Decision Theory based Auto-delegation (DTA-d) scheme for Ubiquitous Computing

Priyanka N. Kamble, Parikshit N. Mahalle
Department of Computer Engineering,
STES's Smt. Kashibai Navale College of Engineering,
Pune – 411041, India

ABSTRACT

Access control is a fundamental and essential mechanism to maintain security in ubiquitous computing (UbiComp). Flexibility is an important property for general access control system, which can be achieved by access or authority delegation. Existing delegation mechanisms are "subject-centered", thus in order to make sure that the unavailability of some users does not prevent the system to be functional; auto-delegation mechanisms are introduced, in particular for emergency-prone environments, such as healthcare, military systems auto-delegation mechanisms are required. Auto-delegation mechanism combines the strengths of delegation systems and "break-the-glass" policies, by stating that the most qualified available user for a resource can access this resource. Further this work is extended by considering availability as a quantitative measure, such that each user is associated with a probability of availability.

The main contribution of this paper is to present decision theory based auto-delegation scheme (DTA-d) for UbiComp. UbiComp poses new security challenges while the information can be accessed anywhere and anytime, hence the access control is required to maintain the security in UbiComp, but along with the strong access control, auto-delegation is also necessary to provide flexibility. While performing the auto-delegation, numbers of alternatives are available, among these alternatives selecting one as best is the important issue and this is addressed in this paper. Decision theory is used to select the best alternative when numbers of alternatives are available and their consequences cannot be forecast with certainty. Using Bayesian decision theory and by applying bays rule access is granted or denied for particular subject to object.

Keywords

Access Control, Ubiquitous Computing, auto-delegation, Decision theory.

1. INTRODUCTION

Access control is the process that decides who is authorized to have what access rights on which object with respect to some security models and policy. It is a fundamental and essential mechanism to maintain security in computer system. An *access control system* is a mechanism that grants or denies requests made by active entities, the *subjects*, to access some passive entities, the *objects* [1]. An access control system consists of two parts: an access control policy and a reference monitor. The access control policy defines which access requests should be granted and which should be denied. The reference monitor intercepts access requests and matching them against the policy. An access control system intercepts any access request made by subject to object in order to decide if an access should be allowed or denied. But in some situations, subjects who have access to a critical object may be unavailable. In such situations restricting access to the object leads to a potentially life-threatening. To overcome such problems delegation mechanism is introduced.

Delegation is a widely used mechanism in access control system. Delegation enables an authorized entity to nominate another entity as its authorized proxy for the purpose of access control [1]. Delegation is an approach that an entity provides all or some of its privileges or rights to other entities. This is considered a useful and effective method to enhance the scalability of a distributed system and decentralize access control tasks. There are two types of users in delegation: delegator and delegatee. A delegator is a user that has privileges to access his or her identity information and to delegate the privileges and delegatee is a user that is provided privileges by a delegator to access the delegator's identity information. A delegator and a delegatee have a prior trust relationship. Existing delegation mechanisms defines manual process of delegation which is initiated by end-users. But the system in which the set of available, authorized subjects fluctuates unpredictably over time requires delegation mechanisms that can respond automatically in the unavailability of appropriately authorized users. Such systems are defined in [1] and [2]. Both have studied about availability of subject.

In current work we provide auto-delegation mechanism for UbiComp (DTA-d). UbiComp is a post-desktop model of human computer interaction in which information processing has been thoroughly integrated into everyday objects and activities. UbiComp is way of integrating computers seamlessly into the world and is also called as pervasive/invisible computing. The purpose of ubiquitous computing is anywhere and anytime access to information within computing infrastructures that is blended into a background and no longer be reminded [3]. Here decision theory is used to select the best alternative when numbers of alternatives are available. Decision theory is theory about decisions [4]. It deals with the methods for determining the optimal course of action when numbers of alternatives are available and their consequences cannot be forecast with certainty. It represents the general approach to decision making. Bayesian Decision Theory is a fundamental statistical approach that quantifies the tradeoffs between various decisions using probabilities and costs that accompany such decisions. Access is granted or denied for particular subject to object by applying bays rule. Bayes decision rule gives method for minimizing the overall risk. The healthcare system is presented as example of this approach. In this process first find out the various attributes of available subject required for comparing them and finally select one of the best available subjects as delegatee. Further categorize them into three types as ideal, average and worst. Each category has attribute value defined for it. And by assigning priorities to defined attribute results are evaluated.

