Biometric Features for Mobile Agents Ownership

Salvatore Vitabile, Giovanni Pilato, Vincenzo Conti, Giuseppe Gioè, and Filippo Sorbello

Abstract — *Multi-Agent System (MAS) architectures can be used for e-Business application due their flexibility, scalability and interoperability. Agent ownership implies that a specific person or organization (the owner) is responsible for the agent's actions. Agents, whose ownership was certainly fixed, could operate on behalf of their owner to make transactions, to buy or sell products. Security requirements in the agent ownership setting process are the identification of the owner and the protection of the identification information carried by an agent. In this paper, we investigate the possibility of using biometrics in mobile agent systems for owner authentication. Biometric features can be used in both agents ownership setting process and in the protection of the agents information. Certification Authorities could also check against the owner reputation level before grant or deny permission of performing certain actions. In order to show the feasibility of the approach, the proposed techniques have been implemented and tested as an extension of the JADE-S platform.*

Index Terms — *agent ownership; biometric authentication systems, multi-agent systems security.*

1. *INTRODUCTION*

An e-Business agent community is a self- organized virtual space consisting of a large number of agents and their dynamic environment. Within a community, highly relevant agents group together offering special e-Services for a more effective, mutually beneficial, and more opportune e-Business. Each agent community consists of agents specializing in a single domain/sub-domain, or highly intersecting domains. AGent Service Providers (AGSP) could provide a network infrastructure with strong network servers and local workstations to allow people use agent-services provided by them.

A mobile agent can be owned by individuals or organizations. An agent owner can use his/her agent to carry out tasks to fulfill its own purposes. Owners can offer agent services to individuals or organizations that are not in a position to own an agent.

Agent ownership implies that a specific person or organization (the owner) is responsible for the agent's actions. Yip and Cunningham raise several issues regarding software agent ownership, such as the related legal hurdles because exiting law does not support the ownership of an active software instance [3]. In a framework supporting agent ownership, agents could be legal entities employed to bring their own principal into contractual relations with third parties. The authentication process establishes the identity of each owner and, consequently, of each agent. A policy, based on the previous identity, can determine the access level of an agent in e-Business systems, the permission to access to certain resources or perform certain tasks. The Agentcities Security Working Group has defined a set of security requirements identified for multiple agent platforms active in open distributed multi-domain networks. Among the application driven requirements, user authentication based on both invasive and non-invasive biometric features is suggested [1].

Manuscript received July 27, 2004; revised November 22, 2004. Vitabile, S*. and Pilato G. are with the Istituto di CAlcolo e Reti ad alte prestazioni of the Italian National Research Council, Palermo, Italy {g.pilato, s.vitabile@icar.cnr.it}. Conti, V., Gioè, G., and Prof. Sorbello, F. are with the Dipartimento di Ingegneria Informatica, University of Palermo, Italy { conti, gioe@csai.unipa.it}, sorbello@unipa.it.

* S. Vitabile is the contact person.

Security requirements in the agent ownership setting process are the identification of the owner and the protection of the identity information carried by an agent. The first issue deals with the user authentication process while the second issue deals with information encryption techniques and certificates.

High security authentication system design still remains an open problem. Complex passwords are easy to forget while simple password are easily guessed by unauthorized persons. An unauthorized person, by stealing a trusted username/password pair, can gain access into a system and run malicious agents to perform unauthorized transactions. The original owner will be the legal responsible of these actions.

In a mobile-agent framework, biometric based authentication systems can be used to improve the owner authentication process security. So, it is possible to authenticate an individual's identity based on "who the user is", rather than by "what the user has" (e.g., an ID card) or "what the user remembers" (e.g., a password) [7], [26]. As a consequence, agent and owner reputations are strictly related and they can be considered as a single entity. A network authority can temporarily or permanently suspend or revoke digital certificates to untrusted agents (users).

In this paper, the mobile agent ownership issue is addressed by introducing biometric based systems in the user (owner) authentication process.

