VOL. 10, NO. 3, FEBRUARY 2015 ISSN 1819-6608

ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A FRAMEWORK OF SECURE KMS WITH RBAC IMPLEMENTATION

Azreena Abu Bakar[1] and Rusli Abdullah[2]

[1]Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, Nilai, Negeri Sembilan, Malaysia

[2]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, UPM Serdang, Selangor, Malaysia

E-Mail: azreena@usim.edu.my

ABSTRACT

Knowledge Management System (KMS) is a tool to support knowledge management (KM) and nowadays it has been a priority to the organizations as to protect the organization intellectual assets. The evolution of internet has brought KMS becomes more powerful while it can serve users in collaborative system. However, though the excitement of expanding KMS capabilities, security issue is critical due to the access and sharing knowledge which from distributed locations. 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 KM activities. Thus, this paper review the characteristics of collaborative KMS in order to ensure that Role Based Access Control (RBAC) is competent to perform as a security model for KMS and at the same time maintain the advantages of such collaborative system. Consequently, the model of Role Based Access Control-Knowledge Management System (RBAC-KMS) has been formulated which concerning three elements; RBAC, KMS and Information Security (IS). Moreover, the quality dimension model also has been constructed which can be the metrics for quality measurement of RBAC-KMS

Key words: collaborative KMS, secure KMS, role based access control, quality dimension.

INTRODUCTION

Knowledge is an intellectual property of an organization which should be well managed. Knowledge Management (KM) is conscious effort to provide proper knowledge in such way at the right time, at the right place, in the right form, to the right knowledge worker, so that people can share and put information into action in turn that improve organization's performance and enhance the value of organizations. Knowledge Management System (KMS) endeavour to 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. This so called collaborative KMS, where knowledge can be shared inter-organization as well as other community of practice (CoP). Therefore security is crucial, since no one can restrict the knowledge sharing geographically and furthermore as an intellectual property, it should be protected. Security is a contributor to knowledge success, which need to assure the knowledge confidentiality and availability is protected, as well as the access control need to be operational (Jennex and Zyngier, 2007).

As the KMS works within collaborative environment, the access control should cater the CoP from different places and access knowledge with different technologies, thus access control model (ACM) established as a great security model to restrict the permission of knowledge access (Zu et al., 2009). This paper reviewed the criteria of ACM when applied in collaborative environment, for the purpose of protecting knowledge regarding its confidentiality and availability.

Security is a major issue when involve with sharing and transferring knowledge activities as knowledge can contribute to a competitive advantage. Form the case study analysis; found that organizations lost critical knowledge because of less or no control over the transfer of knowledge, and also which regard to the process of transferring knowledge (Jennex and Zyngier, 2007). The other risk of not proper managing access was incorrect decision making due to incorrect applying knowledge because the people was not get the right knowledge. Therefore this paper reviewed about security for KMS, as well as the architecture and aspects that enable to be the benchmark for constructing secure KMS. In this paper we also pay attention to the quality dimension of KMS where it then being modelled to be the metrics for the constructed framework.

The rest of this paper is organized as follows: In Section 2, we examine about KMS with considered collaborative environment as well as the characteristics of collaborative KMS. Section 3 presents the access control characteristics in collaborative environment. In Section 4, we review about secure KMS, the aspects and architecture. Section 5, will discuss the way of conducting the study in order to formulate the model. And finally Section 6 and Section 7 discuss the finding which about model of RBAC-KMS and also the conclusion of the paper as well as future works should be done to details out the model.

KNOWLEDGE MANAGEMENT SYSTEM

Knowledge management

The main goal of knowledge management is to improve organizational performance by enabling individuals to capture, share and apply their collective knowledge (Smith and Farquhar, 2000). Knowledge Management System (KMS) is a computer based communications and information systems that supported

knowledge management. On one hand, KMS promotes sharing of knowledge among CoP members but on the other hand it requires security mechanisms to prevent unauthorized access and misuse. Security plays a major issue revolving around KMS (King, 2009).

Collaborative KMS

Collaborative KMS enables members of CoP to contribute their skills, knowledge and strength towards missions or objectives in order to achieve the best result of the projects. First and foremost, before further discussion about the communication in collaborative KMS, we need to have the idea of collaborative KMS framework. The proposed framework of collaborative KMS contains six components (Abdullah et al., 2005):

- KMS functionality and architecture as the backbone towards support KM portal system
- Knowledge Management infrastructure and technology
- Knowledge management taxonomy and process model where this is to categorise the knowledge and process them before the knowledge is stored in KM repositories
- Knowledge management system soft issues which this component is to describes the psychological and sociocultural components necessary
- Knowledge management audit

Subsequently, knowledge process involves collaborative communication which provides synchronous and asynchronous mode, thus an organization need to consider the time and place in order to improve communication among the CoP due to the competency of collaborative computing.

