 2) summarize the different cases that can be played by the brokering layer categorized by the required privacy degrees of both the requester and the provider entities.

TABLE 1:  
BROKERING ROLES AND INTERACTION PROTOCOLS WITH REQUESTERS

Case	Requester's Privacy Attributes		Brokering Interaction
	Req	Id	
1	Revealed	Revealed	<ul style="list-style-type: none"> <li>• Receive service request</li> <li>• Forwards request to broker-provider side</li> <li>• Deliver result to requester</li> </ul>
2	Hidden	Revealed	<ul style="list-style-type: none"> <li>• Retrieve service request posted by a requester</li> <li>• Forwards request to broker-provider side</li> <li>• Store result to be retrieved by requester</li> </ul>
3	Revealed	Hidden	<ul style="list-style-type: none"> <li>• Post service request to service repository</li> <li>• Requester to search repository and request service</li> <li>• Retrieve a service request that was stored by a requester</li> <li>• Forwards request to broker-provider side</li> <li>• Store result to be retrieved by requester</li> </ul>
4	Hidden	Hidden	<ul style="list-style-type: none"> <li>• Requester to store service request</li> <li>• Retrieve service request that was stored by a requester</li> <li>• Forwards request to broker-provider side</li> <li>• Store result to be retrieved by requester</li> </ul>

TABLE 2:  
BROKERING ROLES AND INTERACTION PROTOCOLS WITH PROVIDERS

Case	Provider's Privacy Attributes		Brokering Interaction
	Id	Cap	
1	Revealed	Revealed	<ul style="list-style-type: none"> <li>• Assign capable provider</li> <li>• Forwards request</li> <li>• Get service's result</li> <li>• Broker to deliver result</li> </ul>
2	Hidden	Revealed	<ul style="list-style-type: none"> <li>• Post request to service repository</li> <li>• Providers to access repository</li> <li>• Providers to store result</li> <li>• Broker to retrieve stored result</li> </ul>
3	Revealed	Hidden	<ul style="list-style-type: none"> <li>• Broker to forward service request</li> <li>• Provider to evaluate request</li> <li>• Providers to store result</li> <li>• Broker to retrieve stored result</li> </ul>
4	Hidden	Hidden	<ul style="list-style-type: none"> <li>• Providers to access repository</li> <li>• Provider to evaluate request</li> <li>• Provider to store service result</li> <li>• Broker to retrieve stored result</li> </ul>

A complete brokering session is divided into several stages, starting from Requestor-to-Brokering Layer Interaction, Brokering Layer Intra-Interaction and Brokering Layer-to-Provider Interaction. Note that in the figure, a negation on the privacy attribute variable corresponds to a hidden requirement.

*B. The Brokering Architecture*

Healthcare environments can be modeled and implemented as cooperative Distributed Systems (CDSs). Within this context, the e-health systems is viewed as a collection of autonomous units that can act independently and cooperate in providing services and synergize medical data according to mutual interests.

The dynamic nature of the e-Health entities participating in different brokering scenarios requires that they be able to change their configuration according to their roles. The challenge here is how to adopt a technology that provides means and mechanisms by which these entities would be able to interact with each other and determine an appropriate privacy degree. Clearly such interaction is characterized by the non-determinism aspect and the dynamic nature of the environment where these entities exist and operate. These requirements could not be met using traditional ways of manually configuring software.

We strongly believe that agent-orientation is an appropriate design paradigm for providing coordination services and mechanisms in such settings. Indeed, such a paradigm is essential to modeling open, distributed, and heterogeneous environments in which an agent should be able to operate as a part of a community of cooperative distributed systems environments, including human users.

Here we view agent-orientation as a metaphorical conceptualization tool at a high level of abstraction (knowledge level) that captures, supports and implements features that are useful for distributed computation in open environments. These features include cooperation, coordination, interaction, as well as intelligence, adaptability, economic and logical rationality [9]. In previous work [3][2], an agent architecture was proposed to facilitate privacy-based information brokering for various e-health cooperative distributed systems.

Service providers and requesters are modeled as domain agents. The requester agent can participate with various privacy degrees and request services from the brokering layer. A requester agent (RA) delegates the service's request(s) to the relevant brokering agent (called *Broker* henceforth) according to the interaction protocol associated with the selected privacy degree.

A domain agent playing the role of a service provider (PA) can select the appropriate privacy degree and thus participate on providing the capability that meets the needs of another domain entity.

Responsibilities are separated and defined according to the roles played and the required privacy degree. Within the layer, two sets of agents are available to service requestors and providers. The first set handles interactions with requestors while the other set support privacy degrees required by service providers. Figure 1 shows a logical view of the brokering services and the relevant entities that are involved in any brokering scenario. Note that in the figure, a specific privacy attribute variable represents that the corresponding privacy attribute is not revealed.