Biometric features are conveniently divided into two main categories. The physiological features include face, eye (normally, retinal or iris patterns), fingerprints, palm topology, hand geometry, wrist veins and thermal images [29],[30]. The behavioral features include voiceprints, handwritten signatures and keystroke dynamics. In general, physiological features have been more successful than behavioral features to implement authentication systems of such characteristics. This is not difficult to understand: physiological features essentially do not vary with time, whereas behavioral features such as signature and keystroke dynamics may change greatly even between two consecutive samplings [29],[30].

A biometric based authentication process is based on two sequential phases. In the enrolment phase, the system acquires individual biometric information like a kind of registration template. In the matching phase, the currently acquired biometric information is compared with that stored in order to determine whether or not they belong to the same person.

A fingerprint based authentication system for the JADE-S platform has been proposed by the authors in [2]. JADE-S is a FIPA (Foundation of Physical Intelligent Agents) compliant multi-agent platform supporting a username/password based user authentication process. JADE-S is formed by the combination of the standard version of JADE with the JADE security plug-in [10], [11].

In this paper, we will address the possibility of using biometrics in mobile agent systems starting from the above implementation. Biometric features improve the security in owner authentication, since an owner will be authenticated with his/her intrinsic bodily characteristic. A mobile agent proves its identity by showing its Identity Certificate, signed by a Certification Authority. Using digitally-signed certificates with biometric information, the platform can be sure of the agent owner identity. The Certification Authority could also check against the owner reputation level before granting or denying permission to perform certain actions.

The paper is organized as follows. In section 2 the implications of agent ownership on agents trust and reputation are briefly discussed. In section 3 a brief description of the common biometric features used for human authentication is reported. In section 4 the implementation of the proposed extensions in the JADE-S platform is outlined. Finally, in section 5 some considerations about owner privacy are reported.

2 .TRUST AND OWNER REPUTATION

The problem of trust has many implications in an open distributed environment. In e-business transactions, an agent needs to decide, when another agent is encountered in the network, if that new agent can be trusted or not.

Many researchers treat ownership as a passive ingredient of trust. In [13] Jurca and Faltings proposed to link agent trust to the agent reputation, i.e. the collection of the agent related information about its past behavior. Rahman and Hailes [12] have proposed a distributed trust model based on the assumption that an agent will be able to keep a history of interaction with other agents and hence assign different level of trust to the peers. However, as pointed out in the scenarios, it is not always possible to obtain the necessary records to decide the level of trust towards an agent, especially when there is no direct relationship between the real world legal entity and the software agent representing it.

In the multi-agent system design phase, it is essential to provide individual agents with various forms of social awareness in order to support rich collaborative behavior [4], [5], [6]. Mamdani and Pitt [5] have suggested that an agent should be able to express the fact that an agent is owned by some human entity. Furthermore, the agent should be able to reason about the consequences and responsibilities of the delegation.

In agreement with Yip and Cunningham [3], secure user authentication helps to sustain a trust model including agent ownership. Here, we distinguish two different types of owner:

- The *authors* are people or organizations that write programs to execute an agent;
- The *senders* are people or other entities that send agents to act on their behalf.

In the mobile agent identification issue, X.509v3 digitally-signed certificates, containing owner biometric information, can be adopted. Certificates are useful for agent authentication as well as to carry information about Agent OWner Reputation (AOWR). AOWR can be included in digitally-signed certificates and used by platforms and agents to grant or deny permission to a mobile agent. A trusted multi-agent platform with agent execution tracing capabilities can decrease AOWR for authors and senders whose agents are malicious or untrusted. An enabled Certification Authority (CA) can temporarily or permanently suspend or revoke digital certificates of untrusted agents/owners.

3. *Biometrics for Authentication*

Mobile agent ownership requires reliable personal recognition schemes to determine and confirm the identity of an agent. Common authentication systems for multi-agent platform are based on username and password. Three well-known user authentication systems are Kerberos, NetSP, and SPX [23], [24], [25].

Therefore, the above approaches are based on username and password with the use of cryptography techniques to protect data integrity from possible attacks. Using biometric features, we introduce a second security level in the user authentication process.

The following two procedures are generally used for identity verification with biometric features [14]:

- enrolment: the system acquires an individual biometric information building a template;
- matching: the acquired biometric information is compared with the stored individual biometric information to determine whether or not they belong to the same person.

