



**SCIREA Journal of Computer**

<http://www.scirea.org/journal/Computer>

**February 6, 2017**

**Volume 2, Issue 1, February 2017**

# **The Characteristics of Access Control Model Towards Securing Collaborative Knowledge Management System: Empirical Verification**

**Azreena Abu Bakar<sup>1</sup>; Rusli Abdullah<sup>2</sup>**

<sup>1</sup> Faculty of Science and Technology Universiti Sains Islam Malaysia (USIM) Bandar Baru Nilai, 71800 Malaysia

<sup>2</sup> Faculty of Computer Science and Information Technology Universiti Putra Malaysia (UPM) 43400 UPM Serdang, Selangor, Malaysia

[azreena@usim.edu.my](mailto:azreena@usim.edu.my) ; [rusli@fsktm.upm.edu.my](mailto:rusli@fsktm.upm.edu.my)

## **Abstract**

Knowledge Management System (KMS) is such an application of computer based communications and information systems that grant sharing and transferring knowledge effectively; furthermore with the evolution of Internet, KMS has improved its knowledge process and activities where it can be accessed with varied form of technologies such as email, video conferencing and so forth, from dispersed geographical area. Hence, security becomes major issue as knowledge is an intellectual property of an organization and it must be well managed. Mostly the issues are regard to the restriction of the access permission to knowledge. Therefore, there is a need to construct a security model towards secure KMS, for managing access restriction in order to avoid unauthorized access as well as to protect knowledge throughout Knowledge Management (KM) activities. This research found that Access Control Model (ACM) is competent to overcome these issues, thus, this paper is to

study the characteristics of this security model which considering the criteria of collaborative system as the KMS will be developed in collaborative environment. The study entailed online questionnaire survey and was responded by multi level groups of Community of Practice (CoP). Generally, the result of this study shows that the Quality Dimension which consists of fourteen (14) criteria has been agreed from most of the respondents. These criteria will be applied during the development of the system prototype of secure collaborative KMS.

**keywords** : Knowledge Management System (KMS), Secure KMS, Quality Dimension, Access Control Model.

## **I. INTRODUCTION**

Knowledge Management (KM) is an essential managerial activity for business entities in order to sustain their competitive advantages in today's information economy. The ability of firms to capture, organize, and disseminate knowledge allows them to improve the quality of decision making, process efficiency, customer satisfaction, and cost control. Therefore knowledge has been recognized as a critical resource [1], and should be well managed as it provides foundation for this competitive atmosphere. Knowledge need to be gathered and stored in the right format and right place, so as to access and disseminate the knowledge at the right time and to the right people [2]. Knowledge Management System (KMS) is such an application of computer based communications and information systems (CIS) that typically involve databases that enable to support the knowledge processes. Mainly, KMS permitted sharing knowledge among community of practice (CoP), but it is also requires security mechanism in order to prevent unauthorized access and misuse of knowledge, hence security plays major issue revolving around KMS [3].

The power of sharing knowledge has been enhanced by deploying collaborative computing technology. It brings geographically dispersed team members together, supporting communication, coordination, and cooperation. Moreover the collaboration provides dynamic communications among the team members in exchanging knowledge. When communications involve many users from different domains, probably each domain contains information and resources with different degress of sensitivity. Therefore the access level must be controlled where only the right user can access the knowledge.

Moreover sharing knowledge is about sharing the intellectual assets where it should put into action in turn can improve organization's performance and enhance the value of organizations. Thus, as an asset of organizations, knowledge should be protected because no one can restrict the activity geographically. The integrity and confidentiality of the knowledge should be maintained, therefore security becomes prominent in knowledge sharing and it is contributor to KM success [4].

The right knowledge should be accessed by the right person, hence security becomes standing issue to be focused. Essentially the access to the knowledge should be restricted and should taking into account the characteristics of collaborative environment. The restriction of access is a mechanism by which organizations protect their knowledge assets. Access control model (ACM) is recognized as a model that can control the permission of knowledge access [5]. It is appropriate to be introduced in collaborative environment based on the characteristics it has. Therefore, ACM becomes the ground of this research as it has capability to adopt collaborative system criteria while presenting itself as a role to protect knowledge access. Access control policies and roles have been introduced in order to avoid chaos in collaborative applications [6].