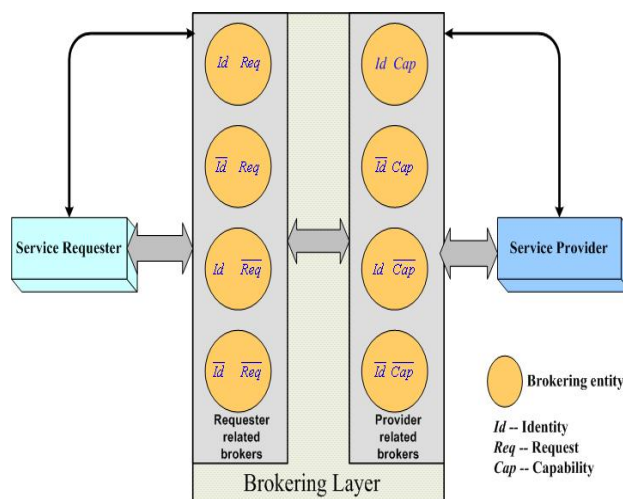


Figure 1 Logical View of the Brokering Architecture

The following subsections describe the different core behaviors of the brokering agents and illustrate the different interactions patterns between the brokering agents and other

agents in the environment categorized by the privacy concern of the Service Requester agent (RA) and the service provider agent (PA) agents<sup>2</sup>.

### C. The Requester-Brokering Layer Interaction

A requester interacts with the environment through sending and receiving messages. In some scenarios (for example, requestors hiding privacy attributes), the broker and the domain entities exhibit a proactive behavior to respond to changes in the environment. The following represent the various roles and the associated interaction patterns that can be played by the brokering in supporting requestors with different privacy degrees.

The interaction requires a set of agreed messages, rules for actions based upon reception of various messages and assumptions of the communication channels. These constraints, rules and patterns can be abstracted and formalized as interaction patterns, which are basis for successful capability-based coordination. The interaction protocols range from negotiation schemas to a simple request for a task.

The interaction protocols are viewed as patterns representing both message communication and the corresponding constraints on the content of such messages. In the proposed model, a protocol is modeled as a set of communicating processes executing concurrently. They express the constraints on the relationship between sending and receiving messages which represent the protocol mechanism. This model emphasizes the entities' collaborative behaviors.

In order to define the messages that are needed to support a specific privacy degree, we first identify the required "message-types" that can satisfy the supporting protocol and next, decide on the possible messages that can be assigned to particular role in a given interaction protocols. Note that messages can be accompanied by guard conditions to describe the constraints on the exchanged messages. To summarize the process, the process will be as follows:

1. Define the possible roles that entities can play is a specific protocol.
2. Identify how many types of messages exist in an interaction protocol. Message types are specified as constructors of the actions initiated by the entities.
3. Decide what messages a role can send, check, receive or store.
4. Next, we have to figure out the rules and constraints on these messages.

A message consists of a sender, a set of receivers, "type" of message and message "content". In all the following

<sup>2</sup> For readability purposes they will be called hereafter as a requester and a provider

interaction protocols, we focus only on message semantics, without caring about its implementation details. For readability purposes, we list the interaction protocols using the message type only.

1) *Requesters Revealing identities and goals:*

Consider the following scenario: a doctor wants to have information about the number of patients who have Hepatitis B in a specific city. The doctor needs to be assessed without exposing its identity and the pertinent request to others. The above scenarios exemplifies privacy degrees in which revealing sensitive information can lead to catastrophic discrimination outcomes, knowing the scientist's identity might lead to a biased and unfair decision; marketing trends can turn into spamming.

Therefore, it might be desirable to not be identified when accessing on-line services. Requester should be able to interact with the corresponding brokering entity to request services, receive service's results, and acknowledge the receipt of service's result. The broker protects the privacy of e-health personnel, patients or staff. It assists service requesters to achieve their goals without exposing their identities to the environment. The following describes the interaction pattern

a) *Intra-Interaction:*

As shown in Figure 2, the broker might extend the pattern to include interaction with various brokers associated with supporting other privacy degrees of service providers, consequently the broker solicits help and forwards request to all available provider-related brokers within the layer incorporating various interaction compositions.

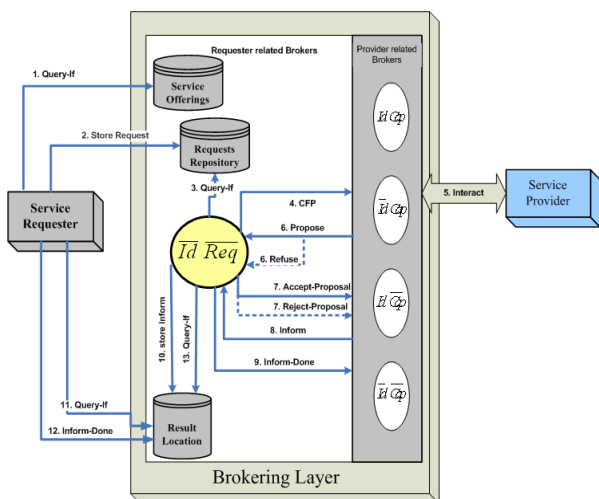


Figure 2 Interaction Pattern for Requesters Revealing Privacy Attributes

Note that for every potential composition, the provider-related brokers receive only a notification of a service

request and accordingly carry on its own interaction pattern to satisfy that request without exaggerating, overstressing or overemphasizing any incurred rights or privileges (for example, cost).