The system serves the Cop with normal communication in synchronous (real time) and asynchronous (different time) mode, and also notification system that are based on the condition of previous profile.

Consequently, expanding traditional KMS to collaborative KMS would give more benefit to KMS's Cop. However security is the issue as the method involves sharing and accessing knowledge within dispersed geography.

Characteristics of collaborative KMS

The dynamic interaction between partners in collaborative environment is a great challenge in terms of synchronous and asynchronous communication (Fuks et al., 2001). Therefore, identifying the characteristics of collaborative KMS are important in order to discover an appropriate security model towards securing KMS.

The characteristics of collaborative system have been categorized to four criteria which are, target group, technological aspect, social or economy aspect, and the nature of activities aspect (Doinea and Van Osch, 2010). Nevertheless only two aspects, target user and technological, have been the focal point of this research as to construct a security model towards secure KMS in collaborative environment.

The Figure-1 shows the other sub- criteria for the particular criteria involved. Therefore, the researcher should aware the characteristics whilst describing a security model for developing a secure collaborative KMS.

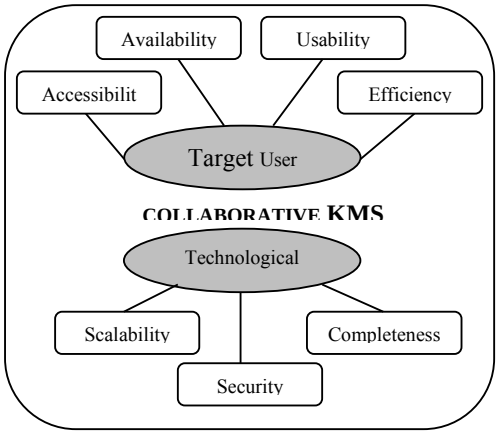

Figure-1. The characteristics of collaborative KMS.

ACCESS CONTROL FOR COLLABORATIVE ENVIRONMENT

Access control model (ACM) characteristics

Access control model can play the role for managing the restrictions toward secure collaborative KMS. Table-1 lists the characteristics of access control identified by (Tolone et al., 2005), (Lu et al., 2009) and (Chen, 2008) for collaborative KMS.

Table-1. 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	√	√	
Context information	√	√	√
Secure inter-organizational services (permission between domains		√	√

The summarization shows that (Lu et al., 2009) agreed on all of the eight criteria listed in the table, however (Tolone et al., 2005) did not mention about the restriction of giving permission for inter-domain, and (Chen, 2008) has stated only for three criteris which are flexibility, information on the context and security in inter-organizational services.

In paper by (Abu Bakar et al., 2011), the authors have categorized the listed criteria into two parts which are static, where can be specified during design time, and dynamic, that regarding on run time enforcement mechanism. As a result, the characteristics can be adopted in order to support collaborative KMS towards constructing secure KMS, as shown in Figure-2.

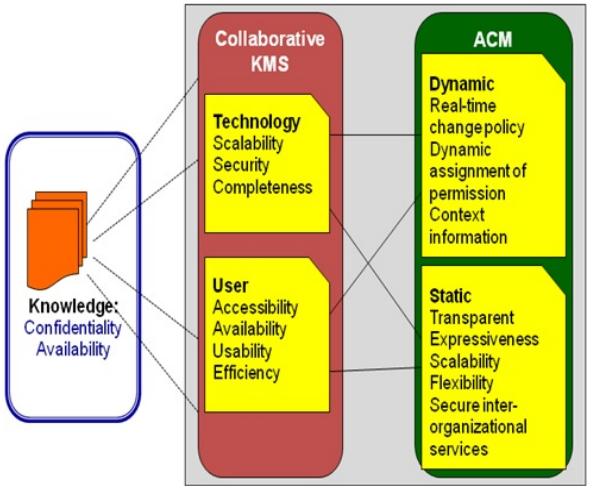

Figure-2. Access control model for collaborative kms.

