Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Trust-Based Access Control in Ubiquitous Computing (TAC-Ubicomp): A Decision Theory Approach

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

Abstract— Decision Theory based Auto-delegation (DTA-d) scheme for ubiquitous computing is presented in previous work. Ubiquitous computing requires strong access control as computing can be take place anywhere, anytime and by using any device. Accompanying the powerful access control, delegation is also being in need of UbiComp. To make the system to be active and working all the time, auto- delegation is the foremost thing. DTA-d defines such an effective and systematic scheme using decision theory. When any of the users is absent in the system, decision theory selects the best user from the available users; in place of absent user temporarily. Further, Instead of providing all the access rights of delegator to delegatee, Trust Based Access Control (TBAC) is implemented. According to the trust of delegatee, access rights are delegated.

This paper presents Trust-based Access Control in Ubiquitous Computing (TAC-UbiComp). The computative process to calculate trust of the user is defined. The algorithm to implement TAC-UbiComp system is given as well. This paper also proposes TAC-UbiComp framework with decision theory and TBAC.

Keywords— TAC-UbiComp, DTA-d, UbiComp, auto-delegation, TBAC

I. INTRODUCTION

Ubiquitous Computing (UbiComp) is a post-desktop model of human computer interaction in which information processing has been thoroughly integrated into everyday objects and activities [1]. UbiComp is way of integrating computers seamlessly into the world and is also called as pervasive/invisible computing. 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 [1]. It is technique of defining who can perform what type of operation on which resource. It provides security to the system by allowing authorized access only. At some point, this strong access control let down the system from the working continuously. When authorized user of the system is not available, for that time system becomes inoperative. To overcome such a break downs of system and making it continues working, Delegation mechanisms are introduced. By delegation process, access rights of one user can be delegated to the other user. The user who is going to delegate the access rights is known as Delegator. And the user who is going to receive the access rights of absent user is known as Delegatee. This process of delegating the privileges is known as Delegation. Delegation is performed temporary until the resurgence of the absent user in the system. After returning of delegator, reverse delegation is performed to cause the system to come to initial stage. Reverse delegation is process of withdrawing the access rights of delegatee which are previously delegated by delegator. Delegator come to have access rights when come backs in the system.

DTA-d scheme is Decision Theory based Auto-delegation scheme for ubiquitous computing, which performs auto delegation using decision theory [1]. It selects best delegatee in place of delegator temporary using decision theory. Decision theory is the theory regarding decision. It performs in satisfactory way to select one alternative when numbers of alternatives are available. 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 [1, 2]. It provides decision making for the set of alternative by selecting one best. Decision making is performed in two steps, first one is prior probability analysis and second one is posterior probability analysis.

Trust based access control is performed, after finding the delegatee. Trust provides device with a natural way of judging other device similar to how we have been handling security and access control in human society [3]. Trust between two devices decides the way of working with each other. Trust value of user indicates how much a user is capable of accepting responsibility. When devices trust each other, they prefer to share services and resources at certain extent [3]. Only the trusted devices have authorized access to system.

In this paper mathematical model is presented for TAC-UbiComp. Algorithm to implement TAC-UbiComp is also given. The overall working of DTA-d is defined using framework. The user is termed as device or subject in the following sections.

II. MOTIVATION

Consider the scenario of database management system users for understanding the need of auto-delegation scheme. Database system involves numbers of different users who processes the client request at the different level. Database administration is not one-person job; it is divided among different users. As shown figure 1, db_owner performs all the configuration and maintenance activities on the database. db_securityadmin can manages permissions and modify role membership. db_accessadmin can add or remove access to the database SQL server logins and windows login. db_backupoperator can back up the database. db_reader can read all the data from all user tables. db_writer can add, delete or update data in all user tables. When client request for any operation, request goes to appropriate DB user. Suppose there is request comes for maintenance such as update statistic task, request goes to the db_owner; which currently not available in the system to process the request. In such a scenario, system is unable to produce response. To prevent the system from letdown, auto-delegation mechanism is required. Auto-delegation process enables the other user act like an absent user for a while, to process the arrived request.