b) *Inter-Interaction:*

The typical interaction pattern for this particular privacy degree comprises that the layer engages in performing the following: (1) Accepting and interpreting service's requests from pertinent Requesters. (2) Identifying and contacting a set of available providers, forwards service requests, and controls appropriate transactions to fulfill any required service's request. (3) Receives result of a service request and delivers it back to the relevant requester.

2) *Requesters hiding identities:*

Requesters such as patients with fatal diseases may wish to access services or seek further assistance without revealing their identities. The brokering service dynamically identifies relevant service providers, and acts on behalf of those requesters to fulfill their goal(s). As shown in Figure 3, requesters will be responsible of checking the availability of the service's result, which implies that requesters should be aware of a designated result location. The interaction imposes a significant effort on the performance and efficiency.

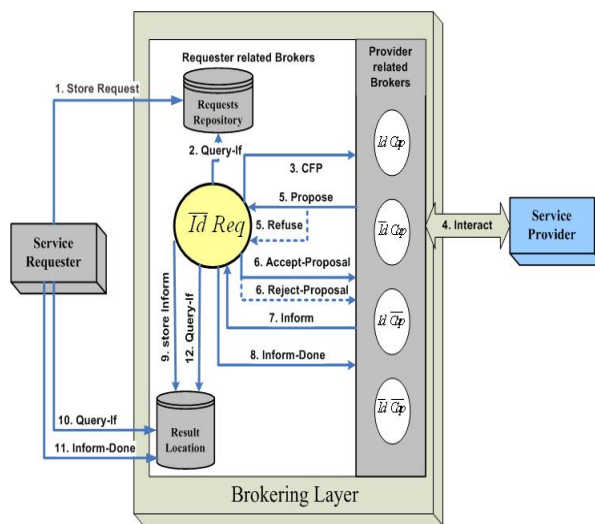


Figure 3 Interaction Pattern for Requester Hiding Identity

a) *Intra-Interaction:*

As describe in the previous case, the broker might extend its pattern to include an interaction composition with various brokers associated with supporting other privacy degrees for service providers. Upon receiving a service's result, the broker stores the result in a dedicated repository (result repository) to be retrieved by the relevant requester.

a) *Inter-Interaction:*

Requesters may wish to access services or seek further assistance without revealing their identities. The interaction pattern for this particular privacy degree is as follows: (1) Requesters are required to store services' requests in a predefined service repository along with preferred parameters (2) As shown in Figure 3, requesters are responsible of checking the availability of the service's result and hence retrieve it, this implies that requesters are able to link a service's result to their own requests.

3) *Requesters hiding goals:*

There might be certain situations where requesters prefer to hide their goals from the environment; the broker forwards every advertised service out to every registered requester with unknown preferences or interests. For example, clinicians might benefit from variety of service advertisements regarding new medications, tools, medical equipments and health related notifications. Those clinicians will be able to check a service's repository for further information or to browse other service offerings that have been previously posted and accordingly determine an appropriate and interested service as shown in Figure 4.

a) *Intra-Interaction:*

Provider-related brokers representing providers with known capabilities will have the possibility to advertise existing service offerings to the broker. It is to be noted that whenever a requester decides on a particular service offering, the inter-interaction is not restricted only to contacting those who had offered such services, but might extend to all available provider-related brokers supporting other privacy degrees. For example, the same advertised service offering might be achieved by other providers in the environment who had the interest of hiding their own capabilities.

b) *Inter-Interaction:*

As shown in Figure 4, once a requester selects a particular service advertisement and forwards that request to the broker, the former determines the most suitable service provider that fulfills that request. Upon achieving the requestor goal, the broker delivers back the service's result to the requestor.

