Application of Fuzzy Logic in Federated Trust Management for Pervasive Computing

Zhengping Wu and Alfred C. Weaver
Department of Computer Science, University of Virginia
151 Engineer's Way, P.O. Box 400740, Charlottesville, VA 22904
{zw4j,weaver}@cs.virginia.edu

Abstract

In federated and pervasive networks, trust management has become a cornerstone for information security and privacy. Although people have recognized the importance of privacy and security for their personal information, they remain uncertain when they have to define and enforce their own access control rules or have to handle indirect information. Indirect information and subjective judgment are the major sources of uncertainty in federated trust management. This paper introduces fuzzy logic into the definition and evaluation of trust, and then provides a formal representation of fuzzy rules. It also offers a set of derivation rules for analyzing and reasoning among fuzzy rules in order to enforce these rules with a certain level of uncertainty. Application of this model to a healthcare environment with pervasive computing devices across trust domains provides a new method to handle uncertainty in trust management for federated and pervasive networks.

1. Introduction

Trust management was first defined by M. Blaze, et al. [1]. With the application of trust management in research for network security, a more general definition is proposed by Grandison [2]: "Trust management is the activity of collecting, encoding, analyzing and presenting evidence relating to competence, honesty, security or dependability with the purpose of making assessments and decisions regarding trust relationships." Trust management has been studied in the context of access control [3], public key architecture [4], and peer-to-peer reputation systems [5]. Meanwhile, industries that require collaboration and sharing such as healthcare, manufacturing, and financial services will also benefit from trust management. For instance, HIPAA [6] requires rigorous privacy and security protection for medical data in healthcare systems. Thus trust management for hospital administration requires being able to create and enforce certain rules to secure healthcare data, for example "public web sites are permitted anonymous access," "patients may access their own records with password protection," "modification of patient data requires fingerprint verification of the physician." Trust management enables us to increase the security and privacy of our shared resources and collaborative activities without increasing our workload. For instance, trust management systems can enforce the tasks stated in the above hospital example and yet not interfere with normal operations.

Federation is the current and future direction of trust management. It is an expansion of local infrastructure to an enterprise-wide and even global one and intensifies the demand for integrating inter-domain networks and services. With the increased flexibility required by distributed yet interconnected networks such as the Internet and pervasive computing environments, trust management becomes more and more important for federation among networks. Federated trust management needs to manage a collection of trust-related activities across multiple and heterogeneous security domains and autonomous systems for federation.

In order to manage a collection of trust-related activities, flexibility is needed in the enforcement of trust policies. For example, we cannot simply reject a cross-domain access request if we cannot find a matching policy. After we discover the intention of that request, we may find it complies with another policy in a different format or a combination of several policies. This introduces fuzziness into federated trust management, because the intention of the request may be fuzzy, or the request itself may be fuzzy, or the policies to be enforced may be fuzzy. Applying fuzzy logic to trust management can help us handle uncertainty in a federated pervasive network environment.

2. Related work

Trust is a complex subject relating to belief in the honesty, trustfulness, competence, and reliability of an entity. In McKnight et al.'s "The Meanings of Trust" [7], the most tangible aspects of trust are trusting behavior and trusting intention. In the context of pervasive computing, trust is usually specified in terms of a relationship between a resource or service requester and a resource or service provider. Trust forms the basis for allowing a requester to use services or manipulate resources owned by a service provider, or it may influence a requester's decision to use a service or resource from a provider. So trust is an important factor in the decision-making process [8]. In many business relationships, trust is based on a combination of judgments or opinions from face-to-face meetings and recommendations of colleagues, friends, and business partners, which involve uncertainties.

Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC'06)
0-7695-2655-1/06 $20.00

Trust management can be considered as a collection of trusting behaviors, which includes capture, evaluation and enforcement of trusting intentions. After Blaze et al. introduced the trust management concept for the first time, they developed several systems with different emphases. These trust management systems are restricted to intra-domain trusting behavior or else only partially solve inter-domain trust related problems. It is these inter-domain problems that require further research in federated trust management systems.