2. MOTIVATION

Consider the scenario of Health care system shown in figure 1, senior attending surgeon is the authorized user of system. He has authorized access to electronic patient record. Now consider the situation where this electronic patient record required for curing a person who is having a heart attack, in the unavailability of senior attending surgeon. In this case other attending surgeon or nurse should have access to electronic patient record so that they can proceed for the treatment of patient. While allowing access to other attending surgeons or nurse to the electronic patient record security parameters should be considered and access should be provided with privacy-preserving manner. Here senior attending surgeon performs auto-delegation to overcome such life-threatening situations where access to a critical object is required when he is unavailable.

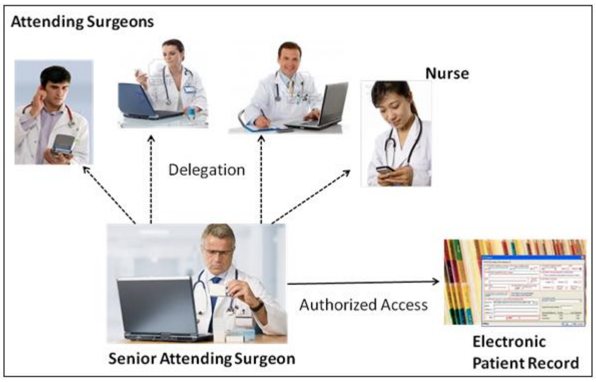

Fig 1: Motivation Scenario

As shown in figure 1, there are three attending surgeons and a nurse is available. So the question arises whom to give access to electronic patient record, whom to choose as delegatee while performing auto-delegation. The delegatee should be selected with considering all the necessary parameters, such as here the one who is going to access electronic patient record must be able to treat the patient correctly and carefully. He must have experience and knowledge of treatment.

The proposed DTA-d framework provides solution to this problem or such types of problems using the decision theory by considering all alternative.

3. RELATED WORKS

The problem of defining a powerful-enough access control system has been identified [5] and since then several well-known policies and systems have been proposed. Examples of access control models are the discretionary model [5, 6], used in operating systems; the Bell-LaPadula model [7], used in a military environment; the Chinese wall model [6], used in the consulting world; and more recently-proposed the Role-Based (RBAC) model [8], used in databases and business information systems.

These models focused on subjects, policy in this model describes which objects a subject can access. Usually, such policy defines a decision about the access for a subject independently from the other subjects [2]. For instance, in a health-care system, a nurse cannot access a medical record regardless of the fact that a physician can or cannot access this medical record. Although this independence property makes sense in the general case, in some situations, subjects who have access to a critical object may be unavailable. In such situations the object cannot be accessed by anyone and this limitation of the access control system leads to a potentially life-threatening situation [2]. An example could be a patient record required for curing a person who is having an heart attack or essential military intelligence report when it is unknown if the responsible officer is alive or not.

Hence, in such life-threatening situations, there is a need to provide the access control mechanism with the possibility of granting an access that was not originally allowed. Two main approaches exist to address this need: "break-the-glass" policies [9, 10] and the enforcement of delegations [11].

3.1 Break-the-glass Policy

"break-the-glass" policies [9, 10] grant access to any subject in case of emergency. These policies do not take into account the existence or availability of qualified subjects; instead they extend the set of authorized accesses for the duration of then emergency, therefore possibly allowing a (normally) unauthorized subject to access an object, even though authorized subjects are available. Thus, a poorly qualified subject may get access to a critical object.

3.2 Delegation Mechanism

The second approach is to use a delegation mechanism [11]: when a subject cannot access an authorized resource, he can delegate her right to do so to another subject. Such an approach requires the delegation to be activated beforehand; that is, a subject must know when she will be unavailable in order to delegate her rights at this time. However, in some situations, the unavailability of a subject can be unexpected, for instance a subject getting injured or killed on a battlefield. The main drawback of delegations is that they need to be activated beforehand, and they are not suitable in case of unexpected unavailability.