Different biometric features can be used in the user identification process. Some of these features can be considered invasive biometrics (e.g. fingerprints, retina) and they may not be desirable as they infringe on privacy, others that are not unique or robust (e.g. hand geometry, voice) are less invasive. User authentication systems can be divided into verification and identification systems. A verification system performs the comparison 1->1 between the sensor acquired biometric features and the single related stored item. An identification system performs a comparison1-> many between the sensor acquired biometric features and many stored items in order to individualize user identity within a group of enrolled users.

The most important parameters to evaluate a biometric based authentication system are the Genuine Acceptance Rate (GAR) and the False Acceptance Rate (FAR). False accept errors are very dangerous for an authentication system, so FAR value is very restrictive. FAR common values range from 10^{-2} (basic security applications) to 10^{-6} (high security applications).

In what follows, a brief description of four primary methods of biometric authentication are reported.

A. Voice recognition.

The authentication process is based on some major characteristics such as cadence, frequency, pitch and tone of an individual's voice. Common implementation of voice based authentication systems give, as best result, the 90% of classification rate [18], [20]. As a consequence, a simple voice based verification system can be used for applications where a high security level is not required. Voice can be used in multi-biometric systems [18].

B. Face recognition.

Face recognition is a non-intrusive method that has advanced considerably in the last decades. The most common approaches to face recognition are: a) the location and shape of facial attributes, b) the global analysis of the face image that represents a face as a weighted composition of a set of canonical faces. A face recognition system needs a generic camera for face images, a very simple recording phase. Furthermore, the matching process is based on a high number of features. In the last competition, FRVT2002, the best obtained results was the 90.3% of recognition percentage with a FAR of 1% and the 71.5% of recognition percentage with a FAR of 0.01%. Experimental trial was performed on a database of 37.437 individuals [16], [17].

C. Iris recognition.

The iris is the annular region of the eye bounded by the pupil and the sclera on either side [28]. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. Iris recognition systems require special iris cameras with very high resolution and infrared illumination abilities. Using standard CASIA Iris database, different methods have been developed for iris based authentication systems. The obtained results range from 92.64% (Boles et al. [19]) to 100% (Daugman [22]).

D. Fingerprints recognition.

Fingerprints have been used for personal identification since the 1880s, and the matching accuracy using them has been shown to be very high [7], [8]. Everyone is presumed to have unique, immutable fingerprints [27]. However, the probability that a fingerprint with 36 minutiae points will share 12 minutiae points with another arbitrarily chosen fingerprint with 36 minutiae points is 6.10 x 10^{-8} [21]. These probability estimates show that fingerprint matching is not infallible and leads to some false associations. Today, the implementation of a fingerprints based authentication system is very simple and inexpensive and shows interesting results. A good system reaches the 99.4% of recognitions percentage with a FAR of 0.01% and the 99.9% with a FAR of 1% [17].

4. CASE STUDIED: THE JADE-S PLATFORM

In this section our experience using a multi-agent platform with a biometric based authentication system is described. Starting from the biometric agent owner setting, x.509v3 digital certificates for agent authentication and certification have been personalized and used.

As framework we have chosen the JADE-S platform, a FIPA (Foundation of Physical Intelligent Agents) compliant multi-agent platform. JADE-S is formed by the combination of the standard version of JADE with the JADE security plug-in [10], [11]. JADE-S platform supports some security issues such as authentication, authorization, permissions and policies, certificates and certification authority. However, neither is biometric authentication module provided nor digital certificates with extended information managed.

Several types of biometric authentication systems could be used for user authentication. A fingerprint based authentication system for the JADE-S platform has been proposed by the authors in [2]. The whole platform as well as each single agent can be activated only by authenticated users. The activated agent will own a digitally-signed X.509v3 certificate containing owner personal information, owner authentication information (matching function and matching score) and the owner reputation rating.

Our solution is based on a set of PKI techniques including certification authorities, private/public keys, and digitally-signed certificates. With more details, the multi-agent platform has been extended implementing a new Login Module (LM) and an enhanced Security Certification Authority (SCA). The LM is able to deal with username, password and fingerprint. The SCA is able to deal with digitally-signed X.509v3 certificates. In what follows, the description of both JADE-S platform and developed modules (LM and SCA) are given.

