# Negative Authorization in Access Control for Cloud Computing

Xiaohui Li[1], Jingsha He[2] and Ting Zhang[1]

[1]*Computer Science and Technology, Beijing University of Technology, Beijing 100124, China*
[2]*School of Software Engineering, Beijing University of Technology, Beijing 100124, China*
*{[1]lixiaohui, [1]zhangting06}@emails.bjut.edu.cn, [2]jhe@bjut.edu.cn*

***Abstract***

*Cloud computing is the next generation of platform over which information and services can be offered to the user in a more convenient and transparent way. On the other hand, however, commercial interests will cause information proliferation, resulting in over-supply of useless information to the user and waste of precious systems and network resources. The problem of controlling such information proliferation has thus received a great deal of interests in recent years. In this paper, we propose an access control model for negative authorization to provide the user with the ability and flexibility of specifying the objects to which access is not desired through the means of negative authorization. The main contributions of this paper include: (1) the concept of negative authorization in access control; (2) negative authorization rules; and (3) specification of negative authorizations by the user. With the ability of specifying negative authorization by the user, access to unwanted information and services offered by the cloud can be disabled through access control. Compared to filtering mechanisms that block unwanted information and services, negative authorization has the advantage of saving precious computation and network resources because access control happens prior to actual access while filtering takes place after system access and network transmission.*

***Keywords:*** *Cloud computing; access control; negative authorization*

## 1. Introduction

There are a variety of access to information services, for example, subscriptions to newspapers, mail, web site, but the access of these services need to provide us with personal information, such as address, e-mail, identity, and so on. The more information provided, the more the services available. As information growth continues to expand at an exponential rate, we are drowning in a rising sea of information. Cloud computing redefines information service and offers a value proposition based on convenient services that you pay for as you go. But we enjoy the same benefits and suffer the same frustrations of the exploding information. How to ensure the information we receive is exactly what we want.

In this paper, we propose a user oriented negative access control model in cloud computing for optimization of information services, improve cloud users satisfaction. The model is flexible enough to provide the cloud users with the capability of giving their selective preferences and making access decisions at their own discretion. Our model adopt the mode of first control last access to lessen system burden ,especially for users.

In the next section, we survey some related works that motivates the discussion in this paper and we also point out the weaknesses. In Section 3, we formally present design of our user oriented negative access control model. We define the various components of the model and describe how the model to handle individuals and systems to select the information needed in the high convergence occasions from a new point of view. We also describe a procedure to show how the model can be used to make negative access control decisions. Finally, we conclude this paper in section 4 in which we also discuss some future work.

## 2. Related work

To our knowledge, there is already some access mechanism to control excessive and useless information.

Lillian Røstad et al. [1] proposed a model for personalized access control which presents a more detailed model suggesting how these issues may be handled in an access control model for a PCHR. The model is semi-formally defined. Core properties of the model are the two sets of access policies and the definition of policy adaption hierarchies stating how policies may be combined.

Personalized search refers to search experiences that are tailored specifically to an individual's interests by incorporating information about the individual beyond specific query provided. Pitkow et al. [2] describe two general approaches to personalizing search results, one involving modifying the user's query and the other re-ranking search results. Personalize search results model their users in different ways. Some rely on users explicitly specifying their interests or on demographic characteristics[3] . But user supplied information can be hard to collect and keep up to date. Others have built implicit user models based on content the user has read or their history of interaction with Web pages [4].

Access control filter [5] is a preliminary authorization scheme that checks if the current user can perform the requested controller action. The authorization is based on user's name, user IP address and request types. Access Control Lists are filters that enable you to control which routing updates or packets are permitted or denied in or out of a network. They are specifically used by network administrators to filter traffic and to provide extra security for their networks. This can be applied on routers.

Personalized access control and access filter can be used to choose value information through subjective ,but access filter is the way to add a barrier by subject while receiving the results; personalized access control is still to provide the more information, more access to the information service. They are both based on the static information and adopt first access last control mode. In essence, they do not reduce the burden of the vast amounts of information to the user and system. In the cloud computing environment, the cloud terminal is resource-constrained, these methods are not applicable. So we propose a novel negative access control model to handle individuals and systems to select the information needed in cloud computing(the high convergence occasions) from a new point of view in this paper.

## 3. Negative access Control Model

In the section, we first introduce the concepts and the entities in the negative access control model and describe the architecture and the components that make up our model in detail.

