Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Process Perspective

By: Rahul Singh and Al F. Salam

Singh, Rahul and Salam, A. F. "Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Process Perspective" *IEEE Transactions on Systems, Man and Cybernetics* - A, (3), May 2006 472-486

Abstract:

Secure knowledge management for eBusiness processes that span multiple organizations requires intraorganizational and interorganizational perspectives on security and access control issues. There is paucity in research on information assurance of distributed interorganizational eBusiness processes from a business process perspective. This paper presents a framework for secure semantic eBusiness processes integrating three streams of research, namely: 1) eBusiness processes; 2) information assurance; and 3) semantic technology. This paper presents the conceptualization and analysis of a secure semantic eBusiness process framework and architecture, and provides a holistic view of a secure interorganizational semantic eBusiness process. This paper fills a gap in the existing literature by extending role-based access control models for eBusiness processes that are done by using ontological analysis and semantic Web technologies to develop a framework for computationally feasible secure eBusiness process knowledge representations. An integrated secure eBusiness process approach is needed to provide a unifying conceptual framework to understand the issues surrounding access control over distributed information and knowledge resources.

Index Terms: Description logics, information assurance and systems security, role-based access control, semantic eBusiness, semantic Web technology.

Article:

I. INTRODUCTION

Businesss operate in an increasingly dynamic knowledge-driven economy and function as knowledge-based organizations [22]. Information and knowledge resources are inherently distributed within and across organizations [45]. Increased IT capabilities, knowledge management, and increased customization of demand are pertinent competitive influences for virtually integrated networks of organizations acting as an extended enterprise [14], [17]. Delivering the value proposition through eBusiness processes, comprising value-added activities, requires that organizations innovatively share and utilize knowledge resources of partner organizations in the knowledge-sharing network [11], [53]. A business process approach provides an integrated perspective to manage information and knowledge sharing within and across organizational boundaries. This provides a basis to analyze and "tie-in" access control and security for business processes by defining the roles, permissions, access, and security of resources (information and knowledge) from a dynamic business process perspective.

In this paper, we define knowledge as information in the context of a specific problem domain upon which action can be advised or taken [56]. Sharing knowledge resources requires a secure knowledge management framework for global interorganizational access to knowledge resources while preserving local access control requirements within the organization. The paper contributes to secure knowledge management in eBusiness processes by presenting an integrative framework for distributed sharing of knowledge resources in a secure way across partner organizations. In this paper, we contend that knowledge codification, storage, retrieval, and sharing does not transpire in vacuum but rather that they transpire in the context of some business process—be that scientific, governmental, or commercial. Additionally, either human or software agent must perform some activity to access organizational knowledge resources. In this context, integrating security in terms of which activity has what permission to access which resource in the context of a business process provides us with a comprehensive framework to develop secure knowledge management architecture.

Moreover, local security and access control (SAC) policies are not designed for distributed resource sharing, while global SAC policies may not take into consideration impediments to the access and control of locally owned resources [50]. Centralized SAC mechanisms fail to capture the distributed nature of systems support required for interorganizational eBusiness processes. There is a paucity in research on the security of distributed eBusiness processes that provide a holistic business process perspective to secure sharing information and knowledge [44]. Our research contributes by filling a part of that gap in the literature by developing a framework and architecture for a secure semantic eBusiness process for secure knowledge management. We use ontological analysis of eBusiness processes and role-based access control (RBAC) and description logics (DL) formalism for theoretical soundness and Web ontology language (OWL-DL-W3C standard for knowledge representation) for system implementation. To the authors' knowledge, this is one of the first attempts at conceptualization, analysis, and development of a secure semantic eBusiness process framework and architecture that provide a comprehensive approach to secure knowledge management.

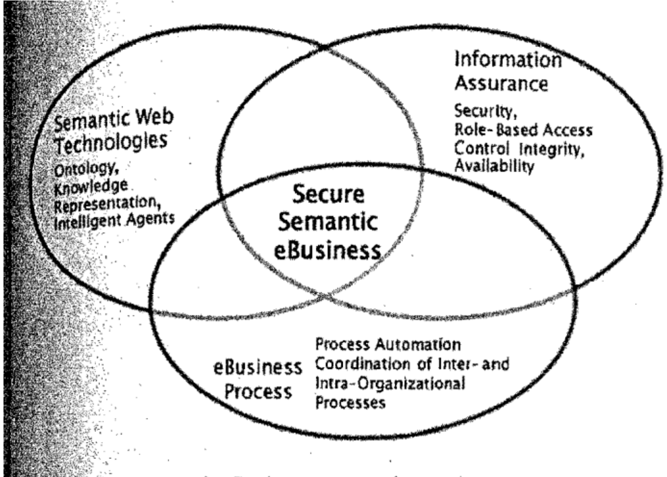

Semantic Web Technologies
Ontology, Knowledge Representation, Intelligent Agents
Information Assurance
Security, Role-Based Access Control Integrity, Availability
Secure Semantic eBusiness
eBusiness Process
Process Automation Coordination of Inter- and Intra-Organizational Processes

Fig. 1. Secure semantic eBusiness process view.

Our proposed framework integrates three streams of research, namely: 1) eBusiness process and knowledge management: 2) information assurance and RBAC; and 3) ontology and knowledge representation, DLs, and semantic technology (Fig. 1).

Specific contributions of this paper include: 1) the ontological analysis of eBusiness process to identify concepts essential to model eBusiness process; 2) the ontological analysis of RBAC to identify concepts essential to model access control requirements for eBusiness process; 3) the integrative framework for semantic modeling of secure knowledge management in eBusiness process; 4) the development of the proposed conceptual framework using DL formalism; and 5) the development of a multiagent architecture using the W3C standard OWL incorporating reasoning and inferencing mechanisms based on OL formalism.

The following sections present the theoretical foundations (Section II) of our approach including an ontological analysis of the essential concepts of semantic eBusiness process (Sections II-A—C) focusing on the secure sharing of resources between coordinated business activities, and RBAC (Section II-D) and information assurance in the context of the secure semantic eBusiness process universe of discourse. DL allows for creating complex descriptions of problem domains based on descriptions of atomic concepts and relationships. The results of the ontological analysis of a problem domain identify the essential concepts and relationships that can be used to develop complex and realistic descriptions of problem domains [20]. We present an introduction to DLs and utilize concepts identified using ontological analysis to develop a conceptual model and DL descriptions of secure semantic eBusiness processes (Sections HI and IV). We present a multiagent architecture for secure semantic eBusiness process and utilize an eBusiness process example to illustrate its workings (Section V). We conclude (Section VII) with a summary of related work (Section VI) and provide directions for future research.

