Univ Access Inf Soc (2003) 2: 293–304 / Digital Object Identifier (DOI) 10.1007/s10209-002-0039-1

Long papers

Intelligent agents for the management of complexity in multimodal biometrics

F. Deravi, M.C. Fairhurst, R.M. Guest, N.J. Mavity, A.M.D. Canuto

Department of Electronics, University of Kent, Canterbury, Kent, CT2 7NT, UK; E-mail: F.Deravi@kent.ac.uk

Published online: 24 June 2003 – © Springer-Verlag 2003

Abstract. Current approaches to personal identity authentication using a single biometric technology are limited, principally because no single biometric is generally considered both sufficiently accurate and user-acceptable for universal application. Multimodal biometrics can provide a more adaptable solution to the security and convenience requirements of many applications. However, such an approach can also lead to additional complexity in the design and management of authentication systems. Additionally, complex hierarchies of security levels and interacting user/provider requirements demand that authentication systems are adaptive and flexible in configuration.

In this paper we consider the integration of multimodal biometrics using intelligent agents to address issues of complexity management. The work reported here is part of a major project designated IAMBIC (Intelligent Agents for Multimodal Biometric Identification and Control), aimed at exploring the application of the intelligent agent metaphor to the field of biometric authentication. The paper provides an introduction to a first-level architecture for such a system, and demonstrates how this architecture can provide a framework for the effective control and management of access to data and systems where issues of privacy, confidentiality and trust are of primary concern. Novel approaches to software agent design and agent implementation strategies required for this architecture are also highlighted. The paper further shows how such a structure can define a fundamental paradigm to support the realisation of "universal access" in situations where data integrity and confidentiality must be robustly and reliably protected.

Keywords: Multimodal biometrics – Intelligent software agents – Universal access

1 Introduction

Universal access to information-society technologies is a broad and multifaceted concept, and one of its dimensions is access *security.* In the design of many systems, and particularly those which impinge on the utilisation and manipulation of essentially private or very sensitive data, the way in which access is controlled, security and integrity of data guaranteed, and monitoring of system use achieved is therefore of particular importance. Thus, for many systems, and on an increasing scale, the adopted approach to the *management of security* is a vital issue in achieving an information society in which universal access is not just facilitated but *controlled* in an appropriate way. This paper focuses on this issue. In particular, the paper examines a specific approach based on the use of intelligent agents as the key to security management when the principal element in guaranteeing secure access is biometric data relating to the physiological or behavioural characteristics of an individual.

Biometric technologies are emerging as important components in regulating online information access [1]. Significant application areas exist in electronic commerce, security monitoring, database access, forensic investigation and telemedicine. Many different technologies are available for person recognition and identity authentication. Examples include measures based on information from handwriting (especially signatures), fingerprint, face, voice, retina, iris, hand geometry and vein patterns [2]. However, recognition based on any one of these modalities alone may not be sufficiently robust, or may not be acceptable by a particular user group or in a particular situation or instance.

It is clear that greater accuracy and robustness can be obtained by *combining* modalities. Sensor fusion has been shown to improve pattern-recognition accuracy and increase the robustness to pattern or classifier degradation in many applications [3–6]. The particular strategy used for the fusion of modalities influences the resulting accuracy and robustness [7]. Pattern variability often causes poor recognition accuracy, and the use of multiple information sources, exhibiting redundancy or complementarity, does not in itself result in robust pattern recognition [8, 9]. Hence, a strategy of classifier combination (or *multiple-expert* classification) must be designed appropriately. Multiple expert classification systems are now well established and have been applied in a wide variety of problem areas. The information redundancy often found across experts which are unable to generate completely independent information can be exploited to incorporate an inherent system of balance and checking into the decision making [10].

Much reported work on classifier combination has concentrated on configurations based directly on simple parallel structures, but recent work has shown the potential advantages of a more flexible hybrid structure allowing an element of re-evaluation to moderate the hard decision making [11–14]. Mismatched recognition and training conditions lead to poorer recognition accuracy than matched conditions, suggesting that robust recognition may require adaptation [15]. These techniques have had limited application to date in the area of biometric processing, but are clearly of great significance in the present context.

This paper addresses explicitly a number of important issues currently being developed and evaluated in the context of a system designated IAMBIC (Intelligent Agents for Multimodal Biometric Identification and Control). The main aim of the IAMBIC system is to provide secure access to remotely stored data using a set of biometric devices to provide authentication of identity. The system will use multiple biometric modalities to verify identity, which can be combined using a series of novel data-fusion techniques to find an optimum degree of reliability in authenticating identity. Data fusion will be modified according to the characteristics of the person attempting to gain access to the system, adapting to such features as significance, confidentiality and cost of data, capture environment and recognition success rate histories of individual biometrics.

A key novel aspect of the IAMBIC system, which constitutes the focus of this paper, is the use of *intelligent agents* to manage the complexity introduced by the use of multibiometrics for remote access. Tasks for the agent systems include handling of multiple authorisation levels, location of data across several repositories, and user interface and performance modification as required by the user or necessitated by the environment.

Figure 1 depicts the general overall structure of the IAMBIC system. A user wishing to access a particular file provides a set of live biometric samples that can be checked, using previously stored identity templates, to verify the identity of the user (User Agent Cluster). Based on the outcome of this authentication process, the system will locate the required information locally or remotely and will act on behalf of the authorised user, in collaboration and negotiation with the Server Agent, to release the requested information.

These ideas are developed in more detail in the following sections, and a first-level structure for a practical system to meet the challenge of exploiting agent-based multimodal biometric processing is presented. Section 2 describes some of the sources of complexity arising from the use of multiple biometrics in the authentication pro-