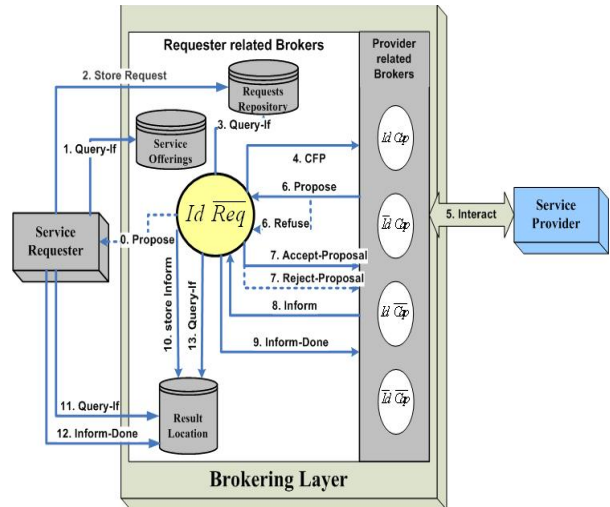


Figure 4 Interaction Pattern for Requestor Hiding Goals

4) *Requesters hiding identities and goals*

In some cases, requesters desire to hide their identities and requests from the entire environment. For example, patients with narcotic-related problems (such as drug or alcohol addiction) can seek services that provide information about rehabilitation centers, specialized psychiatrists, or programs that will help overcoming a particular critical situation without revealing either their identities nor the desired information.

Requesters would have the possibility to hide their identities and goals from the entire environment; as shown in Figure 5, they have the option either to post their wants to the layer's service repository directly, or might check for any services that would be of an interest.

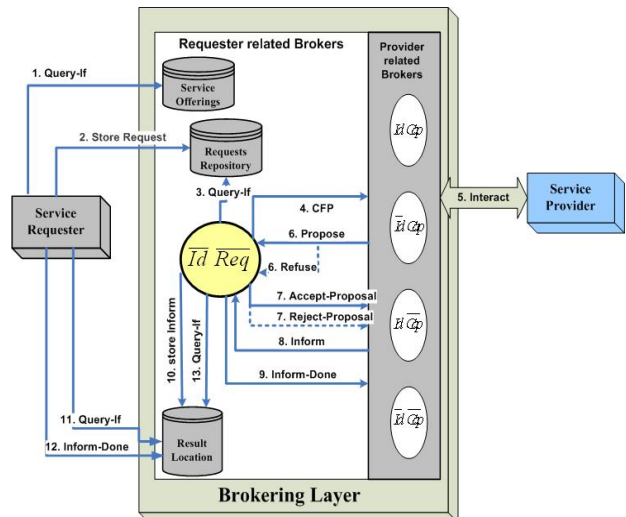


Figure 5 Interaction Pattern for Requestor Hiding Privacy Attributes

a) *Inter-Interaction:*

Requesters will have the option to either post their wants to a service repository directly, or might check for any service offerings that would be of an interest. In both cases, requestors will be permitted to store their service requests and retrieve services' results. Note that, for this degree of privacy, it is the requester's responsibility to check for the availability of the service's result and hence retrieve it.

D. *The Provider-Brokering Layer Interaction*

The interaction patterns allow providers to securely automate their privacy and advertise capabilities; define conditions and constraints that govern the provision of these capabilities. Providers' capabilities are often described in terms of two main aspects, Functional and non-functional properties. The functional properties capture the intended behavior of the service and define the input and output parameters.

The input parameters specify the required information that is needed prior to any service provision, while the output parameters specify the result of the service execution (for example, a service provider with information gathering capabilities generate outputs in electronic PDF file).

The non-functional properties exhibit the constraints over the functionality of a service and specify additional information about the service capabilities, such as availability, service quality, cost, payment, security, trust and ownership.

However, describing the providers' capabilities is beyond the scope of the work presented here. It is assumed that there are appropriate services and tools (for example, capability description languages) by which providers are able to describe the inherent capabilities.

The following interaction patterns depict the different brokering scenarios categorized by the privacy concerns of service providers. In all the interaction patterns, it is assumed that the Brokers are able to interpret services' capabilities, match and locate providers who are capable of fulfilling a particular service request.

1) *Providers revealing identities and capabilities*

In many e-health applications, the primary concern is to simplify the interaction with users and institutions. Many countries have established an on-line presence. In most cases, governments need to make decisions related to national security-threatening issues that might involve citizens, institutions and organizations.

However, making such decisions might require the collaboration of other parties (for example, intelligence-related services) who need to be protected anonymously from perspectives associated to their identities and capabilities. Providers with this degree of privacy will have the ability to register their presence along with the capability of the service they offer.

Although, providers with this privacy degree are required to reveal their privacy attributes to the relevant broker, the protocol suppress any other entity from knowing the provider's attributes.