Intentionally the model was focusing on the successful of protecting the confidentiality and availability of knowledge in the system, and the centre of attention were the characteristics of technological and the target users. Therefore, this model has proved that ACM proficient to be implemented as a security model for collaborative KMS.

Role based access control (RBAC)

The RBAC is an access control technique and notion. It has been regarded as an effective measure to resolve resource unified access control of large information systems by the public. The essence of RBAC is that permissions are granted to roles rather than individuals based on their qualifications and responsibilities. In paper by (Sandhu et al., 1996), the authors have stated that RBAC model consists of two logical independent parts for specifying user authorization which one assigns users to roles and the other one assigns access rights for objects to roles as illustrated in Figure-3.

User membership in roles can revoke easily and new operations established as job assignments. This would facilitate such an easy way to manage the permissions while roles can be updated without updating the permissions for every individual user. Moreover RBAC supports session activation where it enables a single user to activate permissions of a subset of roles to which he/she belongs. In addition it capable to impose constraints on user membership by assigning user to roles and this is uniquely applied to a collaborative environment (Tolone et al., 2005).

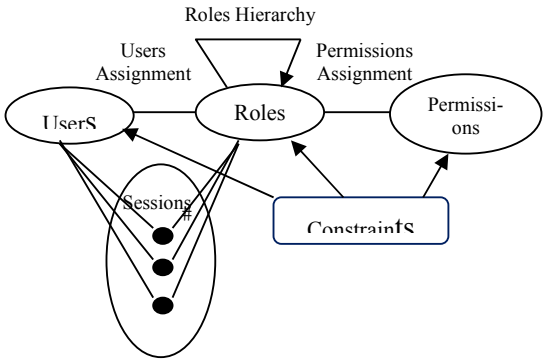

Figure-3. RBAC model.

The main idea of RBAC is to conduct the access authorizing and control according to the role acted by the user in a group deciding a user whether have the right to operate on a specific resource or not. Furthermore, the core feature of RBAC is to give authorities to roles but not users. When a role is designated to a particular user, the user will get all of the authorities that the role has been assigned. However, different users can be designated same or different roles, and a user can hold one or more role in the same time, and a role as well can belong to other users and users' access resources indirectly by roles. It add roles between users and accessed resources, with the agency of roles, RBAC implements the resources access encapsulation of users indirectly and logic separation between users and access authorities (Chuanfan, 2010).

Principally RBAC can help administrator by reducing workload in managing user's authorities, in this way, may save the expense of management as well. Furthermore, in paper by (Mohd Nor et al., 2009) found that roles is one of the main factors to be considered in interactions between persons. Therefore the researchers believe that this research is significant in order to develop secure environment of KMS.

SECURE KNOWLEDGE MANAGEMENT SYSTEM

Aspects of secure KM

KMS is a warehouse of the organization that store and process their very valuable and critical asset. Therefore, the management really wants to ensure that the knowledge must be protected, and also maintain the integrity and confidentiality (Jennex and Zyngier, 2007).

Zhou (Zhou, 2010) defined secure knowledge management consists of some strategies. Secure strategies include the policies and procedures that an organization

set in place for protecting the intellectual property as well as during the sharing data. The strategies should be strongly integrated with business strategies. Furthermore the business process also should be in secure mode where security has to be incorporated. Thus secure processes for knowledge management are one of the elements that to be aware in order to secure KMS. Metrics for secure knowledge management should focus on the impact of security on knowledge management metrics. This research will produce a Quality Dimension Model as to measure the impact of the security model applied in KMS. Secure KMS also contributed by secure technologies which include technologies for data and information management. Hence the component of technologies must be secured in order to handle all the business processes.

Secure KMS

Secure KMS can be described in terms of the three Cs: communication, collaboration and content.

Fundamentally, the organization's asset of intellectual content resides in Secure KMS; it acts as a gateway to the repository. Practically the secure KMS involves multiple machines that located in dispersed geographical area and they are collaborative-enable. Therefore access control is a critical subject to be focused on, as to ensure that the right knowledge accessed or shared by the right person at the right place in the right time for collaborative effort.

A Secure KMS framework has been designed by (Upadhyaya et al., 2006) as shown in Figure-4.