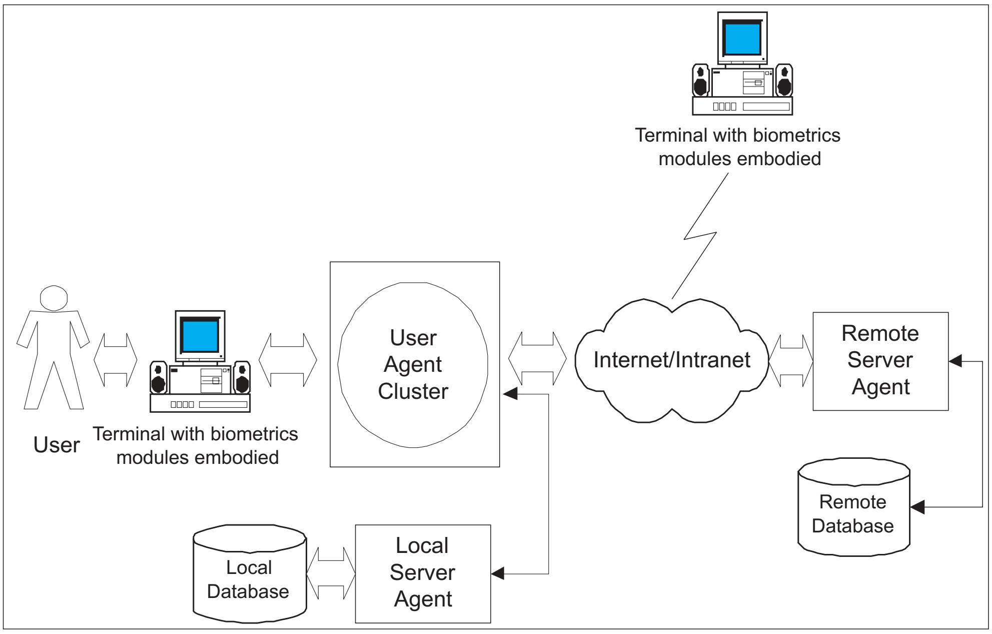


Fig. 1. The structure of the IAMBIC system

cess. Section 3 introduces the idea of biometric agents and the overall system building blocks, while Section 4 discusses the use of the system in a case study involving remote access to medical information. Section 5 explores implementation issues for the system and, finally, Section 6 outlines some conclusions.

2 Complexity in multimodal biometrics

In considering the use of multimodal biometrics in a realistic setting such as, for example, the case of a public system for regulated access to healthcare records, it is clear that there are several inter-related sources of variability which are likely to affect the required performance of the authentication system. These sources include, for example, environmental conditions, users' physiological/behavioural characteristics, users' preferences, variability of the communication channels and so on. Thus, there is a clear requirement for the system to be able to adapt to user needs and conditions and, especially, to be able to determine and maintain an acceptable balance between confidence and convenience for users through negotiations between information users and providers.

There is a wide, extensive and varied literature on multimodal identification systems and typical relevant examples can be found in [3, 8–10, 23–25]. However, in most reported work, attention is generally focused on a multimodal identification procedure based on a fixed set of biometrics. For instance, in [25], fingerprint and face modalities are used, while in [3] and [9] visual and acoustic aspects of speech are processed.

In contrast, in the IAMBIC multimodal system, a variable set of biometrics can be accommodated, according to the demands of a particular task domain or the availability of particular sensors. For example, a multimodal system should be able to deal with situations where a user may be unwilling or simply unable to provide a certain biometric, or where a preferred biometric cannot support a required degree of accuracy or general acceptability. Accordingly, the multimodal system has to adapt to user and environmental needs and use the most appropriate set of biometrics available, based on the characteristics of the current situation. The IAMBIC system encompasses just such an adaptation feature. In the prototype system considered in this paper, a pool of three possible biometric modalities (voice, face and fingerprint) is provided.

The key to the management of the system is the implementation of a system architecture that uses agent technology to realise the biometric-based access control. The next section will describe the overall agent-based control structure for the proposed system.

Once the issue of complexity of the system is mastered the advantages of biometric regulation for enabling universal access can be easily realised. By making available a selection of modalities, the system can be more flexible and adapt to users' capabilities and preferences, enabling controlled and validated access where more restricted systems using only one modality would have denied it. The deployment of a multimodal approach therefore has the potential to help overcome barriers to universal accessibility, for example in the case of users with disabilities (e.g. physical handicap), or in the case of biometric modalities not appropriate for particular sections of the population (e.g. fingerprints of children).

3 Bio-agent architectures

Intelligent autonomous *agents* [16] and *multi-agent systems* form a vibrant and rapidly expanding research field [17]. Agents can be defined as software (sub-)systems that interact with some environment, and are capable of autonomous action. In addition, they are flexible in responding to their environment, pro-active in exploiting opportunities and seeking goals, and "social" in their interactions with other agents where appropriate [16]. Agents may have other valuable properties such as adaptability or mobility.

Multi-agent systems are implemented as a group of several interacting agents, and are well suited to situations where multiple perspectives of a problem-solving situation exist. Types of interaction that may best be suited to biometric security involve co-operation, co-ordination and negotiation between agents. The needs of the information provider for establishing sufficient trust in the user may have to be balanced with the confidentiality of the user's biometric information and the ease of use of the system. A balance may need to be achieved for each service, transaction or session and may even be dynamically modified during use. Work on negotiating agents is of particular importance in the emergence of electronic commerce [18, 19] and the proliferation of Internet-based applications is a driving force for research and development of multi-agent systems. In the area of agent architectures, layered or hybrid architectures, involving reactive, deliberative and practical reasoning architectures, continue to be of considerable research interest [20], as are the development of environments and programming languages [21, 22].

The implications for privacy stemming from the increasing use of intelligent agents have received some attention in the literature recently [36]. However, we believe that the approach proposed here, which makes use of an intelligent agent framework for co-ordinating the biometric authentication process, is novel.

In order to deliver a reliable and efficient implementation of a system such as IAMBIC, five software entities have been identified as being especially important in underpinning its processing capabilities, as shown in Fig. 2.