II. THEORETICAL FOUNDATIONS

A. Interorganizational eBusiness Processes and Workflows

The Workflow Management Coalition [66] describes the business process as "a sequence of activities with distinct inputs and outputs and serves a meaningful purpose within an organization or between organizations." Basu and Kumar [6] provide an excellent research commentary on workflow management issues in eBusiness and point to the special characteristics of interorganizational business processes. Kumar *et al.* [34] provide a comprehensive discussion of the features and shortcomings in workflow systems. Flexibility, adaptability, interorganizational and intraorganizational process models, and the ability of workflow systems to handle exceptions emerge as leading research issues in workflow management systems (WFMSs). Raghu *et al.* [49] present an approach to organizational modeling that integrates both agent-centric and activity-centric approaches using incentive mechanisms. Kumar and Zhao present a general framework to implement dynamic routing and operational controls in WFMS. Van der Aalst and Kumar [63] develop process models of interorganizational workflows and their coordination structures using Petri nets, Van der Aalst and Kumar [63] presented a workflow schema exchange in an eXtensible Markup Language (XML) dialect called XRL that provides a foundation for interorganizational workflow coordination. Kumar and Wainer [32] present control and coordination of interorganizational workflow systems using meta-workflow knowledge of interorganizational eBusiness processes in XML syntax.

Interorganizational eBusiness supports collaborative relationships among customers, suppliers, and complementors as a strategic response to competitive forces [13]. Interorganizational eBusiness processes allow collaborating organizations to provide complementary business products and services to achieve competitive advantage through value networks of organizations that collaborate to create unique and hard-to-imitate customer value propositions [14], [53]. Here, the resource-based view of a firm with focused capabilities as the unit of competition is replaced by a value network with a focal enterprise that coordinates resources of collaborating organizations to create customer value [53]. The complexities of coordinating interorganizational eBusiness processes require a knowledge-driven coordination structure to determine decision authority and knowledge sources [3]. The integrated information system, as an integral part of the coordination structure, offers enhanced matchmaking of resources and coordination of activities to allow the value network to effectively respond to dynamic customer demand [10].

Tallman *et al.* [60] examine the role of knowledge exchange for the competitive advantage of a cluster of organizations and note that simpler, codified, and less tacit component knowledge, including skills and technologies, consumer behavior knowledge, and product knowledge, is amenable to knowledge exchange. Additionally, we define process knowledge as knowledge that is typically embedded in the process models of WFMSs or exists as coordination knowledge among human agents to coordinate interorganizational eBusiness processes. We also define security knowledge as knowledge that is captured through access control mechanisms that permit or deny access to knowledge resources in a distributed value network. An integrative view of secure semantic eBusiness process incorporates the simultaneous management of component knowledge, process knowledge, and security knowledge for interorganizational eBusiness processes. Following Tallman *et al.* [60], in this paper, we focus on explicit knowledge, not tacit knowledge, where knowledge is declarative enough to be represented by standards-based knowledge representation languages. We make these pragmatic restrictions on knowledge for practical reasons that can be processed and shared using reasoning mechanisms to reach useful inferences. We recognize that not all knowledge can be explicated and be effectively represented and reasoned with using decidable and complete computational techniques.

To build effective and practical knowledge-based systems that are both viable and useful, it may be more fruitful to concentrate on declarative and explicit knowledge that can be represented using computationally feasible knowledge representation languages such as DLs. In this paper, we therefore use DLs as the formal knowledge representation language to model a secure semantic eBusiness process. Moreover, DL is also the formalism behind the semantic Web knowledge representation language OWL (www.w3c.org/owl), which can be used for developing knowledge-based systems. In our research, we view the secure semantic eBusiness process as a central part of semantic eBusiness. Semantic eBusiness is "an approach to managing knowledge for the coordination of eBusiness processes through the systematic application of Semantic Web technologies" [56]. Semantic eBusiness applies semantic Web technologies for knowledge management to support the transparent flow of knowledge, content, and know-how, and to enhance eBusiness processes across the value network.

We present a model of the relationships between activities and resources including their coordination in an eBusiness process and agents' access to resources and their permissions to execute business activities. Business processes are decomposed into business activities organized by generalization—specialization hierarchies and require coordination mechanisms to manage their dependencies [37]. Coordination of business activities is embedded in eBusiness processes and in workflows and WFIVIS since they essentially deal with issues of task—task and task—resource dependencies and their coordination [29]. Coordination constructs used in this paper are based on [38] and are similar to those in [62] and [63].

B. Ontologies and Ontological Analysis

DL allows the development of complex concepts (descriptions), problem domains built upon atomic concepts (essential concepts), and their relationships using concept constructors. Ontological analysis identifies essential concepts and their relationships in a problem domain as an essential first step in developing knowledge representations for systems that can reason with problem domain knowledge [28], [29]. We present ontological analysis of eBusiness process in Section II-C and that of RBAC in Section to identify a set of atomic concepts .that can then be used in conjunction with concept constructors to present a DL-based representation of the secure romantic eBusiness process.

Ontological constructs, derived through ontological analysis, provide the basic language to represent and communicate knowledge of a problem domain [29].

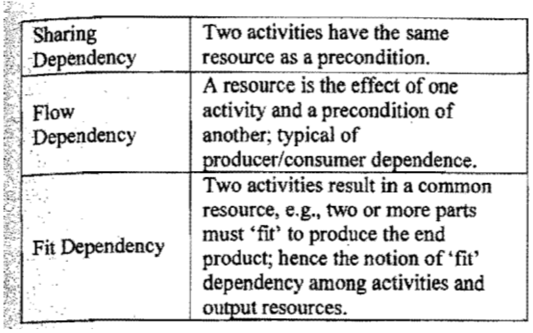
Ontologies provide a common understanding of the specific domain that can be shared between disparate application systems [21]. The computational ontology for systems contains common syntax and semantics to model IT artifacts [65]. Staab *et al.* [58] describe ontology-based knowledge management through knowledge meta-data that describe the information content and structure. Ontologies allow the integration of the online process knowledge used by eBusiness organization when they are shared between software agents to allow systems to use a common vocabulary and standard interpretation meaning of problem-domain constructs [30], [31].