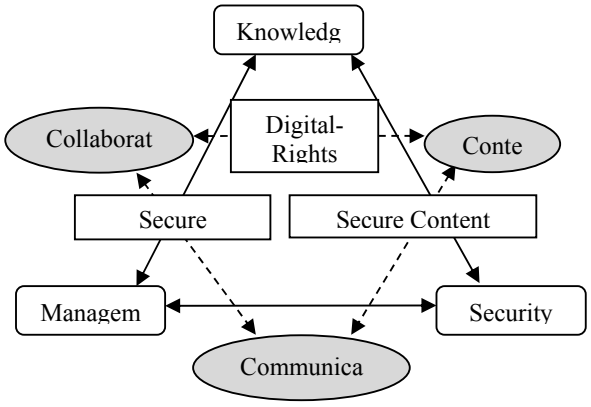

Figure-4. A framework of secure KMS.

The framework consists of two interlinked, triangular chains where the larger chain focuses on Security, Knowledge and Management, and the smaller triangular chain that connected with dotted line focuses on 3Cs: Content, Communication and Collaboration. Moreover different aspects contain within the smaller chain which include Secure Content Management, Secure Language and Digital-Rights Management.

Secure languages are utilized in order to secure the knowledge sharing activity. At the same time, Digital-Rights Management becomes critical in cross-organizational knowledge sharing, while access control and identity management play important role in securing knowledge management system. The final link is Secure Content Management that link between content and communication. Basically internet is a tremendous tool for enterprise to share intellectual property with the CoP, therefore they willing to expense money to support the cost of secure content management tools, which help to correctly label business-related content.

Quality dimensions of KMS

This section is to reveal the dimension of quality in or der to develop secure KMS. In paper of (Owlia, 2010), the quality dimensions of KMS has been described which the author has proposed a framework that consists of eight dimensions called Functionality, Completeness, Reliability, Usability, Access, Serviceability, Flexibility and Security. The credibility aspect can be attributed to reliability dimension where people only use the system that they trust. Credibility is generally related to the trustworthiness of an organization as perceived by the users (Tiwana, 2002). The success story of KMS also depends on accessibility aspect, which information or knowledge is available when the user need it (Tiwana, 2002) and (Owlia, 2010). Furthermore functionality where the system developed must meets organizational objectives, operational standards and user's knowledge need which describe the completeness of the system (Garvin, 1988), (Jennex and Olfman, 2004) and (Owlia, 2010). Usability aspect also can be the issue to get people use the system, the less effort required, the more people involved into the system (Tiwana, 2002) and (Jennex and Olfman, 2004). Another factor contributed to KM success is security (Garvin, 1988), (Owlia, 2010) and (Adalati et al., 2010) as to ensure the privacy and confidentiality confidentiality of the knowledge being protected. The system must prevent unauthorized disclosure of the information.

(Garvin, 1988) in research to proposed the quality dimensions of KMS defined both product and service quality, although they appear to be more products oriented. The factors of accuracy and consistency are attributed to reliability (Sasser et al., 1978) and (Garvin, 1988). Garvin, 1988). Therefore the data transferred must be correct, accurate and up-to-date (Usrey and Dooley, 1996) and (Jennex and Olfman, 2004) and the same service or product must be received each time (Olson and Abrams, 1995) and (Tiwana, 2002). To be more convenience and efficient, the system should be user-friendliness system in terms of ease to use and ease to knowledge retrieval (Sasser et al., 1978) and (Garvin, 1988). The extraordinary process of KMS is to promote knowledge sharing activity, thus the system enable to support the process of communication and knowledge sharing (Garvin, 1988), (Tiwana, 2002) and (Ngai and Chan, 2005). 'Performance' and 'completeness' of service are equivalent to the performance and features dimensions

product. The performance is related to core knowledge and main functions expected through the KM processes (Tiwana, 2002) and (Jennex and Olfman, 2004).

Instead of accessibility, (Tiwana, 2002) also considered Timeliness aspect which define as a quick response to users, it is important for KMS to provide knowledge 'when' needed. The combination of both access and timeliness, KMS may promote 'anytime and anywhere' access. Flexibility can be defined as the degree to which acquiring knowledge in different situations/ conditions is possible. In addition, several features that could be interpreted as quality dimension of the system have been pointed out in describing the structure of KMS, scalability (Tiwana, 2002), (Ngai and Chan, 2005), interoperability (Usrey and Dooley, 1996) and (Tiwana, 2002).

