Managing Access Control Policy From End User Perspective in Collaborative Environment

Abstract—**currently, collaborative environments offer unlimited data sharing for users. Data owners are poorly involved in handling their data for such environment when it deals with data policy. Normally, data access control policy consists of a resource and authorization descriptions which are assigned by the administrator. It is the responsibility of the administrator to set and specify the policy for application services. The policy details are massive and complex for administrator to handle where most of the times there will be cases of unreview services. This paper proposes a framework that allows data owners to provision policies for storing and managing their shared data with third parties. By adapting RBAC model and adding owner's interest on permissions for data operations and objects, the proposed framework will facilitate data access control whereby owners have the freedom to set their own data access policy.**

Keywords-component; Access Control Policy, Colloborative Environment, Data Sharing

I. INTRODUCTION

Practices of making data available for others are becoming common to computer users. Data are either shared to public or selected viewers. Regardless who the target audience is, distributing and accessing data should be controlled and managed properly [1]. The access control decision is enforced by mechanisms that are established by security policy. Several existing access control mechanisms such as role-based, rule-based and reachability based are used to manage data sharing problems [2].

In order to comply with access control, a policy which is relevant to a body, institution or agency should be adapted. Policy will determine on what criteria and condition should be adapted on controlling the data access [3]. The policy will be triggered upon user request on accessing a particular data in a controlled environment [4]. Policy is normally based upon role of the data requestor. Policy will improve the ability of managing access based on information and guidelines that have been provided [2].

Normally, the administrators of service providers take control of handling data policy for users or subscribers who are attached to them. Administrators are responsible for providing administrative services such as system maintenance and user support. Permissions to specific data are performed by granular control of adminstrators' rights [5]. Figure 1 shows a common framework of access control policy adapted by most applications [3].

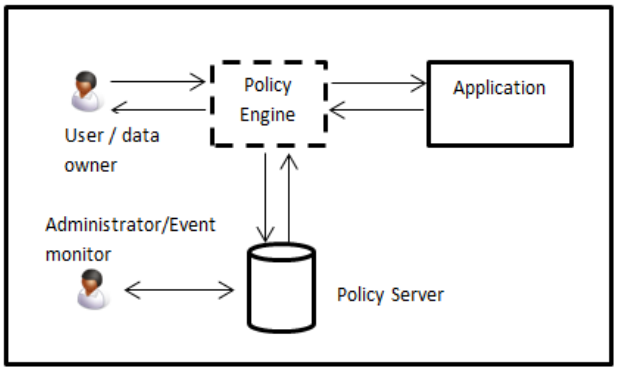

Figure 1. Common Framework of Access Control Policy

The current approach of data handling in an organization's interest access control is organization has the full control of data. Data owners have limited involvement in the management of their own data. Though data are being treated according to the policies agreed among the involved parties, arguments do occur [6]. Policies are also constantly changing from time to time and conflicts between parties mostly lead to bigger issues. Issue of lacking the data owner's involvement in handling their own data is one of the major issues that will be focused in this paper.

This paper presents framework for configuring access control policy based on owner's interest to recapture the missing component in most collaborative data sharing framework. The rest of this paper is organized as follows; Section 2 gives an overview of the access control models. Section 3 reports the implementation and observation of a case study for enhanced policy model. Section 4 deliberates the results of the implementation and observation. Finally, section 5 gives the concluding remarks.

II. ACCESS COTROL MODEL

Unauthorized access is becoming a major concern when dealing with collaborative data [7] within the rapid explosion of information technology and security. Common models for access control are discretionary, mandatory and non-discretionary or role based [8]. The three access models act as elementary guidance for data access control. Combining or extending such models provides adaptable and secure data collaboration which allows data interchange, sharing and dissemination. Discretionary access control (DAC) model is based on object owner's requirement. A system that uses DAC allows object owner to specify whom or which subjects

can access any specific object. The most common implementation of DAC is through access control lists (ACL) which are dictated and set by the owners and enforced by the operating system (OS) [9]. UNIX, Linux and Windows are example of OS that uses DAC as an access control. DAC systems will grant or deny the access based on subject's identity.

Mandatory access control is very structured and authoritarian. It is normally based on security label which are attached to all objects [10]. Users whom are referred to as subjects are given security clearance by specific classifications such as secret, top secret and confidential. Objects are also given the same classifications. The security clearance and classification will be stored in the security labels which bound to the specific subject and object. When the system makes a decision about fulfilling a request to access an object, it will be based on the clearance of the subject. This model is suitable for military system where confidentiality is very important.