C. Ontological Analysis of eBusiness Process

Ontological analysis develops the essential concepts to model eBusiness processes. A business enterprise uses a variety of resources including documentation, plant and equipment, consumable supplies, tools, etc. In this paper, we focus on the information and knowledge resources owned by specific business enterprises. Human and software agents represent business enterprises and carry out business activities to achieve eBusiness process objectives. Fox *et al.* [15] propose ontology for enterprise modeling activities performed by agents than fulfill organizational roles, Agents with appropriate authorizations to fulfill, roles perform business activities that consume or produce resources within the constraints limiting agent operations to role fulfillment [9]. In an integrated enterprise with multiple work systems, multiple agents interact in a highly coordinated manner to achieve individual and shared goals of the overall enterprise [29]. Sikora and Shaw [54] model enterprise systems as multiple agents and present models for the coordination mechanisms and interdependencies in control structures and knowledge exchange required to model agent functions in an enterprise.

Roles group business activities enacted by human or software agents expected to perform the business activities defined in the role. Tillquist *et al.* [61] model interorganizational relationships using dependency network diagrams where role interdependencies are defined as interface relations between activities. Holt *et al.* [23] introduced role activity diagrams (RADs) to model business processes, which were further developed by Ould [46] to partition a business process into a set of interacting roles. In WFMS, process knowledge incorporates coordination mechanisms and control structures to manage business activities of human and software agents in an organization [33].

Coordinating business activities is required to manage interdependencies among activities or among activities and resources [38], [39]. Malone *et al.* [38] define coordination as "managing dependencies among activities" and provide a taxonomy of dependencies among multiple activities and resources.



Sharing Dependency	Two activities have the same resource as a precondition.
Flow Dependency	A resource is the effect of one activity and a precondition of another; typical of producer/consumer dependence.
Fit Dependency	Two activities result in a common resource, e.g., two or more parts must 'fit' to produce the end product; hence the notion of 'fit' dependency among activities and output resources.

Fig 2. ***Dependencies among multiple resources and multiple tasks***

1) From a resource focus:

a) shared resource: a single resource is shared by two or more activities;

b) producer/consumer: an activity produces resources consumed by another activity;

c) common object: two activities are needed to produce a common resource.

2) Using an activity focus:

a) activity consumes multiple resources;

b) activity consumes one resource and produces another;

c) a single activity produces multiple resources.

The taxonomy of dependencies among resources and activities is shown in Fig. 2, adapted from Malone *et al.* [38].

Coordination mechanisms are employed to manage dependencies. Producer/Consumer dependency can be managed using a coordination mechanism such as notification and sequencing. In this paper, we use a simplified view of activity-resource dependency, where activity dependencies exist as a sharing, flow, or fit dependency with another activity through a resource. Here, dependencies do not exist directly between activities and while an activity may consume or produce a resource; it cannot produce or consume another activity. This is consistent with Malone *et al.* [38] and represents a simplification of the activity dependencies found in [62] and [63].

In this paper, we are concerned with information and knowledge resources of an organization. Organizational and process knowledge is central to the business activities of human and software agents. It is important for eBusiness to explicitly recognize knowledge, and the processes and technologies for knowledge management. Newell [43] provides a functional view of knowledge as "whatever can be ascribed to an agent, such that its behavior can be computed according to the principle of rationality." This view forms a basis for functional knowledge management using agents, both human and software, when using explicit declarative knowledge that is represented using standards-based knowledge representation languages that can be processed using reasoning mechanisms to reach useful inferences [55].

From this analysis, we extract an essential set of concepts to model eBusiness processes as business enterprise, agent, role, business activity, coordination, resource, information, and knowledge.

D. Ontological Analysis of RBAC

In this paper, we focus on authorization and access control, the primary mechanism used by organizations to control sharing information and knowledge resources.

Oh and Park [44] provide a comprehensive discussion of the characteristics of information sharing and access control in business enterprises, which we summarize as: 1) business information is characterized by information sharing; 2) information resources are accessed by many agents as they are produced and consumed in the business activities of a business process; 3) rapid changes in the business environment and consequent changes in business activities necessitate dynamic management of access rights to information resources. This makes administration of access control challenging.

Additionally, an enterprise may incur significant cost without appropriate and timely authorization for business activities to access information artifacts. Authorized access to information resources is based on job position and assigned organizational roles since separation of duty is an important security principle. The business activities of an enterprise are interconnected and require multiple constraints for appropriate access control to information resources.

The activity—resource dependency view of coordination used in this paper is also supported by the analysis of a business enterprise using Porter's framework [48] of value activities in a value chain. A value activity is a business activity carried out by a business enterprise engaged in an eBusiness process to create customer value. In eBusiness processes across a value chain, access control policies allow or deny value-added activity access to resources. In this conceptualization, security is viewed as an integral part of the value activities of a business enterprise. This provides a conceptual basis to understand security requirements in distributed interorganizational eBusiness processes. It also allows us to focus on the interdependencies and coordination requirements of the activities and resources. Activities are either internal to a business enterprise or interface with partner organizations. Focusing on the resource requirements of activities that interface with partner organizations allows an organization to develop access control policies to satisfy local intraorganizational and global interorganizational security requirements. Global access control policies are governed by contractual agreements between participating firms and specify the security requirements of activities of partner organization and their access to resources [26]. Research in automated contractual agreements is beyond the scope of this paper, and the interested reader is referred to Grosof and Poon [16].