3.3 The auto-delegation mechanism for access control system

To overcome the drawback of previous two techniques Crampton and Morisset [1] introduced an automatic delegation mechanism (ADM), which is "object-centered": an object can be accessed by one of the most qualified subject available. Consider $S = \{s_1, s_2, \cdot\cdot\cdot, s_n\}$ for the set of subjects, $O = \{o_1, o_2, \cdot\cdot\cdot, o_m\}$ for the set of objects. An *access* is a pair (s, o), meaning that the subject s accesses the object o. The availability of the subjects is considered to be always decidable, and, therefore, the authors introduced a set $Av(S) \subseteq S$, such that a subject is available if and only if, it belongs to $Av(S)$. Each object $o \in O$ is associated with a qualification hierarchy $(Q(o), \leq_o)$, and each subject is associated with a qualification through a function $\lambda_o : S \rightarrow Q(o)$, such that $\lambda_o(s)$ denotes the qualification level of s, with respect to o. Given two subjects s_1 and s_2, $\lambda_o(s_1) \leq_o \lambda_o(s_2)$ means that s_2 is more qualified than s_1 to access o. Note that the relation $\leq_o$ is a partial-order, and therefore two qualifications might not be comparable. Finally, an authorization function $Auth_{adm}$ is given, such that given $\leq_o$, $Av(S)$, and an access request (s, o), $Auth_{adm}(\leq_o, Av(S), (s, o))$ returns allow if (s, o) is authorized according to the auto-delegation mechanism, and deny otherwise. More precisely,

$$Auth_{adm}(\leq, A_v(S), (s, o, a))$$

$$= \begin{cases} deny\ \ if\ there\ exists\ s' \in Av(S) \text{ such that } \lambda(s) < \lambda(s') \\ allow \quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad otherwise \end{cases}$$

In other words, a request by s to access o is allowed if s is one of the most qualified of the available subjects (and denied otherwise). The auto-delegation mechanism can be either used as a standalone policy, for instance in the context of resource management, or as a combination with another policy. In the latter case, the auto-delegation mechanism is consulted only if the "normal" policy denies the access. If a process is one of the most qualified processes and becomes unavailable, all of its children can access the object. Thus they defined the notion of availability as a Boolean notion: a user is either available or she is not. In practice, the availability of a user can depend on many parameters, such as her localisation, her level of commitment for other tasks, etc. Thus, availability can be only estimated with some uncertainty. Refer to [1] for a more detailed presentation.

3.4 Auto-delegation for Probabilistic Availability

To overcome the limitation of [1] further the work is extended in [2] they assumed a level of uncertainty for availability of users to be a quantitative value (probability of availability), and proposed a quantitative approach to the problem of auto-delegation. Whether an access should be granted to a user is decided according to the probability that a more qualified user is available. Usually availability of a subject is considered as a zero-one value, i.e. a subject is either available or not. But sometimes incomplete information about the availability of a subject is available and can only speak about it with some degree of certainty. For example, a doctor may be in a hospital but working on a different floor of the building. Thus another subject with certain availability but lower qualification can get an access to an object (e.g. patient medical record) while the availability of more qualified subject is uncertain. Uncertainty is usually expressed with probability [2]. Probability that a person is available could be simply assigned by an analyst, could be derived out of statistics, could be computed, etc. An example of how the probability is computed can be found in the work of Krautsevich et. al. [12,13]. In this position and movement of a subject modelled with a Markov chain. States (nodes) of the markov chain represent possible spatial positions of the subject. Edges of the markov chain represent possible transitions between the states. Transition probabilities, taken from the analysis of historical data, are assigned to every edge. Knowing the position of a subject at some point of time in the past the probability that the subject is in a specific location (available) at the current moment of time is computed.

In [2] provided very abstract and general model of access control under uncertainty. When there is no uncertainty on the information, then the decision making is straight-forward. However, when there is some uncertainty over the information present in the state, the decision process is more complex, as it is possible to make some errors. For instance, consider a simple policy when an access *a* is allowed if, and only if a parameter *x* is *true*. If the value of *x* is available with certainty, then the decision making simply consists in checking this value, and allowing or denying the access *a* accordingly. On the contrary, if there is an uncertainty over the value of *x*, then four different decisions are available.

