Computers in Industry 63 (2012) 545–556

Contents lists available at SciVerse ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Secure collaboration in global design and supply chain environment: Problem analysis and literature review

Yong Zeng *, Lingyu Wang, Xiaoguang Deng, Xinlin Cao, Nafisa Khundker

Concordia Institute for Information Systems Engineering, Faculty of Engineering and Computer Science, Concordia University, Montreal, Quebec, Canada H3G 1M8

ARTICLE INFO

Article history:
Received 25 February 2012
Received in revised form 2 May 2012
Accepted 2 May 2012
Available online 29 May 2012

Keywords:
Secure collaboration
Information sharing and protection
Collaborative product development
Design and supply chain management
Environment Based Design

ABSTRACT

Increasing global competition has led to massive outsourcing of manufacturing businesses. Such outsourcing practices require effective collaborations between focal manufacturers and their suppliers by sharing a large amount of information. In the meantime, since some of the suppliers are also potential competitors, protection of confidential information, particularly intellectual properties, during the collaboration is becoming an important issue. Therefore, secure collaboration is of critical significance in the global design and supply chain management. This paper aims to collect and analyze systematically the existing scattered research of secure collaboration in global design and supply chain environment, and to give a comprehensive literature review to summarize the problems and the corresponding solutions. By applying the Environment-based Design (EBD) methodology, the existing methods and technologies are classified into four levels: infrastructure, information, agreement, and confidence. Four corresponding research problems are then formulated: information access control, information partitioning, legal information sharing, and partner trust management. As such, research papers scattered in different areas are integrated into this multi-disciplinary field. Future trends and challenges are also discussed in this paper.

1. Introduction

It is well-recognized that product innovation and development ability is a key to enterprises' successes. In today's highly competitive globalized market, in order to make a rapid response to customer needs and technology changes, collaborative and distributed product development has become a trend in manufacturing and service industry. Such collaboration and outsourcing activities require massive data sharing between upstream and downstream partners in a complex design and supply chain environment. However, in the meantime, focal manufacturers must maintain their competitive advantages by protecting their confidential information, such as intellectual property. As a result, secure collaboration is a critical issue in global design and supply chain environment. In this context, research has been conducted to balance "collaboration" and "security" in order to achieve the best competitiveness for organizations in the global economy. This paper aims to collect the existing literature and then provide a systematic overview and analysis of this topic.

Secure collaboration is an emerging research topic, which concerns various disciplines, such as collaboration, product innovation, design and supply chain management, information security and privacy. The corresponding literature review is thus a very challenging task. To the best of our knowledge, there still lacks a comprehensive review of this broad area of secure collaboration in the global design and supply chain environment. In order to organize the scattered research results, guide a systematic problem analysis and define coherent categories of solutions, this review process can be considered as a task of developing solutions for the secure collaboration problem.

Therefore, we will conduct this literature review using a design methodology: Environment-based Design (EBD) [1–4]. EBD can effectively and progressively identify major design problems and generate related solutions through the analysis of complex design environment [5]. It includes three main activities: environment analysis, conflict identification, and solution generation. In the context of the present literature review, environment analysis refers to understanding and formalizing the complex collaborative global design and supply chain environment. Conflict identification aims to identify major problems in the collaborative environment. Solution generation attempts to summarize the related literature that provides solutions for the identified conflicts. By following the EBD approach, our review will systematically depict a grand picture of the broad area of secure collaboration in the global design and supply chain environment.

The rest of this paper is organized as follows: Section 2 introduces collaborative global design and supply chain environment (environment analysis). Section 3 determines the secure

* Corresponding author. Tel.: +1 514 848 2424x5801.
E-mail address: zeng@ciise.concordia.ca (Y. Zeng).

0166-3615/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.compind.2012.05.001

collaboration conflicts in the collaborative environment (conflict identification). The corresponding solutions is provided in Section 4 (solution generation). The conclusion and future research problems are summarized in Section 5.

2. Collaborative global design and supply chain environment

2.1. Product development process

Based on the current literature [6–9], we abstract a process of the global design and supply chain collaboration, which consists of five main phases: formulation, design, prototyping, evaluation, and production.

Formulation refers to formalizing the design specifications according to customer requirements. Design aims to generate the product concept and detail descriptions. Prototyping realizes such design concept and descriptions. Evaluation attempts to verify whether the design meets customer requirements. Production starts once the design has passed the evaluation. Table 1 shows the main elements corresponding to each phase, including partner, methodology, technology, standard and infrastructure. It can be seen from Table 1 that the main human environment includes customers (upstream partners), focal manufacturer and suppliers (downstream partners). A simplified workflow is illustrated in Fig. 1.

As shown in Fig. 1, a focal manufacturer firstly formulates design specifications according to customer requirements. Then the manufacturer shares portion of specifications with suppliers and receives their corresponding Interface Control Documents (ICD). The focal manufacturer can thus generate design descriptions to manufacture prototypes. If the product prototypes fail the evaluation, then the manufacturer is required to review the previous phases (from formulation to prototyping) until the prototypes meet customer requirements. In this case, mass production can be implemented with the parts provided by the suppliers. The end product is finally delivered and transported to the customers.

In order to clarify the complex environment of collaborative global design and supply chain, Sun et al. [10] decomposed it into three activities: Collaborative Product Development (CPD), Design

Table 1
Collaborative global design and supply chain environment.

Phase	Partner	Methodology	Technology	Standard/infrastructure
Formulation	Customers, focal manufacturer	Customer survey, SWOT etc.	CTQ, DOORS, QFD, ROM, RUP etc.	Volere/telecommunication protocols etc.
Design	Focal manufacturer, suppliers	Axiomatic design, DFSS, EBD, FBS, systematic design, TRIZ etc.	CAD, CAE, CAM, PDM, PLM, SysML, UML etc.	DXF/DWG, IGES, STEP(ISO10303), STL/network protocols etc.
Prototyping	Focal manufacturer, suppliers	Modeling, simulation, design of experiments etc.	CAD, CAE, CAM, PDM, PLM etc.	DXF/DWG, IGES, STEP(ISO10303), STL/network protocols, process, facilities
Evaluation	Focal manufacturer, customers	MCDM, V&V etc.	CAD, CAE, CAM, DSS, PDM, PLM etc.	DXF/DWG, IGES, ISO standards STEP(ISO10303), STL/process, facilities etc.
Production	Focal manufacturer, customers, suppliers	TQM, 6-sigma etc.	CIM, FMEA etc.	DXF/DWG, IGES, ISO standards STEP(ISO10303), STL/network protocols, process, machine, facilities etc.

Note: DXF/DWG, IGES, STEP, STL are data exchange formats.

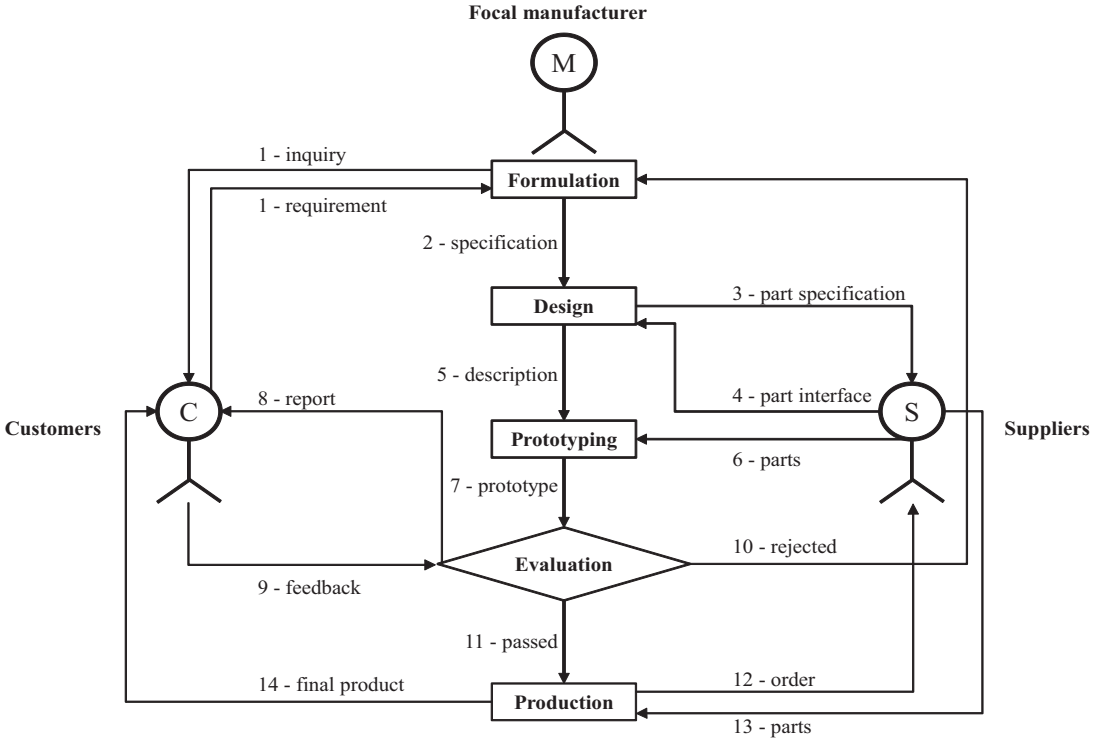


Fig. 1. Workflow of collaborative global design and supply chain environment.

