Available online at www.sciencedirect.com
ScienceDirect
Decision Support Systems 43 (2007) 675–685
Decision Support Systems
www.elsevier.com/locate/dss

Access control in collaborative commerce

Eldon Y. Li [a,b,*], Timon C. Du [c], Jacqueline W. Wong [c]

[a] College of Commerce, National Chengchi University, 64, Sec. 2, Zhi-nan Rd., Wenshan, Taipei 11605, Taiwan
[b] California Polytechnic State University, Orfalea College of Business, One Grand Avenue, San Luis Obispo, CA 93407, USA
[c] Decision Sciences and Managerial Economics, the Chinese University of Hong Kong, Shatin, NT Hong Kong, China

Available online 5 July 2005

Abstract

Corporate collaboration allows organizations to improve the efficiency and quality of their business activities. It may occur as a workflow collaboration, a supply chain collaboration, or as collaborative commerce. Collaborative commerce uses information technology to achieve a closer integration and better management of business relationships between internal and external parties. There are many emerging issues in collaborative commerce and one of them is access control.

To implement collaborative commerce, interfaces between the system elements of the organizations that are involved in the collaboration are needed. However, access control policies are often inconsistent from interface to interface, and therefore conflict resolution should be considered to resolve multilevel access control policy problems. Many studies propose different rules for the resolution of the conflict between access control policies, but little attention has been given to the relationship between the groups or subject classes that represent the different types of corporate collaboration. In this paper, the format of corporate collaboration is considered, and the conflicts between the access control policies of interfaces are addressed. Some general guidelines, other than those that relate to minimum privilege on duty and maximum privilege on sharing, are proposed.

Keywords: Information sharing; Access control policy; Workflow; Supply chain; Collaborative commerce

1. Introduction

Corporate collaboration links organizations together to improve the efficiency of sales, procurement, manufacturing, distribution, replenishment, and other activities. The level of collaboration has moved beyond mere buying and selling to encompass planning, design, development, communication, the sourcing of information, research, and the provision of services among organizations, which are collectively known as collaborative commerce [14]. Collaborative commerce can be defined as the use of "information technology to achieve a closer integration and a better management of business relationships among internal and external parties." Business collaboration can bring

* Corresponding author. College of Commerce, National Chengchi University, 64, Sec. 2, Zhi-nan Rd., Wenshan, Taipei 11605, Taiwan.
E-mail addresses: eli@calpoly.edu (E.Y. Li), timon@cuhk.edu.hk (T.C. Du), jacquelinewong@cuhk.edu.hk (J.W. Wong).

0167-9236/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2005.05.022

a competitive edge to the entire supply chain by decreasing product development costs, shortening the time to market, and improving product quality.

In general, collaborative commerce evolves from collaboration in the workflow to concurrent engineering, a supply chain, and beyond [11]. Three measures can be used to describe the relationship between these different forms of collaboration: the degree of collaboration, the degree of organizational integration, and the degree of business operations (see Fig. 1). Compared with workflow integration, in which business activities are sequential in the collaboration of employees in an organization, concurrent engineering has a deeper collaborative involvement with employees. Note that concurrent engineering brings employees with different expertise together to better integration of various functional operations. In contrast, supply chain collaboration focuses more on inter-organizational integration than workflow and concurrent engineering do. However, the sharing of information is rarely involved at the functional level in a supply chain, and therefore a trend of movement away from workflow collaboration, concurrent engineering, and supply chain collaboration toward a profound level of functional integration is apparent, and is the origin of collaborative commerce.

Potential future applications of collaborative commerce range from collaborative design, collaborative engineering, collaborative decision-making, collaborative forecasting, financial collaboration, the sharing of human resources information, collaborative inventory management, and the consolidation of transportation. In fact, some of these collaborative models are already well known today.

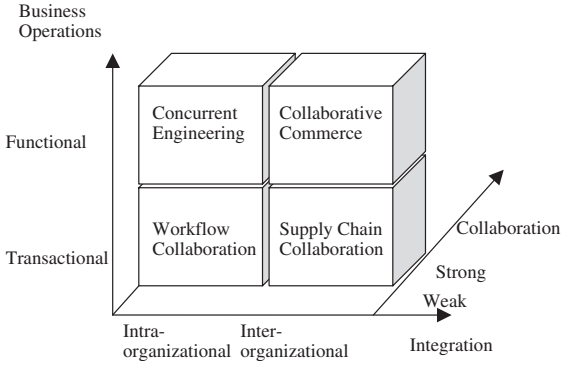

Fig. 1. Collaborative commerce as an evolutionary technology.

There are many emerging issues in collaborative commerce. In this paper, we address the issue of access control in corporation collaboration setting and propose guidelines for setting up multilevel access policies.