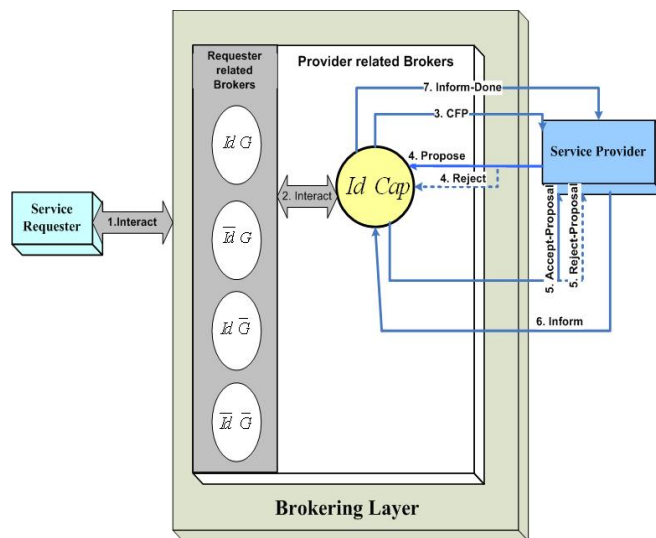


Figure 6 Interaction Pattern for Provider Revealing Privacy Attributes

a) *Intra-Interaction:*

The interaction between the broker with other requestor-related brokers are accomplished through sending and receiving messages related to service proposals, service offerings, and services results.

b) *Inter-Interaction:*

A service provider registers itself with the brokering service, along with the description of its service capabilities which is stored as an advertisement in a repository maintained by the broker. For every request, the broker matches providers who might fulfill that request.

2) *Providers hiding identities*

E-health providers can have the option to hide their identities from the environment and advertise their service offerings to the relevant brokering agent. Service requests will be posted to a dedicated repository for which providers will have the possibility to browse such requests and selects whichever of an interest.

a) *Intra-Interaction:*

The broker's task include: (1) receiving service requests; (2) determine whether these request are within the provider capabilities ; (3) store service requests to be browsed by authorized registered providers (providers hiding identities) and (4) retrieve and delivers back service result.

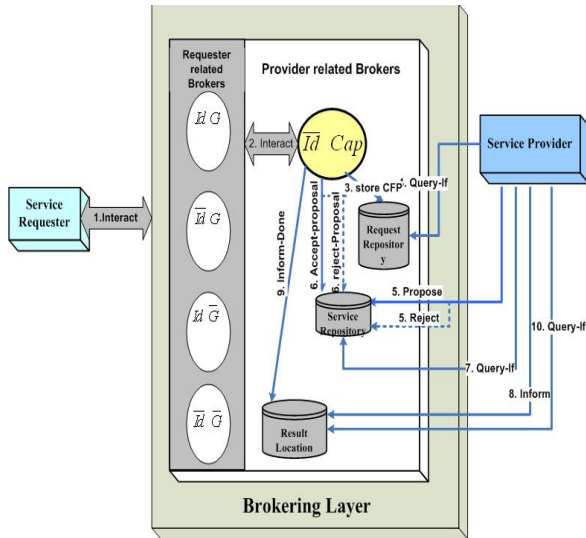


Figure 7 Interaction Pattern for Provider Hiding Identity

b) *Inter-Interaction:*

Upon assigning and delegating a service request to a provider with this degree of privacy, it is the provider's responsibility to store pertinent service result to be retrieved by the broker and thus delivered to the proper destination.

3) *Providers hiding capabilities*

After receiving a request, the brokering interaction protocol exemplifies the farming out of all received service requests to every registered provider with unknown capability. Under the assumption of an open dynamic environment, providers would be deluged by a variety of service requests, which significantly impact performance and efficiency. Figure 8 shows the interaction pattern.

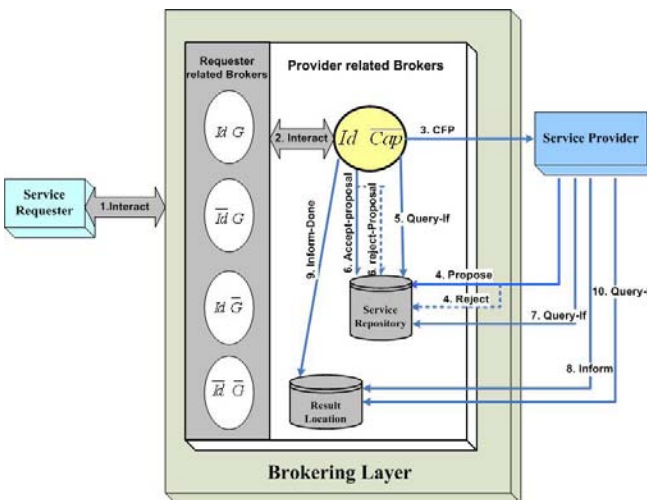


Figure 8 Interaction Pattern for Provider Hiding Capability

a) *Intra-Interaction:*

The broker interacts with other entities in the layer to engage in receiving and sending messages related to service requests and offerings. The broker's task include: (1) receiving service requests from requestor-related brokers; (2) receive service proposals; (3) and receives delivers back service result.

b) *Inter-Interaction:*

After receiving a service request, the broker sends out requests in the form of broadcasting to every registered provider with unknown capabilities. Figure 8 shows the interaction pattern. Once a provider selects a particular service request, it forwards a service proposal to the broker who controls the remaining transaction according the appropriate negotiation mechanisms similar to what has been described in the former patterns.