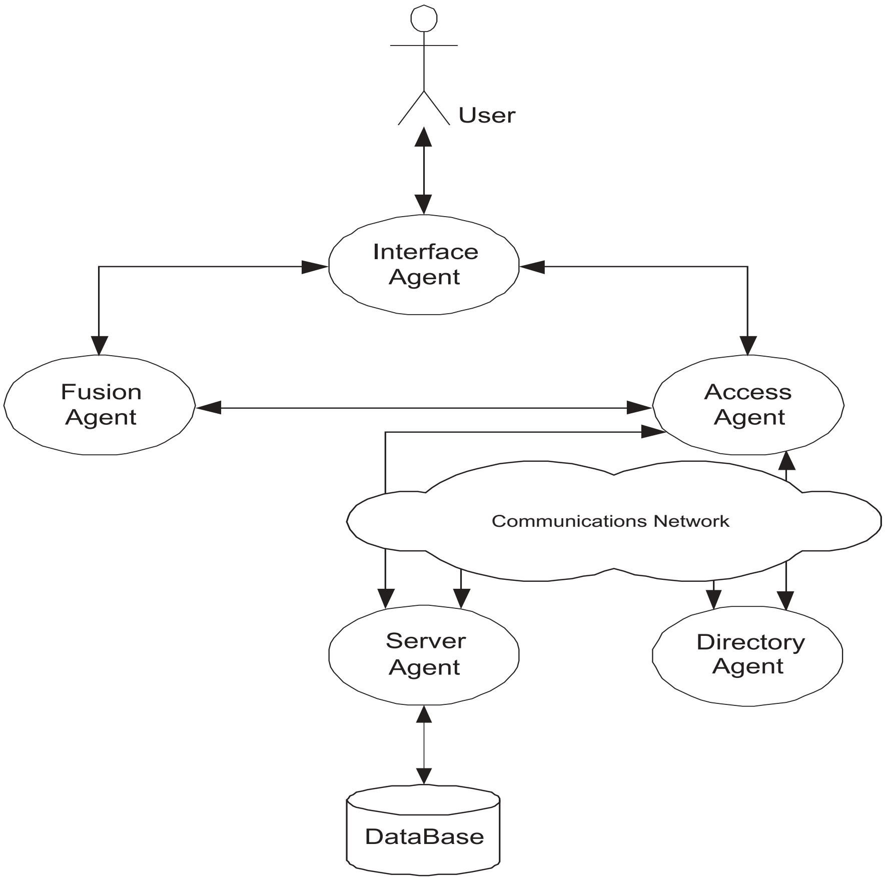


Fig. 2. The functional components of the IAMBIC system

3.1 User Agent Cluster

The User Agent Cluster is responsible for interaction with the user and aims to satisfy the user's specific requirements. In this cluster, three different agents are used, namely the Interface Agent, the Fusion Agent and the Access Agent.

3.1.1 Interface Agent

The Interface Agent is responsible for the direct interaction with the user, defining, according to the current situation, the set of biometric measurements that must be taken from the user, as well as the corresponding confidence characteristics of the related biometric recognition modules. For instance, in a noisy environment, the voice-recognition module is likely to be associated with a low confidence. In addition, this agent defines the level of interaction with the users according to the category of user and user characteristics such as computer literacy, familiarity with the system being used and so on.

The Interface Agent acts as the main interface to the user during biometric capture operations, but is also responsible for the capture of other important non-biometric information. Additional environmental data may be captured by the available sensors (e.g. for the voice modality a sample of background noise may be captured). Analysis can be performed on these samples to determine the quality of any acquired data; this can be used to help the agent to analyse any possible enrolment and/or verification failures. The results from this type of analysis can be used to provide feedback to the user to improve future performance.

3.1.2 Fusion agent

The Fusion Agent is responsible for the fusion of the biometric measures taken from the user. Its main role is to define and implement the best technique for combining several different biometric measures. The design of the Fusion Agent requires knowledge of the types of biometrics measured, as well as of their corresponding characteristics and of the levels of confidence they can generate.

The main goal of the Fusion Agent is the combination of the evidence obtained from the different biometric samples provided by the user. The Interface Agent will provide the biometric samples and environmental information obtained from the user during the verification phase. The global confidence score produced by the data fusion will be passed to the Access Agent for transmission to the Server Agent.

3.1.3 Access Agent

The Access Agent is responsible for negotiating the access to required data (e.g. medical records or other sensitive data) on behalf of the user. Essentially, this agent receives access information from the Interface Agent, locates the data, chooses the best location (in the event that the data can be found in different places), contacts the sources of the desired information and negotiates its release with the Server Agent.

Among the main goals of the Access Agent, the most important is the negotiation for the release of the requested information. As part of this negotiation, a remeasurement of the biometric samples, as well as the recalculation of the combined output, may be required under specific conditions.

3.2 Directory Agent

The Directory Agent is responsible for storing and updating all relevant information about location of services within the network. In a healthcare system, for instance, this agent may store information relating to issues such as which hospitals have beds available, which databases contain information about the patients, and other similar matters. In the search for information, this agent also suggests the best way of accessing required information (for example, in the situation where several databases contain the information specified), based on network traffic, distance and so on.

3.3 Server Agent

This agent is responsible for acting on behalf of the database in order to guarantee that the information to be released is secure. As discussed above, a negotiation process takes place between the Access and Server Agents. Essentially, this negotiation deals with the level of security of the information to be released (the higher the degree of required security associated with a piece of information, the greater is the degree of confidence needed by the system that the user requesting this information is genuine and authorised), the level of encryption of the data to be transmitted and the degree of confidence that the transaction is fraud-free.

This agent is also responsible for detecting fraudulent access to the databases and keeping a log of access to the data. For example, if some unexpected pattern of data access is attempted, a security process will be activated in order to discover whether there is any suspicion of fraudulent system penetration. In addition, a process is executed at regular intervals to analyse the record log and determine if any failure in the access of the data has been detected.

As part of the negotiation phase, the Server Agent has to ensure that the user wishing to access the information requested is authenticated and authorised, and acts on behalf of the “owner” of the stored information.

4 A case study

The use of an agent-based approach to the control of the complexity of a multimodal biometrics authentication system is best illustrated by means of an example. In this case study, we shall examine how such a system may be used in a healthcare scenario. We assume that a physician requires some confidential patient information and that this information is stored remotely. It is also assumed that, prior to the users accessing the system to request information, an enrolment process has been successfully completed to collect the required biometric templates for subsequent authorisation. The flow of information between agents is shown in Fig. 3.

- When a Server Agent is initialised it will register with the Directory Agent and provide a list of the relevant data services it can provide (Fig. 3(A)).
- Upon initiating interaction, the user will be asked to provide details about the information that is required. This might consist of, for example, a patient number and the type of file required (e.g. X-ray result, blood-test result, etc).
- The Access Agent will be supplied with the information about the requested file (Fig. 3(1)), and will attempt to register with the Directory Agent. Upon successful registration the Access Agent will encrypt the information about the requested file and transmit this to the Directory Agent (Fig. 3(2)).
- Upon receipt of this file, the Directory Agent will search its internal dynamic list of data sources and attempt to locate the optimal server for this information. The Directory Agent will periodically refresh the list it maintains to ensure that all data sources are available and online. If multiple sources of information are found, then a list is compiled and this is transmitted back to the Access Agent with a recommended server choice (Fig. 3(3)). Also, at this stage, the Directory Agent will check that the access class of the specific user provides the right to access the requested information. If this is not the case, the Access Agent will be informed that the user does not have the relevant authority to retrieve the file.
- Once the Access Agent receives the server list, it will contact the recommended server, requesting authentication at the security level associated with the file that the user wishes to access (Fig. 3(4)).
- The security level corresponding to this file will be ascertained and transmitted back to the Access Agent (Fig. 3(5)).
- At this stage, the physician may be informed that a number of biometric samples will need to be collected to ensure the release of the information, depending upon the security level of the file (Fig. 3(6)).