Beth et al. [9] categorize the inter-domain trust relationships into two classes: direct trust and recommended trust. Based on the expectation for an entity being able to finish a task, the system can calculate the probability of whether the entity will finish the task based upon positive and negative experience, measure the trustworthiness using this probability, and create a formula for calculating a numeric value of the trustworthiness with a set of formulae. But this mechanism simplifies real life by modeling trustworthiness based only on probability, and equates subjectivity and uncertainty to randomness. Josang proposed a trust model based on subjective logic [10], which introduces the concepts of evidence space and opinion space to describe and measure trustworthiness. Based upon the Beta distribution function that describes the posteriori probability for binary events, the author calculates the trustworthiness for every possible event from every entity. Meanwhile, Josang defines a set of operators for the calculation of trustworthiness. Josang's model literally equates subjectivity and uncertainty to randomness also. But as a cognitive activity, the subjectivity and uncertainty of trust is mainly expressed in its fuzziness. How to model this fuzziness and apply this model to federated trust management is the problem.

In the following sections of this paper, we will identify different kinds of trust, find a suitable categorization for uncertainty from subjective judgment and indirect information sources, and represent uncertainty by fuzzy rules with a set of operations and derivation rules for decision-making and enforcement processes. We will also apply this fuzzy logic approach to a healthcare environment to handle uncertainties from real life. We assume that the authenticity of identities and the integrity of trust-related information can be guaranteed by the application itself, and this is outside the scope of this paper.

3. Classification of trust

3.1. Direct and indirect trust

To manage a collection of trust-related activities across domains, we need to understand trust itself. From different points of views, trust can be categorized into different classes. Following the categorization described by Beth et al. [9], we categorize trust into two classes - direct trust and indirect trust. A trust relationship formed from direct experience or negotiations can be characterized as direct trust; a trust relationship or a potential trust relationship built from recommendations by a trusted third party or a chain of trusted parties, which create a trust path, is called indirect trust. For example, suppose Dr. Jones needs to perform a clinical test, and she asks Dr. Smith for his advice about where to find a good hospital technician. Smith is thus directly trusted by Jones to know about a good technician and to provide his honest opinion. If in another scenario, Smith actually trusted the technician based on his own experience, but Jones thinks Smith knows little about that specific type of test, then Jones's trust of the recommended technician will not be so positive, because Jones's decision is based on fuzzy evidence. Figure 1 illustrates these two scenarios.

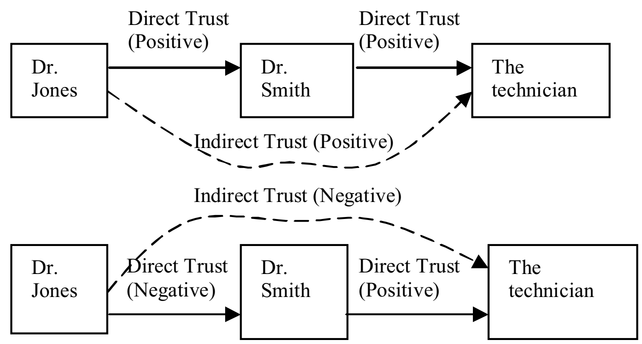

Figure 1. Direct Trust and Indirect Trust

3.2 Objective and subjective trust

From another point of view, trust is a concept everybody understands at some personal level, but for which it is difficult to provide a specific definition. Some people will have objective measures they use to evaluate their level of trust in an entity, while others rely on a more subjective feeling for determining whether to trust an entity. So trust can be either derived from one's belief/feeling or based on a measurement.

