Modelling a Trusted Mechanism for Knowledge Sharing

Marius PETRESCU
Valahia University, Târgovişte, Romania
E-mail: marius.petrescu@orniss.ro
Tel.: +40245206104, Fax : +40245206104
Delia Mioara POPESCU
Valahia University, Târgovişte, Romania
E-mail: depopescu@yahoo.com
Tel.: +40245206104, Fax : +40245206104
Nicoleta SÎRBU
Valahia University, Târgovişte, Romania
E-mail: nicoleta.sirbu@gmail.com
Tel.: +40245206104, Fax : +40245206104

Abstract

Knowledge sharing has been identified as a major focus area for knowledge management. Efforts are made with a view to identify the most effective ways to share knowledge, as a step towards improving organizational performance.

In this striving, various factors have been identified as impediments for knowledge sharing, including inadequate organizational structures, sharing unfriendly organizational cultures, and denominational segregation. Related problems may occur when information systems, such as intranets, distributed libraries, document management systems, or groupware applications, are introduced to support knowledge sharing. The extensive use of the IT&C has only added new questions on how to address issues of trust within the present knowledge -rich environment.

This paper proposes a new way of approaching knowledge sharing in the context of information and communication technology development. The study provides an overview of the manner and extent in which information assurance concepts of integrity, authenticity, availability, non-repudiation and access-control may be employed to ensure a trusted and effective knowledge sharing process.

Keywords*: knowledge sharing, sharing policy, access control, trusted knowledge sharing, barriers in knowledge sharing*

JEL classification: D83, A12

Introduction

The new production of knowledge can be characterized by some main features highlighted by M. Gibbons as being (Gibbons, 1998): knowledge production in context of application, transdisciplinary nature of the approach,

heterogeneity and diversity of institutions involved in research activities, a greater social responsibility of research priorities and its consequences, as well as a wider (social) quality control of the research. And the process of knowledge reconfiguration is held not only in universities and research institutes, but also in consulting and research, industry and governmental agencies or in the framework of partnerships and alliances formed between these categories of organizations. It outlines a distributed knowledge production system, having held such a merger between the university's role (providing general education and basic research) and that of other institutions that produce specialized knowledge (applied research and training in the workplace). Organizations promoting knowledge systems by integrating education, research, innovation and ensuring their competitiveness gain increasing importance in the context of globalization of the knowledge production and dissemination (Saint-Onge H., 2003).

Knowledge is a very complex issue and also inexhaustible. At the same time, it is undoubtedly that the world progress is based on the scientific knowledge gain and on increasingly efficient technologies employed for its exploitation. Note, however, that as the process of scientific knowledge accumulation intensifies, the reality discovered through knowledge becomes more complicated.

Knowledge sharing is something else than but related to communication and to information distribution (Hendriks, 1999). Knowledge sharing presumes a relation between at least two parties, one that possesses knowledge and the other that acquires knowledge. The first party should communicate its knowledge, consciously and willingly or not, in some form or other (either by acts, by speech, or in writing, etc.). The other party should be able to perceive these expressions of knowledge, and make sense of them (by imitating the acts, by listening, by reading the book, etc.). The resemblances between knowledge sharing and information distribution, however, gave us the basis to formulate the premises for the proposed model.

From a historical perspective we cannot ignore the superiority of the present moment in the evolution of knowledge, through worldwide attention to this phenomenon, the awareness of knowledge as a possible solution to problem that humankind will face in the future, through emphasis on continuous learning and scientific research, through the importance granted to the production and use of the knowledge.

The study results in a model of a trusted knowledge sharing mechanism based on information and communication technology, at the level of an organization. The model starts from the premises that within an organization certain knowledge has to be shared to certain employees, in due time. In this, the model exploits the information assurance primary objective of ensuring “the right information, for the right people, at the right moment”. The central element of the knowledge sharing model proposed consists of an organization data base of knowledge on which certain sharing policies are implemented, on the basis of “need-to-share” principle.

The study outlines how this kind of approach creates a more motivating climate for knowledge sharing, streamlines this process within an organization, and ensures a more efficient exploitation of the information and communication resources.

1. Barriers in knowledge sharing

One of the challenges of knowledge management is that of getting people to share their knowledge. The exchange of information is a vital component of the knowledge management process.