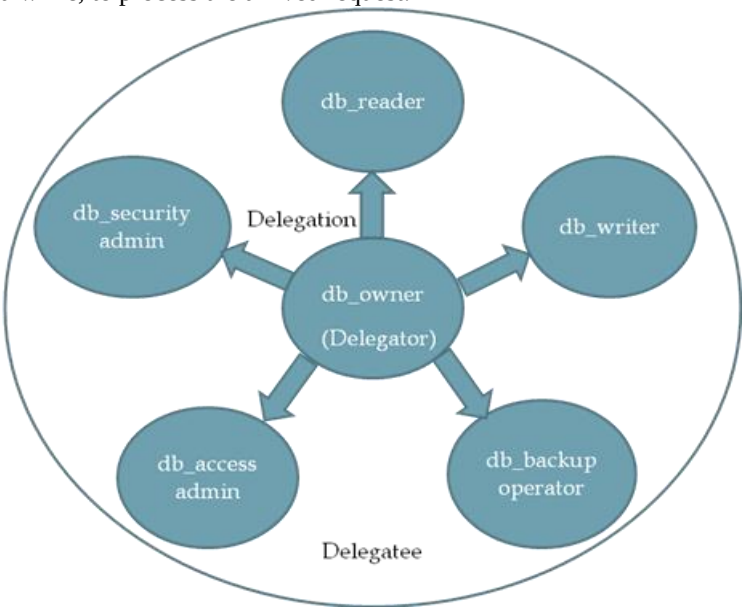

Fig 1: Motivation Scenario

In this process, absent user's access rights are delegated to one of the available user so that system will not be fail from functioning. Here delegator is db_owner and the entire are available users of the system acting as delegatee. Among these users one is selected as delegatee using decision theory and delegation is performed. Further TBAC is performed to grant the access rights. By calculating trust value of delegatee privileges are delegatee.

Thus to provide flexible access control auto-delegation is foremost thing and to prevent access right violation TBAC is necessary.

III. RELATED WORKS

Delegation process is introduced to gain the flexibility in access control system. The problem associated with powerful-enough access control system has been identified [4]. When authorized user of system is not available to perform required work, system fails unavailability. In exigency situation, for example, consider military operation where it requires to access the intelligence report to proceed further and it is not known that if responsible officer is not alive or not. By considering such an emergency situations delegation mechanisms are introduced. There are two types of delegation, manual and automatic. Manual delegations are traditional delegation mechanisms [5] require a user to be present at the time of delegation to perform delegation. Again manual delegation does not provide proper solution as the person may be or may not be available at the time of delegation. The problems of manual delegation are further overcome by "break-the-glass" policy [6, 7]. But possibly it gives access to unauthorized user, even though authorized users are available in the system. Further Auto-delegation mechanism is introduced in [8] which combine the strengths of delegation mechanism and "break-the-glass" policies, by presenting the system that provides access to the most qualified available user for a resource. Crampton and Morisset [8, 1] introduced an automatic delegation mechanism (ADM), which is "object-centered": an object can be accessed by one of the most qualified subject available. This work is extended by considering the uncertain availability of subject in [9]. They assumed a level of uncertainty for availability of users to be a quantitative value (probability of availability), Subjects availability is calculated in terms of probability and proposed a quantitative approach to the problem of auto-delegation [9, 1]. Whether an access should be granted to a user is decided according to the probability that a more qualified user is available. The decision to allow or deny an access is based on the utility of each outcome and on a risk strategy. The main limitation of this approach is the lack of precise utility, gain or damage measures for real-world applications and also the utility function defined is the context-dependant.

Further, a fuzzy approach to the Trust Based Access Control (FTBAC) with the notion of trust levels for identity management is introduced in [3]. In this paper they have presented trust based dynamic access control in distributed IoT.

IoT is Internet of Things refers to the wireless network of devices such as household appliances, office appliances with self-configuring capability [3]. Relationship between trust and access control is given as

$$Level\_of\_Access\_Control_{i \to j} \propto Trust_{i \to j}$$

Different trust factors are considered to calculate the trust. Factors like Experience, Knowledge, and Recommendation. Trust rules are derived using these factors. And trust value for each device is calculated. Proposed FTBAC framework includes the three layers. Mainly device layer, request layer and access control layer. Device layer includes all the IoT devices, Request layer responsible for collecting trust factors which are required to design trust rules and Access control layer involves in the decision making process, it maps the trust values to access permission. Such a way presented FTBAC is scalable and efficient scheme for IoT.

DTA-d [1] provides auto-delegation scheme for UbiComp. The detailed process of DTA-d is presented using DTA-d framework. Step by step process to find delegatee is given by using the decision theory and also the health care system is presented as an application of DTA-d approach.