An entity's trustworthiness is associated with the quality of services it provides to others. If the quality of a service can be objectively measured, then the trust relationship relying on that service is objective. For example, in a telemedicine system the accuracy of a digital image provided by another healthcare provider can be indisputably checked against the original data. So the quality of that information service can be measured objectively, and the trust based on that information service is objective. For some other services, their quality cannot be objectively measured. For example, different doctors may have different opinions about the interpretation of certain digital images. That result is informed from the doctors' subjective judgments combined with their experience. It depends heavily upon each doctor's experience, intuition and other subjective factors. The trust relationships relying on those kinds of factors are subjective. Intuitively, if the quality of a service can be objectively measured, then an entity's

Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC'06)
0-7695-2655-1/06 $20.00 © 2006 IEEE

trustworthiness for that service reflects some intrinsic property of that entity. An entity's subjective trust, however, may vary greatly based on different sources of trust evaluation. Due to this variation, subjective trust is uncertain and needs special representations and enforcement processes.

4. Representation of uncertainty in trust

The trust relationships in pervasive computing environments are hard to assess due to the uncertainties involved. Figure 2 illustrates the comparison of different sources of uncertainties in federated trust management. If a trust relationship relies upon a subjective judgment based on indirect information, it will be very uncertain and any operations related to that trust relationship may cause unexpected results.

	Direct Information	Indirect Information
Objective Judgment	Certain	Uncertain
Subjective Judgment	Uncertain	Most uncertain

Figure 2. Comparison of Different Uncertainties

The theory of fuzzy logic extends the ontology of mathematical research to be a composite which leverages quality and quantity, and which contains certain fuzziness. Introducing fuzzy logic into the research of trust management, we try to solve the issues associated with uncertainty in federated trust management. First, we need to identify the subjects of those issues. These subjects are either the sources of trust-related information needed in federated trust management or the entities with which trust relationships are built. This subject set can be defined as follows.

Definition 4.1 Subjects in federated trust management
The set of subjects in federated trust management is all subjects that are either the sources of trust-related information or are the entities with which trust relationships are built. This set is represented as X *in this paper.*

Then we need to define a general fuzzy set in federated trust management.

Definition 4.2 Fuzzy set for federated trust management
For every element x in the set of subjects X, there is a mapping $x \mapsto \delta(x)$, *in which* $\delta(x) \in [0,1]$. *The set* $\Delta = \{(x, \delta(x))\}$ *for* $\forall x \in X$ *is defined as a fuzzy set for federated trust management.* $\delta(x)$ *is defined as the membership function for every* x *in* Δ.

All the fuzzy sets on X are represented as $Z(X)$. Then we can use a group of fuzzy sets from $Z(X)$ to group all the elements of X into several sets with different levels of uncertainty. For example, we can use a group of five sets $z_i \in Z(X)$ to categorize uncertainty in federated trust management. z_1 represents definitely uncertain; z_2 represents probably uncertain; z_3 represents equivocal; z_4 represents probably certain; z_5 represents definitely certain.

In real life, the level of uncertainty cannot be limited to only one set, and the degrees of these sets are not simply 'total' or 'none'; additionally, it is sometimes difficult to determine which set or sets should be used for certain kinds of uncertainty. In other words, these sets are not exclusive to each other. So when we deal with certain kinds of uncertainty, a vector consisting of the degrees of belongingness to each set $D=\{d_1,d_2,d_3,d_4,d_5\}$ is more appropriate for describing the actual judgment from daily life, in which $d_i(i=1,2,...,5)$ is the degree of belongingness to set $z_i(i=1,2,...,5)$. Meanwhile, there are several ways to determine or calculate the degrees d_i. One way is direct judgment that determines the degree from direct experience or evaluation. Another one is indirect inference that determines the degree via an analysis of an indirect source such as recommendations. The first one is relatively subjective while the evaluation method may be objective; the second one is relatively objective while the source of information may be subjective.