1. A *true-positive* is an access correctly allowed. For instance, allow the access *a* and the value of *x* is *true*.

2. A *true-negative* is an access correctly denied. For instance, denied the access *a* and the value of *x* is *false*.

3. A *false-positive* is an access wrongly allowed. For instance, allow the access *a* and the value of *x* is *false*.

4. A *false-negative* is an access wrongly denied. For instance, deny the access *a* and the value of *x* is *true*.

System allowing every access has a high *gain*, but at the same time it leads to high *damage*. So there is always the right balance between being too strict and being too lax. More precisely utility functions are defined to measure gain and damage of system. It is always possible to compare two or more different utility values and to pick the "best" value. Moreover, the qualification hierarchy for each object needs to be consistent with the utility: intuitively, if a subject s_1 is more qualified than a subject s_2 to access an object *o*, then the utility of the access (s_1, *o*) is better than the utility of (s_2, *o*). Four utility functions C^{TP} , C^{FN}, C^{FP}, and C^{TN} for these respective outcomes, such that, according to decision theory [4], the access should be granted only if following Equation holds.

$$C^{TP} + C^{FP} > C^{TN} + C^{FN}$$

The main drawback of this approach is the lack of precise utility, gain and/or damage measures for real-world applications.

Further Access control management for ubiquitous computing is defined in [3]. UbiComp poses new security challenges while the information can be accessed anywhere and anytime because it may be applied by criminal users. Additionally, the information may contain private information that cannot be shared by all user communities. The heterogeneous devices and mobile users in such dynamic pervasive computing environments make security management difficult, especially the access to authorized users since it is a basic security requirement for guaranteeing user's privacy, information confidentiality, integrity and availability. Several approaches are developed to protect information for pervasive environments against malicious users. In this paper, they present a usage control model to protect services and devices in ubiquitous computing environments, which allows the access restrictions directly on services and object documents. Usage control is considered as the next generation access model. There are eight components: subjects, subject attributes, objects, object attributes, rights, authorizations, obligations, and conditions in usage control model. The basic concept in usage control is the access right to an object, which is called usage. Users are assigned usage when they enter a special space of ubiquitous computing environments, and access policies for services in the space are generated by assigning access rights to users. Users who want to access the space have their accounts created by system administrators and are assigned a usage of access space objects based on their rights and responsibilities within the space. When a user with a usage enters to a space, the user is automatically assigned a space object, which is restricted to a set of rights that make sense within the space. They defined the Authorization models for space objects adopting usage control based on three decision factors: authorizations, obligations, and conditions. The model not only supports complex constraints for pervasive computing, such as services, devices and data types but also provides a mechanism to build rich reuse relationships between models and objects. This paper provides the ongoing continuity for authorizations, obligations and conditions. These methods can be used to control objects in a dynamic environment since they provide a robust access control for ubiquitous computing environments and can protect sensitive messages from dissemination.

An architectural model for contextual-based delegation access control for pervasive computing is presented in [14], particularly access control mechanisms for ad hoc coalition scenarios. A “coalition” is defined as “an alliance of distinct parties, persons, or states for a joint action”. Coalition access control encompasses control mechanisms dealing with access between multiple heterogeneous entities from different security domains. For pervasive computing these coalitions are formed in an ad hoc manner and need to be sensitive to the context of the participating entities. An architecture model called the SIP Session-based Coalition Access Control Architecture (SCACA) is presented that extends the SIP signalling model in order to support long distance delegation access control. Users develop ad hoc coalitions that are formed over pervasive computing mediums like Instant Messaging (IM), phone calls, multimedia conferences. During the conference, each caller wishes to share his/her services as well as services that belong to their organization with others participants. This challenging problem is addressed by developing a contextual-based delegation model and architecture that supports this model in order to facilitate ad hoc coalition access control. The dRBAC model [15] has been chosen by the authors for the basis of extending it to support contextual information. It requires a low administrative overhead since there is minimal involvement of administrative personnel in the delegation action. It also leverages the common RBAC access control model. The dRBAC model implements access control for a multi-party coalition application through delegation. The Session-based Coalition Access Control Architecture (SCACA) is designed to provide security and access control in a distributed system. The main features of SCACA are that it supports session oriented access control, dynamic delegation and context-aware computing. This paper uses the Delegation and activity context information to minimize the amount of administration overhead and facilitate access control in ad hoc and pervasive coalition environments. A secure, scalable, and dynamic coalition access control infrastructure, the Session-based Coalition Access Control Architecture (SCACA) is given and was evaluated by implementing a two-party conference scenario.

By comparing all this techniques we can say that delegation mechanism is required to get access on critical object, in case of emergency. Traditional delegation mechanisms [11] require a subject to explicitly delegate some rights. Further “break-the-glass” policy [9, 10] possibly allows unauthorized subject to access an object, even though authorized subjects are available. Auto-delegation mechanism defined in [1] combines the strengths of delegation systems and “break-the-glass” policies, by stating that the most qualified available user for a resource can access this resource. Further this work is extended by considering the uncertain availability of subject [2]. The decision to allow or deny an access is based on the utility of each outcome and on a risk strategy. The main drawback this approach is the lack of precise utility, gain and/or damage measures for real-world applications and also the utility function defined is context-dependant.