Table 2
Phases related to the activities of global design and supply chain management.

Activity	Phase
Collaborative product development	Design, prototyping
Design chain management	Formulation, design, prototyping, evaluation
Supply chain management	Formulation, design, prototyping, evaluation, production

Chain Management (DCM) and Supply Chain Management (SCM). CPD aims to design and implement products to meet customer requirements. DCM focuses on the entire product development process to enhance product innovation. SCM mainly examines manufacturing and logistic activities to reduce the production cost and time. The phases related to each activity are summarized in Table 2.

In order to better understand the three activities of collaborative environment, many researchers have proposed models related to different issues [6,11,12], such as product model, process model, operation model, and collaboration model. In this paper, only the collaboration model is discussed. In the following sub-sections, we will develop our discussions on the collaboration models and mechanisms related to CPD, DCM and SCM.

2.2. Collaborative product development

The collaborative models and mechanisms of CPD can be classified into two categories [13,14]: horizontal and hierarchical collaboration. The horizontal collaboration occurs in an organization whose members are from the same discipline, and the hierarchical collaboration is between upstream design and downstream manufacturing [15]. The horizontal and hierarchical collaborations are realized in three levels: communication, information and knowledge sharing, and coordination of activities.

Among advanced information technologies, concurrent engineering [16] and Computer Supported Cooperative Work (CSCW) [17] have been largely applied to deal with communication issues in CPD. These technologies employed computer network and techniques to support communication among partners by sharing different formats of content [18]. The format of content can be divided into two types: asynchronous component and synchronous component [19]. Asynchronous component includes mark-up, annotation, forum, email, mail list and version control. Synchronous components contain instant messaging, text chat, voice chat, video conference and whiteboard.

The intra-/inter-organizational design information and knowledge sharing is realized at the communication level. Several research efforts are focused on information modeling and knowledge sharing. Kim et al. [20] established an ontology-based model to explicitly and persistently represent engineering relations imposed in assembly design and information sharing. Rodriguez and Al-Ashaab [21] developed a knowledge driven collaborative product development system architecture to address design requirements from different research and industrial partners. Lawson et al. [22] proposed a theoretical model of formal and informal socialization mechanisms in inter-organizational knowledge sharing.

The coordination of activities consists of many structured and unstructured tasks [18]. Effective coordination of activities is a key to the success of the collaboration process. Many coordination models have been built to classify the dependencies of activities using organizational theory. For example, Thompson et al. [23] proposed three coordination mechanisms (standardization, plan, and mutual adjustment) to classify the dependencies of activities as pooled, sequential and reciprocal. Crowston et al. [24] developed a typology of coordination problems to address specific types of interdependencies. Recently, Cataldo et al. [25] gave a fine-grain view of congruence to measure the dynamic existence of interdependencies among tasks and their relationship with actors.

2.3. Design chain management

Many researchers have proposed reference models to improve the performance of collaboration in design chain. For example, Chuang and Yang [26] established a collaboration complexity trend model to determine collaboration strategy; Deck and Strom [27] established a co-development emergency model to facilitate collaborative work between partners; Choi et al. [28] proposed a product design chain collaboration framework to resolve major obstacles to collaboration during product design; Shiau and Wee [29] developed a distributed change control workflow to maintain the consistency among design activities in a collaborative network.

In order to provide a roadmap and theoretical foundation for supporting collaborative design, Liu and Zeng [6] developed a design chain collaboration hierarchy model, which decomposes DCM activities into seven levels of collaboration, such as goal, strategy, process, information, application, technology standard and infrastructure. Through resolving the internal conflicts of the hierarchy model, Sun et al. [10] developed a formal wheel model which is derived step by step from a natural language description of design chain management requirements.

2.4. Supply chain management

The major objective of supply chain collaboration is to create synergies for competitive advantage among supply chain partners through sharing information. Most of the existing research of supply chain collaboration emphasizes on two issues [30]: supply chain collaboration process modeling and information sharing. Supply chain collaboration process modeling aims to provide a mechanism whereby supply chain partners can jointly plan, forecast and manage supply chain activities. Collaborative Planning, Forecasting and Replenishment model [30–32] is a representative solution of this issue, which is often used to induce collaboration and coordination through information sharing between supply chain partners. Moreover, several researchers have modeled the supply chain collaboration process using other theories and technologies. For example, Fawcett et al. [33] developed a three-stage implementation model in order to manage the dynamic and changing collaboration process based on organizational theories. Zou and Yu [30] built a model driven decision support system to simulate the collaboration process using artificial intelligence techniques.

Information sharing is a major approach to realize supply chain collaboration process. As for the CPD environment, many researchers have proposed different models of information sharing adapted to the diverse structures of supply chains. Zhang [34] studied vertical information sharing in a divergent supply chain, in which two downstream retailers competed on either quantity or the price of output. On the other hand, Li [35], Anand and Goyal [36] have discussed the effect of information leakage of a supply chain with horizontal competition.

Recently, RFID technology has been widely used in supply chain collaboration [37], the information among supply chains can be captured automatically and the visibility of items in supply chains are enhanced. RFID technology can facilitate information sharing among supply chain partners and improves the information sharing between supply chain partners. However, it provokes new challenges in RFID-Enabled supply chain collaboration network (ex. EPCglobal network) regarding new security and privacy protection issues [38].

3. Secure collaboration conflicts

Fig. 1 shows that it has a great amount of information sharing/protection between focal manufacturer and suppliers in design and production phases. One side would request information from the other to realize the design and manufacturing tasks. The other side needs to protect its confidential information and privacy for legal and/or competition purposes. Fig. 2 illustrates the information flow of manufactuer/supplier collaboration in design and production phases. When the focal manufacturer receives the information request from one supplier, manufacturer will position his information base into two parts: information to share and to protect. Focal manufacturer will then extract and provide the information to share to the supplier. The similar scenario exists for the supplier to deal with focal manufacturer's information request. Table 3 presents how the information is to be shared and/or protect between the focal manufacturer and a supplier in design and product phases.

Based on EBD methodology [10,39], Fig. 3 illustrates the scenarios of conflicts related to the sharing and protection of focal manufacturer's information. In completing the design outsourced by the focal manufacturer, suppliers would request complete design and manufacturing information from a focal manufacturer; however, for the reason of confidential information protection, the manufacturer can only authorize suppliers the access to a portion of information. In this case, a conflict appears between information sharing and protection.

The same happens for suppliers when they send back their part design to the focal manufacturer. The suppliers also need to protect their confidential information. The mechanism, however, is the same as that shown in Fig. 3.

Therefore, in the context of the present research field, the principal problem of secure collaboration in global design and supply chain is identified as how to share and protect information simultaneously. Namely, the problem addresses the protection of confidential information while sharing necessary information to partners.

According to our literature review analysis based on EBD methodology, the confidential information can be protected in four levels: infrastructure, information, agreement and confidence.

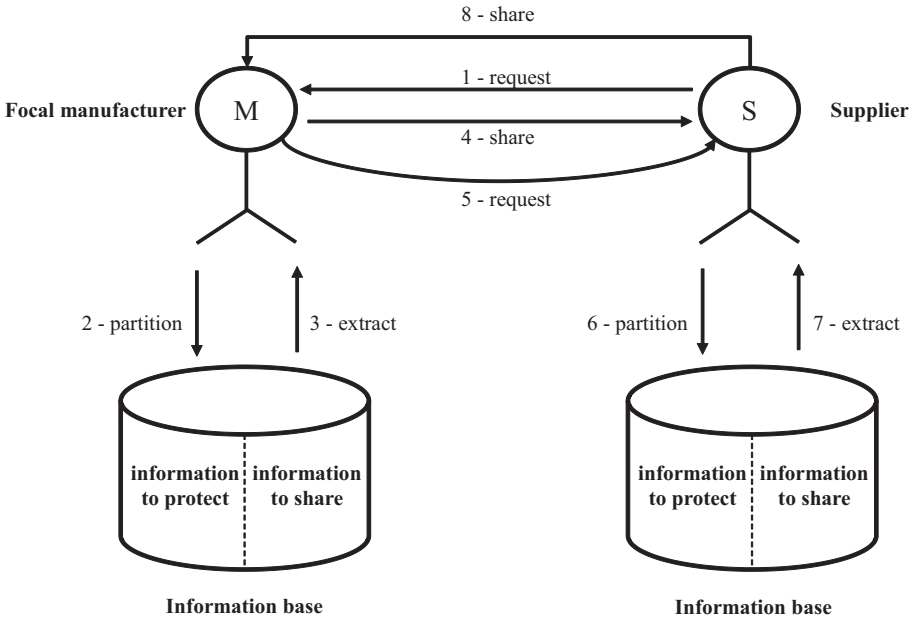


Fig. 2. Information flow of manufactuer/supplier collaboration in design and production phases.