To reason among the degrees of uncertainty in federated trust management for further inference or decision-making, we need to represent uncertainty formally. Direct trust is formally described as $a \xrightarrow{D} b[Z]$, which means entity a is willing to rely upon entity b to degree *D* for the categorized uncertainty *Z*. *D* is a vector with corresponding degrees of belongingness for each set in categorization *Z*. Direct trust is from direct experience of the trustworthiness of the other entity or from a judgment with subjective/objective evaluation. Indirect trust is described as $a \overset{D}{\underset{P}{\rightarrow}} b[Z]$, which means entity a is willing to rely upon *b* to degree *D* following P's recommendation for the categorized uncertainty *Z*. P represents one or more entities constructing a path that gives a recommendation to entity a for entity *b*. *D* is a vector with corresponding degrees of belongingness for each set in categorization *Z*. Indirect trust is derived from the recommendation passed through one or more intermediate entities. There are also two types of recommendations. One type is that the recommender had direct experience with the recommended entity so that the P has only one entity; the other is that the final recommender formed the recommendation from further recommendations of other recommenders so that the P has more than one entity constructing a chained recommending path or a compound recommending graph.

But from the recommendee's (entity a's) point of view, there is no significance to the number of entities forming the recommending path; the recommendee (entity b) only cares about the final recommender's capability to make accurate recommendation based on its own experience and trustworthiness.

5. Fuzzy enforcement

5.1 Fuzzy operations and derivation rules

Zadeh operators $\wedge$ and $\vee$ are commonly used to perform calculation and analysis with fuzzy logic. But they are so imprecise that too much information will be lost. Thus several general class fuzzy operators are proposed. To adapt to different sources of uncertainties in federated trust management, parameterized general intersection and union operators are needed. With different values of the parameters, these operators can maximize the expressiveness and flexibility of the system to capture people's intentions for uncertainties. We choose Dubois-and-Prade operators [11] to perform calculation and analysis, which are suitable for policy analysis and have clear semantic meaning. Thus the intention embedded in fuzzy sets can be easily enforced.

Definition 5.1 T-norm

For fuzzy set $A, B \in Z(X)$ *and* $\alpha \in [0,1]$,

$$(A \cap B)(x) = T(A(x), B(x), \alpha) = \frac{A(x)B(x)}{\max\{A(x), B(x), \alpha\}},$$

in which $A(x)$ *and* $B(x)$ *represent* x *'s degrees of member function to fuzzy sets* A *and* B.

Definition 5.2 S-norm

For fuzzy set $A, B \in Z(X)$ *and* $\alpha \in [0,1]$,

$$(A \cup B)(x) = S(A(x), B(x), \alpha) = \frac{A(x) + B(x) - A(x)B(x) - \min\{A(x), B(x), (1-\alpha)\}}{\max\{1 - A(x), 1 - B(x), \alpha\}},$$

in which $A(x)$ *and* $B(x)$ *represent* x *'s degrees of member function to fuzzy sets* A *and* B.

Then we define two calculators on vectors of fuzzy values. Suppose we have two fuzzy value vectors $D_1 = \{d_{11}, d_{12}, ..., d_{1P}\}$ and $D_2 = \{d_{21}, d_{22}, ..., d_{2P}\}$.

Definition 5.3 Connection calculator

$$D_1 \otimes D_2 = \{T(d_{11}, d_{21}, \alpha), T(d_{12}, d_{22}, \alpha), ..., T(d_{1P}, d_{2P}, \alpha)\}$$

Definition 5.4 Union calculator

$$D_1 \oplus D_2 = \{S(d_{11}, d_{21}, \alpha), S(d_{12}, d_{22}, \alpha), ..., S(d_{1P}, d_{2P}, \alpha)\}$$

Then we define two sets of derivation rules (deduction rules and consensus rules) to handle different types of uncertainty from different trust relationships or recommenders. Deduction rules are used for a recommendation path to transfer trust from one end to the other end. For the trust relationships from the same categorization, deduction rules can form a new path using the trust relationship between the recommender and the recommendee and embed the content of that recommendation into the new path. Consensus rules combine multiple recommendations in the same kind of categorization. When two or more recommendation paths appear, consensus rules can synthesize the opinions to form a comprehensive recommendation.