2. Access control in collaborative commerce

There are three major corporate collaboration formats: workflow, supply chain, and collaborative commerce. Workflows implement collaborative operations within an organization, and supply chains share information to improve the overall performance of all of the collaborating partners. Collaborative commerce further integrates the intra-organizational activities with external collaborative partnerships. These three types of corporate collaboration represent different types of cooperation, and therefore trigger the need for different access control policies for the application data that are used in these collaborations. When there are different policies, any conflict between the policies needs to be resolved. The following sections illustrate the types of application data that are used in workflows, supply chains, and collaborative commerce, and point out the conflicts that occur between the interfaces. The issues of multilevel access control policies are discussed, and guidelines for the resolution of access policy problems are proposed.

It is important that the application data for each of the activities in a collaboration is well protected, so that the partnership can be implemented smoothly. Data protection provides protection from improper access, protection from interference, integrity of data, operational integrity of data, semantic integrity of data, accountability and auditing, user authentication, management and protection of sensitive data, multi-level protection, and confinement to avoid the undesired transfer of information between system programs [6]. These goals are achieved by the application of security controls that ensure that the information does not either explicitly (via placing queries) or implicitly (via inference from related data) flow from higher protected objects to less protected objects. Secrecy problems are managed by security control, such as data security, access control, control of access to a statistical database, and data encryption [9]. Data security problems focus on the protection of data from unauthorized

access, and access control is a control system that directs the flow of objects (data, programs) to subjects (users, processes) through authorized access modes (read, write, run). Two components are needed to do this—a set of access policies and a set of control procedures [6]. A control policy defines the authorization rules on how subjects and objects can be grouped to share access modes. In contrast, a control procedure checks queries against the stated authorization rules to determine the access modes. In this paper, we address the issue of control policies in corporate collaboration.

3. Application data in workflows

A workflow specifies organizational processes into pre-defined tasks, and assigns them to designated roles according to certain principles, such as the separation of duties, least privilege, and data abstraction [12]. These principles assure the successful implementation of the workflow. For example, the separation of duties ensures that different sensitive tasks are assigned to different exclusive roles so that the penetration of the data can be minimized. In contrast, the least privilege policy, which is also known as the "need-to-know" policy [6], provides only the minimum information that is needed to complete a task. Data abstraction considers not only the access modes, such as read and write, but also the abstraction of data, such as credit or debit. The workflow management system (WFMS) manages the workflow on a day-to-day basis in various application domains, such as office automation, finance, healthcare, telecommunications, manufacturing, and production [3].

Many types of data are used in a workflow—process definition data, which include names, descriptions, routings, conditions, content, allocation rules, and the decision rules of tasks; resource classification, which includes role hierarchy, organizational units, and the relationships between them; analysis data, which include the data for analysis and the analyzed results; operational management data, which include information for administrators; historical data, which include data for tracing back or assessment; application data, which include data for various applications, such as ERP; internal data, which include the information that is used for WFMS internal use, such as the network address; and logistical management data, which include the states of the tasks and triggers [1]. In general, the WFMS relies on a database management system (DBMS) to manage the data. The two main streams of access control for workflow applications are role-based access control (RBAC) and predicate-based access control [15]. RBAC is suitable for workflow applications because the tasks are assigned to roles instead of users, which correspond to the natural control mechanism of the workflow. In contrast, predicate-based access control puts the related information along with the major record, and uses a predicate to specify the access rules. In this case, one rule can substitute many records in the access control tabulation, but both access control mechanisms can coexist within the conventional access control approaches of discretionary access control and mandatory access control to enforce data security.

To successfully implement a workflow in an organization, there are four fundamental elements—the DBMS, the WFMS, administration and monitoring, and applications. The DBMS manages the conventional database tasks, such as data maintenance, data integrity, concurrency control, and recovery for the current data and historical data, and the WFMS deals with the workflow process definition, activities, and control. The application tool provides services, such as enterprise resource planning (ERP) and its corresponding data, that are normally managed by the DBMS. The administration and monitoring element handles the administrative tasks other than those that are dealt with by the DBMS and the WFMS, such as statistical analysis, resource management, and operational management, and also implements some of the access control mechanisms, especially those that are related to other organizations. Access control normally applies to the elements themselves and the interfaces of the elements. As is shown in Fig. 2, six interfaces are required in a workflow collaboration.