In many organizations, the need for active knowledge sharing is accepted, but all too often in practice the belief exists that waving a sophisticated and expensive information technology system is all that is needed for good knowledge management (Kluge J. et. al., 2001).

Despite the growing significance of knowledge sharing practices for organizations' competitiveness, several barriers make it difficult for knowledge management to achieve the goals and deliver a positive result. Some of the common reasons people and, ultimately, organizations, are skeptical in sharing knowledge are: the reign of the principle "knowledge is power", not realizing how useful particular knowledge is to others, lack of trust, lack of time, individualism, poor means of knowledge capture, inadequate technology, internal competition and top-down decision making.

Modern information and telecommunication technology is available to support knowledge sharing across time and distance barriers improving access to information about knowledge (Thierauf R. J., 1999). However, organizations investing in this type of technology often face difficulties in encouraging their employees to use the systems to share their ideas (Cabrera, 2002).

Looking at information and communication technology for knowledge sharing in this light, however, cannot by itself solve other problems such as lack of trust. No matter how motivated they are, entities (either organizations or people) do not share knowledge with those they do not trust.

This paper will focus on the lack of trust people manifest in sharing knowledge. We view a directly dependency relationship between inter-organization (or interpersonal) trust and information sharing. Some trust (minimum threshold) is necessary for one party to share information with another party. Thus, some trust is a required condition for information sharing. However, as one party begins to share information with the other party, then trust increases. This begins a relationship characterized by mutual causality (Dyer et. al., 2000).

Efficient and secure knowledge sharing is critical to the success of an organization and, ultimately, for the enhancement of global competitiveness (Tsung, 2008). The central goal of secure knowledge sharing is to "share but protect" where the motivation to "protect" is multiple, comprising the protection of the content to avoid loss of revenue as in copy rights management, ensuring the integrity and authenticity of the information.

The need for secure knowledge sharing has dramatically increased with the explosion of the Internet and the convergence of outsourcing, off-shoring and B2B collaboration in the commercial arena, technology has made the "share" aspect ever easier so has it increased the difficulty of enforcing the "protect" aspect.

2. Premises for the proposed model

In this model, the knowledge sharing is viewed as a communication process, involving transmitting and emitting parties that exchange messages consisting of the knowledge content, across a communication channel, in an environment exercising perturbations over the entire process. In the database model we propose, the "transmitter" from the communication model may be identified with the person responsible with feeding the database and configuring access rights. The knowledge content itself is not transmitted but, only made available to entitled persons, i.e. the "receiver". In order to maintain the communication perspective, we will keep referring to the "transmitter" and "receiver" parties throughout the paper, with the understanding provided above.

From this model's perspective, the communication channel is based on the information and communication technology.

This model assumes that there is a need to share knowledge, either publicly, non-discriminatory, or by exercising a certain level of access control, as established by pre-defined criteria.

The premises of this model are that parties involved in knowledge sharing process have to trust each other (Jost J. T., 1999), have to trust the sharing channel (Lawler III E. E., 2001) and, at the same time, have to trust the content itself. In this trustfulness context, entities (either organizations or persons) would be more opened to share knowledge if they are convinced that the information they share is reaches the intended receiver, at a proper time and in a proper manner.

3. Trusted knowledge-sharing objectives

In the knowledge sharing process, both the transmitting and the receiving parties are interested that the shared knowledge to be as little altered as possible.

In order to create a trusted environment for knowledge sharing, we propose a model based on information assurance objectives. From this perspective, we the model envisages the following objectives in relation with the shared content:

Integrity. The shared knowledge content has to reach the intended receiver without being altered by the environment or by other factors, including human factors. By altering we understand either modification or partially or total deletion of the knowledge content.

Authenticity. The receiving parties of the shared knowledge content have to be sure that the information they receive is genuine, authentic and is generated by the alleged transmitter party, identified as the knowledge source. In the information and communication technology world, another facet of the authenticity

envisages the authenticity of the receiver itself, as well as that of the receiving system throughout which the know ledged is shared.

Non-repudiation. This objective ensures that neither the transmitting party, nor the receiving party can deny the transmission, respectively the receiving of the shared content after they did so.