Table 3
Information to share/protect between focal manufacturer and supplier.

Role	Phase	Information to protect	Information to share
Focal manufacturer	Design	• Customer complete requirements • Market interests • Expertise • Know-how • Core design parameter and data etc.	• Customer requirements • Design parameters and data etc.
	Production	• Productivity • Price of final product etc.	• Number of parts • Transportation requirements • Manufacturing parameters and data etc.
Supplier	Design	• Innovation capability • Know-how • Facility etc.	• Solution • Product data format • Estimated price etc.
	Production	• Raw material cost • Manufacturing cost • Production capability • Facility etc.	• Product data format • Price etc.

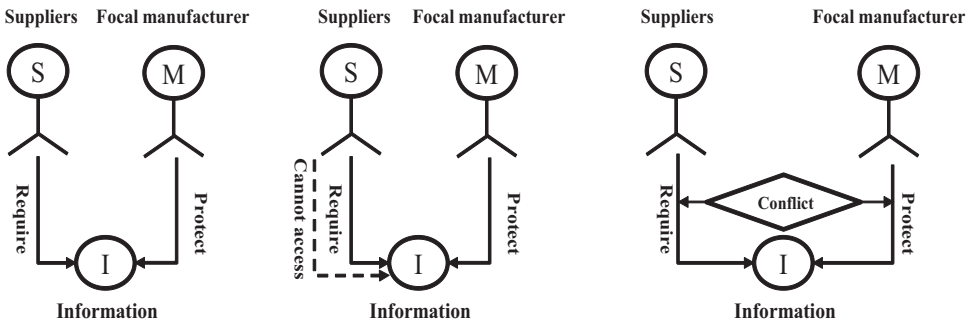


Fig. 3. Focal manufacturer's information to share/protect conflict [10].

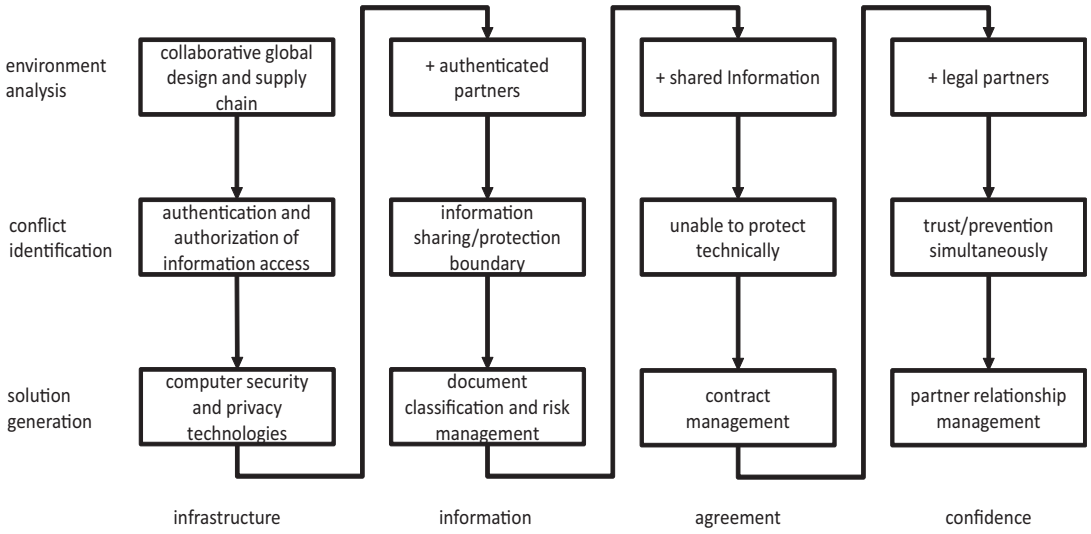


Fig. 4. Secure collaboration scenarios based on EBD methodology.

When some solutions are generated at each level, they produce new environment elements and conflicts, which drives the development of new solutions at the next level. Fig. 4 presents this recursive EBD review results.

Accordingly, Table 4 summarizes the main problem, the objective, and the solutions related to each level. The objective of infrastructure level is to authenticate and authorize the information access of partners. Advanced computer security and privacy techniques have been widely applied to realize this task. The information level aims to partition which part of information can be shared to the authenticated partners, and which part of information should be protected. Due to technical barriers, the shared information may still unavoidably contain some confidential information. Therefore, the confidential information requires to be further protected through legal means. A contract, such as non-disclosure agreement, is usually signed between a focal manufacturer and its partners. However, the kind of contract depends greatly on the level of trust between the collaborative partners. As a result, partner relationship management is critical at the confidence level. The details of the solutions at these four levels will be given in Section 4.

4. Secure collaboration solutions

According to the previous analysis, this section presents the scientific methods and technical solutions of secure collaboration by four categories: computer security and privacy technologies, information partitioning, contract management, and partner relationship management.

4.1. Computer security and privacy technologies

There is a great amount of literature on computer security and privacy techniques related to secure collaboration at the infrastructure level. Nabil et al. [40] conducted a comprehensive survey addressing the problem of providing security to statistical database queries against disclosure of confidential data. More recently, Fung et al. [41] gave a comprehensive survey of

Table 4
Problem analysis of secure collaboration.

Level	Main problem	Objective	Solutions
Infrastructure	Information access control	Authenticate and authorize information access	Computer security and privacy technologies
Information	Information partitioning	Define information sharing/protection boundary	Document classification and risk management
Agreement	Legal information sharing	Protect the shared information legally	Contract management
Confidence	Partner trust management	Trust/prevention simultaneously	Partner relationship management

Privacy-Preserving Data Publishing (PPDP) techniques. The paper systematically reviewed and evaluated different approaches to PPDP, discussed practical challenges in PPDP and unique requirements that distinguish PPDP from other related issues.

Bertino et al. [42] defined security in knowledge management as protecting valuable data, assets, information, and resources, intellectual properties such that only authorized individuals will be permitted to access. The discussion focuses on applying existing access control policies for the purpose of secure knowledge management. Moreover, several researchers [43–45] employ Secure Multi-Party Computation (SMC) to protect confidential information by allowing users to perform joint computation on multiple datasets while not revealing information in these datasets. Recently, Location-Based Service (LBS) has been widely applied in social network and mobile network in a variety of contexts, such as health, indoor object search, entertainment, work, personal life etc. LBS is a general class of computer program-level services used to include specific controls for location and time data as control features [46].

According to existing literature above, in this section, we particularly concentrate on these three computer security techniques, that is, access control, secure multi-party computation and location-based service, regarding confidential information and privacy protection issues.

4.1.1. Access control

Access control ensures that only authorized users can access specific information. In the existing research work, several access control models have been proposed to meet the security requirements of information sharing and collaboration in supply chains. Leong et al. [47] proposed a mixed access control model for a workspace-oriented distributive product data management system. Based on [48,49], Wang et al. [50] combined RBAC (Role-Based Access Control) and cryptographic methods to support RBAC with consideration of time, scheduling and value adding activity, policy delegation relation in distributed context and fine-grained access control at dataset level. Chen et al. [51a] developed a trust evaluation method for virtual project team. Moreover, Mandatory Access Control (MAC) model is proposed and widely applied to government, military and defense industries. This type of access control model permits to access to "classified information" by requiring a certain level of security clearance [51b].

Access control in a collaborative environment has traditionally relied on models based on digital certificates and the Public Key Infrastructure (PKI). Welch et al. [52] proposed a digital certificate-based on authentication and authorization, which is more flexible than traditional approaches of manually editing of policy databases or issuance of credentials in the context of grids. In this case, users may need to be authenticated across different organizations.

Collaborative access control has been studied in the context of a federated database [53]. Jonscher et al. [54] discussed access control in the so-called tightly coupled federations and solutions providing for different degrees of local autonomy, including authorization autonomy. The authors also discussed the interaction between different reference monitors and how an access control mechanism may be applied at the global level and then mapped onto mechanisms of each component database.

Yang et al. [55] proposed a solution for access control in federated database, called subject switching, where the federation translates federated users' identities to those of a pre-determined subject at the remote service provider. This translation may not always be possible due to the heterogeneity of a federation. The authors then proposed using proximity measures between the requester and provider, and presented two algorithms for finding such a proximity minimizing match between subjects.