A. The JADE-S platform

The Foundation for Intelligent Physical Agents (FIPA) developed specifications for the implementation of multi-agent systems. The physical infrastructure in which agents can be deployed consists of: the hardware platforms, the operating system, the agent support software, the FIPA agent management components: the Directory Facilitator (DF), the Agent Management System (AMS), the Agent Communication Channel (ACC), and the Internal Platform Message Transport.

According to the FIPA specifications, there must be at least one DF agent per platform. An agent can register its services in the DF. The DF allows *Yellow Pages* services and the agent can submit a query to the DF in order to find the required service. Furthermore, the DF maintains an accurate, complete, and up-to-date list of agents. The AMS is unique to the platform and is responsible for managing the agent creation, deletion and migration. The ACC routes messages between agents within the agent platform to agents resident on other agent platforms.

JADE (Java Agent DEvelopment framework) is a FIPA compliant software framework fully implemented in Java language which simplifies the implementation of multi-agent systems. The platform can be seen as a middleware providing a set of useful tools that support the debugging and deployment phase[11].

JADE-S is formed by the combination of the standard version of JADE with the JADE security plug-in [10], [11]. JADE-S includes security features such as user/agent authentication, authorization and secure communication between agents into the same platform. With more details:

- Authentication: a user must be authenticated by providing a username and password, to be able to own or perform actions on a component of the platform. Only authenticated users can own AMS, DF, containers and other agents;
- Authorization: JADE-S uses the concept of Principal as an abstraction for a user account, an agent or a container. A Principal must be authorized by the Java security manager. The security manager allows or denies the action according to the JADE platform's policy;
- Permissions and Policies: a permission is an object that describes the possibility of performing an action on a certain resource such as a piece of code, but also executes that code. A policy specifies which permissions are available for various principals;
- Certificates and Certification Authority: the Certification Authority (CA) is the entity that signs all the certificates for the whole platform, using a public/private key pair.
- Delegation: this mechanism allows the "lending" of permissions to an agent. Besides the identity certificate, an agent can also own other certificates given to it by other agents;
- Secure Communication: communication between agents on different containers/hosts, are performed using the Secure Socket Layer (SSL) protocol. This enables a solid protection against malicious attempts of packet sniffing.

B. The Developed Extensions

B1. The Login Module

The Java Authentication and Authorization Service (JAAS) [9] allows:

- user authentication, to reliably and securely determine the user which is currently executing Java code;
- user authorization, to ensure they have the access control rights (permissions) required for the requested actions.

According to the three paradigms illustrated in the previous section (i.e. what the user knows, what the user has, what the user is), JAAS has been configured to deal with agent code ad agent owner authentication.

The developed Login Module manages the platform access system dealing with:

a. owner username and password;

b. a stored key containing owner credential;

c. owner fingerprint information.

The Login Module is depicted in Fig. 1; the module is composed by the following blocks:

- *JAAS LoginContext*: it is responsible for the authentication process. It reads a configuration file, named "jaas.config" and starts the appropriate LoginModule.
- *JAAS LoginModule:* it creates a callback handler to acquire the user's credentials. The credentials are sent to the E-CSAI Authentication Service that verifies them. If the verification is positive, the object session is generated.
- *E-CSAI Authentication*: it verifies the user's credentials and returns "true" or "false". It checks also the username with the associated password, verifies the certificate authenticity, and performs the fingerprint matching.
- *Session object:* it contains a Principal Entity which is an authenticated entity having shared state for trusted multi-platform migration; a Public Credential (a public key); and a Private Credential (a private key).