Definition 5.5 Deduction rules

$$a \xrightarrow{D} b[Z] \wedge b \xrightarrow{D'} c[Z] \Rightarrow a \underset{P''}{\overset{D''}{\rightarrow}} c[Z] \wedge (P'' = \{b\}) \wedge (D'' = D \otimes D')$$

$$a \xrightarrow{D} b[Z] \wedge b \underset{P'}{\overset{D'}{\rightarrow}} c[Z] \Rightarrow a \underset{P''}{\overset{D''}{\rightarrow}} c[Z] \wedge (P'' = \{b, P'\}) \wedge (D'' = D \otimes D')$$

$$a \underset{P}{\overset{D}{\rightarrow}} b[Z] \wedge b \underset{P'}{\overset{D'}{\rightarrow}} c[Z] \Rightarrow a \underset{P''}{\overset{D''}{\rightarrow}} c[Z] \wedge (P'' = \{P, P'\}) \wedge (D'' = D \otimes D')$$

Definition 5.6 Consensus rules

$$a \xrightarrow{D_1} b[Z] \wedge a \xrightarrow{D_2} b[Z] \wedge ... \wedge a \xrightarrow{D_n} b[Z] \Rightarrow a \xrightarrow{D''} c[Z] \wedge (D'' = D_1 \oplus D_2 \oplus ... \oplus D_n)$$

$$a \underset{P_1}{\overset{D_1}{\rightarrow}} b[Z] \wedge a \underset{P_2}{\overset{D_2}{\rightarrow}} b[Z] \wedge ... \wedge a \underset{P_n}{\overset{D_n}{\rightarrow}} b[Z] \Rightarrow a \underset{P''}{\overset{D''}{\rightarrow}} c[Z] \wedge$$
$$(P'' = \{P_m \,|\, |P_m| = \min\{|P_i| (i = 1...n)\}\})$$
$$\wedge (D'' = D_1 \oplus D_2 \oplus ... \oplus D_n)$$

5.2 Decision-making process

With the help of the fuzzy operations and rules defined above, we can form a formal decision-making process to handle uncertainty in federated trust management. The diagram of the process is illustrated in figure 3. Users need to define the categorization for every type of uncertainty first. Then the decision-making process uses fuzzy operations to combine uncertain information from different sources. After defuzzification of the trustworthiness degrees, users need to judge whether the final degree is consistent with the users' intentions or comply with the practical application environment. If not, the parameters of the fuzzy operations need to be adjusted.

This decision-making process can solve the issues with uncertain information or judgment in federated trust management. For example, the diagnosis process for detecting uterine fibroids in diagnostic radiology needs to coordinate display of digital images from pervasive devices, response from doctor's analysis, and other activities across trust domains. If the network transmission is trustworthy, reading the digital image from pervasive devices still raises concerns about the device's location and the technical resolution of the sensor. Because of this indirect information, uncertainty is unavoidable. The doctor's response includes some level of fuzziness too, because the doctor's diagnosis is based on subjective judgment from medical knowledge, previous experience, and possibly additional test results. The categorization of uncertainty in section 4 is a practical response used in medical diagnoses [12]. Thus following the decision-making process, a medical diagnostic system can allow fuzzy input of indirect information and subjective judgment from different entities, combine fuzzy input, and reach a final decision for users. Further, this decision-making process can incorporate users' fuzzy definitions of policies into federated trust management systems to provide more expressiveness and flexibility.