4) *Providers hiding identities and capabilities*

Providers will have the ability to browse a special repository and consequently determine the relevant requests that might be of an interest and within their capabilities. As shown in

Figure 9, the broker responds back with the service's result (a result location within the layer has to be identified to the provider upon registration within the brokering layer).

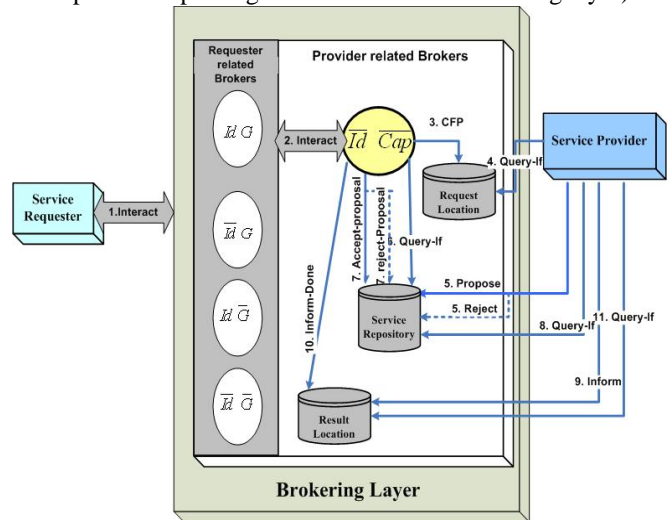


Figure 9 Interaction Pattern for Provider Hiding Privacy Attributes

a) *Intra-Interaction:*

The broker inter-Interaction comprise the following: (1) receiving service requests from requestor-related brokers; (2) store service requests (3) access and evaluate service proposals; (3) retrieve and delivers back service result.

b) *Inter-Interaction:*

In this protocol, the brokering functionality is mainly

seen as a directory service, in which the broker maintains a repository of service's requests along with any required preferences. Providers will have the ability to browse this repository to determine applicable relevant requests that might be fulfilled. As shown in Figure 8, providers with this degree of privacy have to take in consideration linking the result of the service to the request.

IV. IMPLEMENTATIONS

For page limitation, we describe the implementation of one pattern (a requester hiding identities and goals) and three providers; one is revealing privacy attributes, the second is hiding its identity while third is hiding its own privacy attributes (identities and capabilities). Consider an online three information providers, *VirtualMedInfo Inc.*, *E-VirtualDiagnosis Inc.*, and *FutureDocAssistant Inc.*<sup>3</sup> each of them provide medical information, healthcare guidelines and clinical diagnosis in various formats (online delivery, hard copies or access to online medical repositories).

*E-VirtualMedInfo* registered while revealing it privacy attributes, *E-VirtualDiagnosis* comprise diagnosis capabilities jointly derived by retired medical doctors and had selected hiding the its identity whereas *FutureDocAssistant*, (a company that provides various online samples of medical exams and virtual evaluation assessments) has decided to hide both the identity and capabilities. Alice, a fourth year medical student, is conducting a research on the most top fatal diseases in Canada, the mortality death rates of each and the possible diagnosis and prevention procedures that would help a trainee-student in examining and diagnosing patients with such diseases.

Deciding to hide her identity, Alice anonymously requests the relevant information by posting its own request in special repository dedicated to such privacy degree.

Alice's assigned broker interacts with other available brokers within the layer which are associated with supporting other privacy degrees of service providers (including the three mentioned companies) and consequently (acts as a manager) issues and issues a call-for-proposals (CFP) to those brokers (act as potential contractors) informing them of the Alice's request specifications (note that Alice's identity is anonymous to each participant including its own supporting Broker).

Each broker working on behalf of each company contacts the registered company's agent and sends the request. Note that for the *FutureDocAssistant* company, the request is dispatched in special dedicate storing repository allowing its own agent to browse this repository and retrieve the request (if interested).

Every company (through its representing agent) determines the evaluation parameters (such as information quality, expiration time, and cost) and accordingly submits

a bid along with the offer parameters (such as quality, cost, availability...etc.). The *VirtualMedInfo* and *E-VirtualDiagnosis* agents send the bids directly to their assigned broker, while the *FutureDocAssistant* agent stores the bid in a special repository (to be retrieved by the relevant broker).

Alice's dedicated broker receives those bids from every broker and carries on the evaluation process and accordingly determines the most bid (or bids) that fulfill Alice's request and sends an *acceptance-proposal* message to the winners and a *rejection-message* to those who did not meet the evaluation parameters.

The broker stores the result in a special repository for which Alice will be able to retrieve it without having to reveal her own identity. A web-based prototype of the proposed system has been implemented using Jade[13], and Java Web Services Development Pack (JWS DP) platform [14] to support and provide information-gathering capabilities to different participants in e-health environments.