Non-discretionary or role based access control (RBAC), uses a central administrator to set the control and determine how subjects and objects interact [11]. A subject should meet a set of predefined rules before it can access an object. RBAC can be generally used in combination of DAC and MAC systems. RBAC has the ability to adapt the dynamicity of real-world data policies where it requires notion of state, and state of change [8]. For example, RBAC has a notion of activating and deactivating roles within sessions [11] that allows diverse security polices and support efficient access management.

Role based access control (RBAC) models show clear advantages over traditional discretionary and mandatory access-control models with regard to the ability of allowing diverse security policies and support efficient access management [8]. Our approach will be adapting RBAC model with access control at the element-level granularity of data sources and enforces concept-level access control by data owner. RBAC provides a valuable level of abstraction to promote security administration at enterprise level rather than at the user level. Administrator will establish permissions for users based on the functional roles in the enterprise. Users will then be assigning with a role or set of roles. Access decisions are based on the roles of individual users that had been assigned to them (refer to Figure 2).

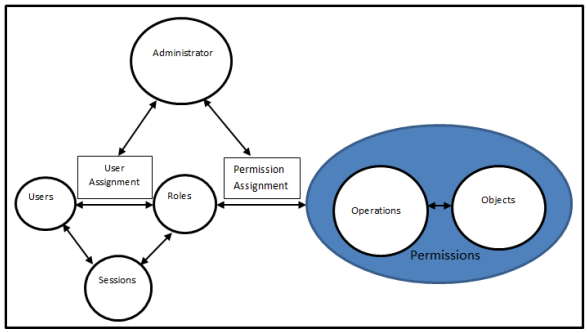

Figure 2. RBAC Model [8]

Common practice tackles traditional RBAC concept of role hierarchy where senior roles would be able to inherit permissions form junior roles (refer figure 3), and whoever at the upper level has the same or more control over lower subordinates

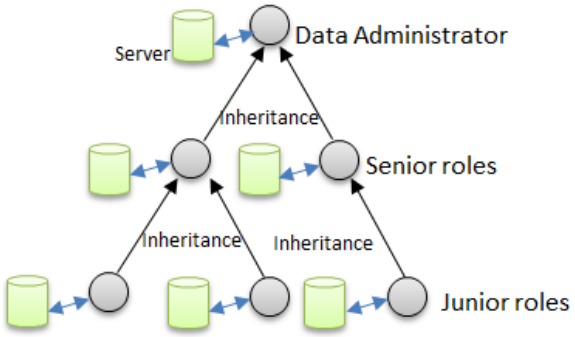

Figure 3. Traditional RBAC Method

This research proposes some new terms; local administrator and global administrator. In this model that is purposely applied to a networked collaborative environment, the data owner can be referred to as a local administrator. Similar to data administrator, local administrator has the authority towards their data in giving delegation and revocation to other users. For example, figure 4 illustrates how a local administrator sets an access control policy by sharing data with a local administrator B (as indicated by symbol).

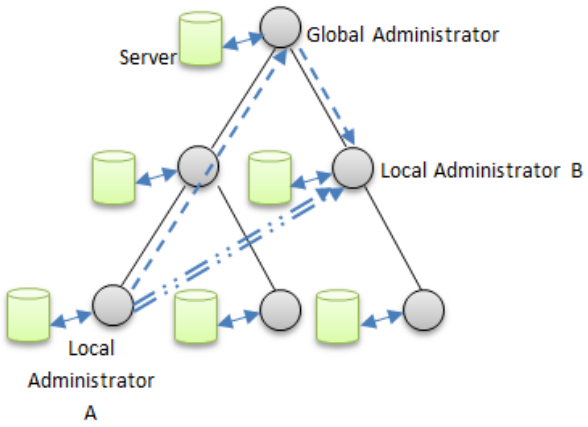

Figure 4. Anticipated Access Control Model

With the common approach, it is only the global administrator who can set the policy on behalf of the local administrator A. However, in the proposed method, the local administrator A is allowed to set the policy of the shared data by sending the specifications to the global administrator so that the data can be passed on the local administrator B (as indicated by ⇢). This will extend data owner's sharing power based on their own interest through user interest management concept. This idea was first introduced in 2007 by Abidin [12] and this research is an extension of the work.

III IMPLEMENTATION AND OBSERVATION

In order to look into feasibility of the proposed method, the data sharing scenario is mapped into a collaborative scrabble game for a controllable environment. Two versions of collaborative data sharing application on a scrabble game are implemented. Both applications are constructed using JACIE, a rapid prototyping development tool for CSCW [12]. The first version involves an appointed administrator to control the data sharing, while the second allows additional control policy from the data owner. Figure 5 shows the screenshot of the application.