3.1. Interface 1 (data management tool)

This interface links the administration and monitoring with the DBMS to provide for the usage of the data. The access control models of either discretionary access control (DAC) or mandatory access control (MAC) can be used for this purpose, depending on

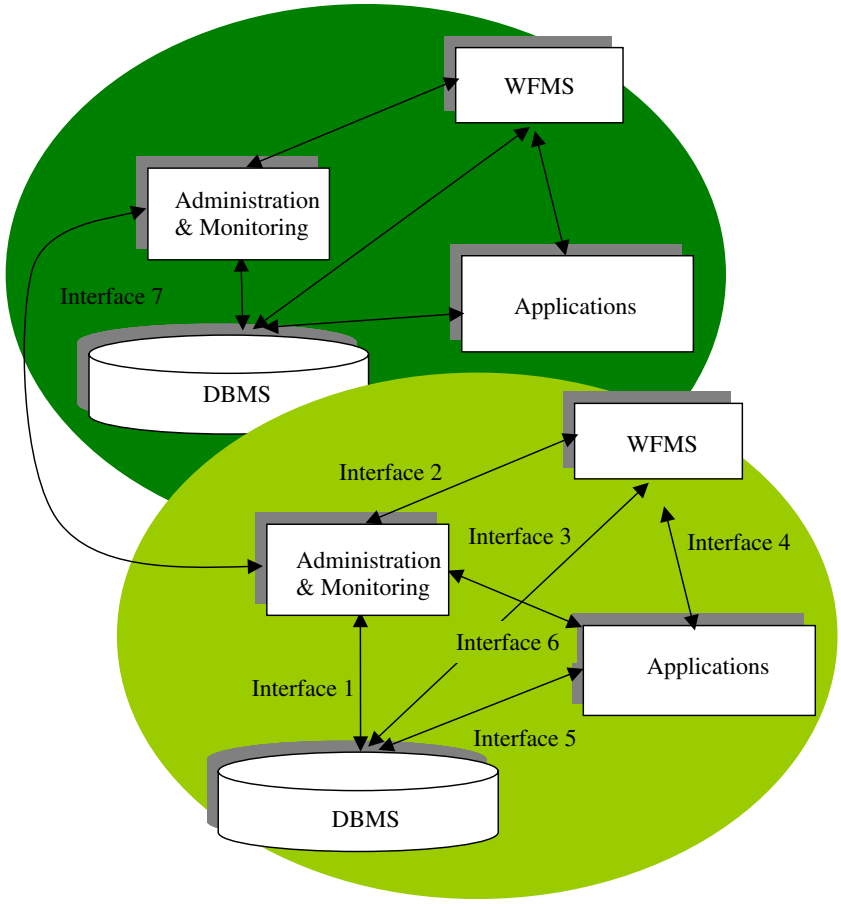

Fig. 2. Essential system elements and interfaces in corporate collaboration.

the reliability of the system and the degree of rigor of the security policy.

3.2. Interface 2 (process management tool)

This interface associates the administration and monitoring with the WFMS to ensure that access control in the workflow is sustained. Both lattice models and role-based models are suitable for this purpose [6], and privilege propagation and dynamic authorization need to be observed in the workflow.

3.3. Interface 3 (authorization management tool)

This interface links the WFMS and the DBMS to support the data for the workflow. The access control in this interface should coexist with the tool in *Interface 2*. Note that a multilevel access control policy (which will be discussed later) is needed so that any conflict between the data access control and the role-based access control can be resolved.

3.4. Interface 4 (application invoked tool)

This interface links applications with the WFMS so that the tasks in the workflow can obtain the application data that are needed to support operations. For example, in an ordering task, it might be necessary to refer to some historical contracts before the order is issued. A multilevel access control policy is also needed to resolve any conflict between the application access control and the role-based access control.

3.5. Interface 5 (application data management)

This interface controls the data for the applications. The access control in this interface is normally resolved when the applications are customized. For example, in ERP, the functions and options are designed differently for different roles, and users can only use the designated interfaces to complete their tasks. Similar to the role-based model, users will be assigned to appropriate roles and therefore acquire the corresponding privileges of those roles.

3.6. Interface 6 (application administration tool)

This interface deals with the interaction between the administration and monitoring element and the application element. Data are retrieved from the database directly in some administrative jobs in which the security is handled by *Interface 1*. However, this interface will become very important when we discuss collaborative commerce, as some application functions will be exposed to the collaborative partners, and therefore the conflict of access policies between the inter-organization and the intra-organization must be resolved. This will be discussed later.