The National Institute of Standards and Technology (NIST) adopted RBAC as a National Standard in 2004 (csrc.nist. gov/rbac). A key benefit of RBAC over previous security mechanisms lies in its use of roles as a layer of abstraction to decouple and simplify the association between users and permission to resources [52]. Access control policies specify users' permissions to specific system resources through relationships between users, roles, and permissions. Organizational role hierarchies reflect organizational hierarchies of responsibility. Users fulfill a role within an organization based on job function. Roles describe the authority and responsibility conferred on users assigned to a role. The relationships between roles and permissions and between users and roles users play define the access control policies for a security domain. Constraints add pragmatic considerations and exceptions to role hierarchies by implementing an organizational access control policy [47]. RBAC facilitates the specification of the user—role, role—permission, and particularly role—role mappings for entire security domains. Roles provide nonrepudiation and auditability of business activities and users fulfilling the roles. Distributed environments require assurance of authenticated local entities with appropriate authorization to fulfill their roles in the distributed environment. Permission to access specific information is controlled by role mapping and assignment of users to roles based on the functions they are entrusted to perform.

The above analysis identifies the following essential concepts (atomic concepts) to model RBAC: agent, role, permission, and resource.

Combining analyses in the above sections provides the following essential concepts to model the secure semantic eBusiness process problem domain: business enterprise, agent, role, business activity, coordination, resource, information, knowledge, and permission. We use these atomics concepts to build complex concepts using DL concepts and relationship constructors for our secure semantic eBusiness process. In the following section, we provide a brief overview of the semantic Web technology and standards.

E. Semantic Web Technology and Standards

The Semantic Web vision comprises: knowledge representation, structured collections of information and inference rules linked into a single system for automated reasoning; ontologies, to discover common meanings for entity representations and ways to interpret ontology; and intelligent agents, which collect content from diverse sources and exchange data enriched with semantics [7]. This vision provides the foundation for the semantic framework presented in this paper.

XML-based technologies (www.w3.org/XML) allow knowledge management in a meaningful way for supporting the flexible exchange of unambiguous content representation over heterogeneous platforms. ebXML (www.ebxml.org) and RossettaNet (www.RossettaNet.org) assist in the creation of common XML-based vocabularies for automated eBusiness processes. Technical advances in semantic technologies make the content of the Web unambiguous, computer interpretable, and amenable to agent interoperability and automated reasoning techniques [40]. The OWL is a W3C standard knowledge representation language for the semantic Web. OWL documents can be used to capture domain ontologies and rules for knowledge sharing among agents. OWL has robust theoretical foundations in DL and provides the standards-based foundation for semantic knowledge representation and management. In the next section, we present a DL-based representation of the secure semantic eBusiness process.

DL AND KNOWLEDGE REPRESENTATION FOR SECURE SEMANTIC eBUSINESS PROCESS

DLs model a problem domain using constructs that describe domain-specific objects and their relationships [5]. Domain entities are represented with the concept construct, a unary predicate, while relationships between constructs are represented with a relations construct, which may be an *n*-ary. Subsumption hierarchies of primitive and derived concepts and relationships express specialized relationships between derived concepts. Subsumption and disjointness operations on descriptions use the hierarchy to suggest comparable concepts that appear equivalent, disjoint, or overlapping. A variety of operators, such as generalize, specialize, or delete, are available to refine the hierarchy. In this paper, we use DL SHIQ [24], a superset of Attributive Language (AL) that includes cardinality restrictions, role hierarchies, inverse roles, transitive roles, and data types. OWL-DL is based on the SH family of DL. Satisfiability and logical implication in SHIQ are ExpTime complete [5]. Even though theoretical complexity results are discouraging, empirical analyses of real applications have shown that their applying some simple optimization techniques leads to a significant improvement in the empirical performance of DL systems [57]. More recently, FaCT, DLP, and RACER systems have demonstrated that even with very expressive logics, highly optimized implementations can provide acceptable performance in realistic applications [25].

DLs describe the semantic schema of a domain through specifications of complex concepts and relation expressions built upon atomic concepts and relations. DLs are particularly adept at representing real-world data semantic [101. The semantic model, in primitive and derived DL concepts, and the relationships among them form a semantic knowledge representation of the problem domain. Specific instance level descriptions, using the schema descriptions, provide illustrative examples useful for verification and refinement of the schema and for the implementation of the DL for automated reasoning and semantic data models. Reasoning procedures allow suitable inferences from the concepts and the relationships between them. DL derives descriptive power from the ability to enhance the expressiveness of the atomic descriptions by building complex descriptions of concepts using concept constructors including:

$\exists\ R.C$ (full existential value restriction);
$\neg\ C$ (atomic negation of arbitrary concept);
$\leq nR$ (at-most cardinality restriction);
$\geq nR$ (at-least cardinality restriction);
$= nR$ (exact cardinality restriction);
$\leq nR.C$ (qualified at-most cardinality restriction);
$\geq nR.C$ (qualified at-least cardinality restriction);
$= nR.C$ (qualified exact cardinality restriction);
$\leq nR$ (concrete domain max restriction);
$\geq nR$ (concrete domain min restriction);
$= nR$ (concrete domain exact restriction).

Terminological axioms comprising definitions and descriptions of problem domain concepts further describe the relationships between concepts and roles. The reader is referred to [5] for a full treatment of DLs.

The recent W3C OWL standard includes OWL-DL to represent DL models in OWL documents. OWL-DL knowledge representation is machine interpretable and can be shared, understood, and processed by software agents [40]. Tools like The Protege Ontology Editor (protege.stanford.edu) and Racer (www.racer-systems.com) allow the ontological analysis of problem domains and verify conformance to DL formalism and modeling requirements including model consistency. These tools generate standard OWL-DL documents for the schema and instance level documents to illustrate proof of concept and provide direction for the implementation of semantic knowledge representations of the problem domain. DL and OWL-DL are used to model domain concepts and relationships and create process models. This develops a knowledge base of machine-interpretable knowledge representation for secure knowledge management in eBusiness processes.

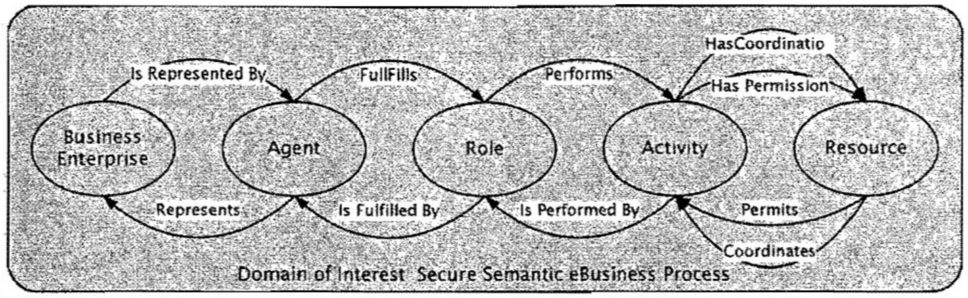


Fig. 3. ***Secure semantic eBusiness process conceptualization is the universe of discourse***

IV. SECURE SEMANTIC eBUSINESS PROCESSES

A. *Conceptualization of Secure Semantic eBusiness Processes*

The ontological analysis of secure semantic eBusiness processes, presented in Section II, allows us to model concepts and their relationships, including access control relationships that satisfy the requirements of the secure interorganizational eBusiness process. In this paper, we conceptualize the secure semantic eBusiness process problem domain as follows.