In this paper DTA-d scheme provides auto-delegation for UbiComp and for that decision theory is used. It is the theory about decision making. Bayesian decision theory quantifies the tradeoffs between various decisions using probability and the costs that accompany such decisions. And also bayes decision rule which gives method for minimizing the overall risk.

4. PROPOSED WORK

This section presents an approach to perform auto-delegation in UbiComp. The decision theory is used which provides general approach to decision making. It deals with the methods for determining the optimal course of action when numbers of alternatives are available and their consequences cannot be forecast with certainty. This paper provides DTA-d framework in which all available information is used to deduce which of the decision alternatives is best. Consider the figure 2, in which subject 1 has authorized access to object 1 and there are two more subjects are available subject 2 and subject 3.

For instance, if subject 1 wants to perform delegation so that in case of emergency when he is unavailable, object can be accessed by other subject to complete the task, then he has two alternatives available.

To choose best alternative decision theory is used. Bayesian decision theory is used, which is a fundamental statistical approach that quantifies the tradeoffs between various decisions using probabilities and costs that accompany such decisions.

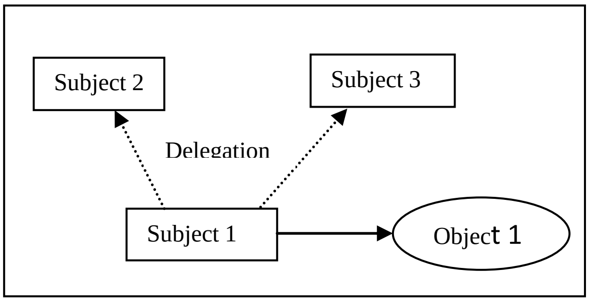

Fig 2: General scenario

Assumptions made in Bayesian decision theory:

1. Decision problem is posed in probabilistic terms.
2. All relevant probability values are known.

Bayesian decision theory defines the progression of decision rules as follows:

1) Decide based on prior probabilities
2) Decide based on posterior probabilities
3) Decide based on risk

Applying this decision rules to the above scenario
Let, S= Set of available subject
S_1 = Subject 1
S_2 = Subject 2
$P(S_1)$ = prior probability that Subject 1 is the best delegatee
$P(S_2)$ = prior probability that Subject 2 is the best delegatee

1. Decide based on prior probabilities

It is based on prior information:

$$Decide\ (Subject) = \begin{cases} s_1 & P(s_1) > P(s_2) \\ s_2 & otherwise \end{cases}$$

Probability of error for this decision is given as

$$P(error) = min[P(S_1), P(S_2)]$$

2. Decide based on posterior probabilities

For posterior probabilities collect data about individual subject. Here consider experience of subject, denoted *x*, to improve decision making by applying bayes rule combine data and prior information. Bays rule is used to convert priori probability to posterior probability.
By using Class-Conditional probabilities

$P(x \mid S_1)$ = probability of experience given subject 1

P(x | S_2) = probability of experience given subject 2

$$P(S_i|\, x) = \frac{P(x \mid S_i)\, P(S_i)}{P(x)}$$

Thus decision is given by,

Decide (Subject) = $\begin{cases} s_1 & P(s_1|x) \ > \ P(s_2|x) \\ s_2 & \quad otherwise \end{cases}$

Probability of error for this decision is given as

P (error) = min [P (S_1|x), P (S_2|x)]

3. Decide based on risk

L (a_i | w_j) = loss incurred when take action a_i and the true state of the world is w_j