4. Application data in the supply chain

Supply chains link organizations together to share information, products, funds, and others elements to satisfy customer requests efficiently. Supply chain processes can be broken down into four cycles—the customer order cycle, the replenishment cycle, the manufacturing cycle, and the procurement cycle [7]. The customer order cycle links customers with retailers to fulfill the orders of customers, and activities in this cycle include order entry, order fulfillment, and receiving orders. The replenishment cycle focuses on replenishing the retailer's inventory through coordination between the retailer and distributors, and activities in this cycle include retail order entry, retail order fulfillment, and receiving retailer orders. The activities that take place between distributors and manufacturers are considered to be part of the manufacturing cycle. In this cycle, the replenishment of the distributor's inventory is the focal point, and activities include order arrival from the distributor, retailer, or customer; the production scheduling of the manufacturer; manufacturing and shipping; and receiving the goods by the distributor, retailer, or customer. The final cycle is the link between manufacturers and suppliers, which is known as the procurement cycle. This cycle ensures that the materials are available for manufacturing through the consideration of orders that is based on the manufacturer's production schedule and the supplier's stocking needs, production schedule, and shipping schedule.

There are many popular methods for the implementation of a supply chain. For example, in the customer order cycle, the online catalogue is a useful mechanism that allows customers to order products online. This provides significant advantages by giving up-to-date information to customers. Similarly, sales force automation maintains the relationship between sellers and buyers by providing product and price information. In the replenishment cycle, vendor-managed inventory relies on the distributor or manufacturer to manage inventories for the wholesalers or retailers, and continuous replenishment programs allow the suppliers to regularly replenish the inventory of the retailers based on point of sale (POS) data. In the manufacturing cycle, advanced planning and scheduling develop the detailed production schedules that determine what, where, when, and how to make parts or products by considering the availability of materials, the capacity of the plant, and other business objectives. It is the objective of each organization to optimize its manufacturing capacity, distribution, and transportation resources based on the data that is collected from an ERP or legacy systems. In the procurement cycle, the content catalogue, which focuses on the activities between a manufacturer and its suppliers, can simplify the procurement process, and is able to keep track of parts, specifications, prices, order processes, and suppliers for the manufacturer.

However, to maintain a supply chain relationship, a high degree of trust is needed. In general, trust is nurtured from deterrence-based trust, knowledge-based trust, and identification-based trust [14]. Deterrence-based trust uses a variety of formal contracts to ensure the cooperation between parties, and knowledge-based trust is built on the knowledge of the other trading partner (trustee), which allows a partner to understand and predict the behavior of that trustee. However, to build a strong relationship, identification-

based trust that allows each party to consider the other party's objective, as its own co-identification is beneficial. To reach such a high degree of trust, the fostering of the relationship is important, and an appropriate system design, such as access control, can improve the interaction between the parties.

4.1. Interface 7 (partners coordination tool)

This interface shares the data between different administrative and monitoring elements of the organizations in a collaborative relationship. Access control for the supply chain should be at least the RBAC3 model, which is a consolidated role-based access control model that includes role-hierarchy and constraints [12]. It should be noted that the supply chain role hierarchy is contained within an organization, whereas collaborative constraints exist both within organizations (workflow) and between organizations (supply chain) (Fig. 3). There are two conflicts that need to be resolved in this interface—the schema conflict and the privilege propagation conflict. The