### 3.1. Formally Description

**Negative access control (NAC).** For a particular information service, we have two options: passive acceptance or active choice, the interval is from 1(all) to 0(none).We can adopt the NAC solution. It is a type of optimization information services access control that restricts object access via an access policy determined by an object's user group and/or subjects. NAC mechanism controls are defined by user's proper information, such as users' requirement and context information. NAC is first control by user/subject last negative access decided by server that is the mechanism of more subject information provided, the more accurate object available. In other words, the information user determines object negative access privileges.

**Context**. It is any information that can be used to characterize the situation of entities that are considered relevant to the interaction between a user and an application, including the user and the application themselves. Context is typically the location, identity and state of people, groups and computational and physical objects.

**Fuzzy set**. Let X be the universe of discourse, for any fuzzy set A, the function μA represents the membership function[6-8] for which μA(x) indicates the degree of membership that x, of the universal set X, belongs to set A and is, usually expressed as a number between 0 and 1

$$\mu_A(x): X \rightarrow [0,1]; x \rightarrow \mu_A(x) \quad (1)$$

The operation of union, intersection and complementation are defined exactly the same as they are for standard sets in terms of the characteristic function; i.e.:

- Union: $\mu_{A\cup B}(x) = \max(\mu_A(x), \mu_B(x))$
- Intersection: $\mu_{A\cap B}(x) = \min(\mu_A(x), \mu_B(x))$
- Complement: $\mu_{notA}(x) = 1-\mu_A(x)$

The notation for fuzzy sets: For the member of a discrete set with membership μ,we use the notation μ/x .

$$A = \mu_1 /x_1+\mu_2/x_2+\cdots..+\mu_n/x_n \quad (2)$$

### 3.2 Entities in the model Architecture of the model

Our model is made up of three types of entities:

- User's proper information include: Users' requirement, such as active input, feedback; Context information, such as identity, habit, hobby, history of information service.
- Cloud user: the user of information services in the cloud computing environment, All the information service (choice of information services) must be directly or indirectly made by the user.
- Cloud server: The main part of model to make negative access decision, through the user's proper information to offer the Cloud user information needed, the information comes from two parts: the public useful information of read rate as a standard; the information collection of user's proper information as input conditions.

### 3.3 Architecture of the Model

The architecture of our negative access control model is illustrated in Figure1. And this model can be described five building blocks. To get a good picture of our model we should describe:

- Cloud user segment: Specify as cloud computing environment information service users
- Requirement segment: User active require information services by request or feedback
- Context segment: Relatively active requirement speaking, this segment generates filter term of whole information for user without users' any instruction
- Cloud sever segment: The most important activities performed to implement our model
- Information service: The bundles of services that satisfy our user segment' s needs.

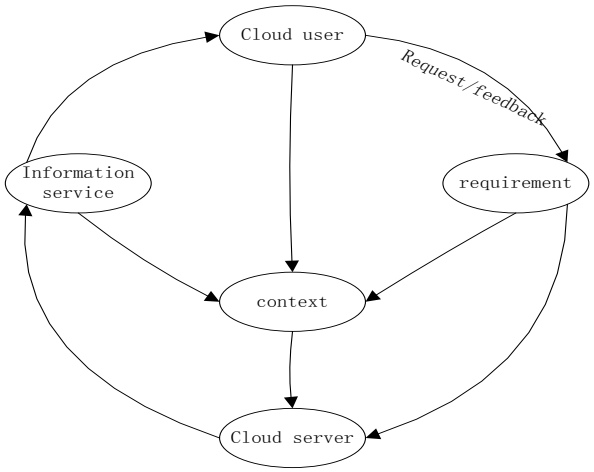


**Figure 1. The Negative Access Control Model**

The negative access control model will allow us to:

1. In contrast with the access control ， Negative access control is a mechanism by which a system grants or revokes the right not to access some data or perform some action. In our model , we focus on information data.
2. Allowing the user to solve information overload problem, and achieving higher quality information service for user [9], seeing the information what the user want to see.

As the most important part of the model, the following describes the cloud segment in details.

**Cloud sever segments**: this module process the context information by four steps.

Step 1. Scan the context information that consists of the users' requirement and context information as the input conditions, Based on user interest categoriesA1, A2, ..., An. To ensure that A1, A2, ..., An.independent, there is no intersection.

Step 2. let A be a finite universe U = {X1, X2, ..., Xn}fuzzy sets, U is the collection of all information in the cloud server, A is the collection of cloud user information composed byA1, A2, ..., An. X is the element of U in the cloud server, that is the composition of our cloud user information service set.

According to formula 2, A = μ1/x1+μ2/x2+⋯..+μn/xn Where "+" shows a concepts of collection , not the sum of arithmetic. The denominator is the element of domain, molecule is the membership degree of element to A.