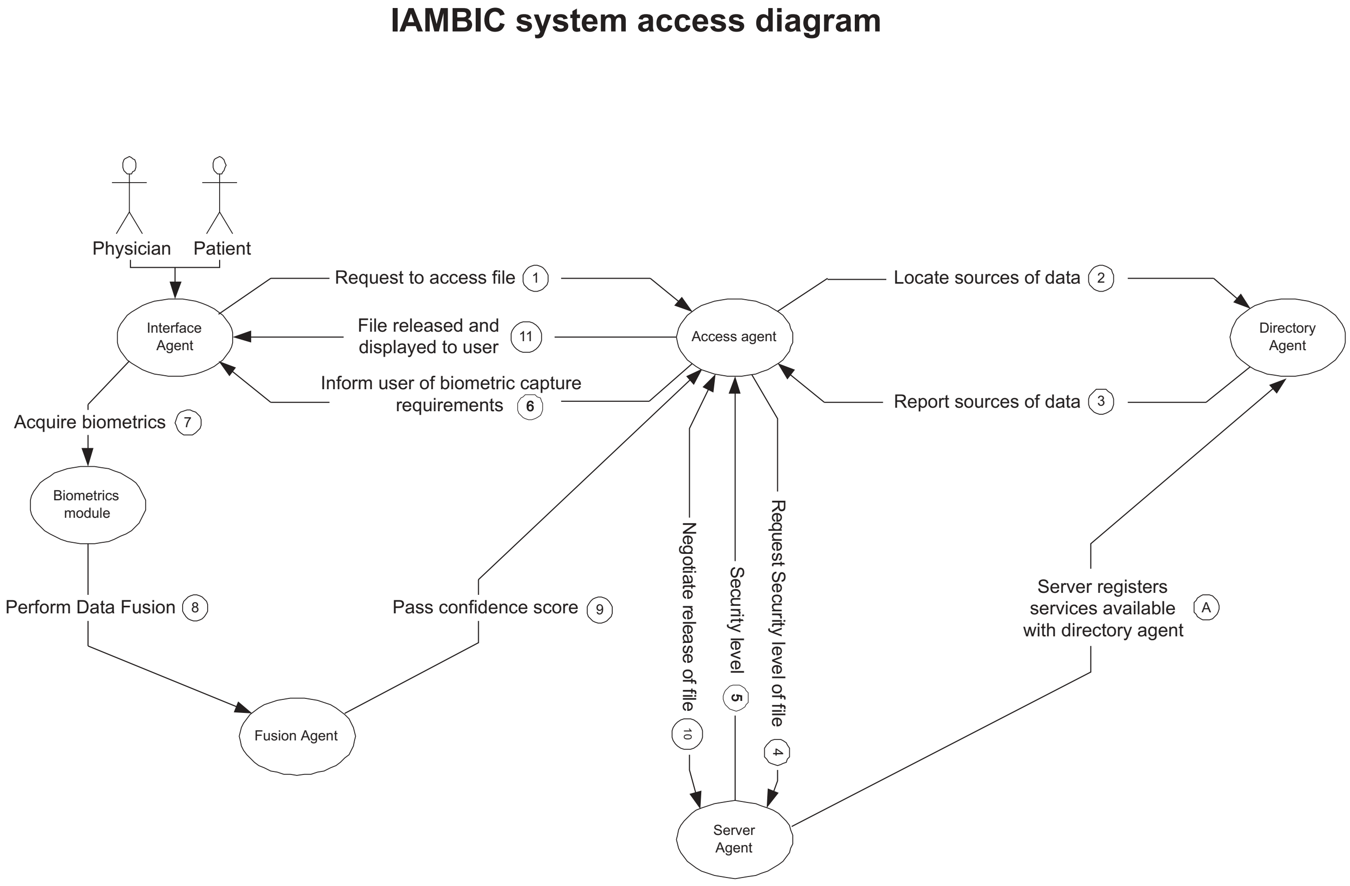


Fig. 3. Possible agent interactions in a healthcare scenario

Security levels in the system will be determined by the degree of confidentiality associated with the particular medical file. For example, a simple standard blood-test result would be likely to have a relatively low security level compared to, say, test results for a sexually transmitted disease. In the context of the present scenario, we shall assume that the physician has asked for a file with a relatively high security level.

- The Server Agent requests from the Access Agent that appropriate biometric evidence be gathered to satisfy its confidence requirements. The Interface Agent will invoke the biometric module for verification and acquire the relevant samples (Fig. 3(7)).
- Once these samples have been acquired, the information is passed to the Fusion Agent for combination (Fig. 3(8)).

In this brief case study we shall assume that the confidence score associated with the voice sample is low, due to environmental noise, to demonstrate how the flexibility of the system copes with this situation.

- The combined confidence score is then passed to the Access Agent (Fig. 3(9)), which in turn transmits this result to the Server Agent. It is now the job of the Server Agent to decide whether the score is sufficiently high to release the information. Assuming it is not, the Server Agent has several viable options:

1. Ask the Interface Agent to resample the biometrics.
2. Ask the Interface Agent to sample specific additional biometric modalities.
3. Ask the Interface Agent to invoke the Fusion Agent to re-fuse the existing data using a different fusion technique.
4. Ask the Interface Agent to request from the user appropriate non-biometric personal data that may assist in authentication.

Let us assume that, in this case, the Server Agent has decided to suggest to the user that another biometric modality needs to be acquired to complete the requested action. For example, a facial image might be considered appropriate.

- The physician is informed that there has been a problem verifying personal identity, and that another biometric is required. The biometric module is invoked and the specified modality is sampled. Once again this information is passed to the Fusion Agent for combination. The overall confidence score is then passed to the Access Agent again for transmission to the Server Agent. Assuming that this new score exceeds the confidence threshold set by the Server Agent, the server will release the file in an encrypted state. The Access Agent will decrypt this file and pass it to the Interface Agent for the physician to view.

- If the confidence score is still not sufficient to allow release of the information, the Server Agent can enter a period of extended negotiation (Fig. 3(10)) with the Access Agent as it attempts to ensure that identity is validated. This is achieved through the use of the options available to the Server Agent as detailed above. Once the Server Agent is assured of the identity of the user the system will release the requested file to the Access Agent, and the Access Agent will decrypt the file and pass it to the Interface Agent so the user can view the file. (Fig. 3(11)).