4.1.2. Secure multi-party computation

Secure Multi-party Computation (SMC) means to protect confidential information by allowing users to perform joint computation on multiple datasets while not revealing information in these datasets. Atallah et al. [45] introduced SMC into the area of preventing information leakage in supply chains. It enables supply chain partners to collaboratively achieve desired system-wide goals without revealing any private information, even though the jointly computed decision requires this information. In an early survey of the SMC problems and solutions [56], the authors classified SMC problems into several domains, including privacy-preserving cooperative scientific computations (e.g. linear system of equations, linear programming), privacy-preserving database query (matching a database to a query string, with both being secret), privacy preserving intrusion detection through profile matching (matching a normal behavior profile database to actual behaviors, with both being secret), privacy-preserving data mining, privacy-preserving geometric computation, and privacy-preserving statistical analysis. The privacy-preserving data mining of association rules over databases that have been vertically (i.e. by columns) divided between two mutually distrusted parties is discussed in [57]. The problem is reduced to that of securely computing the scalar product of two vectors. An algebraic solution based on hiding true values by placing them in equations masked with random values is given for computing the scalar products. A later work [58] addressed the privacy-preserving data mining of association rules over databases that have been horizontally (i.e. by rows) divided, that is, split among various parties. The proposed methods incorporate cryptographic techniques (commutative encryption) to discover candidate itemsets that are frequent on at least one site which is then examined to determine whether they may pass the global support or confidence thresholds.

Yet a later work [59] addressed the privacy-preserving computation of linear regression analysis. The solution allows multiple parties to compute exact coefficients of the global regression equations and to perform goodness-of-fit diagnostics, without disclosing the underlying data.

Clifton et al. [60] observed that one data mining problem may result in multiple research work due to differences in terms of, for example, the way data are partitioned and varying privacy constraints, etc. The authors also observed that many data mining problems may actually share similar underlying computations at various stages such as counting. Therefore, the authors proposed a toolkit-based approach for privacy-preserving primitive computations, which may be assembled to solve specific data mining problems. Four sample computations are studied, namely, secure SUM, secure set union, secure size of set intersection, and scalar product. These are then applied to association rule mining in horizontally and vertically partitioned data and EM clustering, in order to demonstrate the proposed approach.

Under a slightly different architecture than that of SMC, privacy preserving data mining at a central location with private data collected from individual users is discussed in the classic work of [61]. The solution asks users to apply random noises to their private data before submitting the data to a server. The noises are drawn from a common statistical distribution known to the server such that the server may later approximately recover the distribution of submitted data for data mining purposes, such as classification discussed in this paper. There have been tremendous efforts following this work. Rizvi et al. [62] stated the similar problem of privacy-preserving mining, but for the purpose of association rule mining instead of classification is discussed. The solution, called the Mining Associations with Secrecy Konstraints (MASK), is based on probabilistic distortion of users' data prior to data submission. Fong and Weber-Jahnke [63] proposed a slightly different approach of transforming the given dataset into a number

of so-called unreal datasets such that the original dataset can only be re-constructed with all the unreal datasets; moreover, it is shown that decision trees may be correctly constructed from those unreal datasets directly, without the need for re-constructing the original dataset. Du et al. [64] studied the SMC issue of two-party multivariate statistical analysis, including two-party multivariate linear regression and secure two-party multivariate classification.

4.1.3. Privacy-preserving location-based services

Location-Based Service (LBS) is a milestone in Information and Communication Technology based service delivery. Through this service mobile phones or laptops can use numerous services like finding nearby restaurant, locating nearest health center or bank etc., based on user's current location. In this service users exchange information with LBS provider or sometimes with other users. It is possible to track user location, user movement, consumer habit and many more if someone wants to make misuse of this service. Ensuring personal information security in such an environment depends on third party most of the time. But trusting third party for security is always not a good choice. Solanas et al. [65] proposed a distributed and moduler based TTP (Trusted Third Party) free location privacy. Their solution is applicable where the exact location of user is not required for LBS. They calculated the location without revealing personal information of user. This solution shows a method to mask the real location among a number of users and also sharing a inaccurate location information in the system. The modularity of the system also provides the user a facility to choose particular module as per their need.

Rebollo-Monedero et al. [66] suggested TTP-free system where the privacy depend on collaboration among multiple untrusted users. This solution is related to a situation where the service provider is not trusted. Users can use a service from an untrusted service provider without sharing its personal information or exact location. They suggested a way to use mixed query from several user. In this way the untrusted service provider will unable to access the privacy information of any user.

4.2. Information partitioning

The main task of information partitioning is to classify the documents (definition of sharing/protected information boundary) in order to minimize the risk of confidential information leakage with authenticated partners. According to above analysis, this section is developed in two aspects: document classification methods and risk management.

4.2.1. Document classification

Document classification is often referred to as a kind of process to classify a set of documents into different partitions so that each partition has some common features [67]. Document classification is a fundamental technique for understanding documents and to help people browse and navigate documents more efficiently.

Document classification is often an unsupervised process, which is involved with two principal phases. The first one is document representation. The second phase includes learning from training corpus, modeling for classes and classifying the new documents [68]. The whole process of a typical document classification can be found in [69] and [70]. The first issue to be addressed in the document classification area is how to represent the documents. The textual documents in their raw form cannot be used for classification or machine learning algorithms directly; hence, another representation is required. Documents are mostly represented by vector space model. For example, the bag-of-words is a kind of such representation where vector elements are words and each vector element represents the number of times that a given word occurs in that document [71]. Weighting schemes such as Term Frequency Inverse Document Frequency (TF-IDF) [72] are often used as well.

After the documents are represented by vectors, documents pre-processing or Dimensionality Reduction (DR) are used to obtain more efficient representation and to support their further processing by algorithms [73]. The performance of document classification can be boosted by reducing dimensionality [73]. Feature Extraction (FE) and Feature Selection (FS) are common methods of DR techniques [73]. An FE process often includes tokenization, stop words removal, and stemming while FS aims to select subset of features by the measurement of the importance of the word [73]. The TF-IDF (Term Frequency-Inverse Document Frequency) approach is commonly used to weigh each word in the text document and is more effective than simple word frequency counting [73,74].

Machine learning techniques are used to classify documents. Many algorithms and approaches were proposed in this area, including bayesian classifier [75–78], decision Tree [79,80], *K*-Nearest Neighbor (KNN) [81], Support Vector Machines (SVM) [82,83], neural networks [84,85], latent semantic analysis [86,87], Rocchio's Algorithm [88], fuzzy correlation and genetic Algorithms [89]. The disadvantage of the decision tree method is that it tends to make more mistakes with numerous categories. SVM classifier has been recognized as one of the most effective methods [90]. The detailed review of those methods can be found in [73].

Nogueira et al. [91] introduced a classification framework meeting the user needs by the integration of a fuzzy method and text mining approach. In their method, they use fuzzy rules to classify text documents to manage the imprecision and uncertainty. The authors claimed that the experiment result of the methods is promising compared to Naive Bayes and OneR classification method [92]. Jiang et al. [93] proposed a graph-based approach to document classification. The authors argued that the graph representation considers more expressive document encoding compared to standard bag of words/phrases approach and better accuracy tends to be acquired.

4.2.2. Risk management

Risk management in design and supply chains is a growing research area. Jutter et al. [94] gave the related definition as "the identification and management of risk for the design and supply chain, through a coordinated approach amongst members of chains, to reduce supply chain vulnerability as a whole." The process of risk management may be divided into the following three steps: risk classification and identification, risk assessment and analysis, and risk mitigation.

Research has been done to classify risk sources. For example, Juttner et al. [95] suggested that supply chain risk sources fall into three categories: environmental, network-related and organizational. Mason-Jones and Towil [96] proposed a classification of five categories: environment, supply, demand, process and control. Lockamy and McCormack [97] classified the risk sources in design and supply chain into three groups: operational, network and external.

According to the risk classification above, a few researchers aimed to provide a control mechanism to identify and select the risk categories related to their research interests. Hallikas et al. [98] focused the risks on supplier relationships and networks, Neiger et al. [99] determined process-based risks in supply chain based on Value-Focused Process Engineering (VFPE), Kleindorfer et al. [100] concentrated on the disruption risks in supply chain. However, Zhang et al. [101] stated that current research ignore general risk sources that affect supply chains in a less visible manner, such as information leakage. According to such analysis, Sun et al. [10] identified the risks of information leakage in collaborative design chain environment.

For risk assessment and analysis, Zsidisin et al. [102] conducted seven case studies to analyze supply risk assessment techniques. Lockamy III and McCormack [97] presented a methodology for analyzing risks in supply networks to facilitate outsourcing decisions associated with revenue impact. Klinke et al. [103] proposed a three-strategy method to risk evaluation. For information leakage issue, Zhang et al. [104] modeled and evaluated the risk caused by inferences in supply chains.

Concerning the risk mitigation issue, Juttner et al. [95] adapted four generic risk mitigating strategies for single organizations to supply chains, namely avoidance, control, cooperation and flexibility. Christopher and Lee [105] suggested that improved confidence is one key element in any strategy to mitigate supply chain risk. Khan et al. [106] addressed the importance of the impact of product design on supply chain risk based on an in-depth longitudinal case study of a major UK retailer. For the purpose of intellectual property protection, Zhang et al. [101] mitigated the risk of confidential information leakage through optimal supplier selection.