The focal point of this study concerning on restriction of access permission. However in this paper we will pay special attention to the security model of access control for collaborative KMS which will focus on the verification, specifically related to characteristics of the model.

The proposed access control model taking into account the collaborative environment which contributes to dynamic communication. But this paper spotlight on the verification of the characteristics towards deploying the access control model within collaborative environment, particularly KMS.

The reason to deploy access control model (ACM) is due to its capability to adopt collaborative system criteria while presenting itself as a role to protect knowledge access. Access control policies and roles have been introduced in order to avoid chaos in collaborative applications [7]. ACM for collaborative KMS is categorized into two parts, which is static, mainly can be specified during design time and dynamic, is principally regarding on run time enforcement mechanism. The verification study shows that the criteria of ACM model are important to secure KMS in collaborative environment.

The rest of the paper is organized as follows: The next section describes the problem of security in KMS, which relate to access control. Section 3 will present and analyze some related works, while Section 4 introduces the RBAC Model for secure KMS and the way of conducting the verification study. The RBAC model approached is evaluated in Section 5 and, finally, the paper is concluded in Section 6.

## **II. PROBLEM DEFINITION**

The case study done by the previous researchers found that organizations have lost critical knowledge where there was a little or no coordination or control over the transfer of tacit knowledge [4]. The more devastating risk was regard of transferring knowledge, where conceivably the knowledge was not going to the right people for decision-making process and this would results incorrect decision making due to inappropriate applying knowledge. Nevertheless the most frequent issues when dealing with KMS are related to unauthorized access. Colarik [8] pointed out that there are threats in organizations, which commonly targeted to critical knowledge such as stealing knowledge by terrorists, espionage agents, and other organized criminals. Therefore, these risks must be controlled and we need to restrict the access in order to protect knowledge repositories, knowledge mnemonic functions, and knowledge communication processes. Ultimately, confidentiality and availability of knowledge could be maintained.

## **III. RELATED WORKS**

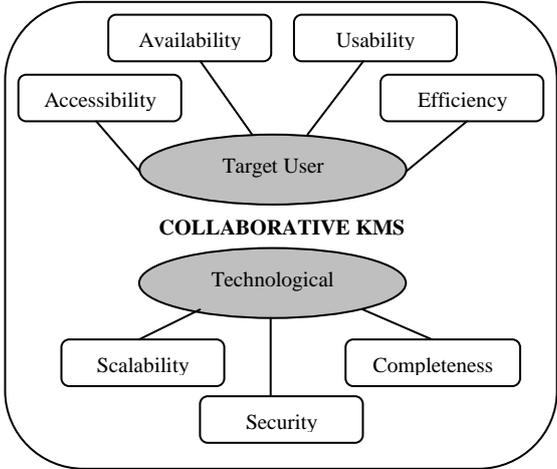
### **A. Collaborative Knowledge Management System (KMS)**

KMS is a computer based communications and information systems that supported knowledge management activities. Furthermore, collaborative KMS enables members to contribute their skills, knowledge and strength towards missions or objectives in order to achieve the best result of the projects. Knowledge process in collaborative KMS involves collaborative communication which provides synchronous (real time) and asynchronous (different time) mode where an organization needs to consider time and place during communication as to improve communication due to the competency of collaborative computing. Expanding

traditional KMS to collaborative KMS would give more benefit to KMS' CoP as knowledge can be shared and accessed from dispersed geography in secured environment.

**B. Collaborative KMS Characteristics**

Collaborative system characteristics have been categorized into four aspects which are, technological, social and economy, nature and activities, and target group [9]. However this research spotlight only on two aspects; technological and target user, towards constructing a security model for collaborative KMS. Nevertheless, the researcher need to aware as each aspect identified is constructed with other sub-criteria as shown in Fig 1.