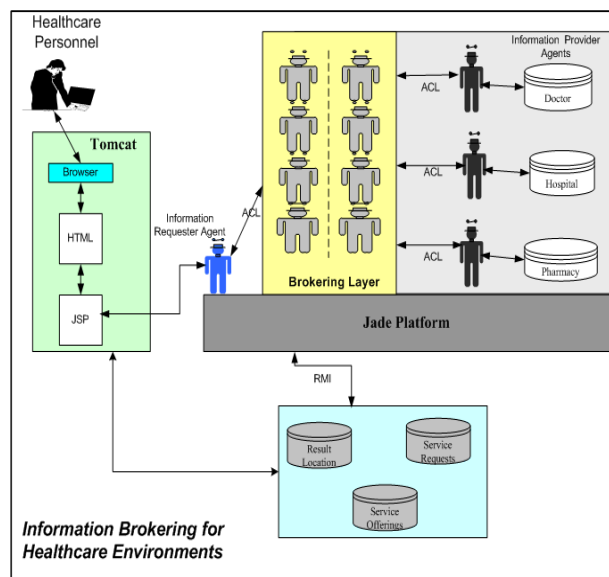


Figure 10 Privacy Based Brokering Prototype for Information Gathering in E-Health Cooperative Distributed Systems

V. CONCLUSION

The increasing demand and dependency on information in e-health organizations has brought the issues of privacy to every aspect of the e-health environments. It is expected and with no doubt that medical data such as genome information, medical records, and other critical personal information must be respected and treated with a great concern. The proposed architecture classifies the brokering role into several sub-roles based on the attributes designated to describe the desired privacy degree of both the information provider and the information requester.

Within the context of brokering, we model privacy in

<sup>3</sup> Names are fictitious

terms of the ability of CDS entities to reveal or hide information related to the identities, requests and and/or capabilities. Each privacy degree is supported by a dedicated brokering entity (agent) with a specific architecture and interaction protocol. Requesters and providers are able to conceal their privacy concerns from the whole environment including the brokering layer itself.

By utilizing the Agent-Oriented paradigm, the privacy-based information brokering is modelled at a high level of abstraction, in which the distributed environment is viewed collectively as a coherent universe of interacting and collaborative agents and consequently provides high degree of decentralization of capabilities, which is the key to system scalability and extensibility.

Within the context of brokering, we model privacy in terms of the ability of ubiquitous healthcare entities to reveal or hide its information related to the identities, requests and and/or capabilities. Each privacy degree is supported by a dedicated brokering entity (agent) with a specific architecture and interaction protocol. Requesters and providers are able to conceal their privacy concerns from the whole environment including the brokering layer itself.

Another important aspect of the model is that it treats the privacy as a design issue that has to be taken into consideration in developing e-health information brokering systems.

The feasibility of the proposed agent-based model has been demonstrated by applying it to a vital application domain (the healthcare domain) in which the increasing demand and dependency on information in healthcare organizations has brought the issues of privacy to every aspect of the healthcare environment. It is expected that medical data such as genome information, medical records, and other critical personal information must be respected and treated with caution.

Nevertheless, privacy concerns over the inappropriate use of the information make it hard to successfully exploit the advantages of sharing such information. This restricts the willingness of healthcare individuals and personnel to disseminate or publicize information that might lead to adverse outcomes.

Within this context, a healthcare environment is modeled as a cooperative distributed system, in which entities are able to exercise some degree of authority in sharing information about their identities, preferences and capabilities. T

he privacy model is very desirable in different healthcare sectors where it can efficiently govern different types of health data such as genetic, HIV, mental health and pharmacy records from being distributed or abused.