— In an eBusiness process, a Business Enterprise authorizes representation to an actor or Agent to fulfill a Role, which performs Activities that have access permissions to resources.

— Resources permit activities performed by Roles fulfilled by Agents that represent Business Enterprises, engaged in an eBusiness Process.

This conceptualization of a secure semantic eBusiness process presented in Fig. 3.

B. DL Model for Knowledge Representation of Secure Semantic eBusiness Processes

DL provides a basis for knowledge representation of the problem domain that includes a set of vocabularies. This includes atomic concepts that define individuals in the problem domain, and atomic relationships that define relationships between atomic concepts.

Essential atomic concepts in the secure semantic eBusiness process domain include the following:

1) BusinessEnterprise (BE);
2) Agent (Ag);
3) Role (Rl);
4) BusinessActivity (Ac);
5) Resource (Rs).

Essential atomic relationships in the secure semantic eBusiness process domain include the following:

1) Represents (≡ IsRepresentedBy -);
2) Fulfills (≡ IsFulFilledBy -);
3)Performs (≡ IsPerformedBy -);
4) Permits (≡ HasPermission -);
5) Coordinates (≡ HasCoordination -).

Here, R--denotes the inverse of the relationship R. These concepts and relationships in the problem domain are used to define the terminology for the secure semantic eBusiness process domain using the following terminological axioms. This forms the knowledge representation terminology for the secure semantic eBusiness process problem domain and the basis for the machine-interpretable representation of the ontology in OWL format.

A Business Enterprise concept is represented by at least one Agent in the problem domain, i.e.,

$$\begin{aligned}\text{BusinessEnterprise} \subseteq\ & (\geq 1\ \text{IsRepresentedBy} \bullet \text{Agent}) \wedge \\ & (\geq 1\ \text{HasClassificationID} \bullet \text{StringData}) \wedge \\ & (\geq 1\ \text{HasDescription} \bullet \text{StringData}) \wedge \\ & (\geq 1\ \text{HasAddress} \bullet \text{Address}) \wedge \\ & (\geq 1\ \text{HasProfile} \bullet \text{Profile}).\end{aligned}$$

An Agent concept represents a Business Enterprise and fulfills a Role for the Business Enterprise, i.e.,

$$\begin{aligned}\text{Agent} \subseteq\ & (\geq 1\ \text{Represents} \bullet \text{BusinessEnterprise}) \wedge \\ & (\geq 1\ \text{Fulfills} \bullet \text{Role}).\end{aligned}$$

A Role concept is a Thing fulfilled by an Agent and performs at least one Business Activity, i.e.,

$$\begin{aligned}\text{Role} \subseteq\ & (\geq 1\ \text{IsFullfilledBy} \bullet \text{Agent}) \wedge \\ & (\geq 1\ \text{Performs} \bullet \text{Activity}).\end{aligned}$$

A Business Activity is performed by a Role, has at least one permission to a Resource, coordinates Resources, and has a Begin Time and an End Time, i.e.,

$$\begin{aligned}\text{BusinessActivity} \subseteq\ & (\geq 1\ \text{HasLabel} \bullet \text{StringData}) \wedge \\ & (\geq 1\ \text{IsPerformedBy} \bullet \text{Role}) \wedge\end{aligned}$$

$(\geq 1\ \text{HasPermission} \bullet \text{Resource}) \wedge$
$(\geq 1\ \text{IsCoordinatedBy} \bullet \text{Resource}) \wedge$
$(= 1\ \text{HasBeginTime} \bullet \text{DateTimeData}) \wedge$
$(= 1\ \text{HasEndTime} \bullet \text{DateTimeData}).$

A Resource is a thing owned by exactly one Business Enterprise and permits Business Activities to perform operations on it and coordinates Business Activities, i.e.,

$\text{Resource} \subseteq (= 1\ \text{HasID} \bullet \text{StringData}) \wedge$
$(\geq 1\ \text{HasOwner} \bullet \text{BusinessEnterprise}) \wedge$
$(\geq 1\ \text{Permits} \bullet \text{BusinessActivity}) \wedge$
$(\geq 1\ \text{Coordinates} \bullet \text{BusinessActivity}).$