4.3. Contract management

There is a vast debate on the impact of contract making on the development of collaboration relationships. On the one hand, Markovits [107] believed that contracts give legal promises and guarantees to collaborations by mitigating the risk of intellectual property leakage. On the other hand, Malhotra et al. [108] denoted that the imposed constraints of binding contract reduce the likelihood of trust development between partners. Woolthuis et al. [109] studied the relation between trust and contract in the collaboration relationship development, and found that trust and contract to be both complements and substitutes. They made a close examination of a contract's content, which offers alternative insight into the presence and use of contracts in collaboration relationships. Furthermore, Weber and Mayer [110] argued that the contract frame determines the impact on the exchange and relationship between partners. For example, a prevention-framed contract that emphasizes infringement will induce negative emotions to partners, whereas a promotion-framed contract that highlights positive reinforcement will stimulate flexible and creative behavior.

Research also shows that value of information sharing to design and supply chain strongly depends on the contract type and the mode of competition [111]. Lee and Whang [112] denoted that, for a simplified manufacturer-retailer supply chain under linear price contracts, information makes more incremental profit to manufacturer rather than retailer. However, Ha and Tong [111] believed that, under quantity-based contract menus, more information allows the manufacturer to avoid the negative quantity distortions and to improve the overall supply chain performance in cournot competition. Ryall and Sampson [113a] stated that the effects of learning, trust, reputation-building and relational mechanisms may simultaneously exert their influences on the design of a formal contract. Particularly, when focal manufacturer wants to develop an on-going relationships with their partners, a relational (or informal) governance mechanisms become relevant.

4.4. Partner relationship management

How to manage the relationships with the legal partners is a critical issue for focal manufacturers. On the one hand, focal manufacturers need to build trust with partners. On the other hand, they have to mitigate the risk from reserve engineering as much as possible. This section will discuss these two aspects: trust management and reverse engineering mitigation.

4.4.1. Trust management

With respect to trust management in collaboration, different parties in collaboration should deal with trust with the same semantics, especially when trust propagates along supply chain or partnerships; otherwise, trust may be misunderstood and misused [113b]. Fawcett et al. [114] stated that trust is the catalyst for collaborative innovation, collaboration can neither be built nor sustained without a foundation of trust. Ruohomaa et al. [115] summarized the definition of trust as "the extent to which one party is willing to participate in a given action with a given partner, considering the risks and incentives involved".

According to Fawcett et al. [114], trust can be characterized by two main dimensions: benevolence and capability. Particularly, Fawcett et al. [114] argued that supply chain trust is capability based, which consists of two matrices: performance capability and commitment capability. Based on capability-commitment matrix, a trust maturity framework was proposed, along with time, experience and relationship identity, the maturity framework divides trust collaboration process into four stages: limited trust, transactional trust, relational trust and collaborative trust.

Huang et al. demonstrated their efforts to quantify trust. They constructed an ontology of trust through formalizing formal semantics and transitivity [116]. Based on this ontology, they developed a Formal-Semantics-Based (FSB) trust calculus [117] by integrating into other formal trust models [119].

Grudzewski et al. [120] gave the managerial definition of trust management as the activities of creating systems and methods that allow relying parties to make assessments and decisions regarding the dependability of potential transactions involving risk, and to allow players and system owners to increase and correctly represent the reliability of themselves and their systems.

Technically, trust management is realized though digital certificates of authentication and authorization, which are proofs of identity or membership in a group. Trust management deals with the propagation and delegation of trust among multiple parties of a group using pre-defined rules. Li et al. introduced [121] a role-based trust-management language called RT0. Credential graphs are used as a formal representation of credentials in RT0, and the reach ability in credential graphs is shown to exactly match the formal semantics of RT0. Based on the credential graphs, goal-directed algorithms are introduced to find credential chains in RT0, which begins with an access request and searches for credentials relevant to the request.

4.4.2. Innovation capability and reverse engineering mitigation

Innovation is recognized as a critical capability to enterprise business success [122,123]. Miles et al. [124] defined enterprise's innovation capability (also called innovativeness) as "the ability of creating new value propositions through offering of new products and services, adopting new operating practice, technological, organizational, or market-oriented, or creating new skills and competencies".

According to Arnold et al. [125], innovation capability can be roughly divided into two categories: radical innovation and incremental innovation. Radical innovation refers to incorporating substantially different technology and fulfilling novel and emerging customer needs, whereas the incremental innovation refers to involving minor technology changes based on existing know-how and relatively incremental customer benefits. In addition, Christensen [126] proposed a new concept of disruptive innovation in 1997. In contrast to radical and incremental innovations which focus on customer mainstream market, disruptive innovation aims to improve new product and service development meeting unexpected but potential market space [127].

The integration of new knowledge in the innovation process is an important issue to an innovation success. Therefore, Cassiman

Table 5
Future development of literatures on secure collaboration.

Problem	Solutions	Current state of art	Future directions
Information access control	Computer security and privacy technologies	Authentication and authorization	Cloud computing, impact of social networking
Information partitioning	Document classification and risk management	Risk of intellectual property leakage	Multi-criteria risk assessment and control
Legal information sharing	Contract management	Contract design	Text mining techniques
Partner trust measurement	Partner relationship management	Trust management and reverse engineering mitigation	Supplier reverse capability modeling

et al. [128] summarized three innovation strategies, such as internal R&D, external knowledge acquisition, and collaboration, to combine different innovation activities and to access knowledge sources. For the reasons of reducing R&D time and cost, enterprises are typically engaged in the acquisition of knowledge on the available technology market, and/or in the collaboration with their partners or suppliers. In addition to collaborative product development (previously mentioned in Section 2), external know-how from available and legal sources may enhance the productivity of internal R&D activities.

Reverse engineering (RE) is one of the main approaches of external knowledge acquisition. Chikofsky et al. [129] defined reverse engineering (RE) as a process of analyzing a subject system to identify the system's components and their interrelationships, and to extract and create system abstractions and design information. RE facilitates the rapid innovation and product development by accessing external knowledge and know-how [130], which has been widely applied in various industrial sectors [131].

For manufacturers, however, reverse engineering may be a threat to their intellectual property. For the purpose of avoiding and controlling the threat of reverse engineering, several RE mitigation techniques have been developed. The goal of those techniques is to maximize the RE cost experienced by competitors (attackers) with the minimal protection cost incurred to the focal manufacturer (protector). McLoughlin et al. [132] divided those techniques into two classes: passive and active methods. Passive methods are statically introduced and implemented at fixed time, such as obfuscation [133] and watermarking [134]. For example, watermarking is widely used to prove the ownership of a give file, database or media content [135]. Active methods protect the intellectual property during an attack, like information hiding [132] and deliberate confusion [136]. These techniques attempt to mask confidential information and privacy when it has a risk of information threat.

However, to the authors' best knowledge, in the existing literature, there is a lack of study on modeling supplier reverse engineering capability by considering its innovation capability and facilities. This is however an important research issue for focal manufacturers to prevent the threat from reverse engineering techniques.

5. Conclusions and future directions

In today's global economy, secure collaboration has become a critical issue in design and supply chain management. Since this emerging research topic is rather broad due to its involvement with various disciplines, the corresponding literature review is a challenging task. This paper provides a systematic overview on secure collaboration in global design and supply chain environment, which defines the interconnections of various research topics and reviews the state of the art of each topic in terms of the concerned research problem.

By viewing the development of secure collaboration as a design problem, the Environment-Based Design (EBD) methodology is used to analyze the research problems and to identify the necessary solutions. The identified problems and solutions thus provide a coherent framework that systematically integrates various remotely related research areas. As such, the present literature review firstly analyzes the global design and supply chain environment by abstracting the workflow of collaborative product development process. Secondly, based on the environment analysis, the major problem of secure collaboration is identified as a conflict resulted from the simultaneous sharing and protection of product information. Finally, the identified major problem is decomposed into four levels: infrastructure, information, agreement, and confidence, for each of which the solutions are summarized based on the analysis of existing literature. Accordingly, the approaches to mitigate those risks are reviewed and analyzed.

Table 5 gives some potential future directions related to this multidisciplinary research field. In the infrastructure level, social networking is a phenomenon of application that needs to be taken into considerations. Moreover, cloud computing is attracting attentions from computer security and privacy community. For the solution of risk management at information level, multiple risk factors (e.g. information leakage, reverse engineering, cost, quality etc.) will be integrated into the secure collaboration risk control. For the agreement level, the text mining techniques can be applied to analyze the impact of contract making on intellectual property protection. Moreover, for the confidence level, it has a strong research necessity to model suppliers' reverse engineering capability according to their innovation capabilities and available facilities.

Acknowledgements

The research review reported in this paper is partially supported by Natural Sciences and Engineering Research Council (NSERC) of Canada through a CRD project (PJ 350114-06) and an Engage project (EGP 411677-11). We are grateful to the financial support from NSERC, CRIAQ, Pratt & Whitney Canada Corp., Bombardier Inc., CMC Electronics Inc., Rolls-Royce Canada Limited and Mecanica Solutions Inc. Moreover, we express our thanks to Suo (Tandy) Tan, Thanh An Nguyen, Maomao (Maggie) Pan from Design Lab at Concordia University for their constructive comments to enhance the quality of this paper. We also thank the anonymous reviewers to help us greatly in revising this paper.