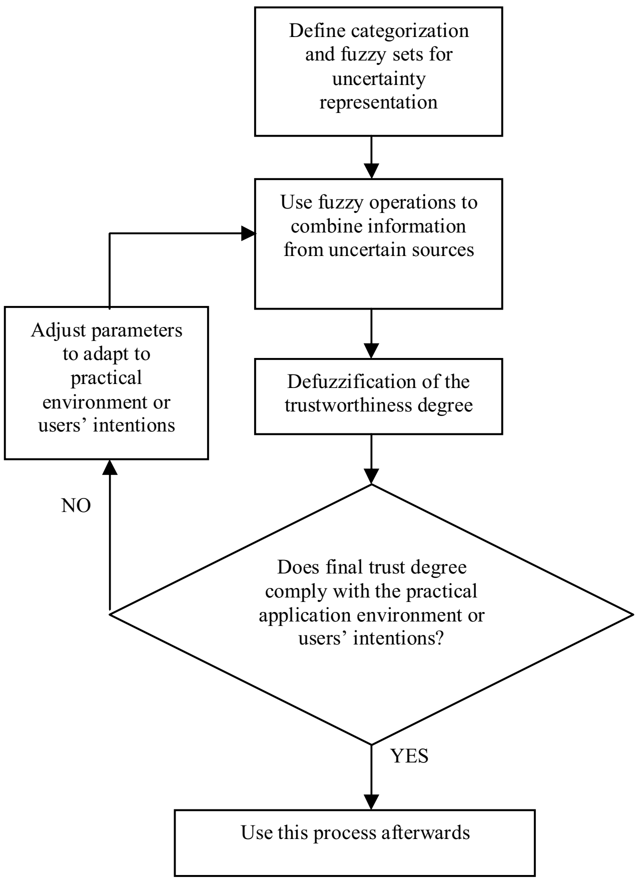

Figure 3. Decision-making Process for Uncertainty in Federated Trust Management

6. Case study: an application in healthcare environment

Following the example described above, we illustrate the practical fuzzy policies, the user interface to input fuzzy policies, and the enforcement mechanism to enforce these policies for a healthcare environment. Since the diagnosis of uterine fibroids involves both indirect information and subjective judgment, we have two sets of fuzzy policies to describe corresponding fuzzy rules. We also have a regular policy set without fuzziness. The fuzzy policy for indirect information is defined as "*The confidence level of the technical resolution or technician's skill at the remote sensor is high/medium/low.*" High, medium and low are membership functions describing levels of uncertainty. The fuzzy policies for subjective judgment are defined as "*The existence of focal fibroid tumors is definitely uncertain/probably-uncertain/equivocal/probably-certain/definitely-certain,*" "*If focal fibroid tumors are (probably/definitely) certain, more than one tumor is definitely-uncertain/probably-uncertain/equivocal/probably-certain/definitely-certain,*" "*If focal fibroid tumors are (probably/definitely) certain, their locations being within or bordering the endometrial canal is definitely-uncertain/probably-uncertain/equivocal/probably-certain/definitely-certain.*" Definitely-uncertain, probably-uncertain, equivocal, probably-certain and definitely-certain are membership functions too. And the overall policy is defined as "*If more than one focal fibroid tumor is within or bordering the endometrial canal, the patient needs a hysteroscopy (treatment).*"

Then we provide a user interface to assist doctors to input these policies consistent with the accurate rules from general medical practices and their intentions. We allow doctors to change the flexible parts in fuzzy policies such as 'more than one focal fibroid tumor' and 'within or bordering' according to diagnostic needs. Also, we provide default membership functions for all the fuzzy terms according to general medical practices. Meanwhile, doctors are allowed to modify all the membership functions if the default membership functions do not accurately capture the doctors' own rules or intentions. After doctors define new member functions, we visualize the curves of new membership functions to refine them step by step as a feedback mechanism.

Once the definitions of fuzzy polices are finally determined, we use a policy generator to translate the fuzzy policies into XACML [13] format, and store them in a policy database. Then once the digital images from pervasive devices are present and the doctor's judgment has been input, the system can tell the patient what treatment they will need using a web service interface. And the patient can use that service anytime, anywhere. Figure 4 illustrates the system architecture. The enforcement engine is triggered when a request from a patient is received, and it will use a fuzzy policy filter to go through the decision-making process to reach the final decision and recommendation for the patient.

With the help of fuzzy logic, cooperating pervasive devices and services can provide convenient healthcare services via a web interface or a telemedicine system with some level of uncertainty in input information and measurement. Meanwhile federation is needed if these devices and services are cross trust domains. Fuzzy logic can help handle uncertainty caused by indirect information and subjective judgment in trust management for these federated activities.