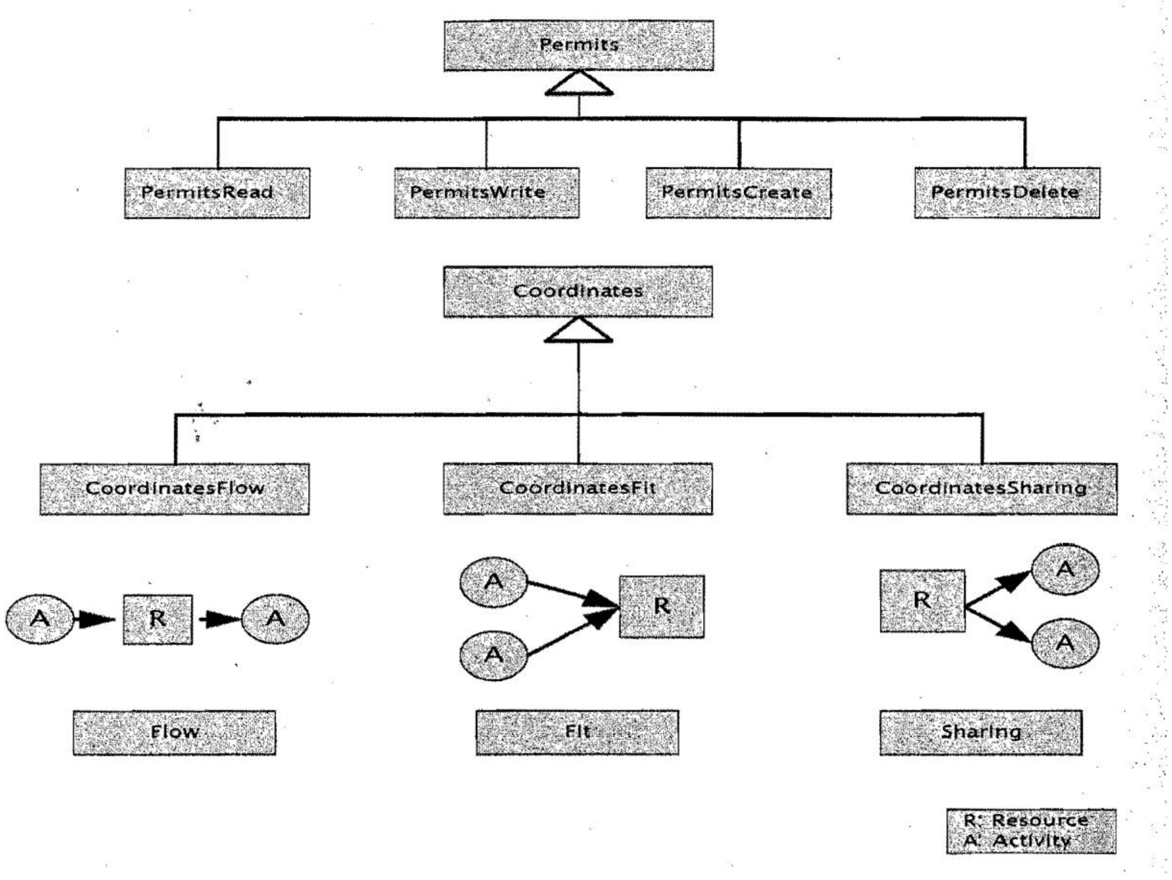


Fig. 4. Relationships between activities and resources.

A resource is related to business activities through operations that it permits business activities to perform. A resource specifies the permissions specific to business activities. Therefore, if a business activity has permissions, it is allowed to perform an operation on a resource. Permits and HasPermission are inverse relationships, i.e.,

$\text{Resource} \ni (\text{Permits} \bullet \text{BusinessActivity})$
$\text{BusinessActivity} \ni (\text{HasPermission} \bullet \text{Resource}).$

Activities depend on resources and require coordination mechanisms in order to resolve dependencies. A resource is related to an activity by the Coordinates relationship, i.e.,

$\text{Resource} \ni (\text{Coordinates} \bullet \text{BusinessActivity})$
$\text{BusinessActivity} \ni (\text{HasCoordination} \bullet \text{Resource}).$

DL SHIQ allows inheritance hierarchies of relationships. We use the inheritance hierarchies of relationships between activities and resources as shown in Fig. 4. Here, the Coordinates relationship between resources and activities is a generalization, which is specialized as CoordinatesFlow, CoordinatesFit, or CoordinatesSharing relationships, i.e.,

$$\begin{aligned}\text{Coordinates} \subseteq\ & \text{CoordinatesFlow}\\ & \text{CoordinatesFit}\\ & \text{CoordinatesSharing.}\end{aligned}$$

We utilize the inheritance hierarchy of the Coordinates relationship to develop a complex description of the relationship between Resources and Business Activities, i.e.,

$$\begin{aligned}\text{Resource} \ \exists\ & (\geq 0\ \text{CoordinatesFlow} \bullet \text{BusinessActivity}) \wedge\\ & (\geq 0\ \text{CoordinatesFit} \bullet \text{BusinessActivity}) \wedge\\ & (\geq 0\ \text{CoordinatesSharing} \bullet \text{BusinessActivity}).\end{aligned}$$

Coordination requirements lead to specific permissions on resources. Generally, a resource is related to an activity through the abstract Permits relationship. More specifically, Resources are related to Business Activities through the specialized PermitRead, PermitWrite, PermitCreate, or PermitDelete relationships, i.e.,

$$\begin{aligned}\text{Permits} \subseteq\ & \text{PermitRead}\\ & \text{PermitWrite}\\ & \text{PermitCreate}\\ & \text{PermitDelete.}\end{aligned}$$

We use the inheritance hierarchy of the Permits relationship to develop a more description of the relationship between Resources and Business Activities, i.e.,

$$\begin{aligned}\text{Resource} \ \exists\ & (\geq 0\ \text{PermitsRead} \bullet \text{BusinessActivity})\\ & (\geq 0\ \text{PermitsWrite} \bullet \text{BusinessActivity})\\ & (\geq 0\ \text{PermitsCreate} \bullet \text{BusinessActivity})\\ & (\geq 0\ \text{PermitsDelete BusinessActivity}).\end{aligned}$$

For the purpose of this paper, Information and Knowledge the primary resources pertinent to the problem domain. This ,51, ides the definition

$$\begin{aligned}&\text{Information} \subseteq \text{Resource}\\ &\text{Knowledge} \subseteq \text{Resource.}\end{aligned}$$

These definitions define the terminology for the secure semantic process problem domain, including the defined and primitive, concepts and the relationships between them. This provides the schema for the knowledge base for the secure semantic eBusiness process. In addition to the terminology, or TBox, is the world description, or ABox, with descriptions about individuals in the problem domain. Together, these comprise the DL-based knowledge representation system to provide the knowledge base used to reason about the problem domain.

V. PROPOSED SECURE eBUSINESS PROCESS ARCHITECTURE AND IMPLEMENTATION

Semantic eBusiness processes are enacted by human or software agents within predefined "knowledge domains." Conceptually, the value chain is a knowledge network where participating firms share local process and product/service knowledge with business partners to cocreate customer value. Product and meta-ontologies describe relationships between resources, whereas process knowledge maps how activities as part of business processes use these resources to create the customer value. In this view, the notion of knowledge domains is an extension of the context in which eBusiness activities transpire. In our conceptualization, explicit knowledge resources describing both product/service knowledge and process knowledge, across the value network, can be used to coordinate business activities across knowledge domains using software agents in collaboration with human agents. Additionally, embedding security knowledge of the shared resources, in terms of which activity has what permission to access which resource, along with both product/service knowledge and process knowledge, we can build systems for secure distributed knowledge management across different business partner organizations [42]. In the next section, we present our architecture that incorporates security knowledge as part of the business process to allow for the secure sharing of knowledge resources among partner organizations.