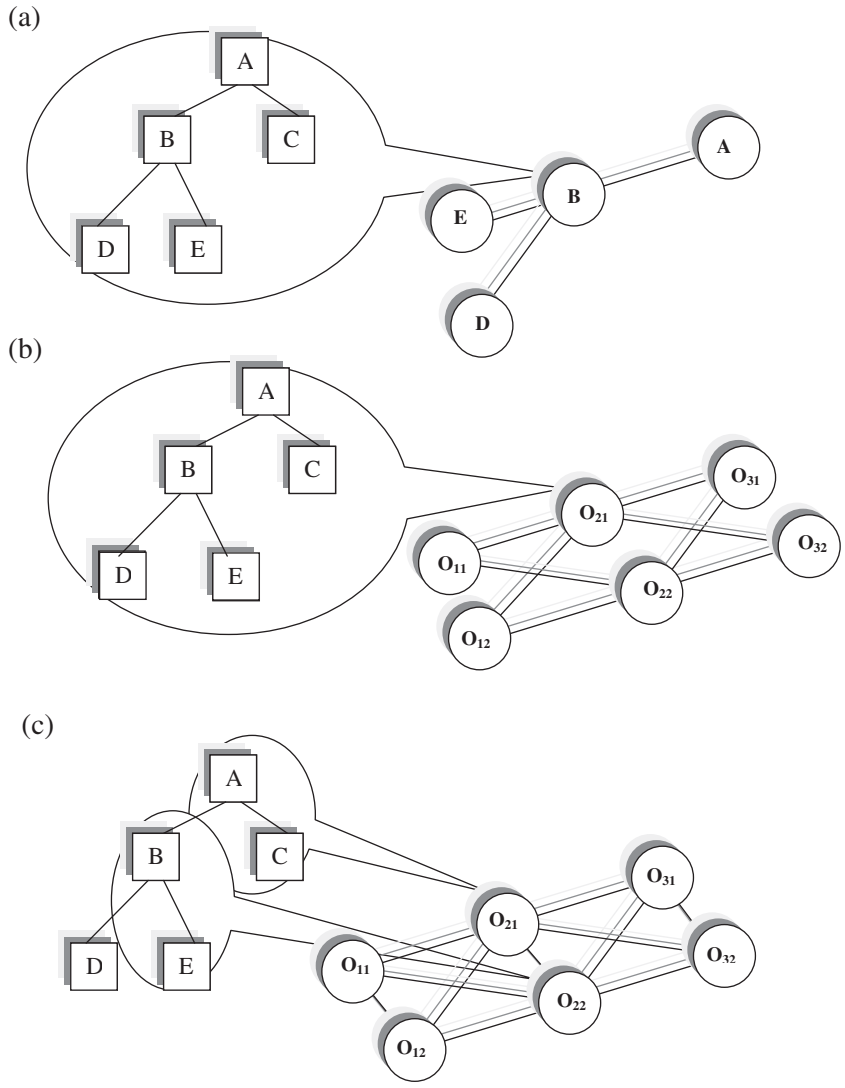

Fig. 3. Collaborative frameworks with organizations and role-hierarchy in (a) a workflow, (b) a supply chain, and (c) collaborative commerce.

schema conflict appears because different access control policies are adopted both within an organization and between organizations. The access model within an organization can apply DACs or MACs to the data and a role-based model to the information flow, as for a workflow. However, the access model between organizations should consider the degree of business coordination. The higher the degree of coordination, the better the supply chain performance, which is manifested in a lessened bullwhip effect, lower inventory levels, less transportation overheads, a lower manufacturing capacity requirement, and other considerations. However, it also makes keeping the information secret more difficult, and privilege propagation conflicts are also an issue. In an organization, privilege can be propagated as long as access control models are observed. Similarly, privilege can also be propagated to the supply chain, but there are some issues that need to be resolved, for example, whether company A should authorize company B to access its statistical data, which includes information about company C, assuming that company B has already been authorized by company C to access company C's data, and if so, the extent to which this would be beneficial. Another issue might be whether company A should permit access to the information of company C through company B if company A is authorized to do so by company B, and company B is authorized by company C, but company A is not authorized by company C. These scenarios happen even when the principles, such as the attenuation of privilege when the privilege should be decreased during propagation, hold. Moreover, the dynamic authorization mechanism becomes more complicated when the privilege can be propagated. For example, a company can form a virtual enterprise with another company and allow that company to access the related data. However, the relationship may change dynamically, and therefore the privileges would need to be revised accordingly.

5. Application data in collaborative commerce

Today, many businesses cement their relationship with their partners through the use of digital technologies. The level of collaboration has thus shifted to encompass planning, design, development, communication, the sourcing of information, research, and service between and within organizations. In general, collaborative commerce integrates business processes, such as demand planning, planning and scheduling, order management, product development, vendor management, sales support, and knowledge sharing, between partners through the electronic sharing of information (see Fig. 4). Moreover, collaborative commerce has a set of techniques that allows companies to maintain better relationships with their trading partners through the automation of their cross-enterprise process logic, rules, heuristics, and workflow.

A survey of over 300 business executives by Deloitte Research in mid 2002 showed that collaborative commerce leads to better business operations and information exchange, and provides up to 70% higher profitability for those companies that adopt this

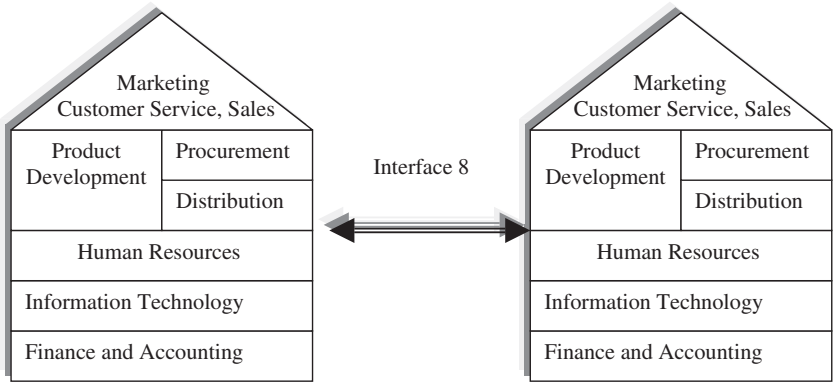

Fig. 4. Collaborative tasks hierarchy in collaborative commerce.