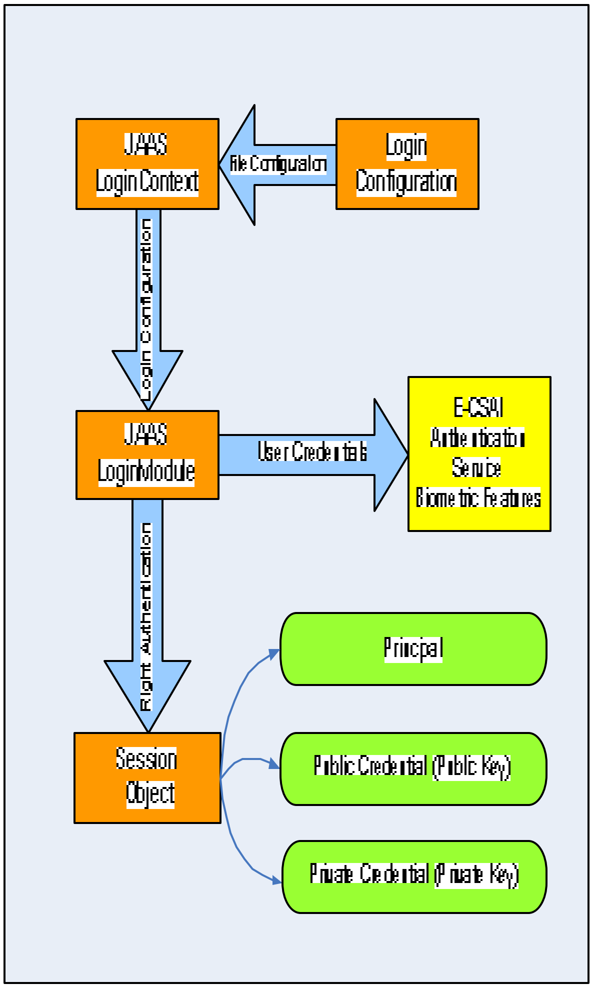

Figure 1. The Login Module and its components.

Authentication system procedure is the following:

1. username and password request;

2. user data verification;

3. if the user is not registered (enrolment phase)

3.1 a Registration Module starts requiring user personal data;

3.2 user personal data acquisition;

3.3 user fingerprint acquisition;

3.4 X.509v3 certificate and signed biometric information releasing;

4. if the user is registered (matching phase)*:*

4.1 signed biometrics data and certificate requests;

4.2 owner fingerprint acquisition;

4.3 fingerprint matching.

The triplet (*username*, *password*, *fingerprint*) is adopted in order to have three different *authentication items and to prevent Denial of Service (DoS) attacks* for the fingerprint verification process.

B2. The Security Certification Authority

Agent communications are managed with an extended version of the X-Security 2.0 package [15]. X-Security 2.0 supplies a secure model for inter-platform communication, opening several secure communication channels at the same time also with untrusted networks (differently from SSL).

X-Security 2.0 package has the following basic functionalities:

- a Security Certification Authority (SCA) – SCA is an independent agent which can temporarily or permanently suspend, renew or revoke agents digital certificates. It is not a part of the platform (like AMS or DF);
- a Security Module (SM) – SM is an optional module that each agent adopts for secure communications. If no secure communications are required, the agent use the standard Agent Communication Channel.

The SCA has been extended adding the described Login Module (based on fingerprint), a Registration Module (for the enrolment phase), and a Certificates and Keys Manager for X.509v3 certificates.

The Extensions field of the X.509v3 certificate contains:

- the name of the function to use in the matching phase. The function must be shared by the SCA;
- the minimum score needed for a positive match;
- the owner reputation rating.

The developed SCA is able to deal with the above items implementing the related policies to grant or deny permission for performing certain actions. A mobile agent proves its identity to the platform by showing its Identity Certificate, signed by a SCA. The Certification Authority also checks against the owner reputation level before to grant the possibility of performing an action or accessing to a resource.

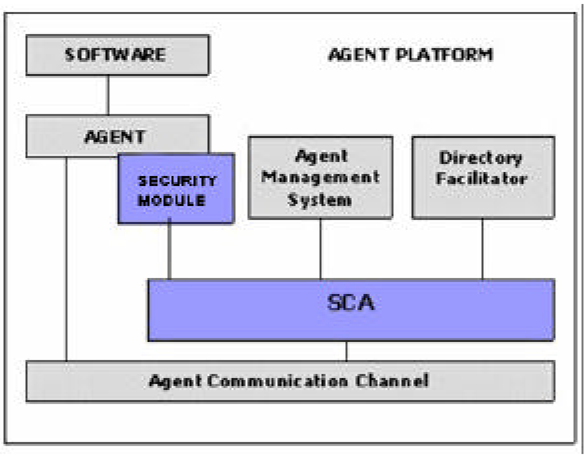

Figure 2. Agent platform structure with the emphasized SCA and Security Module.