Availability. Taking into consideration that we started from the premises that there is a need-to-share, the main scope of the communication process is to exchange the knowledge content to the intended receiving party. That is why one of the main objectives of the knowledge sharing process is the accessibility to shared content itself and to the systems throughout which it is transmitted.

There are situations when the knowledge content is addressed to only well-defined entities. In this case, the knowledge sharing should be performed discretionary, on a need-to-know principle basis, in accordance with well-defined criteria. This is the case when access-control mechanisms must be implemented in order to ensure access to the content only for authorized entities.

In reaching these objectives, certain measures have to be taken. The measures address both the system throughout which the knowledge content is shared and the human factors involved in the communication process.

4. Proposed trusted knowledge sharing model

As we mentioned above, the model is based on two pillars: the technical component, meaning the systems throughout which the content is shared in a trustful manner and the human factor involved in the sharing process that has to be aware of their responsibilities related to trusted knowledge sharing.

The model is developed to be applied at the level of an organization but, as the principles and objectives are generally applicable, it can be extended to inter-organizational sharing or more complex processes. The extension refers primarily to the extension of the technical component of the model. As for the human factor component, it plays a more sensitive role when different organizational cultures are involved in the sharing process.

4.1 Trusted knowledge sharing system

The central element of the proposed trusted knowledge sharing model consists of an organization data base of knowledge on which certain sharing policies are implemented, on the basis of "need-to-share" principle. Synthetically, this model's objectives can be summarized by saying that it seeks to ensure "the right information, for the right people, at the right moment".

Literature on information integration across databases tacitly assumes that the data in each database can be revealed to the other databases. However, there is an increasing need for sharing information across autonomous entities in such a way that no information apart from the answer to an authorized query is revealed.

The philosophy of ensuring trust requires that the access of entities (i.e. processes, users of the systems, knowledge recipients) to objects (i.e. sharing systems, shared knowledge) be mediated in accordance with an existing and well-defined access policy.

The design of mechanisms to control the sharing of information in communication and information system has to ensure the attaining of the sharing objectives specified above. The key mechanisms include access control lists, hierarchical control of access specifications, identification and authentication of users, and primary memory protection.

Our model tries to address, in an integrated vision, the specified objectives of integrity, authenticity, non-repudiation and availability. The key concept employed is the access-control to the database resources.

In ensuring an efficient o the knowledge content and, at the same time, an efficient access control, i.e. the data within the database, a centralized administrated database is proposed. And, when talking about administration of the knowledge database in the context of the proposed model, we do not refer only to implementing and maintaining access policies, but also ensuring the input of knowledge content into the database. In other words, the database is fed with knowledge content from a unique point, by authorized personnel. Access to knowledge content may be granted to the intended person by configuring the access control policy within the database application. By doing this, only entitled persons will have access to the piece of knowledge he or she needs to know.

This access control policy builds trust both on transmitter's side and on receiver's side. Both parties will be more willing to share knowledge: transmitter will be confident that the knowledge content will be accessed by the intended receiver and, on the other hand, the receiver will be confident that the knowledge contents he / she accesses is genuine.

Access control policies are a first step towards ensuring the integrity of the knowledge content. The term integrity is used in databases context with the meaning of accuracy, correctness and validity. The problem of integrity is the problem of ensuring that the data in the database is accurate – that is the problem of guarding the database against invalid modifications. Invalid modifications nay be caused by errors in data entry, by mistakes on the part of the operator or the application programmer, by system failures or even by deliberate falsification.

A control mechanism for validating data is to use a tamper-resistant counter, which cannot be decremented, in place of generic tamper-resistant storage. After each database update, the database increments the counter and generates a certificate containing the counter value and the database hash (Maheshwari, 2005).

Authenticity of the knowledge content results from the combined implementation of access control mechanisms and integrity mechanisms. In order to ensure non-repudiation of the knowledge content, from both transmitter side and receiver side database should be configured in such a way as to provide audit facilities and to keep record of the log files. Audit should be configured for data input and data access. The audit logs should be analyzed by the database

administrator, with a periodicity established in accordance with specific criteria such as: the sensibility of the data within the database, the periodicity of database consultation etc.

Availability plays a major role in knowledge sharing. From the information technology perspective, availability takes two forms: the availability of the systems throughout which the knowledge is shared that determines the availability of the knowledge content itself. In this respect, measures should be taken in order to ensure the redundancy of the systems themselves, especially when the knowledge content is vital for those who have a need to know for it. Another aspect knowledge content administrators should be aware is the necessity to create backups of the database, in order to be able to reinstall it on other systems, if an unpredicted situation occurs.