References

[1] Y. Zeng, Axiomatic theory of design modeling, Transactions of the SDPS: Journal of Integrated Design and Process Science 6 (3) (2002) 1–28.
[2] Y. Zeng, Environment-based formulation of design problem, Transactions of the SDPS: Journal of Integrated Design and Process Science 8 (4) (2004) 45–63.
[3] Y. Zeng, Recursive object model (ROM): modeling of linguistic information in engineering design, Computers in Industry 59 (6) (2008) 612–625.
[4] Y. Zeng, Environment-based design (EBD), in: Proceedings of the ASME 2011 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference IDETC/CIE 2011, DETC2011-48263, August, 2011.

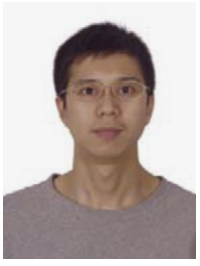
[5] X. Sun, Y. Zeng, F. Zhou, Environement-based design approach to developing quality management systems: a case study, Transactions of the SDPS: Journal of Integrated Design and Process Science 15 (2) (2011) 53–70.
[6] W. Liu, Y. Zeng, Conceptual modeling of design chain management towards product lifecycle management, Global Perspective for Competitive Enterprise, Economy and Ecology (2009) 137–148.
[7] C. Wang, Adsche: design of an auction-based framwork for decentralized scheduling, Transactions of the SDPS: Journal of Integrated Design and Process Science 15 (2) (2011) 17–36.
[8] H. Narayanan, S.B. Khoh, Deploying design for six sigma new product development, in: 4th IEEE International Conference on Management of Innovation and Technology, 2008. ICMIT 2008, 2008, 1110–1115.
[9] X. Deng, P. Vroman, X. Zeng, B. Laouisset, Intelligent decision support tools for multicriteria product design, in: 2010 IEEE SMC, 2010, 1223–1230.
[10] X. Sun, Y. Zeng, W. Liu, Formalization of design chain management using environment-based design (EBD) theory, Journal of Intelligent Manufacturing, in press.
[11] K.H. Han, N. Do, An object-oriented conceptual model of a collaborative product development management (CPDM) system, International Journal of Advanced Manufacturing Technology 28 (7) (2006) 827–838.
[12] S. Tayur, R. Ganeshan, M. Magazine, Quantitative Models for Supply Chain Management, vol. 17, Springer, Netherlands, 1999.
[13] L. Wang, W. Shen, H. Xie, J. Neelamkavil, A. Pardasani, Collaborative conceptual design state of the art and future trends, Computer-Aided Design 34 (13) (2002) 981–996.
[14] D. Zhang, L. Wang, Y. Zeng, Secure collaborative product development: a literature review, in: PLM'08, 2008, 331–340.
[15] W.D. Li, W.F. Lu, J.Y.H. Fuh, Y.S. Wong, Collaborative computer-aided design-research and development status, Computer-Aided Design 37 (9) (2005) 931–940.
[16] F.E.H. Tay, C. Ming, A shared multi-media design environment for concurrent engineering over the internet, Concurrent Engineering 9 (1) (2001) 55–63.
[17] W. Shen, Q. Hao, W. Li, Computer supported collaborative design: retrospective and perspective, Computers in Industry 59 (9) (2008) 855–862.
[18] S.R. Gorti, A. Gupta, G.J. Kim, R.D. Sriram, A. Wong, An object-oriented representation for product and design processes, Computer-Aided Design 30 (7) (1998) 489–501.
[19] W.D. Li, W.F. Lu, J.Y.H. Fuh, Y.S. Wong, Collaborative computer-aided design – research and development status, Computer-Aided Design 37 (9) (2005) 931–940.
[20] K.Y. Kim, D.G. Manley, H. Yang, Ontology-based assembly design and information sharing for collaborative product development, Computer-Aided Design 38 (12) (2006) 1233–1250.
[21] K. Rodriguez, A. Al-Ashaab, Knowledge web-based system architecture for collaborative product development, Computers in Industry 56 (1) (2005) 125–140.
[22] B. Lawson, K.J. Petersen, P.D. Cousins, R.B. Handfield, Knowledge sharing in interorganizational product development teams: the effect of formal and informal socialization mechanisms, Journal of Product Innovation Management 26 (2) (2009) 156–172.
[23] J.D. Thompson, Organizations in Action: Social Science Bases of Administrative Theory, Transaction Pub, 2003.
[24] K. Crowston, Towards a Coordination Cookbook: Recipes for Multi-agent Action, Alfred P. Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA, 1991.
[25] M. Cataldo, P.A. Wagstrom, J.D. Herbsleb, K.M. Carley, A fine-grain measure of coordination: implications for the design of collaboration and awareness tools, in: HCIC Winter Workshop 2006, 2009.
[26] W.C. Chuang, H.H. Yang, Design chain collaboration – a strategic view, International Journal of Electronic Business Management 2 (2) (2004) 117–121.
[27] M. Deck, M. Strom, Model of co-development emerges, Research-Technology Management 45 (3) (2002) 47–53.
[28] Y. Choi, K. Kim, C. Kim, A design chain collaboration framework using reference models, The International Journal of Advanced Manufacturing Technology 26 (1) (2005) 183–190.
[29] J.Y. Shiau, H.M. Wee, A distributed change control workflow for collaborative design network, Computers in Industry 59 (2) (2008) 119–127.
[30] H. Zou, T. Yu, The research on decision model of supply chain collaboration management, in: 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08, IEEE, 2008, pp. 1–6.
[31] S.H. Williams, Collaborative planning, forecasting, and replenishment, Hospital Materiel Management Quarterly 21 (2) (1999) 44.
[32] H. Min, W.B.V. Yu, Collaborative planning, forecasting and replenishment: demand planning in supply chain management, International Journal of Information Technology and Management 7 (1) (2008) 4–20.
[33] S.E. Fawcett, G.M. Magnan, M.W. McCarter, A three-stage implementation model for supply chain collaboration, Journal of Business Logistics 29 (1) (2008) 93–112.
[34] H. Zhang, Vertical information exchange in a supply chain with duopoly retailers, Production and Operations Management 11 (4) (2002) 531–546.
[35] L. Li, Information sharing in a supply chain with horizontal competition, Management Science 119 (2002) 6–1212.
[36] K.S. Anand, M. Goyal, Strategic information management under leakage in a supply chain, Management Science 55 (3) (2009) 438–452.
[37] M. Attaran, RFID: an enabler of supply chain operations, Supply Chain Management: An International Journal 12 (4) (2007) 249–257.
[38] J. Shi, Y. Li, W. He, D. Sim, SECTTS: a secure track and trace system for RFIDenabled supply chains, Computers in Industry 63 (6) (2012) 574–585.
[39] B. Yan, Y. Zeng, Design conflict: conceptual structure and mathematical representation, Transactions of the SDPS: Journal of Integrated Design and Process Science 15 (1) (2011) 75–89.
[40] R.A. Nabil, C.W. John, Security-control methods for statistical databases: a comparative study, ACM Computing Surveys 21 (1989) 515–556.
[41] B.C.M. Fung, K. Wang, R. Chen, P.S. Yu, Privacy-preserving data publishing: a survey of recent developments, ACM Computing Surveys 42 (June (4)) (2010) 14:1–14:53.
[42] E. Bertino, L.R. Khan, R. Sandhu, B. Thuraisingham, Secure knowledge management: confidentiality, trust, and privacy, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans 36 (May (3)) (2006) 429–438.
[43] A.C.C. Yao, How to generate and exchange secrets, in: 27th Annual Symposium on Foundations of Computer Science, IEEE, 1986, pp. 162–167.
[44] R. Agrawal, R. Srikant, Privacy-preserving data mining, in: ACM Sigmod Record, vol. 29, ACM, 2000, pp. 439–450.
[45] M.J. Atallah, H.G. Elmongui, V. Deshpande, L.B. Schwarz, Secure supply-chain protocols, in: IEEE Conference on e-Commerce, 2003, 293–302.
[46] J.H. Schiller, A. Voisard, Location-Based Services, Morgan Kaufmann, 2004.
[47] K.K. Leong, K.M. Yu, W.B. Lee, A security model for distributed product data management system, Computers in Industry 50 (2) (2003) 179–193.
[48] T. Kim, C.D. Cera, W.C. Regli, H. Choo, J.H. Han, Multi-level modeling and access control for data sharing in collaborative design, Advanced Engineering Informatics 20 (1) (2006) 47–57.
[49] C.D. Cera, I. Braude, T. Kim, J.H. Han, W.C. Regli, Hierarchical role-based viewing for multilevel information security in collaborative CAD, Journal of Computing and Information Science in Engineering 6 (2) (2006) 2–10.
[50] Y. Wang, P.N. Ajoku, J.C. Brustoloni, B.O. Nnaji, Intellectual property protection in collaborative design through lean information modeling and sharing, Journal of Computing and Information Science in Engineering 6 (2006) 149.
[51] (a) T.Y. Chen, Y.M. Chen, H.C. Chu, Developing a trust evaluation method between co-workers in virtual project team for enabling resource sharing and collaboration, Computers in Industry 59 (6) (2008) 565–579;
(b) Z. Shan, X. Wang, T. Chiueh, Enforcing mandatory access control in commodity OS to disable malware, IEEE Transactions on Dependable and Secure Computing (2012) 540–554.
[52] V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, S. Tuecke, Security for grid services, in: Proceedings. 12th IEEE International Symposium on High Performance Distributed Computing, June, (2003), pp. 48–57.
[53] A.P. Sheth, J.A. Larson, Federated database systems for managing distributed, heterogeneous, and autonomous databases, ACM Computing Surveys 22 (September) (1990) 183–236.
[54] D. Jonscher, K.R. Dittrich, An approach for building secure database federations, in: Proceedings of the 20th International Conference on Very Large Data Bases, VLDB'94, San Francisco, CA, USA, Morgan Kaufmann, 1994, pp. 24–35.
[55] J. Yang, D. Wijesekera, S. Jajodia, Subject switching algorithms for access control in federated databases, in: Proceedings of the Fifteenth Annual Working Conference on Database and Application Security, Das'01, Norwell, MA, USA, Kluwer Academic Publishers, 2002, pp. 61–74.
[56] W. Du, M.J. Atallah, Secure multi-party computation problems and their applications: a review and open problems, in: Proceedings of the 2001 Workshop on New Security Paradigms, NSPW'01, New York, NY, USA, ACM, 2001, pp. 13–22.
[57] J. Vaidya, C. Clifton, Privacy preserving association rule mining in vertically partitioned data, in: Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD'02, New York, NY, USA, ACM, 2002, pp. 639–644.
[58] M. Kantarcioglu, C. Clifton, Privacy-preserving distributed mining of association rules on horizontally partitioned data, IEEE Transactions on Knowledge and Data Engineering 16 (9) (2004) 1026–1037.
[59] A.P. Sanil, A.F. Karr, X. Lin, J.P. Reiter, Privacy preserving regression modelling via distributed computation, in: Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD'04, New York, NY, USA, ACM, 2004, pp. 677–682.
[60] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, M.Y. Zhu, Tools for privacy preserving distributed data mining, SIGKDD Explorations Newsletters 4 (December) (2002) 28–34.
[61] R. Agrawal, R. Srikant, Privacy-preserving data mining, in: Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, SIGMOD'00, New York, NY, USA, ACM, 2000, pp. 439–450.
[62] S.J. Rizvi, J.R. Haritsa, Maintaining data privacy in association rule mining, in: Proceedings of the 28th International Conference on Very Large Data Bases, VLDB'02, VLDB Endowment, 2002, pp. 682–693.
[63] P. Fong, J. Weber-Jahnke, Privacy preserving decision tree learning using unrealized datasets, IEEE Transactions on Knowledge and Data Engineering (99) (2010) 1.
[64] W. Du, S. Chen, Y.S. Han, Privacy-preserving multivariate statistical analysis: linear regression and classification, in: Proceedings of the 4th SIAM International Conference on Data Mining, 2004, pp. 222–233.
[65] A. Solanas, A. Martí nez-Ballesté, A TTP-free protocol for location privacy in location-based services, Computer Communications 31 (6) (2008) 1181–1191.
[66] D. Rebollo-Monedero, J. Forné, A. Solanas, A. Martí nez-Ballesté, Private location-based information retrieval through user collaboration, Computer Communications 33 (6) (2010) 762–774.
[67] J. Ji, T.Y. Chan, Q. Zhao, Clustering large sparse text data: a comparative advantage approach, Information and Media Technologies 5 (4) (2010) 1208–1217.