The development of RBAC model for secure KMS has taking into account of information security as well. Referring to (Olson and Abrams, 1995) knowledge confidentiality and integrity need to be protected, where these factors are main objectives in Information Technology (IT) security. In paper of (Usrey and Dooley, 1996), also stated these factors are consist withing 11 factors that still inclusive and form the basis for ISO/IEC 9126 standard for software quality evaluation. Other objective of IT security is availability (Sasser et al., 1978) and (Olson and Abrams, 1995) which to ensure knowledge is available to authorized users. However, it is being attributed to Access dimension. Futhermore (Owlia, 2010) also consider confidentiality, so thus (Jennex and Olfman, 2004) that stated integrity are such factors contribute to the success of KMS.

We believe that these dimensions are essential and need to be considered in order to construct a model of secure KMS, and probably it can be the metric for measuring the model performance later on. Figure-5 illustrates the analysis of previous researchers who highlighted the quality dimensions for KMS.

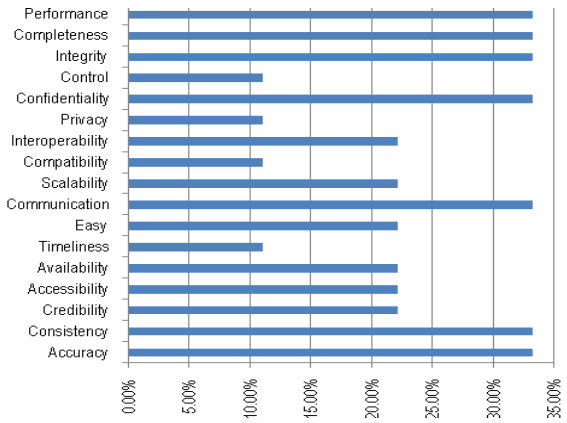

Figure-5. Analysis of quality dimension for KMS.

Figure-5 shows that the graph is uniform. About 33% agreed with the dimension of performance, completeness, integrity, confidentiality, communication (sharing of knowledge), consistency and accuracy. Besides, 22% choose the dimension of interoperability, scalability, easy to use, availability, accessibility and credibility. Whereas, control, privacy, compatibility and timeliness mentioned by 11% of the researchers. Therefore these dimensions need to take into account while developing the model of RBAC-KMS.

METHODOLOGY

In the process of developing a framework for secure KMS in collaborative environment, we have conducted an empirical study with quantitative approach. We started the work by searching related resources and previous works done by other researchers. Furthermore, we also got opinion from the experts via the questionnaire of survey. The domains that we focused on for the study were KMS, access control model and secure KMS regarding the architecture and characteristics.

The theories of KMS that we studied have considered the collaborative KMS, which taking into account the criteria of KMS in collaborative environment. Therefore access control to be implemented as the security model should be designed for collaborative KMS. Thus the study concentrated on the characteristics of access control to ensure that the right security model will be implemented which can deal with collaborative KMS. The researchers as well should acknowledge the requirements or the criteria of secure KMS in order to construct the framework. For that purpose, the study's scope involved also the aspects and architecture of the secure KMS. Coincidently the study grasped another sub domain, which is quality dimension of KMS. This can be applied as a metric for the framework afterwards.

This stage of study includes a preliminary survey as well. The survey was in likert scale form and the questions divided into some categories: knowledge concepts and understanding, security awareness, secure KMS, knowledge collaboration, RBAC-KMS architecture, and quality dimension. The survey has been distributed to some groups of people from higher learning institutions; lecturers, researchers and IT people. At this stage the survey was only distributed via on-line and six institutions have been chosen. The objective from the survey was to validate the requirements that have been gathered for constructing RBAC-KMS model. Therefore we would ensure that the things are right and we develop a right thing to reach the purpose.

Finally, we formulated framework of secure KMS in collaborative environment which apply role based access control as a security model. In addition, this paper constructed a model of Quality Dimension for the framework. This model will serves as a metrics for the framework in order to ensure that all the components that constructed the framework are in the right place and the

framework meet the objective as to improve the security of the KMS.

SECURE KMS FRAMEWORK

Framework of RBAC-KMS

This section will discuss the propose framework of RBAC-KMS. Initially the components of the framework were formulated from the preliminary study by reviewing the related studies. Nevertheless it has been validated via pre-survey questionnaire, which the respondents were the experts in this particular field. Basically, the topic in the survey for validating the components was under RBAC-KMS Architecture. The Figure-6 illustrates the analysis of the results from the respondents.