Thus in previous work powerful access control problem is figure out by delegation mechanism. And manual delegation process and break-the-glass policy is overcome by auto-delegation mechanism. First auto-delegation mechanism introduced which is "object-centered", access is granted by considering authorization level. In next, probability of user's availability is considered. Further DTA-d is introduced, which uses the decision theory for performing auto-delegation.

In current work we introduce trust based access control for DTA-d and present the proof of concepts for DTA-d system using decision theory and trust based access control. The functioning block diagram of DTA-d is also described in detail. Algorithm to implement the TAC-UbiComp is given as well.

IV. PROPOSED TAC-UBICOMP FRAMEWORK

The TAC-UbiComp framework presents the overall process to perform auto-delegation and TBAC in UbiComp. Figure 2 shows distinct steps using decision theory to select the appropriate subject as a delegatee. The first step identifies the problem that is there are a number of subjects present in the system, out of which one has to be selected as a delegatee. The second step is the collection of data that is the credentials of available subjects. In this step find out the attributes, benefits and risk associated with each subject. Using these credentials a comparison of subjects is possible. To select the best delegatee, the third step contains evaluation of the system using DT that is decision theory. A general mathematical model is presented and probability set is calculated. The next step is to select one of the subjects as a delegatee, which is given by the previous step that is final output of decision theory. After selecting the delegatee, the next important step is to perform the access control. For that trust of delegatee is calculated using trust rules defined in mathematical model. According to the trust value, which access rights must be granted to the delegatee is decided. This is the trust based access control in, which trust associated with a subject is used to decide subject's capability to access the information. And finally after selecting delegatee and calculating trust, delegation is performed.

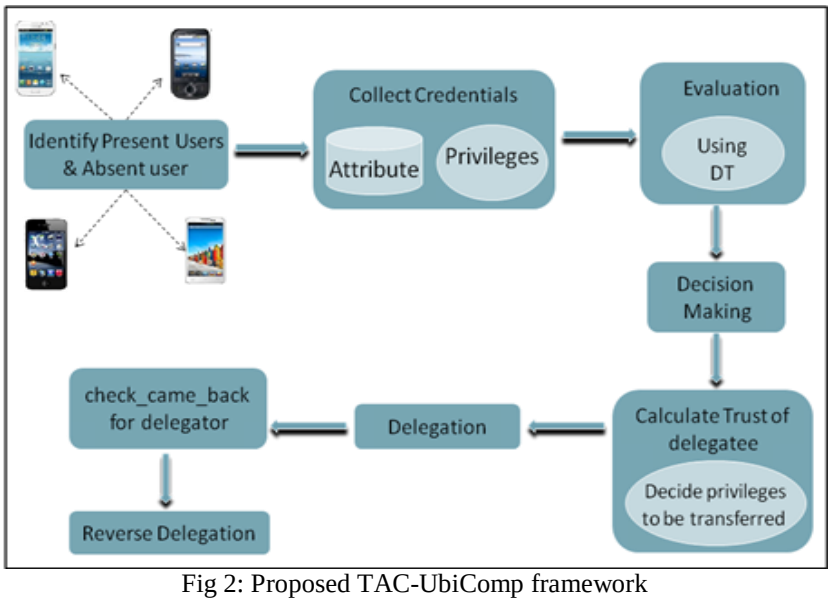

Fig 2: Proposed TAC-UbiComp framework

With this, system also checks for comeback of absent user. If delegator is come back, then reverse delegation is performed. Delegator gets delegated privileges back and also is then withdrawal from delegatee. After reverse delegation, delegatee cannot access the privileges of delegator.

V. PROOF OF CONCEPT

In this section presented mathematical model and algorithm for TAC-UbiComp which gives the step by step processing required to implement TAC-UbiComp. It defines the input and overall processing for the TAC-UbiComp framework using the decision theory. Further, technique to perform trust based access control is also presented.

Input:-Input is given as data structure, which includes the following fields Where,

DR_i	DE_j	AR_i

DR_i– Delegator's identity
DE_j– Delegatee's identity
AR_i – Access rights of the delegator to access the particular data.

Process:

DTA-d uses the decision theory, which provides a solution to the delegation problem. It is the theory about decision making [4]. The decision theory provides a way to choose the best delegatee among the available devices.

Decision theory can be applied in two approaches:

1. When the probabilities are known.
2. When the probabilities are completely unknown.

The first approach is known as Priori probability analysis. It assumes the prior probability to be the best delegatee for each available user. By comparing prior probability with each other, highest probability device get selected as delegatee. Further, using this solution a posterior probability analysis is performed for making the selection procedure more accurate and efficient, in which some attributes are considered and bays rule is applied to calculate the result.