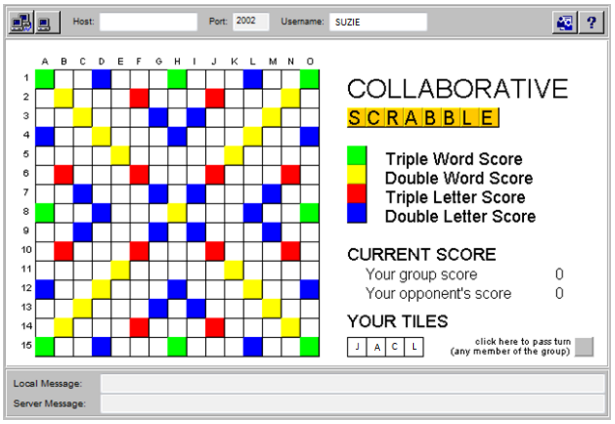

Figure 5. Screenshot of Scrabble Game Version I

The first version of the application portrays common collaborative data sharing that lets the administrator to have a total control on data access management. The responsibility of the administrator will increase when a number of data owners want to modify their data access policy. However, by allowing the data owners to act as the administrator to their own data, the responsibility of the actual administrator is reduced tremendously. Therefore, in the second version of the game, each data owner will be able to set their own policy setting before or during the game. A simplified interface is provided to the data owner to set their own policy as shown in Figure 6. There are three basic states of object policy which are readable, updatable, and unavailable had been extended to view, update and exchange, and challenge, respectively to suit the nature of the game.

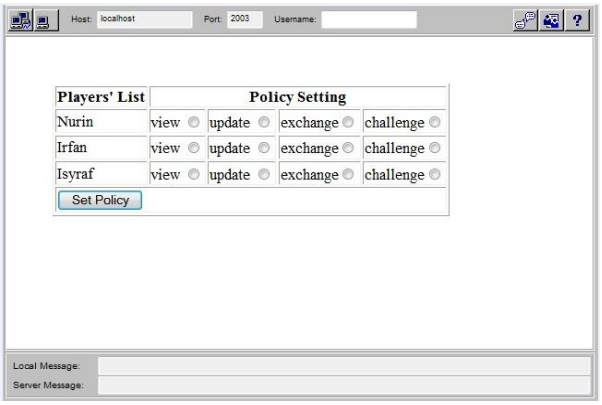

Figure 6. Screenshot of Data Owner's Policy Setting

This work adds a few entities to the RBAC model for a little enhancement so that data owners can implement temporal constraints to their own object by specifying who the eligible target users are as shown in Figure 7.

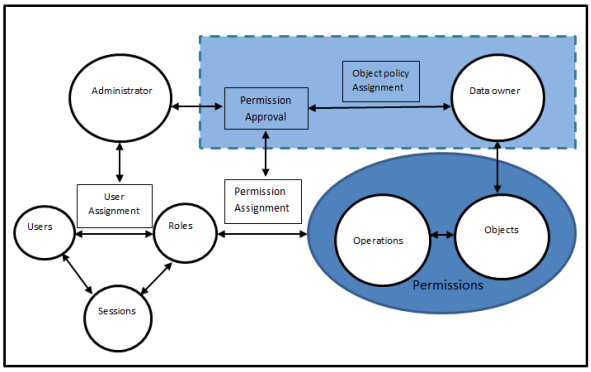

Figure 7. Enhanced Role based Access Control (RBAC) model for interactive NCVE

This model adds a permission to object assignment relation. The use of proposed model is to manage data owner privileges for interactive networked collaborative virtual environment (NCVE).

From the observation that has been made, data owner has the ability to manage their own data in the second version as compared to the first version. The processes of data access policy for both versions of the game are summarized in Table I.

Table 1. Summary of Observation of extended Scrabble Process on Data Access Policy

	Version One	Version Two
Data Owner	• Send request to administrator for any changes on policy	• Change policy accordingly before or during the game.

	• Wait until is policy updated by administrator	• Update the policy server
Administrator	• Set default policy for all data before the game	• Set default policy for all data before the game
	• Wait for policy changes request from data owner during the game.	• Update the policy server
	• Change policy accordingly and update the policy server.	

Underlying our enhanced RBAC model is the notion that data owner can implement temporal constraints to their own object by specifying who the eligible users are. This new model reflects a notion by associating different states of policy to different object. The notions are as follows:

- Readable – the object can only be readable by a particular role
- Updatable – the users who hold specific role can retrieve and change objects
- Unavailable – neither users who hold specific roles can't update nor read the object.

Since permissions are organized into policy functions through roles, allowing the owner to alter data permission will create conflict between the owner and administrator. In order to resolve the conflict, we proposed an enhanced model that provides data owners with additional capabilities to specify and enforce enterprise policy to individual users. In the enhanced model, data owners are given the authority to specify their policy towards their own data. Therefore, this will lessen the difficulties faced by the administrator to entertain each data owner specification towards data access control.