[68] S. Chagheri, C. Roussey, S. Calabretto, C.et al. Dumoulin, Technical documents classification, in: 15th International Conference on Computer Supported Cooperative Work in Design, 2011.
[69] B. Baharudin, L.H. Lee, K. Khan, A review of machine learning algorithms for text-documents classification, Journal of Advances in Information Technology 1 (1) (2010) 4–20.
[70] A. Bilski, A review of artificial intelligence algorithms in document classification, International Journal of Electronics and Telecommunications 57 (3) (2011) 263–270.
[71] N. Oza, J.P. Castle, J. Stutz, Classification of aeronautics system health and safety documents, IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews 39 (6) (2009) 670–680.
[72] S. Robertson, Understanding inverse document frequency: on theoretical arguments for IDF, Journal of Documentation 60 (January (5)) (2004) 503–520.
[73] A. Khan, B. Baharudin, L.H. Lee, K. Khan, A review of machine learning algorithms for text-documents classification, Journal of Advances in Information Technology 1 (February (1)) (2010) 4–20.
[74] G. Salton, C. Buckley, Term-weighting approaches in automatic text retrieval, Information Processing and Management 24 (5) (1988) 513–523.
[75] A. McCallum, K. Nigam, A comparison of event models for Naive Bayes text classification, in: AAAI-98 Workshop on Learning for Text Categorization, vol. 752, 1998, 41–48.
[76] I. Rish, An empirical study of the Naive Bayes classifier, in: IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence, vol. 3, 2001, 41–46.
[77] P. Domingos, M. Pazzani, On the optimality of the simple bayesian classifier under zero-one loss, Machine Learning 29 (2) (1997) 103–130.
[78] S.B. Kim, H.C. Rim, D.S. Yook, H.S. Lim, Effective methods for improving Naive Bayes text classifiers, in: PRICAI 2002: Trends in Artificial Intelligence, 2002, 479–484.
[79] C. Apte, F. Damerau, S.M. Weiss, Towards language independent automated learning of text categorization models, in: Proceedings of the 17th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, 1994, pp. 23–30.
[80] C. Apte, F. Damerau, S.M. Weiss, Automated learning of decision rules for text categorization, ACM Transactions on Information Systems (TOIS) 12 (3) (1994) 233–251.
[81] V. Tam, A. Santoso, R. Setiono, A comparative study of centroid-based, neighborhood-based and statistical approaches for effective document categorization, in: 16th International Conference on Pattern Recognition: Proceedings. vol. 4, 2002, pp. 235–238.
[82] T. Joachims, Text categorization with support vector machines: learning with many relevant features, Machine Learning: ECML-98 13 (1998) 7–142.
[83] V.N. Vapnik, The Nature of Statistical Learning Theory, Springer-Verlag, 2000.
[84] P. Myllymaki, H. Tirri, Bayesian case-based reasoning with neural networks, in: IEEE International Conference on Neural Networks, 1993, 422–427.
[85] M.E. Ruiz, P. Srinivasan, Automatic text categorization using neural networks, in: Proceedings of the 8th ASIS SIG/CR Workshop on Classification Research, 1998, pp. 59–72.
[86] S. Deerwester, S.T. Dumais, G.W. Furnas, T.K. Landauer, R. Harshman, Indexing by latent semantic analysis, Journal of the American Society for Information Science 41 (6) (1990) 391–407.
[87] B. Yu, Z. Xu, C. Li, Latent semantic analysis for text categorization using neural network, Knowledge-Based Systems 21 (8) (2008) 900–904.
[88] J.J. Rocchio, Relevance Feedback in Information Retrieval, 1971.
[89] Z. Zhu, P. Liu, L. Ran, Research of text classification technology based on genetic annealing algorithm, in: International Symposium on Computational Intelligence and Design. ISCID'08, vol. 1, 2008, 265–269.
[90] S. Deng, H. Peng, Document classification based on support vector machine using a concept vector model, in: IEEE/WIC/ACM International Conference on Web Intelligence. WI 2006, December, (2006), pp. 473–476.
[91] T.M. Nogueira, S.O. Rezende, H.A. Camargo, On the use of fuzzy rules to text document classification, in: 10th International Conference on Hybrid Intelligent Systems (HIS), August, (2010), pp. 19–24.
[92] S.B. Kim, K.S. Han, H.C. Rim, S.H. Myaeng, Some effective techniques for Naive Bayes text classification, IEEE Transactions on Knowledge and Data Engineering 18 (11) (2006) 1457–1466.
[93] C. Jiang, F. Coenen, R. Sanderson, M. Zito, Text classification using graph mining-based feature extraction, Knowledge-Based Systems 23 (May) (2010) 302–308.
[94] U. Jüttner, Supply chain risk management: understanding the business requirements from a practitioner perspective, International Journal of Logistics Management 16 (1) (2005) 120–141.
[95] U. Jüttner, H. Peck, M. Christopher, Supply chain risk management: outlining an agenda for future research, International Journal of Logistics: Research and Applications 6 (4) (2003) 197–210.
[96] R. Mason-Jones, D.R. Towill, Shrinking the supply chain uncertainty circle, IOM Control 24 (7) (1998) 17–22.
[97] A. Lockamy III, K. McCormack, Analysing risks in supply networks to facilitate outsourcing decisions, International Journal of Production Research 48 (2) (2010) 593–611.
[98] J. Hallikas, V.M. Virolainen, Risk management in supplier relationships and networks, in: Supply Chain Risk, Ashgate Publishing Ltd, 2004, pp. 43–65.
[99] D. Neiger, K. Rotaru, L. Churilov, Supply chain risk identification with value-focused process engineering, Journal of Operations Management 27 (2) (2009) 154–168.
[100] P.R. Kleindorfer, G.H. Saad, Managing disruption risks in supply chains, Production and Operations Management 14 (1) (2005) 53–68.
[101] D. Zhang, X. Cao, L. Wang, Y. Zeng, Mitigating the risk of information leakage in a two-level supply chain through optimal supplier selection, Journal of Intelligent Manufacturing (2011) 1–14. , http://dx.doi.org/10.1007/s10845-011-0527-3.
[102] G.A. Zsidisin, L.M. Ellram, J.R. Carter, J.L. Cavinato, An analysis of supply risk assessment techniques, International Journal of Physical Distribution and Logistics Management 34 (5) (2004) 397–413.
[103] A. Klinke, O. Renn, A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies, Risk Analysis 22 (6) (2002) 1071–1094.
[104] D. Zhang, Y. Zeng, Y. Wang, H. Li, Y. Geng, Modeling and evaluating information leakage caused by inferences in supply chains, Computers in Industry 62 (3) (2011) 351–363.
[105] M. Christopher, H. Lee, Mitigating supply chain risk through improved confidence, International Journal of Physical Distribution and Logistics Management 34 (5) (2004) 388–396.
[106] O. Khan, M. Christopher, B. Burnes, The impact of product design on supply chain risk: a case study, International Journal of Physical Distribution and Logistics Management 38 (5) (2008) 412–432.
[107] D. Markovits, Contract and collaboration, Yale Law Journal (2004) 1417–1518.
[108] D. Malhotra, J.K. Murnighan, The effects of contracts on interpersonal trust, Administrative Science Quarterly 47 (3) (2002) 534–559.
[109] R.K. Woolthuis, B. Hillebrand, B. Nooteboom, Trust, contract and relationship development, Organization Studies 26 (6) (2005) 813–840.
[110] L. Weber, K.J. Mayer, Designing effective contracts: exploring the influence of framing and expectations, The Academy of Management Review (AMR) 36 (1) (2011) 53–75.
[111] A.Y. Ha, S. Tong, Contracting and information sharing under supply chain competition, Management Science 54 (4) (2008) 701–715.
[112] H.L. Lee, S. Whang, Information sharing in a supply chain, International Journal of Manufacturing Technology and Management 1 (1) (2000) 79–93.
[113] (a) M.D. Ryall, R.C. Samspson, Formal contracts in the presence of relational enforcement mechanisms: evidence from technology development projects, Management Science 55 (6) (2009) 906–925;
(b) D. Artz, Y. Gil, A survey of trust in computer science and the semantic web, Journal Web Semantics: Science, Services and Agents on the World Wide Web 5 (2) (2007) 58–71.
[114] S.E. Fawcett, S.L. Jones, A.M. Fawcett, Supply chain trust: the catalyst for collaborative innovation, Business Horizons (2011).
[115] S. Ruohomaa, L. Kutvonen, Trust management survey, Trust Management 7 (2005) 7–92.
[116] J. Huang, M.S. Fox, An ontology of trust: formal semantics and transitivity, in: Proceedings of the 8th International Conference on Electronic Commerce: The New e-Commerce: Innovations for Conquering Current Barriers, Obstacles and Limitations to Conducting Successful Business on the Internet, ACM, 2006, pp. 259–270.
[117] J. Huang, D. Nicol, A formal-semantics-based calculus of trust, IEEE Internet Computing 14 (5) (2010) 38–46.
[119] P.R. Zimmermann, The Official PGP User's Guide, MIT Press, 1995.
[120] W.M. Grudzewski, I.K. Hejduk, A. Sankowska, Trust Management in Virtual Work Environments: A Human Factors Perspective, vol. 2, CRC, 2008.
[121] N. Li, W.H. Winsborough, J.C. Mitchell, Distributed credential chain discovery in trust management, in: Proceedings of the 8th ACM Conference on Computer and Communications Security, 2001, pp. 156–165.
[122] T. Jakimavicius, P. Kataria, R. Juric, Semantic support for dynamic changes in enterprise business models, Transactions of the SDPS: Journal of Integrated Design and Process Science 14 (2) (2010) 1–11.
[123] G.C. O'Connor, Major innovation as a dynamic capability: a systems approach, Journal of Product Innovation Management 25 (4) (2008) 313–330.
[124] R.E. Miles, C.C. Snow, A.D. Meyer, H.J. Coleman Jr., Organizational strategy, structure, and process, Academy of Management Review 54 (1978) 6–562.
[125] T.J. Arnold, E. Fang, R.W. Palmatier, The effects of customer acquisition and retention orientations on a firm's radical and incremental innovation performance, Journal of the Academy of Marketing Science 39 (2) (2011) 234–251.
[126] C.M. Christensen, The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail, Harvard Business Press, 1997.
[127] G.M. Schmidt, C.T. Druehl, When is a disruptive innovation disruptive? Journal of Product Innovation Management 25 (4) (2008) 347–369.
[128] B. Cassiman, R. Veugelers, Centre for Economic Policy Research, Complementarity in the innovation strategy: internal R & D, external technology acquisition and cooperation. Discussion Paper Series, Centre for Economic Policy Research London, 2002.
[129] E.J. Chikofsky, J.H. Cross, Reverse engineering and design recovery: a taxonomy, IEEE Software 7 (1) (1990) 13–17.
[130] M. Sokovic, J. Kopac, RE (reverse engineering) as necessary phase by rapid product development, Journal of Materials Processing Technology 175 (1) (2006) 398–403.
[131] B. Bidanda, Reverse Engineering for Medical, Manufacturing and Security Applications, Springer, 2010.
[132] I. McLoughlin, Secure Embedded Systems: The Threat of Reverse Engineering, IEEE, 2008, pp. 729–736.
[133] G. Naumovich, N. Memon, Preventing piracy, reverse engineering, and tampering, Computer 36 (7) (2003) 64–71.
[134] C.S. Collberg, C. Thomborson, Watermarking, tamper-proofing, and obfuscation-tools for software protection, IEEE Transactions on Software Engineering 28 (8) (2002) 735–746.
[135] F. Sebe, J. Domingo-Ferrer, A. Solanas, Noise-robust watermarking for numerical datasets, Modeling Decisions for Artificial Intelligence 13 (2005) 4–143.
[136] X. Zhuang, T. Zhang, H.H.S. Lee, S. Pande, Hardware Assisted Control Flow Obfuscation for Embedded Processors, ACM, 2004, pp. 292–302.