## REFERENCES

- [1] A. Aldea, B. López, A. Moreno, D. Riaño and A. Valls "A Multi-Agent Systems for Organ Transplant Coordination", *Artificial Intelligence in Medicine, Lecture Notes in Computer Science*, Springer Verlag, 413-416, 2001.
- [2] A. Masaud-Wahaishi, H. Ghenniwa and W. Shen, "Agent-Based Information Brokering For Healthcare Environments", WAC04- 5th International Symposium on Soft Computing for Industry, Seville-Spain, June 28 - July 1, 2004.
- [3] A. Masaud-Wahaishi, H. Ghenniwa, and W. Shen, "Healthcare Information Brokering: The value of Privacy" The 16th International Conference on Advanced Information Systems Engineering CAiSE04, Latvia June 2004.
- [4] A. Moreno and D. Isern, "Accessing distributed health-care services through smart agents", *the 4th IEEE Int. Workshop on Enterprise Networking and Computing in the Health Care Industry - HealthCom 2002 -France*, 2002.
- [5] A. Moreno, A. Valls, and J. Bocio, "Management of Hospital Teams for Organ Transplants Using Multi-Agent Systems", *Artificial Intelligence in Medicine, Lecture Notes in Computer Science*, Springer Verlag, 413-416, 2001.
- [6] D. Kuokka and L. Harada, "On using KQML for Matchmaking". In proc. ICMAS-95. AAAI Press, June 1995.
- [7] G. Brox, "MPEG-21 as an access control tool for the National Health Service Care Records Service", *Journal of Telemedicine and Telecare*, volume 11, pp. 23-25, (Suppl. 1), July 2005
- [8] G. Yee, L. Korba, and R. Song, "Ensuring Privacy for E-Health Service", *Proceedings of the First International Conference on Availability, Reliability and Security (ARES 2006)*. Vienna, Austria. April, 2006.
- [9] Ghenniwa, H. and Huhns, M., "Intelligent Enterprise Integration: eMarketplace Model", *Creating Knowledge Based Organizations*, J. Gupta and S. Sharma (Eds.), Idea Group Publishing, Hershey, Pennsylvania, USA, pp. 46-79, 2004.
- [10] *Health Insurance Portability and Accountability Act (HIPAA)*. Available :<http://www.intellimark-it.com/privacysecurity/hipaa.asp>
- [11] *Initiative for Privacy Standardization in Europe (IPSE)*, available: <http://www.hi-urope.info/files/2002/9963.htm>
- [12] J. Gialelis, P. Foundas, A. Kalogeras, M. Georgoudakis, A. Kinalis and S. Koubias, "Wireless Wearable Body Area Network Supporting Person Centric Health Monitoring", *Proceedings of the 7th IEEE International Workshop on Factory Communication Systems (WFCS 2008)*, May 20-23, 2008.
- [13] Java Agent Development Framework: Jade, Home Page: <http://jade.cselt.it/>
- [14] Java Web Services Developer (JWS DP); [Online]: URL:<http://java.sun.com/webservices/jwsdp/index.jsp>
- [15] K. Decker, K Sycara and M. Williamson " Middle-agents for the internet" In IJCAI97 International Joint Conference on Artificial Intelligence, Nagoya, Japan, 1997.
- [16] L. Camarinha-Matos, and H. Afsarmanesh, "Virtual Communities and Elderly Support", *Advances in Automation, Multimedia and Video Systems, and Modern Computer Science*, WSES, pp. 279-284, 2001.
- [17] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments", *UbiComp, Lecture Notes in Computer Science*, Volume 2498, pps. 237- 245, Springer, 2002.

- [18] R. Clarke, " Identification, Anonymity and Pseudonymity in Consumer Transactions : A Vital System Design and Public Policy Issue", available at <http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html>
- [19] The Association of American Physicians and Surgeons , "Doctors Lie to Protect Patient Privacy" –*Survey* , Available online : <http://www.aapsonline.org/press/nrnewpoll.htm>
- [20] V. Shankaraman, V. Amorosiadou, and B. Robinson, "Agents in Medical Informatics", in Proc. Of IASTED International Conference on Applied Informatics, Austria, 2000

**AbdulMusalib Masaud-Wahaishi** is an Assistant Professor at the United Arab Emirates University, College of Information Technology. Dr. AbdulMusalib received a B.Sc. degree (1986) in Computer Engineering from Al-Fateh University, Tripoli Libya; M. Eng. Sc. (2003) and Ph.D. (2007) degrees in Software Engineering from the University of Western Ontario , Department of Electric and Computer Engineering, London, Canada.

His research expertise includes theoretical and engineering foundations of computational intelligence with a special focus on agent-orientation, coordination and cooperation in distributed "systems" environments; Engineering design of agent-oriented, service-oriented (SO), and Grid computing to improve the "quality" of cooperative distributed systems. Application areas include enterprise integration, electronic business and Information gathering. His research has resulted in several publications in world-class conference proceedings.

Prior to joining the academia, Dr. AbdulMusalib had more than 14 years of industrial experience. Duties include technical supervision, support and design, and project management.

**Hamada H. Ghenniwa** is an Associate Professor at the University of Western Ontario, and is the head of Cooperative Distributed Systems Engineering Group.

Dr. Ghenniwa internationally renowned for his expertise in computational intelligence for coordination and cooperation in distributed "systems" environments. It includes theoretical and engineering foundation of agent-oriented, service-oriented, and Grid computing to improve the "quality" of cooperative distributed systems. Application areas include enterprise integration, electronic business, collaborative manufacturing and complex real-time systems. He published the findings of his research in more than 150 publications in world-class journals, books and conference proceedings.

Dr. Ghenniwa's research activities also include industrial R&D in collaboration with industrial partners and government institutes to develop sophisticated system architectures, tools and prototypes that range from mobile physical robots, to integration and collaborative tools, to intelligent manufacturing and business solutions. All of these activities are conducted in three specialized Labs: Distributed Intelligent Systems Lab focuses on complex real-time systems and intelligent manufacturing; Software Engineering Lab focuses on cooperative distributed systems architecture and technologies; *EK3 Innovation Lab* focuses on information technology & knowledge engineering.