technology compared with those that do not integrate with their trading partners. This is because an integrated environment can enhance the value chain of suppliers, business partners, customers, and employees through flexible business processes, better product quality, rapid fulfillment, improved reliability, improved capital efficiencies, and prompt information exchange and knowledge sharing. The applications are various, and include collaborative design, collaborative engineering, collaborative decision-making, collaborative forecasting, financial collaboration, the sharing of human resources information, collaborative inventory management, and the consolidation of transportation. Several applications can be considered as a form of collaborative commerce. For example, collaborative planning, forecasting, and replenishment (CPFR) as defined by the Voluntary Inter-industry Commerce Standards Association, use ERP and a demand planning system for collaborative forecasting and to plan facilities. An example is the collaborative forecasting and replenishment (CFAR) that was jointly initiated by Wal-Mart and P&G to ensure that there was no gap between what Wal-Mart planned to sell and what P&G planned to produce [7].

5.1. Interface 8 (collaboration tools)

This interface links the business processes of organizations. The interface can link any process, such as those that are shown in Fig. 4, financial and accounting, human resources, product development, procurement engineering, distribution and transportation, marketing, customer service, or sales force. In this case, there are more access control conflicts than schema conflicts and privilege propagation conflicts in the supply chain environment. For example, to jointly develop products, product definition management (PDM) data should be shared to some degree. To manage a joint production process, manufacturing execution system (MES) data should be communal. Similarly, to successfully carry out joint procurement, some of the process and data of the ERP should be integrated. These tight relationships often create authorization conflicts. Designer A may be allowed to read sensitive data but designer B is not allowed to read it as designer B belongs to an allied company, even though designers A and B are undertaking a job together.

6. Multilevel access control policies

In a collaborative relationship, it is clear that there will be conflicts over the access control policies that are used both within an organization and between organizations. The interfaces that are discussed in the previous section show that conflicts exist at Interfaces 3 and 4 in the workflow collaboration, at Interfaces 1, 3, 4, and 7 in the supply chain collaboration, and at all interfaces in collaborative commerce. These conflicts can be resolved by the appropriate design of access control policy that proposes different conflict resolution schemes when the access modes and privileges vary.

The earliest multilevel schema model was proposed by Wood in 1979, and adopted the concept of a three-level schema architecture of ANSI/SPARC, that is, an external level for users, a conceptual level for the presentation of objects, and an internal level for physical maintenance [9]. The model uses two levels of design—conceptual level rules, which categorize data into entity sets, relationship types and attributes; and external level rules, which categorize data into tables, views, and fields. Mapping functions are responsible for the transformation of external-level rules into a set of operations for conceptual-level objects. In this case, the user can maintain a consistent security setting without worrying about the internal operations. However, the mapping function only specifies how the predicates that refer to the external objects can be mapped to the predicates of the conceptual objects, and do not resolve the conflict between the levels. Shen and Dewan [13] discuss the access model in a collaborative environment. The focal point of their study is to define the conflict resolution rules on fine-grained data to improve concurrency when there are many users working on a collaborative application. Their model supports both positive and negative authorizations in a collaborative environment. Positive authorization specifies the privileges of the subjects against the objects, and negative authorization specifically excludes the privileges of the subjects.

Conflict resolution is mainly based on either an explicit priority or a precedence relationship, in which the first entity that appears in the access control list (ACL) wins. The model was further expanded to encompass access administration, or the ownership

of object owners [8], and the same conflict resolution policies are adopted when an ownership inheritance conflict appears. However, the policies reveal some problems. Based on the explicit priority policy, the members of the groups will always override the authorization of the group as a whole, as the members are more specific, which negates the need to set up group security. Based on the precedence-first policy, it is possible that a new subject can be inserted into a prior position in the ACLs if the sequence of the ACLs is not strictly maintained. In this case, the newly inserted subject can easily grasp the higher priority, and the proper authorization scheme will be overridden. This problem becomes more serious in a decentralized administrative environment, such as occur in collaborative commerce. Moreover, when the negative authorization list is kept before the positive authorization list, the denials-take-precedence scheme is adopted. Similarly, if the positive authorization list is kept before the negative list, then the permissions-take-precedence scheme is adopted. That means that the precedence-first policy may give different results when different schemes are applied. To solve these problems, Bertino et al. [4] propose the concept of subject groups and ownership. In this design, users are assigned to groups in which both the users and their privileges are defined. A strong authorization is assigned to groups in which the authorization scheme must be rigorously obeyed. In contrast, an exception may exclude a specific user of a group from being granted privileges if a weak authorization is assigned to the group. Technically, this can be done by adding the group to the positive ACL and the user to the negative ACL, and access is therefore granted only when a user holds a positive strong authorization or a positive weak authorization. The conflict will be resolved in such a way that the strong authorization overrides the weak authorization. Moreover, the specification of ownership allows owners to keep control of access to their objects by specifying the strong authorization and by delegating only the weak authorization. This can improve decentralized administration, as only the owner can specify strong authorization.