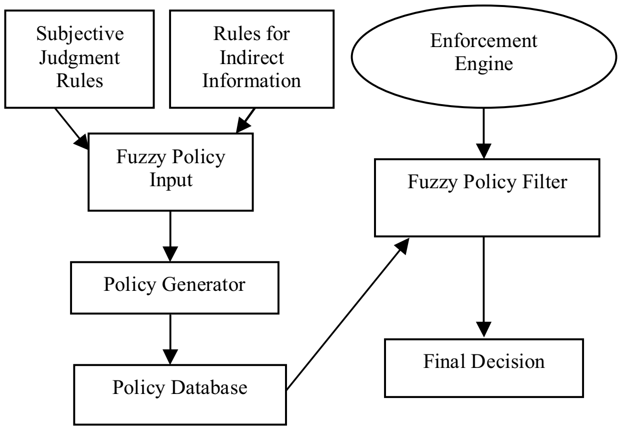

Figure 4. Application System Architecture

7. Conclusion

This paper proposes a model of uncertainty based on fuzzy logic to handle uncertainty and fuzziness in trust management. It also identifies different sources of uncertainty in trust management, and finds that this uncertainty cannot be treated as a probability and thus cannot be described by a probability model. Meanwhile a general categorization is described to capture various types of trust in practical application environments. In addition, the parameterized derivation rules make the system adapt better to actual application environments, which solves the inadequacies in the model proposed by Josang [10] and the model proposed by Beth et al. [9]. The model proposed in this paper can be used in evaluation, analysis and derivation of policies in trust management directly. As illustrated in section 6, application of this model in a healthcare environment can help doctors provide diagnosis policies online with pervasive computing devices for fast consultations.

8. References

[1] M. Blaze, J. Feigenbaum, and Jack Lacy, "Decentralized Trust Management", *Proc. of the 1996 IEEE Symposium on Security and Privacy*, 1996, pp. 164 -173.

[2] T. Grandison, "Trust Management for Internet Applications", PhD thesis, Imperial College London, 2003.

[3] N. Li and J. C. Mitchell, "Datalog with Constraints: A Foundation for Trust-management Languages", *Proc. of the Fifth International Symposium on Practical Aspects of Declarative Languages*, 2003, pp. 58 - 73.

[4] G. Caronni, "Walking the web of trust", *Proc. of 9th IEEE International Workshops on Enabling Technologies*, 2000, pp. 153 - 158.

[5] C. Duma, N. Shahmehri, and G. Caronni, "Dynamic trust metrics for peer-to-peer systems", *Proc. of 2nd IEEE Workshop on P2P Data Management, Security and Trust*, August 2005.

[6] S. J. Dwyer III, A. C. Weaver and K. K. Hughes, "Health Insurance Portability and Accountability Act," *Security Issues in the Digital Medical Enterprise*, Society for Computer Applications in Radiology, second edition, April 2004.

[7] D. Harrison McKnight and Norman L. Chervany, "The Meanings of Trust," *MISRC Working Papers Series*, 2000.

[8] D. W. Manchala, "Trust Metrics, Models and Protocols for Electronic Commerce Transactions," *18th International Conference on Distributed Computing Systems*, 1998.

[9] T. Beth, M. Borcherding, and B. Klein, "Valuation of Trust in Open Networks," *Proc. 1994 the European Symposium on Research in Security*, Springer-Verlag, 1994, pp. 3 – 18.

[10] A. Josang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, 2001, 9 (3), pp. 279 – 311.

[11] D. Dubois and H. Prade, "New results about properties ans semantics of fuzzy set theoretic operators," *Fuzzy sets: theory and applications to policy analysis and information systems*, Plenum, New York, 1980, pp. 59-75.

[12] G.. A. DeAngelis, et al., "Diagnosis efficacy of compressed digitized real-time sonography of uterine fibroids," *Academic Radiology*, Volume 4, Number 2, February 1997, pp. 83-90.

[13] OASIS standard, "eXtensible Access Control Markup Language (XACML) Version 2.0", http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

0-7695-2655-1/06 $20.00

IEEE COMPUTER SOCIETY