IV RESULTS

Collaborative data sharing infrastructure consists of several users, network provider and data sharing application which each of them are discontinuously connected. Each user has a local database instance and spends the majority of its time operating in locally independent mode where they may also upload their work to the centralized database. Data sharing application allows users to pose queries and make modifications directly over data owner's local database instance or application's centralized database. These could only happened upon an administrator's permissions via data access control policy that being adapted by the data sharing application. Policy on activity such as update and exchange are critical for allowing data to flow between users in the system.

In general, a policy should be able to protect and secure available data. Our approach provides a mechanism to configure the subject's own data and its authorizations as depicted in Figure 8.

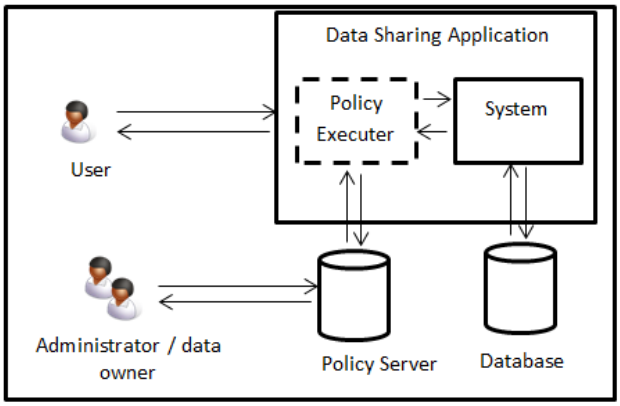

Figure 8. Proposed Framework of Access Control Policy

The mechanism will secure the execution of basic functions towards a basic data. Proposed mechanisms are implemented in adaptation of enhanced Role-based access control (RBAC) models.

The presented architecture features are as follows:

- Policies can be configured dynamically at runtime
- Policies must be extensible for future requirements for new authorizations requirements
- Dynamic policies update by both administrator and data owner.

In this architecture, data owners have been given a control together with the administrator in managing their own data.

V CONCLUSIONS

Current approach of data handling in most institution is relied on the policy set by the organization's access control. This approach will give administrators the full control of access policies for giving out permission to users while neglecting data owner's involvement in handling their data. With enhancement of RBAC model, data owners are allowed to involve directly in the data control management by having their own policies on their own data. We believed that the proposed architecture could provide flexible, adaptive and contextually driven personal access control for data sharing in network collaborative virtual environment.

REFERENCES

[1] Villegas, W., Ali, B., and Mahaeswaran, M., An Access Control for Protecting Personal Data, Privacy, Security and Trust, 2008. PST'08, pp. 24 – 35.

[2] Gofman, I.M., Luo, R., and Yang, P., User-Role Reachability Analysis of Evolving Administrative Role Based Access Control, Computer Security, ESORICS 2010, pp. 455 – 471.

[3] Gorton, S., and Reiff-Marganiec, S., Policy for Business-oriented Web Service Management, LA-WEB 2006,

[4] Reiff-Marganiec S. and Turner K. J., "Feature Interaction in Policies,", *Computer Networks*, vol 45/5 pp 569-584, August 2004. Elsevier Science.

[5] Gupta, P., Stroller, D.S., and Xu, Z., Abductive Analysis of Administrative Policies in Rule-Based Access Control, S. Jajodia and C. Mazumdar (Eds.), ICISS 2011, pp. 116-130.

[6] Joshi, J.B.D., "Access-control language for multidomain environments," *Internet Computing, IEEE* , vol.8, no.6, pp.40,50, Nov.-Dec. 2004

[7] Ahmad S., Abidin S.Z.Z. and Omar N., "Data Sharing in Networked Environments: Organization, Platforms and Issues", Proceeding WSEAS 2011, pp 207-213.

[8] Sandhu R. and Munawer Q., "How to do discretionary access control using roles", Proceeding RBAC 98 ACM Workship on Role-based access control pp 47-54 1998

[9] Bhatti R., Bertino E. and Ghafoor A., "A Trust-Based Context-Aware Access Control Model for Web-Services", Distributed and Parallel Databases July 2005, vol 18, Issue 1, pp 83-105 2005

[10] Samarati, P. and Vimercati, C. S., "Access Control: Policies, Models, and Mechanisms", Lecture Notes in Computer Science Vol 2171. 2001. Pp 137-196 2001

[11] Sandhu, R.S.; Coyne, E.J.; Feinstein, H.L.; Youman, C.E., "Role-based access control models," *Computer* , vol.29, no.2, pp.38,47, Feb 1996

[12] Abidin S. Z. Z. (2006). Interaction and Interest Management in a Scripting Language. Ph.D. Thesis. University of Wales, Swansea; UK.