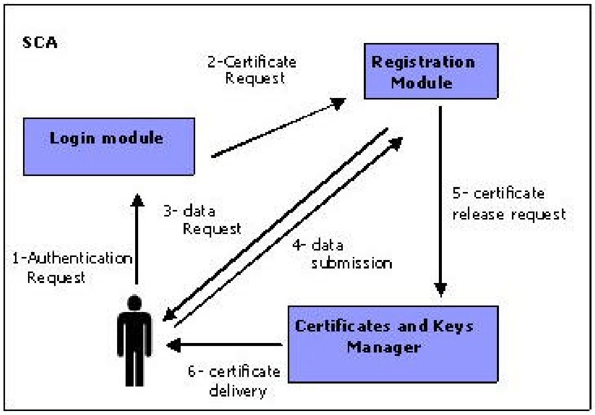

Figure 3. The extended SCA with the Login Module, the Registration Module, and the Certificates and Keys Manager for X.509v3 certificates.

In Fig. 2, the agent platform structure with the emphasized SCA and Security Module is depicted. In Fig. 3, the new extended SCA with the Login Module, the Registration Module, and the Certificates and Keys Manager is depicted. In the figure the sequential steps of the enrolment with the final certificate delivery step is also reported.

C. Experimental Results

It is well known that attempts to compare biometric error rates with password and token security have had only a limited degree of success because the factors that influence security are substantially different for biometrics than for traditional authentication mechanisms.

We have developed a new multi-agent platform with the characteristics illustrated in the previous sections in order to test the feasibility of the proposed approach. We have made use of 56 people, usually attending our laboratory, to test the authentication system easy-of-use. It is worthwhile to point out that 2 people refused to give us their fingerprints, while the remaining 54 people were willing to contribute. Experimental trials, conducted with 54 fingerprint pairs, show the feasibility of the system, which attained a 100% rate of success.

5. CONCLUSIONS

Strong owner agent authentication implies interesting discussions about the existing trust models developed for intelligent agents. Agent and owner reputation can be considered as a single entity and a network authority can temporarily or permanently suspend or revoke digital certificates to untrusted agents (users).

Some biometric methods can be considered invasive (e.g. fingerprints, retina) and may not be desirable as infringing on privacy. To protect the privacy of the persons involved, it is important that these personal data are used with care. They must be used if and only if they are necessary for legitimate purposes. Personal data will not be disclosed to the wrong persons and they will not be processed without the knowledge of the persons concerned. A Security Certification Authority holds these issues in high regard. Therefore, the use of agents and the processing of personal data have to meet certain conditions. These conditions derive from the principles of privacy which are laid down in many laws and international treaties.

The use of biometric characteristics for ownership determination, will allow an increased level of security for all those applications, like e-commerce, e-banking, and so on, for which the determination of agent ownership is crucial.

REFERENCES

[1] J.J. Tan, J.P. Pimentão, S. Poslad, M. Calisti, A. Yip, N. Foukia, R. Jurca, D. Khadraoui, S. Vitabile (2004), Agentcities/Opennet Forum, Security Working Group: Security Requirements for the Agentcities Network, URL: http://www.agentcities.org/out/00023/actf-out-00023a.pdf

[2] V. Conti, S. Vitabile, G. Pilato, F. Sorbello. “An Enhanced Authentication System for the JADE-S Platform”, WSEAS Trans. on Information Science and Application, Issue 1, Vol. 1, Jul. 2004, pp. 178-183.

[3] Yip and J. Cunningam. Some Issue on Agent Ownership, LEA Workshop on the Law of Electronic Agents, 2002.

[4] Castelfranchi, C. and Falcone, R. “Principles of Trust for MAS: Cognitive Anatomy, Social Importance, and Quantification”, Proc. of ICMAS-98, pp. 72-79, 1998.

[5] Mamdani and J. Pitt. Responsible Behavior for Networked Agents – A Distributed Computing Perspective, IEEE Internet Computing, Vol. 4, No. 5, Sept./Oct. 2000, pp. 27-31.