Expected loss (or conditional risk) when taking action a_i:

$$R(a_i|x) = \sum_j L(a_i|w_j)P(w_j|x)$$

4.1 Proposed DTA-d Framework

This section presents the proposed DTA-d framework. As shown in figure 3, the framework defines the different steps to perform auto-delegation in UbiComp. There are six steps to select the appropriate subject as delegatee. In first step identify the problem is that there are number of subjects present, out of which one will selected as delegatee. The next step is collection of data that is the credentials of available subjects. In this step find out the attribute by which comparing of subjects is possible and also the benefits and risk associated with each subject. In third step produce the possible solution to this approach. These are nothing but designed profiles which contain the different profiles like ideal, average and worst, referred as training data set. Each has different value of attribute and by matching to this profile with available subject one is selected as delegatee. For example first of all search for best profile that is ideal, if it is present then this subject is selected and if it is not present then go for average profile and likewise. The next important step is evaluation of system using BDT that is Bayesian decision theory. A general mathematical model is presented and probability set for training data set is calculated. In the next step priority to attribute is assigned which are identified in second step. By assigning and changing the priority results are measured. The last step is to select one of the subjects as delegatee by comparing the result of previous step. After selecting the delegatee, the last step is to perform the access control. This is the capability based access control (CBAC) in which capability associated with subject is used to decide whether the subject is authorized user of system or not. A capability is a token or key that gives possessor permission to access an entity or object in a computer system. By CBAC access is granted or denied to subject.

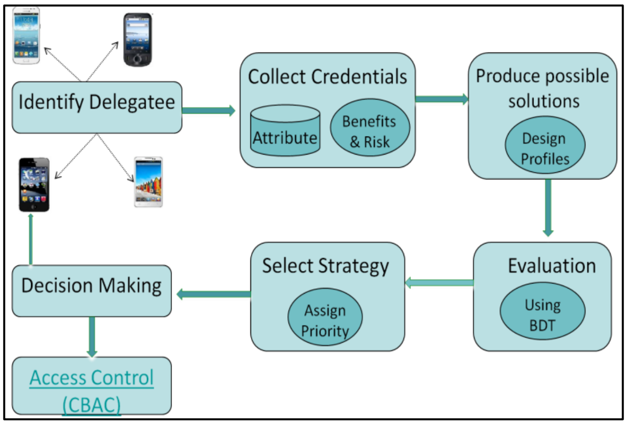

Fig 3: Proposed DTA-d framework

4.2 Case Study: Health Care System

Consider the scenario of health care system where *physician* wants to perform auto-delegation, five steps to perform auto-delegation:

1. Identification of the problem

In this first step identify the problem, in given scenario senior attending physician wants to perform auto-delegation so that when he is unavailable another subject can perform the task required in case of emergency. For example, *nurse* or *attending physician* must have access to the patient record required for curing a person who is having a heart attack, in the unavailability of *senior attending physician*. But further there is problem associated with whom to give access to patient record if more than one attending physicians are available. Figure 1 of Motivation section gives the idea about this scenario.

2. Obtaining necessary information

To choose the best alternatives obtain the necessary information about each alternative, then select best alternative by comparing benefits and risk associated with each alternative. Here consider lots of attributes to categorize them into specific priority group. For given scenario consider attributes like experience, specialty, previous risk handled or created, history records which helps to choose them as delegatee. For example, consider Table 1.

Table 1: Credentials of alternatives

Attribute	**Attending Physician**	**Attending Physician**	**Nurse**
Experience	2 years	2 years	1 year
Specialty	Heart	Pathologist	-
Risk Handled	4 times	3 times	2 times
Risk Created	2 times	2 times	1 time

3. Production of possible solutions

As Bays rule, first assumes that all probabilities are known, and then create ideal subject profile as training data set. This ideal profile has attribute value that required being present in delegatee. Similarly average and worst subject profiles are created. By comparing to this profile select one of the best delegatee. First of all search for the ideal profile if it found in system, then this is chosen as delegatee. If not available then go for the average profile and likewise. Consider the Table 2 for more detail.

Table 2: Training data set (profiles)

Attribute	**Attending Physician**	**Attending Physician**	**Nurse**
Experience	4 years	3 years	1 year
Specialty	Heart	Pathologist	-
Risk Handled	4 times	2 times	1 time
Risk Created	1 time	2 times	4 times

4. Evaluation of such solutions

In this step, use the Bayesian decision theory to evaluate system. A general mathematical model for a wide-range of situations is presented and scenario-specific examples with exact equations are also provided.

Here decide probability sets and sample space that is the training data set or predicted profiles of possible delegate.

5. Selection of a strategy for performance

Here calculate possible solutions by setting priorities to attributes found in second step. And by comparing them get best alternative. In given scenario, assign priority to attribute like risk handle by the attending surgeon has higher priority than the experience he has. Similarly for each attribute some priority is assigned and results are measured.