Another case illustrating the flexibility of the system is that of a patient travelling outside the geographic catchment area of the usual physician. In this case, the patient would be able to see a physician in any location where the authentication facility is available. Any confidential information required can then be authorised through the patient also providing a biometric sample in order to confirm that the physician has the authority to access the records on behalf of the patient.

An enrolment process is invoked when the user accesses the system for the first time. This procedure uses a software wizard to guide the user through the process of enrolling with each of the modalities the system employs, and generates the user templates that will be used in subsequent verification attempts. The system will automatically attempt to obtain the best-quality samples from the user during the enrolment procedure. The user will be allowed a number of attempts to enrol on each modality, but in the event that a template for a given modality cannot be generated, the system will note this and can attempt to re-enrol the user at a later stage.

5 Implementation

This section describes some of the lower-level issues surrounding the practical implementation of the software agents. In particular, the methodology used for this level of specification is introduced and the choice of messaging and implementation language is considered.

5.1 Design methodology

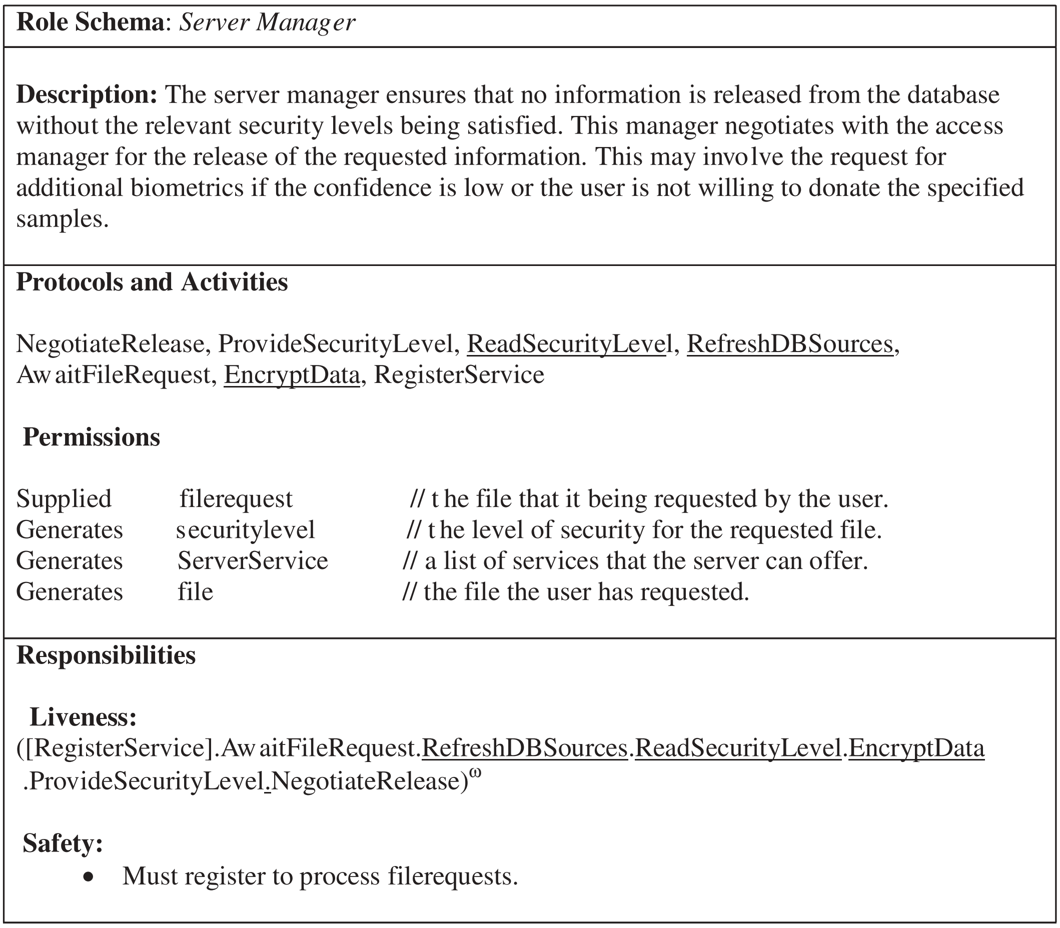
It is generally accepted that a comprehensive and rigorous methodology for developing multi-agent systems has still not been achieved [26]. However, there exist a large number of different methodologies that could be used to model the functionality required for a particular system [27–29, 31]. For the project reported in this paper, the GAIA methodology has been chosen due to its high-level nature and suitability for describing the agent society domain [27].

The GAIA process begins with finding the *roles* in the system, and subsequently modelling the *interactions* between the roles. Roles may have four attributes: responsibilities, permissions, activities and protocols. There are two types of *responsibilities*. In general, *liveness* responsibilities are those which add something beneficial to the system while *safety* responsibilities prevent unwanted events happening. *Permissions* represent the information that a user role is allowed to access, and the tasks it is allowed to perform in general. *Activities* are tasks that a role performs without interacting with other roles. *Protocols* are the specific patterns of interaction. GAIA has formal templates and operators for representing roles and their attributes, as well as schemas for representing interactions. The lack of low-level design and implementation capability of GAIA allows these issues to remain open-ended so that the designer retains the flexibility to choose the architecture and the language in which the agents are constructed.

In the GAIA methodology, the designer is encouraged to think of an agent-based system as a society or an organisation. This is useful when defining the *role models* that specify the expected function of each entity. These can be based on the goals of each agent as described in Sect. 3. It is therefore possible to express the functionality of each agent entity in the system as a “Manager” responsible for overseeing the work that must be carried out to achieve the stated goals.

Using the concept of the role schema, within the GAIA methodology, it is possible to identify some key permissions (relating to the resources which can and cannot be used) and responsibilities (relating to the functionality of the role). A role schema for the Server Agent is shown in Fig. 4. The responsibilities of a role can be broken down into two different types of components, an activity that does not involve interaction with another agent, and a protocol that involves interaction with another agent. The liveness equation shows the order of operation of these protocols and activities within this agent, whilst the safety conditions state that certain conditions must be met in order to prevent situations arising that would be undesirable.