Step 3. According to the previous formula, select μA(x) ≤0.6, Choose to meet a fuzzy set A1 of all x, delete operation. for A1∩ A2, ..., ∩An ⊆…, ⊆ A1∩ A2⊆ A1, Process as shown in Figure 2.

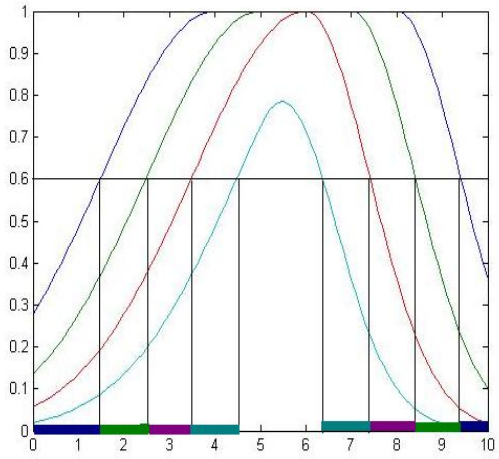


**Figure 2. Relationship of user's proper information and the information service accepted.The horizontal axis represents the information service element, Collection range from large to small, the color bars mean remove portions. The whole process is summarized as: the more user information A, the less information elements of the cloud user accepted x the set of numbers "close to 0".**

Step 4. The information service results include two parts: a public concern (selected according to the read rate); one is the selection results of the third step.

The negative access control model is designed for the scene of the cloud users acceptance of information services, but can also be applied in other similar occasions. It reflects the psychological needs of the cloud users to information services. When the users want the information provided in the cloud resource pool to obtain the information they most want, we need some specific information of the users, the cloud server make the control of negative access and give the results. It is different from the keyword-based search, the results include information that has nothing to do with the specific information of the users.

## 4. Conclusions

In this paper we describe a novel negative access control model to better improve user's satisfaction to information services in cloud computing. Our model has at least three advantages. First, it is very novel of first control last access and can support user oriented

information requirements in cloud computing. Second, the users provide the more information themselves the more accurate information obtained. Third, the cloud users can decide their information obtained from cloud server without requiring any additional burden.

The model proposed in this paper exposes us to a number of possible research directions in the future. One such direction that we will take is to refine our model to balance privacy preservation and cloud user satisfaction. We will also focus on selection of user interest and membership to help us further optimize the model.

## References

[1] A. Kobsa, "Personalized hypermedia and international privacy", J. Communic ACM. 45(5), 64–67 **(2002)**.
[2] J. Pitokow, T. Cass, "Personalized search", J. Communications of the ACM (CACM) 45 (9): 50–55 **(2002)**.
[3] E. Frias-Martinez, S. Y. Chen and X. Liu, "Automatic cognitive style identification of digital library users for personalization", JASIST.58 (2): 237–251 **(2007)**.
[4] J. Teevan, S. T. Dumais and E. Horvitz, "Personalizing search via automated analysis of interests and activities", SIGIR: 415–422 **(2005)**.
[5] S. Haykin, "Adaptive Filter Theory", Fourth Edition［M］. New Jersey: Pearson Hall, **(2002)**.
[6] L. A. Zadeh, "Fuzzy sets", Information and Control 8 (3) 338–353**(1965)**.
[7] C. Castelfranchi, R. Falcone and Pezzulo, « Integrating trustfulness and decision using fuzzy cognitive maps", Trust Management 2003, LNCS 2692, **(2003)**, pp. 195-210.
[8] L. Sweeney, "Achieving k-Anonymity Privacy Protection Using Generalization and Suppression", International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, 10(5): 571-588 **(2002)**.
[9] X. Li and J. He, "A User-Centric Method for Data Privacy Protection in Cloud Computing", 2011 International Conference on Computer, Electrical, and Systems Sciences and Engineering, pp. 355-358 **(2011)**.

## Authors

**Xiaohui Li** is currently a Ph.D. candidatein theCollegeofComputer Scienceand Technology at Beijing University of Technology. Her research interests include network security and trust management. Email:lixiaohui@emails.bjut.edu.cn

**Jingsha He** is currently a professor of the School of Software Engineering at Beijing University of Technology. His research interests include network security and wireless communication technologies. Email: jhe@bjut.edu.cn

**Ting Zhang** is currently a Ph.D. candidate in Beijing University of Technology, Her research interests include localization technology and network security in wireless sensor networks. Email: zhangting06@emails.bjut.edu.cn