General access control policies can be found in Jajodia et al. [10] who propose a unified framework to enforce multiple access control policies in a system. The model amalgamates various policies for different users, groups, objects, and roles, and the focal point is to provide flexibility in setting multiple policies on a single system, rather than a corporate collaboration. A study that emphasizes the decentralized of access control is that of Atluri et al. [2] in which inter-organizational workflow problems are solved using the Chinese Wall Security Policy that is proposed by Brewer and Nash [5]. This study addresses the dependency relationships of objects and subjects, and the Chinese Wall policy is used to ensure that sensitive data objects in a decentralized workflow will not be seen by execution agents who do not belong to the company. However, the model still does not consider the need for different levels of security within and between organizations, as is the case for supply chains and collaborative commerce.

7. Discussion

In the literature, a conflict resolution policy can be identified as an explicit-priority policy, a precedence-first policy [8, 13], a denials-take-precedence scheme, a strong authorization policy [4], a mutually disjoint policy [2], and a flexible authorization framework [10]. However, most of these studies focus on the protection of the object, and little attention has been given to the relationship between groups or subject classes. In fact, the group relationship represents the type of collaboration, whether workflow, supply chain, or collaborative commerce. Moreover, in corporate collaborations, access controls appear in different aspects—organizations versus individual users, and applications versus data objects. The security at the organization level is centered on the relationship and the degree of trust between the organizations that are involved in the collaboration, and the individual user level focuses on the clearance of the user for both the organization and the objects. The application level places emphasis on system performance, and the data object level deals with data security.

There are more issues that need to be considered in access control in collaborative commerce. For example, is it possible to have more than one ACL, say, one that is used within an organization and another that is shared between organizations? If it is possible, then how could different security levels be applied to the collaborative network and how would conflict be

resolved when it appeared? Another issue is the decision about who has the authority to grant or revoke access rights. Should there be a hierarchical decentralized authorization or a centralized authorization, such as cooperative authorization? How can one prevent Trojan Horses, that is, a new record with a higher privilege, from being inserted by a delegated user without the agreement of the data owner? The definition of the ownership of objects also needs consideration—should the object creator be the owner or the organization? The sequence of authorization also needs attention when the denials-take-precedence or permissions-take-precedence policies are adopted and a sequential effect exists. The way in which dynamic authorization is handled presents a problem, as it is expected that virtual cooperation can be formed to help company strategies. How can privilege propagation be managed in a collaborative environment, given that the higher the degree of privilege propagation, the lower the degree of control in a decentralized administration environment? What is the optimum granularity of the application objects to achieve a balance between security and performance? Coarse granularity can simplify the system operation and improve automation, but fine granularity can provide a high degree of security. Should access control be set at the application, task, document, drawing, analyzed data, or value level?

The two general principles that govern the issue of how much information should be accessible to each subject in a collaboration are the minimum privilege on duty and the maximum privilege on sharing. These principles mean that only the minimum quantity of information is provided to subjects to carry out their activities, but that information should be on the maximum sharing ability. However, over-limitation may decrease the effectiveness of innocuous subjects, and too much openhandedness may endanger data protection. Therefore, other general guidelines are needed in addition to these two general access policies, which are proposed here as follows. The degree of collaboration is determined by the rule that the tighter the relationship, the greater the degree of sharing; the degree of sophistication of the information system is determined by the rule that the more sophisticated the system that an organization has, the more complex the security system that can be adopted; the need for the committee of authorization administration is governed by the rule that the faster the response, the greater the need for a decentralized committee; the security level of data objects is guided by the principle that the more sensitive the data that the organizations own, the tighter the level of security; the sequence of business processes is determined by the principle that the greater the dependency on the business process, the higher the level of security that should be applied; the granularity of the application objects should be founded on the basis that the better the system performance that is expected, the coarser the granularity of the operation units should be; and the privilege revoking and provoking procedure is based on the principle that the higher the degree of organizational trust and the higher the degree of automation, the looser the privilege propagation.

8. Conclusions

In this paper, the conflicts that occur between access policies in corporate collaboration are addressed. Collaborations are categorized into workflow collaboration, supply chain collaboration, and collaborative commerce. In collaborative organizations, several interfaces manage the information flow of applications. However, the access control policies of these applications may not be coordinated, and therefore multilevel access policies are needed.