Let,

D be the set of available devices

$D= \{D_1, D_2, D_3, \dots, D_n\}$

Prior probability for each device is given as,

$P(D_1)$= Prior probability that device D_1 is the best delegatee.

$P(D_2)$= Prior probability that device D_2 is the best delegatee.

$P(D_n)$= Prior probability that device D_n is the best delegatee.

A decision made with only prior information is given as Eq(1)

Decision (Device) =

$$\begin{cases} D_1, & P(D_1) > P(D_2), P(D_3) \dots P(D_n) \\ D_2, & P(D_2) > P(D_1), P(D_3) \dots P(D_n) \\ & \vdots \\ D_n, & P(D_n) > P(D_1), P(D_2) \dots P(D_{n-1}) \end{cases} \quad (1)$$

Now, improve the decision using Posterior probability analysis. Here, bays rule is used to convert prior probability to posterior probability.Consider,

x is the set of attribute for D,

x is used to improve the decision making by applying Bays rule, which combines x and prior information of D

x is given as,

x= {x.1, x.2, x.3, ……. ,x.n}

By using class-conditional probability,

$$P(D_1|x.1) = \frac{P(x.1|D1)\,P(D1)}{p(x.1)}$$

$$P(D_2|x.1) = \frac{P(x.1|D2)\,P(D2)}{p(x.1)}$$

..

$$P(D_n|x.1) = \frac{P(x.1|Dn)\,P(Dn)}{p(x.1)} \quad .$$

(2)

Now, calculate for each attribute,

$$P(D_1|x.1) = \frac{P(x.1|D_1)\,P(D_1)}{p(x.1)}$$

$$P(D_2|x.2) = \frac{P(x.2|D_2)\,P(D_2)}{p(x.2)}$$

..

$$P(D_n|x.n) = \frac{P(x.n|D_n)\,P(D_n)}{p(x.n)} \quad .$$

(3)

By considering Eq(2) and Eq(3) we can write as,

$$P(D_i|x.j) = \frac{P(x.j|D_i)\,P(D_i)}{p(x.j)} \quad (4)$$

Where,

$P(D_i|x.j)$ = posterior that is what we know about D_i after seeing x.j

$P(x.j|D_i)$ = likelihood that is observing certain value of x.j given D_i
$P(D_i)$ = prior probability of D_i
P(x.j)= evidence that is to ensure that the left hand side has valid distribution and is given as,
$P(x.j) = \sum_{i=1}^{n} P(x.j|D_i)P(D_i)$
i= 1,2,3, …. ,n
j= 1,2,3, …. ,n
Thus, the decision made with posterior information analysis is given by comparing the values calculated by Eq(5)
$P(D_1|x.1)$, $P(D_2|x.1)$, …….. , $P(D_n|x.1)$, $P(D_1|x.2)$, $P(D_2|x.2)$, …….. , $P(D_n|x.n)$
Decision (Device) =

$$\begin{cases} D_1, & P(D_1|x.1) > P(D_2|x.1), P(D_3|x.1) \dots P(D_n|x.1) \\ D_2, & P(D_2|x.2) > P(D_1|x.2), P(D_3|x.2) \dots P(D_n|x.2) \\ & \vdots \\ D_n, & P(D_n|x.n) > P(D_1|x.n), P(D_2|x.n) \dots P(D_{n-1}|x.n) \end{cases} \quad (5)$$

Output:
Thus posterior probability analysis result is considered as final output of decision theory as it gives more accuracy than priori. After selecting the delegatee by posterior probability analysis of decision theory, TBAC is the last step to perform.

Trust Based Access Control (TBAC):
In the proposed system, when one of the users is absent (Delegator), the other present user is selected as delegatee and Access privileges are granted to the selected delegatee using trust. Trust relationship between two devices helps in influencing the future behaviours of their interactions [3]. When devices trust each other, they prefer to share services and resources at certain extent [3]. Trust helps to make the communication reliable and efficient between the devices.
Fuzzy approach for calculating Trust
Calculation of the trust depends on the two factors
(a) Experience of the user.
(b) Knowledge of the user.
In given scenario, we will assign above factor's values to each user.
Fuzzy values of the user experience are
(a) High (above 5 years)
(b) Moderate (above 3-5 years)
(c) Low (below 3 years)
Possible values of the Knowledge about the system are
(a) Advanced
(b) Moderate
(c)Basic