For the more low level details, such as the individual classes and the communications between the agents, it is proposed here to use, in combination with GAIA, a modified version of the unified modelling language (UML), named Agent UML (AUML) [28], which contains specific constructs to accommodate the agent-specific communications. This novel approach, which merges core components of each of the above-mentioned methodologies, was found to provide a suitable design methodology for this particular system, as it both encompasses high-level concepts for the description of the agents behaviour, and provides the low-level technical software details that are a pre-requisite to the implementation process.



Role Schema: *Server Manager*

Description: The server manager ensures that no information is released from the database without the relevant security levels being satisfied. This manager negotiates with the access manager for the release of the requested information. This may involve the request for additional biometrics if the confidence is low or the user is not willing to donate the specified samples.

Protocols and Activities

NegotiateRelease, ProvideSecurityLevel, ReadSecurityLevel, RefreshDBSources, AwaitFileRequest, EncryptData, RegisterService

Permissions

Supplied	filerequest	// the file that it being requested by the user.
Generates	securitylevel	// the level of security for the requested file.
Generates	ServerService	// a list of services that the server can offer.
Generates	file	// the file the user has requested.

Responsibilities

Liveness:
([RegisterService].AwaitFileRequest.RefreshDBSources.ReadSecurityLevel.EncryptData .ProvideSecurityLevel.NegotiateRelease)$^{\omega}$

Safety:

- Must register to process filerequests.

Fig. 4. Server agent role schema using the GAIA methodology

5.2 Communication and implementation languages

The choice of the communication language between the agents is another crucial factor in the performance of the system. Several Agent Communication Languages (ACL) have been developed by the research community.

Notable examples include KQML (Knowledge Query and Manipulation Language) [30], for which there are a number of available implementations [31], and FIPA-OS (Foundation for Intelligent Agents Operating System) [32, 33]. Sun Microsystems have also developed a message service known as the Java Messaging Service (JMS) that is a suitable candidate as an agent communication language [34].

The content of the messages that are passed in the system can be represented in XML (eXtensible Markup Language), a markup language similar in syntax to HTML (Hyper Text Markup Language) [35]. XML was designed to describe and encapsulate data. XML can also be used to exchange data between systems. In our example this means that the agents in the system can all interact using the XML payload in the message, and this can be used to retrieve data from the server database directly. The reason for choosing XML is its universal syntax that allows ease of translation, transformation, parsing, presentation and validation with a variety of standard mechanisms. XSL (eXtensible Stylesheet Language) can be used to transform and format XML messages so that the interface agent can directly display the retrieved data in a browser window.

For the IAMBIC project it was decided to use a combination of KQML as a communication language with XML message payloads to provide optimum compatibility with existing agent-based systems and extensibility for future applications.

5.3 Detailed implementation example

In this section we shall examine the Server Agent in some detail, as it illustrates the communication aspects of the system and the negotiation required to obtain the information requested by the user.

Figure 4 shows the initial GAIA role schema for this agent.

The GAIA methodology provides a useful starting point from which further specifications can be elaborated using some of the components of the AUML methodology, as detailed below.

Figure 5 shows the proposed AUML use case diagram for the Server, capturing its functionality.

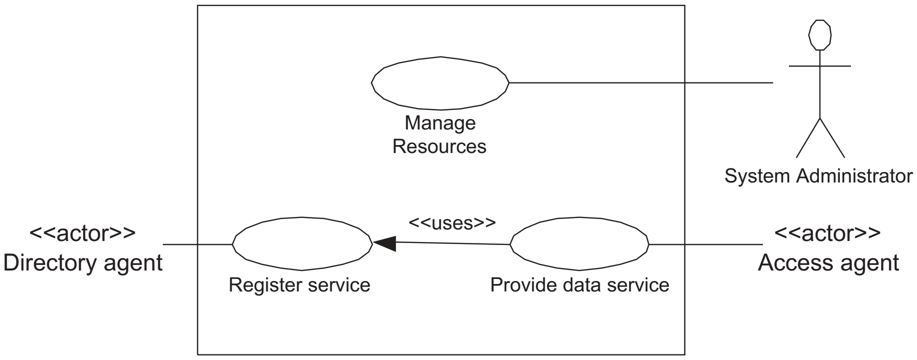


Fig. 5. Use case diagram for server agents

From this use case and the associated role schema (Fig. 4), the class relationship diagram for this entity can be constructed, using the AUML methodology, as shown in Fig. 6.

The classes themselves are self-explanatory, and encapsulate the required functionality of the system, but a brief description of each class is given below.

- Serverinfo
  This class represents the information services that the server can offer. The information contained in this class will be transmitted to the Directory Agent upon registration. If the details of the services offered change during the lifetime of the server, this information can be conveyed to the Directory Agent so that it can update its dynamic information list.
- Confidence analyser
  This class will be used during the negotiation phase of the conversation with the Access Agent. The knowledge contained within this class will enable an informed decision to be made whether the level of confidence received from the user with respect to the requested file is sufficient to warrant the release of the file. This class can also make suggestions based on the information received in order to attempt to validate the user through other means, such as resampling of biometrics or modification of the fusion process, or even the supply of non-biometric personal data.
- Database
  This class is responsible for the maintenance of the information contained within the server's database. It will also retrieve the security level associated with the requested file and extract the file itself. Provision will be made in this class for facilities to modify the data contained within the database as required.
- Communications
  This class is responsible for implementing the particular ACL that will be employed in the system. It will provide methods for sending and receiving messages and reporting any message-failure conditions that may occur.

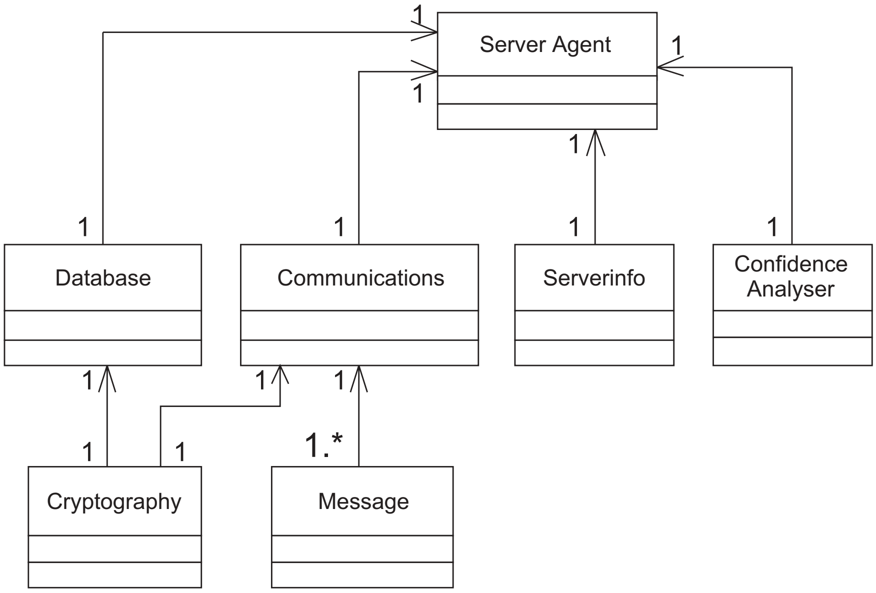


Fig. 6. Class diagram for server agent

- Message
  This class encapsulates the ACL message that will be passed to the communications class for transmission.
- Cryptography
  This class will be responsible for the cryptography used in order to protect the content portion of any message passed between the agents. It will also be used to protect sensitive data contained within the server database.