Yong Zeng is Canada Research Chair in Design Science (Tire 2) and professor in Concordia Institute for Information Systems Engineering at Concordia University, Canada. His research is focused on the modeling and computer support of creative design activities. He and his research group have been approaching the research from philosophical, mathematical, linguistic, neurocognitive, and computational perspectives. His research results, which range from the science of design, requirements engineering, human factors engineering, computer-aided product development, product lifecycle management, finite element modeling, to design and supply chain management, have been applied to manufacturing, pharmaceutical, entertainment, construction industries, and municipality.

Lingyu Wang is an associate professor in Concordia Institute for Information Systems Engineering at Concordia University, Canada. He received his Ph.D. degree in information technology from George Mason University, USA. His current research interests include database security, data privacy, vulnerability analysis, intrusion detection, and security metrics. His research has been supported in part by the Discovery Grants from the Natural Sciences and Engineering Research Council of Canada (NSERC) and by Fonds de recherche sur la nature et les technologies (FQRNT).

Xiaoguang Deng is postdoctoral research fellow in Concordia Institute for Information Systems Engineering at Concordia University, Canada. He received his Ph.D. degree in Industrial Information Systems from Université des Sciences et Technologies de Lille, France. His research interests address decision-making, risk management, product design and development, supply chain management, and product lifecycle management.



Xinlin Cao is a Ph.D. student in Mechanical Engineering Department at Concordia University, Canada. His research interests include design methodology and computer-aided design.

Nafisa Khundker is a graduate student in Concordia Institute for Information Systems Engineering at Concordia University, Canada. She has done her B.Sc. from Jahangirnagar University, Savar, Dhaka, Bangladesh. She has worked as a research assistant in the field of e-Government interoperability framework in an UNDP project at Prime Minister's office, Dhaka, Bangladesh from April 2008 to November 2009. Her research interests include secure collaborative development, supply chain security, database security.