Trust Rules
By using these two factors following trust rules are derived. And using this trust rules access privileges are granted to the delegatee.
Experience: ex= {High, Moderate, Low}
Knowledge: k= {Advanced, Moderate, Basic}
Trust: t= {fully_trusted; semi_trusted; not_trusted}
Rule 1:

```
if (ex > k) then
    t = ex
```

Rule 2:

```
if (ex < k) then
    t = k
```

Rule 3:

```
if(ex==k)
t=ex||t=k
```

If any user is absent in the system then decision theory will give name of the most appropriate user for privilege delegation of the absent user. After that trust theory will estimate trust of the delegate from above trust rules. Depending on the trust of the delegate, privileges of the delegator are delegated to the delegate as per following table.
Table I shows the access right allocation using trust value. Trust of the delegatee is varies with file privilege. File privilege defined in MySQL works with the files located on server host. File read operation includes reading the data from file and writing into table. And file write operation includes writing data into file and reading from table. Table can be located at client machine. File privilege provide file writing and reading from server and also back up related benefits

TABLE I: ACCESS RIGHT ALLOTMENT USING TRUST

Trust	Allowed to grant Privileges	Description
Fully Trusted	All privileges of the delegator are allowed to assign to the delegatee.	Both Read and Write allowed on file
Semi Trusted	All privileges of the delegator are allowed to assign to the delegatee except insert, update.	Only Read allowed on file
Not Trusted	All privileges of the delegator are allowed to assign to the delegatee except file privileges.	None (No read & no write) Only table related privileges are granted.

Algorithm for TAC-UbiComp

TAC_UbiComp(N)

1. {
2. N= number of devices
3. While(N)
4. {
5. Login_devices.get(N)
6. Absent_device.get(N)
7. Get_privilege(DR)
8. Decision_theory(DR,priv)
   // call to the DT, in which delegatee is selected by priori and posterior probability analysis using mathematical model
9. Get_trust(DE)
   // calculate the trust of delegatee by Trust rules defined in mathematical model
10. Assign_priv_by_Trust(DE,trust)
    If(trust==high) then
        Grant FILE_READ, FILE_WRITE and Table related privileges
    Else if(trust==moderate)
        Grant FILE_READ and Table related privileges
    Else
        Grant only Table related privileges
11. Auto-delegation(DE, priv_granted_by_trust)
12. Check_came_back(DR)
    If yes then
        Reverse_delegation(DE,DR,priv)
13. End

Where,
N= number of devices in the system
DR= Delegator that is absent device in the system
DE= Delegatee that is device who is going to receive the access rights from absent device
priv= privileges or access rights of the delegator and to be assigned to the delegatee

VI. CONCLUSIONS AND FUTURE ENHANCEMENT

This paper presents the TAC-UbiComp scheme with the TBAC and decision theory. To provide flexible access control, delegation mechanism is necessary. Instead of manual delegation, auto-delegation is performed to provide efficiency and reliability. Decision theory is applied in UbiComp to select one alternative when numbers of alternatives are available. Presented trust based access control prevents the access right violation, as the access rights are granted by calculating the trust of delegatee. Trust value of device decides the way of working and sharing the resources, services with device. Mathematical model is presented to select delegatee using decision theory which is performed in two steps that is priori probability analysis and posterior probability analysis. Out of which posterior analysis is more accurate as it considers some attributes related to the device for computation. Computative process to calculate the trust of the device is also presented. According to the trust value access right allocation is carried out.

Future enhancement includes implementation of capability based access control (CBAC) with TAC-UbiComp scheme.

REFERENCES

[1] Priyanka N. Kamble, Parikshit N. Mahalle, "Decision Theory based Auto-delegation (DTA-d) scheme for Ubiquitous Computing", International Journal of Computer Applications (0975 – 8887) Volume 79 – No7, October 2013.

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

[3] Parikshit N. Mahalle, Pravin A. Thakre*, Neeli Rashmi Prasad and Ramjee Prasad, "A Fuzzy Approach to Trust Based Access Control in Internet of Things.", IEEE 3rd International conference on Wireless ViTAE-2013, IEEE, 2014.

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

[5] 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).

[6] 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)

[7] 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)

[8] Crampton, J., Morisset, C.: An Auto-delegation Mechanism for Access Control Systems. In: Cuellar, J., Lopez, J., Barthe, G., Pretschner, A. (eds.) STM 2010.

[9] 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.