Figure 7 shows the Agent Interaction Protocol (AIP) diagram, depicting the request for a file from the Access Agent to the Server Agent. Such AUML diagrams are used to depict the flow of communications between separate agents.

The Access Agent requests the file from the server. The server can respond in one of three ways:

1. The Server Agent can refuse. This failure condition could represent the condition where the requested file was not found within the server's database.
2. The message could be corrupted, in which case the server responds with the not-understood condition. The receipt of this type of message would require a retransmission of the specified message by the Access Agent.
3. If the file is found, then the Server Agent replies to the Access Agent with the relevant security level associated with the file.

The Access Agent then replies with the global confidence score obtained from the user biometric after the data-fusion process. The Server Agent is then is a position where the following messages could be sent back to the Access Agent.

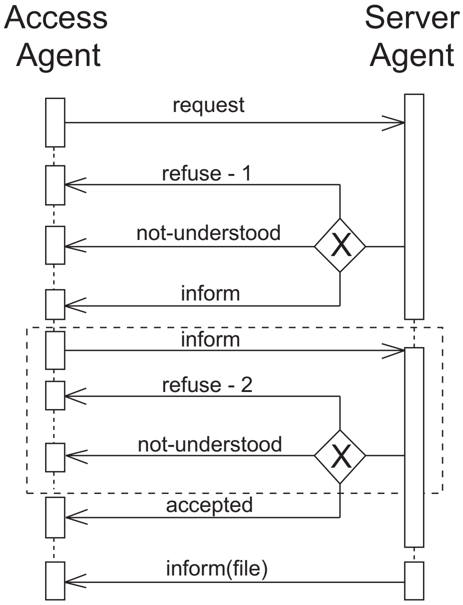


Fig. 7. Agent iteration protocol diagram (AIP)

1. The server has examined the confidence score and has determined that the received level is not high enough to warrant the release of the file. The message returned will indicate this, and a suggestion will be conveyed back to the Access Agent from the confidence-analyser class.
2. The message could be corrupted, in which case the server responds with the not-understood condition. The receipt of this type of message would require a retransmission of the specified message by the Access Agent.
3. The confidence score received has been deemed satisfactory by the confidence-analyser class and the server can release the file. The Access Agent is informed of this.

Upon successful authorisation the file is released as denoted by the last message condition on the AIP.

The dashed box shown in Fig. 7 indicates possible conversation iterations, as the Access Agent may need to send several modified confidence scores to the Server Agent while attempting to authenticate the user for the requested file.

The message types in this AIP are general; the actual *performatives* used in the implementation would depend on the ACL that is used. KQML and FIPA share a very similar set of these performatives, whilst the JMS is an open-ended solution where the designer can set message types. It is assumed that the particular ACL employed will cater for the condition where messages cannot be delivered, as well as the acknowledgement of messages, and hence these details are not explicitly included in the state charts and interaction diagrams presented here.

The novel combination of GAIA and AUML for the design of the agent-based architecture of the IAMBIC system, together with the implementation strategy of using KQML together with XML message payloads, has provided a flexible and expandable framework for system implementation.

6 Conclusions

An increasingly important aspect of system design and implementation, which relates to "universal access", is the question of *authorisation* and *control* of the means of access to systems and the data they hold and process. This is especially true for access to data where confidentiality and integrity are issues of paramount importance. Biometric access control offers, in principle, a strategy for ensuring the protection of such data in an effective and convenient way, but many problems can be encountered in moving from a theoretical system design to a practical situation.

Multimodal biometrics, however, provide a viable approach for overcoming the performance and acceptability barriers to the widespread adoption of biometric systems. However, it is essential that the resulting complexities are managed in a seamless and effective way. This paper has introduced the basis of an architecture for the management of multimodal biometrics within an overall security framework for trusted information exchange, which can embody exactly the requirements noted above.

In the context of remote and unsupervised authentication of identity, it is essential to build in protection against replay attacks and the use of forged samples as well as to establish "liveness" of the biometric input. While some progress has been made in integrating liveness detection in individual modalities (e.g. eyeblink detection in face recognition) it is clear that an agent-managed multimodal framework such as the one presented here provides a platform which readily supports more advanced robustness measures. The agent interface can be deployed to provide a sophisticated challenge/response mechanism making it much more difficult to use replay attacks and much easier to establish confidence in the liveness of samples.

The concepts and implementation strategy presented in this paper represents a novel and efficient approach for realising the potential of biometric access control by offering an appropriate framework for managing the complexity inherent in the typical practical scenarios outlined here. The issues addressed, and the approach defined, lead to a paradigm which contributes an essential element to the set of tools which are required to underpin any practical realisation of universal access in the information society when the data or systems under consideration embody confidential, sensitive or commercially valuable data to which unrestricted access is inappropriate.

Although applications for the processing framework described here are widespread and varied, an immediate objective of the IAMBIC programme is to introduce these concepts into application domains within the healthcare sector, where there is a very clear match between the capabilities embedded in the structures described above and the practical requirements for viable system exploitation in the future.

Acknowledgements. The authors wish to acknowledge the contribution of the industrial collaborators on the IAMBIC project, Neusciences and Cardionetics Ltd. The support of the UK Engineering and Physical Sciences Research Council and the Department of Trade and Industry, as part of the Management of Information LINK Programme, is also gratefully acknowledged.