All these control mechanisms can be implemented in most of the database platforms. We do not intend here to make recommendations for a specific database platform, but to create an access control model in order to ensure the trust among sharing parties.

4.2 Human factor component

However strong and complex technical control mechanisms are, they cannot be efficient if they are not backed by a strong awareness of the personnel with a view to their responsibilities in ensuring the protection of the knowledge content. The human factor has to be addressed as an important one in this equation of ensuring a trusted knowledge sharing mechanism.

The awareness may be built by developing training programs for personnel involved in the knowledge sharing process, both administrators and users.

The personnel issue is proportional with the number of "receivers" of the knowledge content, with the complexity of the system and with the sensitivity of the data to be shared.

Conclusions

The model is scalable and may be applied by both small organizations and larger ones in order to ensure a more flexible and trusted system of sharing data among their personnel, as well as with other partner organizations.

At the same time, the model may result in cost reduction, due to its centralized concept with a view to resources. By creating and exploiting a centralized, uniquely administered knowledge database both IT&C and human resources are exploited more efficient than in a distributed system. Control over the resources, including material and knowledge is also better controlled in a centralized administered system.

Even throughout the paper we did not touch the confidentiality aspects of the knowledge content, but only those implying the integrity and authenticity, mechanisms may be implemented as an additional protection layer, in order to ensure

confidentiality, whenever necessary. These mechanisms consist in cryptographic solutions that may also provide non-repudiation and authenticity services.

References

1. Cabrera, Angel; Cabrera, Elizabeth F., 2002, "Knowledge Sharing Dilemma, Organization Studies", *Organization Studies*, vol. 23, No. 5, pp. 687-710
2. Dyer, Jeffrey H.; Nobeoka, Kentaro, 2000, "Creating and Managing a High Performance Knowledge-Sharing Network: the Toyota Case", *Strategic Management Journal*, 21; pp. 345–367
3. Chen, Tsung-Yi, 2008, *Knowledge sharing in virtual enterprises via an ontology-based access control approach*
4. Hendriks, Paul, 1999, "Research Article: Why Share Knowledge? The Influence of ICT on the Motivation for Knowledge Sharing", *Knowledge and Process Management*, Volume 6 Number 2 pp. 91–100
5. Gibbons, Michael, 1998, *Higher Education Relevance in the 21st Century*, The World Bank.
6. Jost, John T.; Kruglanski, Arie W. & Simon; Linda, 1999, *Effects of Epistemic Motivation on Conservatism, Intolerance, and Other System-Justifying Attitudes,* pp. 91-117 *from Shared Cognition in Organizations: The Management of Knowledge*, Editors: Leigh L. Thompson, John M. Levine, David M. Messick, ISBN 0-8058-2890-7, Lawrence Erlbaum Associates Publisher, Mahwah, NJ.
7. Kluge, Jurgen et. al., 2001, Knowledge *Unplugged: The Mckinsey & Company Global Survey on Knowledge Management*, ISBN 0-333-96376-8, Palgrave Publisher, New York
8. Lawler III, Edward E. et. al., 2001, *Title: Organizing for High Performance: Employee Involvement, Tqm, Reengineering, and Knowledge Management in the Fortune 1000 The CEO Report,*: ISBN: 0-7879-5689-9, Jossey-Bass Publisher, San Francisco
9. Maheshwar, U.; Vingralek, R. & Shapiro, W., 2005, *How to Build a Trusted Database System on Untrusted Storage*, Operating Systems Design and Implementation, Proceedings of the 4th conference on Symposium on Operating System Design & Implementation, Volume 4, San Diego, California
10. Saint-Onge, Hubert, 2003, *Creating and Implementing a Knowledge Strategy*, pp. 278-297 from *Knowledge Capital: How Knowledge-Based Enterprises Really Get Built*, Editor: Jay L. Chatzkel, ISBN 0-19-516114-9, Oxford University Press, New York
11. Thierauf, Robert J., 1999, *Knowledge Management Systems for Business*, ISBN 1-56720-218-7, Quorum Books, Westport, CT.