In the environment of corporate collaboration, subjects should have different privileges with respect to objects that belong to different departments or organizations. Therefore, it is clear that a multilevel access policy such that different clearance and security levels for both subjects (organizations and users) and objects (applications and data) is needed. In such policy, the same object may be presented to different security level subjects differently. Either DAC or MAC can be used to maintain data security, depending on the degree of sophistication of the system that is adopted, and role-base access control can be used to manage the information flow in collaborative relationships. Moreover, when collaborative relationships move from workflow collaboration to supply chain collaboration, and on again to collaborative commerce, more conflicts between the different access policies will arise, and multilevel access policies then become important.

References

[1] W.V.D. Aslst, K.V. Hee, Workflow Management: Models, Methods, and Systems, MIT Press, 2002.

[2] V. Atluri, S.A. Chun, P.A. Mazzoleni, Chinese wall security model for decentralized workflow, Proceedings of the ACM Conference on CCS'01, 2001, pp. 48–57.

[3] E. Bertino, E. Ferrari, V. Atluri, The specification and enforcement of authorization constraints in workflow management systems, ACM Transactions on Information and System Security 2 (1) ((1999) February) 65–104.

[4] E. Bertino, S. Jajodia, P.A. Smarati, Flexible authorization mechanism for relational data and management systems, ACM Transactions on Information Systems 17 (2) 1999 (April) 101–140.

[5] D.F.C. Brewer, M.J. Nash, The Chinese wall security policy, Proceedings of IEEE Symposium on Security and Privacy, 1989, pp. 206–214.

[6] S. Castano, M. Fugini, G. Martella, P. Samarati, Database Security, ACM Press and Harlow: England: Addison-Wesley, 1995.

[7] S. Chopra, P. Meindl, Supply Chain Management: Strategy, Planning, and Operation, Prentice Hall, Upper Saddle River, NJ, 2001.

[8] P. Dewan, H. Shen, Flexible meta access-control for collaborative applications, Proceedings of the ACM Conference on Computer-Supported Cooperative Work, 1998, pp. 247–256.

[9] R. Elmasri, S. Navathe, Fundamentals of Database Systems, 3rd edition, Addison-Wesley, Reading, MA, 2000.

[10] S.P. Jajodia Samarati, M. Sapino, V.S. Subrahmanian, Flexible support for multiple access control policies, ACM Transactions on Database Systems 26 (2) (2001 (June)) 214–260.

[11] E.Y. Li, T.C. Du, Collaborative commerce, in: E.Y. Li, T.C. Du (Eds.), Advances in Electronic Business, Volume I (Collaborative Commerce), IGI Press, Hershey, Pennsylvania, 2005, pp. 1–18.

[12] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, Role-based access control models, IEEE Computer (1996 (February)) 38–47.

[13] H. Shen, P. Dewan, Access control for collaborative environment, Proceedings of the ACM Conference on Computer-Supported Cooperative Work, 1992, pp. 51–58.

[14] E. Turban, D. King, Introduction to E-Commerce, Prentice-Hall, 2003.

[15] S. Wu, A. Sheth, J. Miller, Z. Luo, Authorization and access control of application data in workflow systems, Journal of Intelligent Information Systems 18 (1) (2002) 71–94.

Eldon Y. Li is University Chair Professor of the College of Commerce at the National Chengchi University in Taiwan. He was Professor and Dean of College of Informatics at Yuan Ze University in Taiwan during 2003–2005. He was a professor and the Coordinator of MIS Program at the College of Business, California Polytechnic State University, San Luis Obispo, California, U.S.A. He visited the Department of Decision Sciences and Managerial Economics at the Chinese University of Hong Kong during 1999–2000. He was the Professor and Founding Director of the Graduate Institute of Information Management at the National Chung Cheng University in Chia-Yi, Taiwan. He holds a PhD from Texas Tech University. His current research interests are in human factors in information technology (IT), strategic IT planning, software engineering, quality assurance, and information and systems management. He is the Editor-in-Chief of International Journal of Electronic Business, International Journal of Information and Computer Security, International Journal of Information Policy and Law, International Journal of Internet and Enterprise Management, International Journal of Internet Marketing and Advertising.

Timon C. Du received his BS degree in Mechanical Engineering from the National Chung-Hsing University, Taiwan, in 1989. He obtained his Master's and PhD degrees in Industrial Engineering from the Arizona State University. Currently, Dr. Du is an Associate Professor at The Chinese University of Hong Kong, Hong Kong and director of MSc in E-Business Management Program. His research interests are in e-business, data mining, collaborative commerce, and semantics webs.

Jacqueline W. Wong received her BBA degree in Information Management from the Catholic Fu Jen University, Taiwan, in 1990. She obtained her Master's and PhD degrees in Computer Science from the Chinese University of Hong Kong. Currently, Dr. Wong is a Senior Instructor at The Chinese University of Hong Kong. Her research interests are Business Intelligence, Information Retrieval, Knowledge Management, and System Analysis and Development.