References

1. Deravi F, Lockie M (2000) Biometric industry report – market and technology forecasts to 2003. Elsevier Advanced Technology, Oxford
2. Jain A, Bolle R, Pankanti S (eds) (1999) Biometrics: personal identification in networked society. Kluwer, Boston, MA
3. Chibelushi CC, Deravi F, Mason JSD (1999) Adaptive classifier integration for robust pattern recognition. IEEE Trans Syst, Man Cybernet – Part B: Cybernet 29(6):902–907
4. Nahin PJ, Pokoski JL (1980) NCTR plus sensor fusion equals IFFN or can two plus two equal five? IEEE Trans Aerospace Electron Syst 16:320–337
5. Su Q, Silsbee PL (1996) Robust audiovisual integration using semicontinuous hidden Markov models. In: Proceedings of the fourth international conference on spoken language processing, vol 1, pp 42–45
6. Wagner T, Dieckmann U (1994) Multi-sensorial inputs for the identification of persons with synergetic computers. Proceedings of the first IEEE international conference on image processing, vol 2, pp 287–291
7. Dasarathy BV (1991) Decision fusion strategies in multisensor environments. IEEE Trans Syst, Man Cybernet 21(5):1140–1154
8. Chibelushi CC, Mason JSD, Deravi F (1997) Feature-level data fusion for bimodal person recognition. In: Proceedings of the sixth IEE international conference on image processing and its applications, pp 399–403
9. Chibelushi CC, Deravi F, Mason JSD (1997) Audiovisual person recognition: an evaluation of data fusion strategies. Proceedings of the second European conference on security and detection, pp 26–30
10. Chen K, Wang L, Chi H (1997) Methods of combining multiple classifiers with different features and their applications to text-independent speaker recognition. Pattern Recogn Artificial Intell 11(3):417–445
11. Ho TK, Hull JJ, Srihari SN (1994) Decision combination in multiple classifier systems. IEEE Trans Pattern Anal Mach Intell 16:66–75
12. Lam L, Suen CY (1997) Application of majority voting to pattern recognition: an analysis of its behaviour and performance. IEEE Trans Pattern Anal Mach Intell 27:553–568
13. Rahman AFR, Fairhurst MC (1999) Enhancing multiple expert decision combination strategies through exploitation of a priori information sources. IEE Proc Vis Image Signal Process 146:40–49
14. Fairhurst MC, Rahman AFR (2000) Enhancing consensus in multiple expert decision fusion. IEE Proc Vis Image Signal Process 147:39–46
15. Meier U, Hurst W, Duchnowski P (1996) Adaptive bimodal sensor fusion for automatic speechreading. Proceedings of the IEEE international conference on acoustics, speech, and signal processing, vol 2, pp 833–836
16. Wooldridge M, Jennings NR (1995) Intelligent agents: theory and practice. Knowledge Eng Rev 10(2):115–152
17. Jennings NR, Sycara K, Wooldridge M (1998) A roadmap of agent research and development. In: Autonomous agents and multi-agent systems, vol 1, Kluwer, Boston, MA, pp 275–306
18. Sandholm T, Lesser V (1995) Issues in automated negotiation and electronic commerce: extending the contract net protocol. In: Proceedings of the first international conference on multiagent systems (ICMAS-95), San Francisco, CA, pp 328–335
19. Zheng D, Sycara K (1997) Benefits of learning in negotiation. In: Proceedings of the fourteenth national conference on AI, AAAI-97, Providence, RI, July 1997, pp 36–41
20. Pollack ME, Ringuette M (1999) Introducing the tileworld: experimentally evaluating agent architectures. Proceedings of the eighth national conference on AI, AAAI-90, Boston, MA, pp 183–189
21. Wooldridge M (1997) Agent-based software engineering. IEEE Trans Software Eng 144(1):26–37
22. Mayfield J, Labrou Y, Finin T (1996) Evaluating KQML as an agent communication language. In: Intelligent agents II (Lect. Notes Artif. Intell. vol 1037), Springer, Berlin, pp 347–360
23. Ross A, Jain A, Qian J-Z (2001) Information fusion in biometrics. In: Third international conference on audio- and video-based biometric person authentication, AVBPA 2001, Halmstad, Sweden, June 6–8, 2001 (Lect. Notes Comput. Sci. vol 2091), Springer, Berlin, pp 354–359
24. Verlinde P, Druyts P, Chollet G, Acheroy M (1999) A multilevel data fusion approach for gradually upgrading the performance of identity verification systems. In: Proc SPIE – The International Society for Optical Engineering, vol 3719, pp 14–25
25. Hong L, Jain A (1997) Integrating faces and fingerprints for personal identification. IEEE Trans Pattern Anal Machine Intell 20(12):1295–1307

26. Arazy O, Woo CC (1999) Analysis and design of agent-oriented information systems (AOIS). University of British Columbia, Working Paper 99-MIS-004
27. Wooldridge W, Jennings NR (2000) The GAIA methodology for agent-oriented analysis and design. Autonomous Agents Multi-Agent Syst 3:285–312
28. Odell J, Van Dyke Parunak H, Bauer B (2000) Extending UML for agents. In: Wagner G, Lesperance Y, Yu E (eds) Proceedings of the agent-oriented information systems (AOIS) workshop at the 17th national conference on artificial intelligence, Austin, TX, pp 3–17
29. Iglesias CA, Garijo M, Gonzalez JC, Velasco JR (1998) Analysis and design of multiagent systems using MAS-commonKADS. In: Singh MP, Rao A, Wooldridge MJ (eds) Proceedings of the 4th international workshop on agent theories, architectures, and languages (ATAL97) (Lect. Notes Artif. Intell. vol 1365), Springer, Berlin, pp 313–328
30. Finin T, Fritzson R, McKay D, McEntire R (1994) KQML as an agent communication language. Proceedings of 3rd international conference on information and knowledge management (CIKM94), ACM Press
31. SACI simple agent communication infrastructure. A KQML implementation – Universidade de São Paulo – http://www.lti.pcs.usp.br/saci/
32. Poslad S, Buckle P, Hadingham R (2000) The FIPA-OS agent platform: open source for open standards. In: proceedings of the 5th international conference and exhibition on the practical application of intelligent agents and multi-agents, pp 355–368
33. FIPA-OS, an open source implementation of the mandatory elements contained within the FIPA specification for agent interoperability. Nortel Networks, http://www.nortelnetworks.com/fipa-os
34. Java Message Service, Sun Microsystems Corporation, http://java.sun.com/products/jms/jms-092-spec.pdf
35. XML, Extensible Markup Language, http://www.w3.org/XML/
36. Borking JJ, van Eck BMA, Siepel P (1999) Intelligent software agents and privacy. Registratiekamer, The Hague, ISBN 90 74087 13 2