The survey was to get the feedback from the respondents about some ideas on the architecture of RBAC-KMS. The scale of the feedback was totally disagree, disagree, agree and totally agree. The first half of the questions, we want to know regarding the importance of some components in storing and organizing knowledge or information, such as KMS portal, knowledge repository, access control and policies, as well as authentication and authorization process. Next, we need to know their opinion on the levels of permission which depends on task or function (least privilege), and to verify that using role for managing the access is more convenience and it is useful feature.

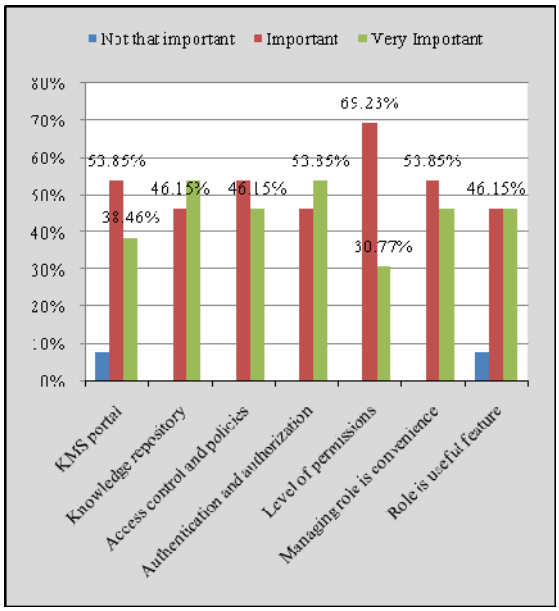

Figure-6. Analysis result of RBAC-KMS architecture.

The result of analysis shows that only KMS portal got a small percentage on not agree feedback, and also at role as a useful feature. However the rest of the components, the respondents have decided that they are significant for constructing RBAC-KMS.

The framework of RBAC-KMS built upon three areas of knowledge concerning the KM, RBAC and IS, and including the access authority authentication, design of authority management control module, access control logic and so on. The IS component is to construct a secure KM to serve the process of capturing, storing, organizing and disseminating knowledge in a secure environment. The basic framework of RBAC implementation of KMS is shown in Figure-7.

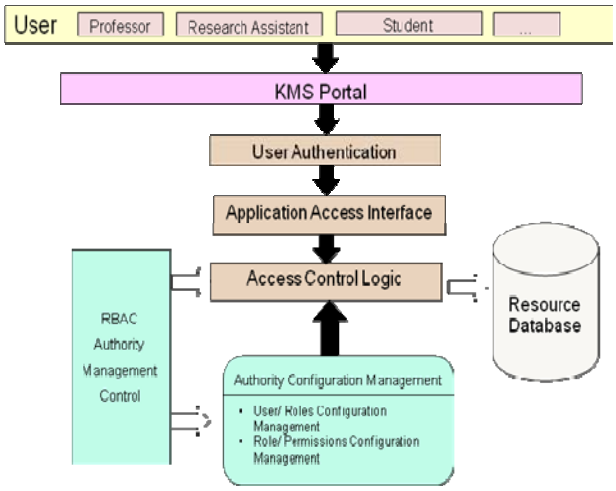

Figure-7. Framework of secure KMS: RBAC implementation.

When user access the system, their identities will be authenticated and followed by the authentication process of their access authorities, which the related authentication information such as username and password will be recognized and determined through information security services of the system.

The authority management module is maintainability and extendable as to keep modulate authority control with the iterative process of policy and regulation due to collaborative system that related with lots of people from different places. This module contains two parts which are authority list structure design and authority management mechanism design. The authority list structure design is to provide related information of authenticating users holding roles and roles holding authorities. While principally the design of authority management mechanism implements the configuration and management of roles and adding, deleting, maintaining user's profile and distributing roles to the users.

Moreover, the implementation of information resource access control logic is regarding the authority verification which is the main part to implement information resources access control mode, such as the access control of system menu and button display, the authority access control of information resource database.

Quality dimensions of RBAC-KMS

Secure KMS is the cornerstone of offering protected knowledge towards safe knowledge sharing. Therefore RBAC is used to complement sharing knowledge in secure environment.

The quality of RBAC-KMS is important in satisfying the needs of knowledge users. The criteria that found from the related studies regarding the quality dimensions of KMS by considering information security entities has contributes a basis for developing a model of RBAC for Secure KMS.

The Quality Dimension Model of RBAC-KMS is incorporated of six groups of domains; Reliability, Functionality, Access, Usability, Flexibility and Security. Principally the domains are determination of how quality dimensions/ factors are perceived and consequently the quality of RBAC-KMS can be measured or improve. The Table-2 shows the list of dimensions that consumed for the model.