A key characteristic of the architecture is information transparency through machine-interpretable semantic knowledge in OWL documents that comprise all information flows. By capturing product/service knowledge in terms of ontologies, process knowledge describing coordination across activities in business processes and security knowledge describing activities having access permission to resources—all using OWL documents—we are able to present domain knowledge to software agents. These agents are then able to apply a DL-based inferencing mechanism to reach practical and useful conclusions. Each agent encapsulates an OWL-Reasoner (such as RACER) to interpret OWL documents.

We utilize two primary agent families in our secure semantic eBusiness process architecture. The security agent is responsible for the implementation of pragmatic security and information assurance requirements [12] of the architecture. The coordination agent is responsible for fulfilling the requirements of the coordination structure of the eBusiness process. A coordination agent is responsible for managing the coordination of activities and resources in each, knowledge domain. Knowledge of the eBusiness process description provides the coordination structure of individual services to fulfill customer requirements. This knowledge is encapsulated in a service coordination requirement (SCR) OWL document for a coordination agent responsible for coordinating the execution of the activity plan that is drawn up by the coordination agent by reasoning about the knowledge specified in the SCR. A coordination agent is responsible for coordinating the execution of the SCR and managing the constraints and coordinating multiple activities to fulfill customer requests. The coordination agent converses with the customer agent and value network partner agents responsible for individual subprocesses to complete the business activities in the end-to-end eBusiness process to satisfy customer requirements. Business activities are invoked, sequentially or in parallel, and enacted by the value network partner. eBusiness process results are provided to the customer agent when the eBusiness process is complete.

The security agent ensures that the business enterprise is represented by the actor or agent that is authorized to represent the business enterprise in the eBusiness process. The security agent also ensures that the specified role is able to perform the activities that it is authorized to perform and that the activities utilize their authorized access to the resources, including read, write create, or delete. These relationships are represented in RBAC research as security policies, which manifest themselves as constraints placed on the interactions between entities.

Each value net partner has a security agent. The focal film security agent converses With each value net partner security agent in terms of service requests fulfilled through roles made available by the partner security agent. Each security agent brokers the access for every resource activity by verifying the role performing the activity and the agent that fulfills the role. Once access is granted, the security agent for a knowledge domain (within the focal firm or within a partner domain) monitors the progress of the activity as it performs operations on the resource to ensure compliance with the security access policies of the entities within the domain.

Value network partners enter into contractual agreements with the focal firm to provide predetermined services and have contractual agreements on the levels of services provided. In addition, each value network partner provides partner capability documents (OWL) with the capability profile of the value network partner. These documents represent a negotiated agreement containing detailed definitions of operational characteristics, such as lead times, schedules, and constraints that define the service capabilities of value network partners [16]. It allows management of service expectations and partner capacities for every value network partner. Value net partner agents are responsible for providing updates for every service made available to the value network. Upon successful registration, the value net partner receives suitable ontology to specify the vocabulary for conversations in the value network and partners can enact eBusiness processes in the value network. The focal enterprise is responsible for managing OWL documents and delegating work to intelligent agents.