**Fig. 1: The characteristics of collaborative KMS**

**C. Access Control For Collaborative Environment**

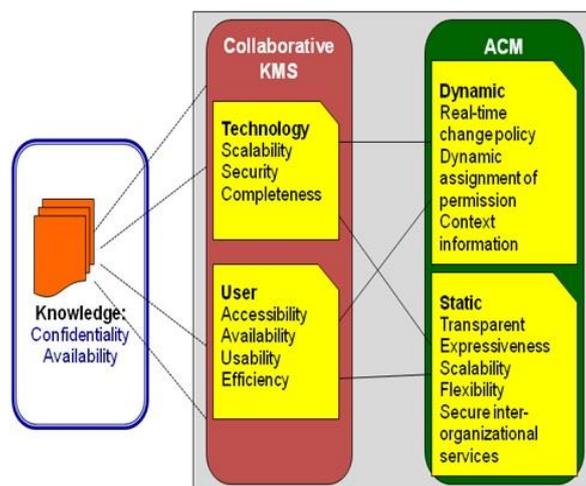
Access control model can play the role for managing the restrictions toward secure collaborative KMS. Table 1 summarize the characteristics of access control determined in previous researches by Tolone et al. [10], Lu et al. [11] and Chen [12].

**TABLE I CHARACTERISTICS OF ACCESS CONTROL IN COLLABORATIVE ENVIRONMENT**

Characteristics	Tolone et al.	Yahui Lu et al.	Tsung-Yi Chan
Transparent	√	√	
Expressiveness	√	√	
Scalability	√	√	
Flexibility	√	√	√
Runtime change of policy	√	√	
Dynamic assignment of permission	√	√	

Characteristics	Tolone et al.	Yahui Lu et al.	Tsung-Yi Chan
Context information	√	√	√
Secure inter-organizational services (permission between domains)		√	√

Furthermore, Abu Bakar et al. [13] have distinguished the criteria into two parts which are static; can be specified during design time and dynamic; that regarding on run time enforcement mechanism. Hence, they found that these criteria can be adopted in constructing secure environment of collaborative KMS.



**Fig. 2: Access Control Model for Collaborative**

## IV. METHODOLOGY

In order to verify the model of ACM, we go through these steps: review the ACM model and detail up each possible criteria, categorized the criteria under main characteristics and finally do a survey using questionnaire to the targeted group of users.

### A. Table of ACM Characteristics

As discussed earlier, ACM for collaborative KMS is categorized into two parts, which static and dynamic. In addition, there are relevant relationships of criteria that can be adopted to support collaborative KMS towards constructing secure KMS (Fig 2). In order to get more comprehensive criteria of the model, we have conducted further study and managed to wrap up the criteria by grouping based on main characteristics. The outcome is called Quality Dimension Table as shown in Table 2. There six main characteristics that ACM should grant towards secure collaborative KMS: reliability, access, usability, flexibility, security and

functionality. Moreover, the ACM should cater as well the other criteria in the proposed model while constructing secure collaborative KMS.

**TABLE II QUALITY DIMENSION TABLE**

Dimension	
<b>Reliability</b> [14][15][16]	Accuracy [15][16][17]
	Consistency [15][18][19]
	Credibility [19][14]
<b>Access</b> [14][17]	Accessibility [14][19]
	Availability [18][20]
	Timeliness [19]
<b>Usability</b> [14][19][17]	Easy to Use and retrieve knowledge [18][15]
	Communication and Knowledge Sharing [15][19][6]
<b>Flexibility</b> [14][15][19]	Scalability [19][6]
	Compatibility [14]
	Interoperability [16][19]
<b>Security</b> [14][15][21]	Privacy [14]
	Confidentiality [14][16][20]
	Control [19]
	Integrity [16][17][20]
<b>Functionality</b> [14][19]	Completeness [14][15][17]
	Performance [15][17][19]