Table-2. List of quality dimension.

Dimension	Description
Reliability	The degree of data transferred is correct, accurate and up-to-date.
Functionality	The degree to which the system meets organizational objectives, operational standards and user's knowledge needs
Access	The extent to which knowledge available for users
Usability	The effort required for using and involving in the system
Flexibility	The degree to which acquiring knowledge in different situations/ conditions is possible
Security	Confidentiality of information/ knowledge shared when necessary.

Furthermore, we found that the quality dimensions discussed in the previous section which shown in Figure-5 are significant in constructing the particular quality model. On top of that in our preliminary study of the survey questionnaire, the result shows that almost all respondents choose the dimensions stated as an important in developing the quality model for RBAC-KMS as shown in Figure-8.

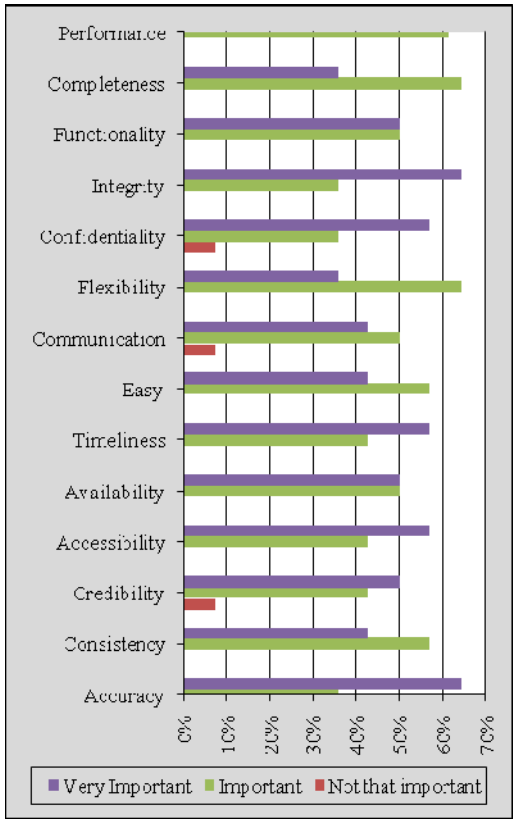

Figure-8. Analysis result of quality dimension from preliminary survey.

The analysis explains that the identified dimensions are significant in order to measure the quality of RBAC-KMS. Therefore the items have been categorized to the domains accordingly and become sub-domains for the Quality Dimension model. The Figure-9 illustrates the Quality Domains Model that can see for each domain consists of other sub-domains.

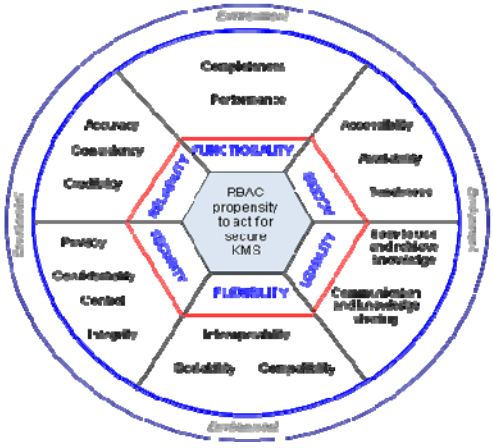

Figure-9. RBAC-KMS quality dimension model.

The domains that covered in the model are propensity of RBAC to act as to ensure KMS in secured for offering KM process.

CONCLUSIONS

Knowledge Management System in collaborative environment offer the best practice of knowledge sharing where CoP could share their skills, knowledge and so forth at any time and any place, however, the security aspect must be managed very well as the knowledge is asset for the organization and it will be shared among the users from dispersed geographical area. Therefore, RBAC will be deployed as to control the access without reduce the advantages of collaborative characteristics. The RBAC reduces the dependencies to the specific staffs and authorities through the change from user-based access authority to role-based access authority, and it also reduces the complexity of authority management and the management expense. Finally RBAC-KMS will ensure the quality of collaborative KMS by designing the Quality Dimension Model which can use as metrics to measure its performance.

In the future works, the researcher should study the issues in managing the access particularly on four activities of KM: create, store, share and apply. Then it should be tackled by defining the complete model of RBAC-KMS. The model afterwards will be translated to a prototype system which will emphasize every components of the model that constructs to secure KMS.