[6] Dignum, D. Morley, E.A. Sonenberg and L. Cavedon. Toward socially sophisticated BDI agents, Proceedings of the ICMAS 2000, pp. 111-118, 2000.

[7] Jain, L. Hong and R. Bolle. On-Line Fingerprint Verification, IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 19, n. 4, 1997.

[8] Z.M. Kovacs-Vajna. A Fingerprint Verification System Based on Triangular Matching and Dynamic Time Warping, IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 22, number 11, 2000.

[9] Java Authentication and Authorization Service (JAAS). URL: http://java.sun.com/products/jaas/index.jsp

[10] Poggi, G. Rimassa and M. Tomaiuolo. Multi-User and Security Support for Multi-Agent Systems. Proc. AI*IA - TABOO. 2001.

[11] Jade home page: http://jade.telecomitalialab.it/

[12] Abd ul-Rahman & S. Hailes, A Distributed Trust Model, New Security Paradigms 97, URL: http://citeseer.nj.nec.com/347518.html

[13] R. Jurca and B. Faltings, An Incentive Compatible Reputation Mechanism, URL: http://citeseer.nj.nec.com/585086.html

[14] A.K. Jain, A. Ross, S. Prabhakar. An Introduction to Biometric Recognition, IEEE Trans. on Circuits and Systems for Video Technology, Special Issue on Image and Video-Based Biometrics, Vol. 14, No. 1, 2004.

[15] P. Novak, M. Rollo, J. Hodik, T. Vlcekand and M. Pechoucek. X-Security Architecture in Agentcities, URL:http://agents.felk.cvut.cz/security/main/index.php

[16] Phillips P. J., Grother P., Micheals J. Ross, Blackburn Duane M., Tabassi E., Bone M., Face Recognition Vendor test 2002, Overview and Summery, 2003

[17] Hicklin A., Korves H., Ulery B., Zoepfl M., Bone M., Grother P., Michaels R., Otto S., Watson C., Fingerprint vendor Technology Evaluation 2003: Summary of results and analysis Report, June 2004

[18] Fairhurst M.C., Document Identity, Authentication and Ownership: The Future of Biometric verification, Proc. of 7th IEEE International Conference on Document Analysis and Recognition, ICDAR 2003

[19] Boles, W.W.; Boashash, B.; A human identification technique using images of the iris and wavelet transform; IEEE Trans. on Signal Processing, Volume: 46 , Issue: 4 , April 1998, pp:1185 – 1188

[20] Su Qin, Silsbee P.L., Robust Audiovisual Integration Using Semicontinuos Hidden Markov Models, Proc. of 4th International Conference on Spoken Language, ICSLP 96.

[21] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", IEEE Transactions on PAMI, Vol. 24, No. 8, pp. 1010-1025, 2002.

[22] Daugman J (2001) "Statistical richness of visual phase information." Int'l Journal of Computer Vision, 45(1), pp 25-38.

[23] http://web.mit.edu/kerberos,

[24] http://www.ibm.com

[25] http://www.dec.com.

[26] Watson, Jr. Thomas J., The Considerations of Data Security in a Computer Environment, IBM (Hrgs.), 1968 04 05, IBM, ISBN/Best-Nr: G520-2169-00.

[27] Maltoni M., Maio M., Jain A., Prabhakar S., "Handbook of FingerPrint Recognition", Springer, 2003.

[28] L. Ma, T. Tan, Y. Wang and D. Zhang, "Personal Identification Based on Iris Texture Analysis", IEEE-Trans. on Pattern Analysis and Machine Intelligence, Vol. 25, No. 12, pp.1519-1533, 2003.

[29] Venayagamoorthy G.K., Moonasar V., Sandrasegaran K., "Voice recognition using neural networks", in Communications and Signal Processing, 1998. COMSIG '98. Proc. of the 1998 South African Symposium on , 7-8 Sept. 1998, pp:29 – 32

[30] Ashbourn , J., "Practical implementation of biometrics based on hand geometry", Image Processing for Biometric Measurement, IEE Colloquium on , 20 Apr 1994 pp:5/1 - 5/6