### **B. Verification Works on ACM Characteristics**

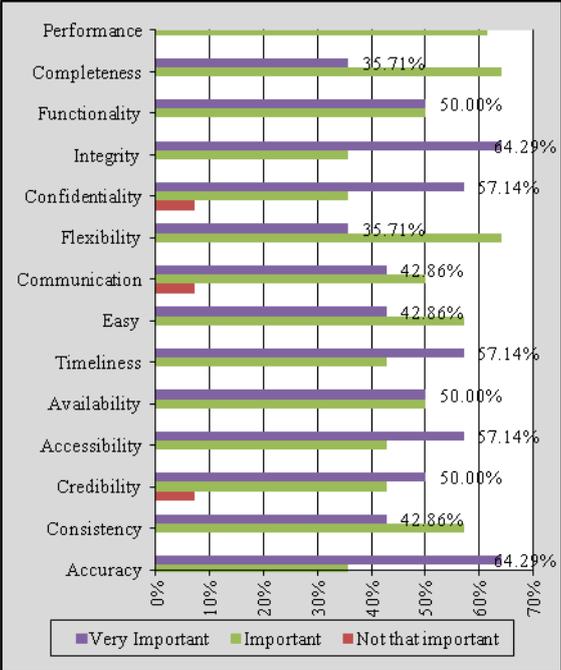
We have organized a study to investigate security awareness among KMS's practitioners in Higher Learning Institution (HLI) which focus on knowledge sharing activity. A set of survey questionnaire has been prepared for assessing respondent's understanding and insights. It was designed with several sections; however there is a section specifically to assess respondent's view on quality dimensions on security model pertaining to secure collaborative KMS.

The survey questionnaire was developed using online application and sent randomly to six public HLI in Malaysia by email. The targeted groups were from different groups of users, who post different roles in the organizations, such as lecturers, admin staffs, researchers,

system admin and IT people, and they were also from various departments or faculties. The questionnaire was opened in online for two weeks and we got 12% respondents returned the questionnaire with fully answered and were chosen for this analysis. The analysis was done using Microsoft Excel for basic data analysis.

### V. RESULT OF VERIFICATION STUDY

Result of the study shows in Fig 3, where the most important characteristics for ACM in constructing secure collaborative KMS are *Accuracy* and *Integrity* which 64% of respondent highlight it as very important criteria. This is to ensure that the degree of data transferred is correct, accurate and up to date. The data also must proper so that the system can work correctly.



**Fig. 3: Result on ACM characteristics**

However, the characteristics of *Availability* and *Functionality* got equal result from respondents, where 50% of respondents chose it as a very important criteria and another half chose it as important only. This shows that KMS have to meets the organizational objectives, operational standards and users’ knowledge need. It is also must be available to the authorized users when they need it. Moreover, secured KMS ought to be sufficient and comprehensive system. It is possible to acquire knowledge in different situations or conditions and the main functions are expected throughout KM processes within this system. Therefore, most of the

respondents where about more than 60% agreed with the criteria of *Flexibility*, *Completeness* and *Performance* to be considered for ACM in order to secure KMS.

Nevertheless, while most of the respondents agreed the *Credibility*, *Communication* and *Confidentiality* are important criteria to take into account, but there is small number of respondents which about 7.14% thought the criteria not that important in developing secure KMS. Ultimately, all respondents agreed with the criteria of Consistency, Accessibility, Timeliness and Easy to Use, where the result showed almost equal response from the respondents which they chose Important and Very Important.

## **V. CONCLUSION & FUTURE WORKS**

One of the most important pillars in KMS for organization is distributing knowledge where it is about sharing knowledge. In collaborative environment of KMS, this practice could allow the CoP to share their skills, knowledge and so forth at any time and any place. However, security becomes very significant element as knowledge will be shared among users from dispersed geographical area. The most frequent issues regarding security of KMS are related to unauthorized access. Thus, it is important to deploy a suitable security model in order to control the risks such as stealing knowledge by unauthorized users or other organized criminals. Therefore, this research study on ACM which this model is recognized as excellent model to restrict the permission to knowledge access [5]. However, for this research, the security model of ACM should looking into the characteristics of collaborative system as the KMS will be developed in collaborative environments.

Preliminary stages of this research, we have defined characteristics which known as Quality Dimensions. The dimensions highlighted were the criteria that can use as benchmark in order to construct secure KMS in collaborative environment. The researcher has done a study in order to get feedback from CoP regarding the highlighted criteria by distributing online questionnaire to multi level groups of respondents. Therefore, this paper is to report the result of the study so called verification study pertaining the Quality Dimensions.

Generally, respondents agreed almost all fourteen (14) criteria highlighted in the Quality Dimensions, and *Integrity* seems to be very important characteristics which majority chose on that dimension as 'Very Important'. However for criteria of *Credibility*, *Communication* and

*Confidentiality*, there were small percentage which about 7.14% of respondents thought it were not so important criteria to be considered in constructing secure KMS.