REFERENCES

Abdullah R., Sahibuddin S., Alias R. A. and Selamat, M. H. (2005). Collaborative Knowledge Management Systems for Learning Organisations. Journal of Information & Knowledge Management, 4(4), pp.237-245.

Abu Bakar A., Abdullah R., Udzir N. I. and Ibrahim, H. (2011). An Empirical Study of the Characteristics of Access Control Model Towards Secure KMS in Collaborative Environment. In International Conference on Electrical Engineering and Informatics. Bandung, Indonesia: IEEE.

Adalati M. S., Akhavan P. and Hosnavi, R. (2010). Essential Issues in Knowledge Management System Implementation: Lessons from Iranian IT-Based. In 11th International Conference of Social Responsibility, Professional Ethics, and Management, pp. 24–27.

Chen T.-Y. (2008). Knowledge sharing in virtual enterprises via an ontology-based access control approach. Computers in Industry, 59(5), pp.502-519.

Chuanfan L. (2010). Research on Role-Based Access Control Policy of E-government. 2010 International Conference on E-Business and E-Government, pp. 714-716.

Doinea M. and Van Osch W. (2010). Collaborative Systems : Defining and Measuring Quality Characteristics. Journal of Applied Collaborative Systems, 2(1), pp.50-61.

Fuks H., Raposo A. B., Magalhiies L. P. and Ricarte, I. L. M. (2001). Coordination of Collaborative Activities : A Framework for the Definition of Tasks Interdependencies. In Seventh International Workshop on Groupware, pp. 170-179.

Garvin D. A. (1988). Managing Quality: The Strategic and Competitive Edge (p. 319). New York: The Free Press.

Jennex M. E. and Olfman L. (2004). Modeling Knowledge Management Success. In Conference on Information Science and Technology Management (CISTM).

Jennex M. E. and Zyngier S. (2007). Security as a contributor to knowledge management success. Information Systems Frontiers, 9(5), pp.493-504.

King W. R. (2009). Knowledge Management and Organizational Learning, 4, pp.3-13.

Lu Y., Zhang L. and Sun J. (2009). Task-activity based access control for process collaboration environments. Computers in Industry, 60(6), pp.403-415.

Mohd Nor M. Z., Abdullah R., Selamat M. H. and Azmi Murad M. A. (2009). Knowledge Sharing Interactions in Collaborative Software Maintenance Environment. 2009 International Conference on Computer Technology and Development, pp.201-205.

Ngai E. and Chan E. (2005). Evaluation of Knowledge Management Tools using AHP. Expert Systems with Applications, 29(4), pp.889-899.

Olson I. M. and Abrams M. D. (1995). Information Security Policy. In Information Security: An Integrated Collection of Essays (pp. 160-170). Los Alamitos, California: IEEE Computer Society Press.

Owlia M. S. (2010). A framework for quality dimensions of knowledge management systems. Total Quality Management & Business Excellence, 21(11), pp.1215-1228.

Sandhu R. S., Coyne E. J., Feinstein H. L. and Youman, C. E. (1996). Role-Based Access Control Models yz 1 INTRODUCTION, 29(2), pp.38-47.

Sasser W. E., Olsen R. P. and Wyckoff D. D. (1978). Management of Service Operations (2nd ed.). Boston: Allyn & Bacon.

Smith R. G. and Farquhar, A. (2000). The Road Ahead for Knowledge Management: An AI Perspective. AI Magazine, 21(4), pp.17-40.

Tiwana A. (2002). The Knowledge Management Toolkit: Orchestrating IT, Strategy, And Knowledge Platforms (2nd Edition) (2nd ed., p. 416). Prentice Hall.

Tolone W., Ahn G.-J., Pai T. and Hong S.-P. (2005). Access control in collaborative systems. ACM Computing Surveys, 37(1), pp.29-41.

Upadhyaya S., Rao H. R. and Padmanabhan G. (2006). Secure Knowledge Management. IGI Global, pp.795-801.

Usrey M. and Dooley K. (1996). The Dimensions of Software Quality. Quality Management Journal, 3(3), pp.67-86.

Zhou H. (2010). The Study on Secure Strategy for Knowledge Management. Journal of Computers, 5(10), pp.1597-1605.

Zu X., Liu L. and Xu R. (2009). Access Control Architecture Design Issues in Enterprise Collaborative Environment. 2009 International Conference on Management and Service Science, pp.1-4.