5. CONCLUSIONS AND FUTURE WORK

In this paper we have presented an auto-delegation scheme for UbiComp. UbiComp poses new security challenges while the information can be accessed anywhere and anytime because it may be applied by criminal users, hence the access control is required to maintain the security in UbiComp, but along with the strong access control, flexibility is also important. To provide flexible access control, auto-delegation is necessary. Further while performing the auto-delegation, numbers of alternative is available in the system, among these alternatives selecting one as best is the important issue. For that decision theory is used and presented an approach for making delegation decisions when more than one subjects are available to act as delegatee, here Bayesian Decision Theory is used to select appropriate subject as delegatee. It is a fundamental statistical approach that quantifies the tradeoffs between various decisions using probabilities and costs that accompany such decisions. Access to object is granted or denied by comparing the information about the subjects which are currently available. Various attributes are identified and compared for decision making. Results are evaluated by considering priorities of attribute, using Bayesian Decision Theory. And, also Bayes decision rule is applied to minimize the overall risk. In case study, Health care system is considered as example of this approach.

Future work includes the implementation of the DTA-d framework for UbiComp.

6. REFERENCES

[1] Crampton, J., Morisset, C.: An Auto-delegation Mechanism for Access Control Systems. In: Cuellar, J., Lopez, J., Barthe, G., Pretschner, A. (eds.) STM 2010. LNCS, vol. 6710, pp. 1–16. Springer, Heidelberg (2011)

[2] Leanid Krautsevich1, Fabio Martinelli2, Charles Morisset2, and Artsiom Yautsiukhin2, Risk-Based Auto-delegation for Probabilistic Availability *, J. Garcia-Alfaro et al. (Eds.): DPM 2011 and SETOP 2011, LNCS 7122, pp. 206–220, 2012. Springer-Verlag Berlin Heidelberg 2012.

[3] Wang, Hua, Yanchun Zhang, and Jinli Cao. "Access control management for ubiquitous computing." Future Generation Computer Systems 24.8 (2008): 870-878.

[4] Hanson, S.O.: Decision theory: A brief introduction (August 1994)

[5] Lampson, B.: Protection. In: Proceedings of the 5th Annual Princeton Conference on Information Sciences and Systems, pp. 437–443. Princeton University (1971)

[6] Harrison, M.A., Ruzzo, W.L., Ullman, J.D.: Protection in operating systems. Communications of the ACM 19(8), 461–471 (1976)

[7] LaPadula, L.J., Bell, D.E.: Secure Computer Systems: A Mathematical Model. Journal of Computer Security 4, 239–263 (1996)

[8] Ferraiolo, D.F., Kuhn, D.R.: Role-based access control. In: Proceedings of the 15th National Computer Security Conference, pp. 554–563 (1992)

[9] Ardagna, C.A., De Capitani di Vimercati, S., Grandison, T., Jajodia, S., Samarati, P.: Regulating Exceptions in Healthcare Using Policy Spaces. In: Atluri, V. (ed.) DAS 2008. LNCS, vol. 5094, pp. 254–267. Springer, Heidelberg (2008)

[10] Wainer, J., Barthelmess, P., Kumar, A.: W-RBAC - a workflow security model incorporating controlled overriding of constraints. International Journal of Cooperative Information Systems 12, 455–485 (2003)

[11] Chander, A., Mitchell, J.C., Dean, D.: A state-transition model of trust management and access control. In: Proceedings of the 14th IEEE Computer Security Foundations Workshop, pp. 27-43. IEEE Computer Society Press, Los Alamitos(2001).

[12] Krautsevich, L., Lazouski, A., Martinelli, F.,Yautsiukhin, A.: Influence of Attribute Freshness on Decision Making in Usage Control. In: Cuellar, J., Lopez, J.,Barthe, G., Pretschner, A. (eds.) STM 2010. LNCS, vol. 6710, pp. 35–50. Springer,Heidelberg (2011)

[13] Krautsevich, L., Lazouski, A., Martinelli, F.,Yautsiukhin, A.: Risk-aware usage decision making in highly dynamic systems. In: Proceedings of the Fifth International Conference on Internet Monitoring and Protection. IEEE (2010)

[14] Liscano, Ramiro, and Kaining Wang. "A context-based delegation access control model for pervasive computing." Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on. Vol. 2. IEEE, 2007.

[15] E. Freudenthal, T. Pesin, L. Port, and E. Keenan, “dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments”, In 22nd Int. Conf. on Distributed Computing Systems (ICDCS '02), pp. 411-420, IEEE, July 2002.