For future works, a researcher will develop a prototype system of Collaborative KMS where applying RBAC as a security model. The Quality Dimensions will be the benchmark for making KMS really secured and knowledge in KMS will be protected from unauthorized access.

## REFERENCES

- [1] J. H. Wu and Y. M. Wang, "Measuring KMS success: A respecification of the DeLone and McLean's model," *Inf. Manag.*, vol. 43, pp. 728–739, 2006.
- [2] R. Abdullah, *Knowledge Management System in a Collaborative Environment*. Serdang, Malaysia: Penerbit Universiti Putra Malaysia, 2008.
- [3] W. R. King, "Knowledge Management and Organizational Learning," vol. 4, pp. 3–13, 2009.
- [4] M. E. Jennex and S. Zyngier, "Security as a contributor to knowledge management success," *Inf. Syst. Front.*, vol. 9, no. 5, pp. 493–504, Oct. 2007.
- [5] X. Zu, L. Liu, and R. Xu, "Access Control Architecture Design Issues in Enterprise Collaborative Environment," 2009 *Int. Conf. Manag. Serv. Sci.*, pp. 1–4, Sep. 2009.
- [6] E. Ngai and E. Chan, "Evaluation of Knowledge Management Tools using AHP," *Expert Syst. Appl.*, vol. 29, no. 4, pp. 889–899, 2005.
- [7] H. Zhu, "Role Mechanisms in Collaborative Systems," *Int. J. Prod. Res.*, vol. 44, pp. 181–193, 2006.
- [8] A. M. Colarik, *Cyber Terrorism: Political and Economic Implications*. Igi Global, 2006.
- [9] M. Doinea and W. Van Osch, "Collaborative Systems : Defining and Measuring Quality Characteristics," *J. Appl. Collab. Syst.*, vol. 2, no. 1, pp. 50–61, 2010.
- [10] W. Tolone, G.-J. Ahn, T. Pai, and S.-P. Hong, "Access control in collaborative systems," *ACM Comput. Surv.*, vol. 37, no. 1, pp. 29–41, Mar. 2005.
- [11] Y. Lu, L. Zhang, and J. Sun, "Task-activity based access control for process collaboration environments," *Comput. Ind.*, vol. 60, no. 6, pp. 403–415, Aug. 2009.
- [12] T.-Y. Chen, "Knowledge sharing in virtual enterprises via an ontology-based access control approach," *Comput. Ind.*, vol. 59, no. 5, pp. 502–519, May 2008.

- [13] A. Abu Bakar, R. Abdullah, N. I. Udzir, and H. Ibrahim, "An Empirical Study of the Characteristics of Access Control Model Towards Secure KMS in Collaborative Environment," in *International Conference on Electrical Engineering and Informatics*, 2011, no. July.
- [14] M. S. Owlia, "A framework for quality dimensions of knowledge management systems," *Total Qual. Manag. Bus. Excell.*, vol. 21, no. 11, pp. 1215–1228, Nov. 2010.
- [15] D. A. Garvin, *Managing Quality: The Strategic and Competitive Edge*. New York: The Free Press, 1988, p. 319.
- [16] M. Usrey and K. Dooley, "The Dimensions of Software Quality," *Qual. Manag. J.*, vol. 3, no. 3, pp. 67–86, 1996.
- [17] M. E. Jennex and L. Olfman, "Modeling Knowledge Management Success," in *Conference on Information Science and Technology Management (CISTM)*, 2004.
- [18] W. E. Sasser, R. P. Olsen, and D. D. Wyckoff, *Management of Service Operations*, 2nd ed. Boston: Allyn & Bacon, 1978.
- [19] A. Tiwana, *The Knowledge Management Toolkit: Orchestrating IT, Strategy, And Knowledge Platforms (2nd Edition)*, 2nd ed. Prentice Hall, 2002, p. 416.
- [20] I. M. Olson and M. D. Abrams, "Information Security Policy," in *Information Security: An Integrated Collection of Essays*, Los Alamitos, California: IEEE Computer Society Press, 1995, pp. 160–170.
- [21] M. S. Adalati, P. Akhavan, and R. Hosnavi, "Essential Issues in Knowledge Management System Implementation: Lessons from Iranian IT-Based," in *11th International Conference of Social Responsibility, Professional Ethics, and Management*, 2010, no. November, pp. 24–27.