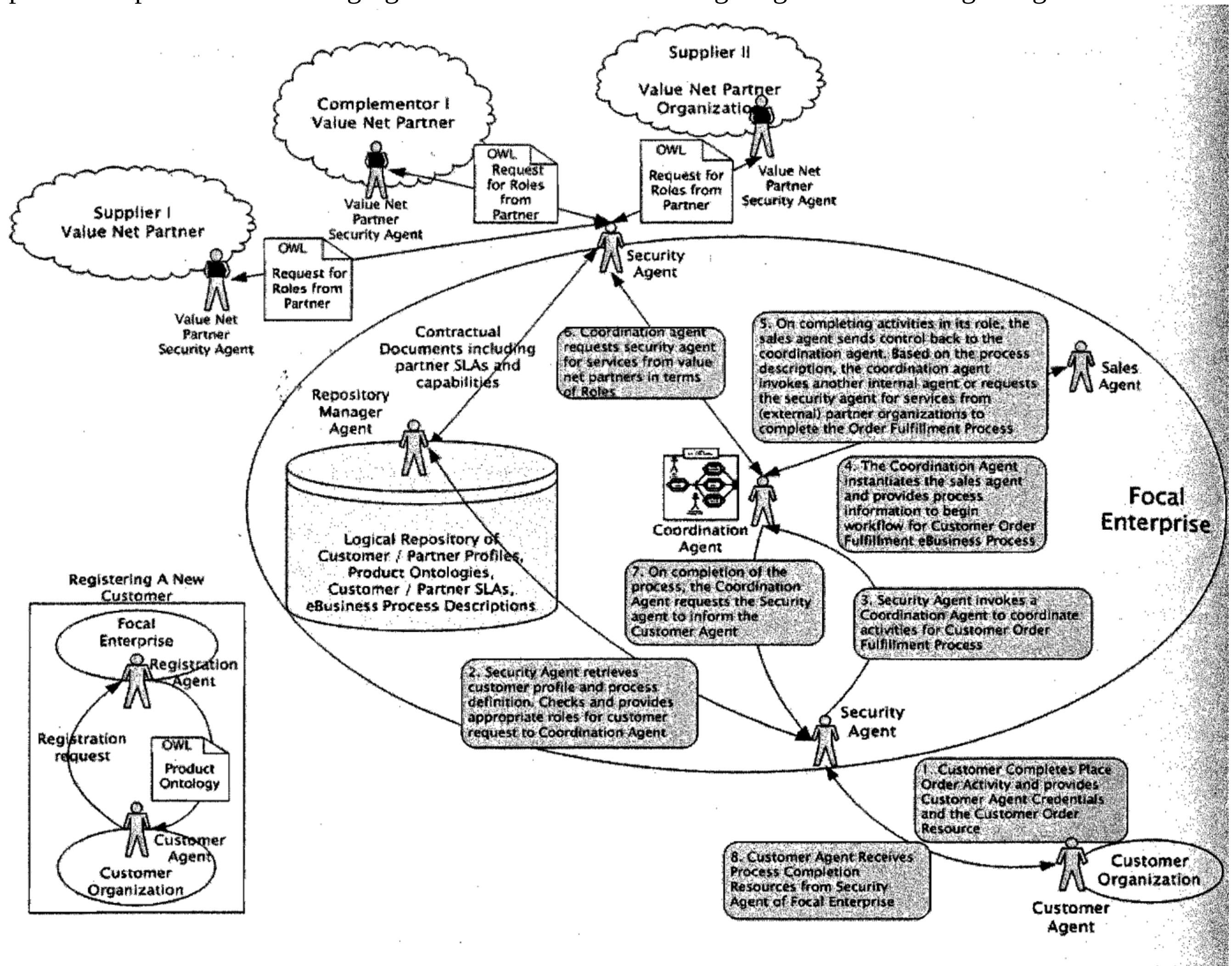

Supplier II
Value Net Partner Organization
Value Net Partner Security Agent
Complementor I
Value Net Partner
Value Net Partner Security Agent
OWL
Request for Roles from Partner
OWL
Request for Roles from Partner
Supplier I
Value Net Partner
OWL
Request for Roles from Partner
Value Net Partner Security Agent
Security Agent
Contractual Documents including partner SLAs and capabilities
Repository Manager Agent
Logical Repository of Customer / Partner Profiles, Product Ontologies, Customer / Partner SLAs, eBusiness Process Descriptions
6. Coordination agent requests security agent for services from value net partners in terms of Roles
5. On completing activities in its role, the sales agent sends control back to the coordination agent. Based on the process description, the coordination agent invokes another internal agent or requests the security agent for services from (external) partner organizations to complete the Order Fulfillment Process
Sales Agent
4. The Coordination Agent instantiates the sales agent and provides process information to begin workflow for Customer Order Fulfillment eBusiness Process
Coordination Agent
Focal Enterprise
7. On completion of the process, the Coordination Agent requests the Security agent to inform the Customer Agent
3. Security Agent invokes a Coordination Agent to coordinate activities for Customer Order Fulfillment Process
2. Security Agent retrieves customer profile and process definition. Checks and provides appropriate roles for customer request to Coordination Agent
Security Agent
1. Customer Completes Place Order Activity and provides Customer Agent Credentials and the Customer Order Resource
8. Customer Agent Receives Process Completion Resources from Security Agent of Focal Enterprise
Customer Organization
Customer Agent
Registering A New Customer
Focal Enterprise
Registration Agent
Registration request
OWL
Product Ontology
Customer Agent
Customer Organization

Fig. 5. Secure semantic eBusiness process architecture. An order-processing example.

Customers, registered with the focal enterprise, are represented by authorized customer agents that represent customer organizations in communications with the focal enterprise. The focal enterprise manages customer descriptions specifying customer preferences and requirements including identification, location, and contractual information. Customer agents represent customer interests in the value network and communicate a customer's needs. This is shown in the offset in Fig. 5. Upon successful registration, the customer business enterprise, through interactions of the customer agent, is provided with product ontologies (product knowledge) that specify the common and shared vocabulary to be used for all communication with the focal enterprise. In the case of the order processing eBusiness process example, a customer agent, representing the customer business enterprise, fulfils the CustomerProcurement role for the customer business enterprise and completes the place order business activity. This activity creates the customer order resource. The customer order resource specifies the coordination requirements of the activity for the order fulfillment eBusiness process as a flow coordination relationship with the receive order activity of the focal enterprise. At this time, the customer agent interacts with the focal enterprise through the security agent of the focal enterprise, which is the only possible means of interorganizational interaction. This interaction entails the customer agent presenting the security agent of the focal enterprise with the credentials of the customer agent and its representation of the customer business enterprise. In addition, the customer agent supplies the security agent of the focal enterprise the customer order resource. This is shown as information flow #1 in Fig. 5. In our model, a customer is a business enterprise represented by a customer agent, i.e.,

$$\begin{aligned}\text{Customer} \subseteq\ & (\text{BusinessEnterprise}) \wedge \\ & (\geq 1\ \text{IsRepresentedBy} \bullet \text{CustomerAgent}) \wedge \\ & (\geq 1\ \text{IsRepresentedBy} \bullet \text{AccountingAgent}).\end{aligned}$$

A customer agent represents a customer and fulfills the customerProcurement role

$$\begin{aligned}\text{CustomerAgent} \subseteq\ & (\text{SoftwareAgent}) \wedge \\ & (\geq \text{Represents} \bullet \text{Customer}) \wedge \\ & (\geq 1\ \text{FullFills} \bullet \text{CustomerProcurement role}).\end{aligned}$$

The place order activity has to create permission to the customer order resource, i.e.,

PlaceOrder

$$\begin{aligned}\subseteq\ & (\text{BusinessActivity}) \wedge \\ & (\geq 1\ \text{IsPerformedBy} \bullet \text{CustomerProcurement role}) \wedge \\ & (\geq 1\ \text{HasCoordinationFlow} \bullet \text{CustomerOrder}) \wedge \\ & (\geq 1\ \text{HasPermissionCreate} \bullet \text{CustomerOrder}) \wedge \\ & (= 1\ \text{HasBeginTime} \bullet \text{DateTimeData}) \wedge \\ & (= 1\ \text{HasEndTime} \bullet \text{DateTimeData}).\end{aligned}$$

The security agent of the focal enterprise locks the customer order resource and validates the customer agent credentials with the profile of the customer business enterprise available in the repository of the focal enterprise. This is shown as information flow #2 in Fig. 5. This process of validation includes authentication procedures. Upon successful authentication, the security agent examines the role of the customer agent in the eBusiness process description and determines the validity of the customer agent's request. In the case of the order processing example, he customer agent is representing the customer organization in fulfilling the CustomerProcurement role. The description of the CustomerProcurement role specifies the required set of business activities. Here, the security agent conducts matching (see Appendix for a discussion of DL matching and Agent interaction for security) and reasoning with the description of the agent’s role and its relationship with the predetermined activities and the resource permissions required for the activities that the customer agent requested. The security agent then invokes a coordination agent and provides the appropriate business process description from the repository of the focal enterprise and the authenticated customer order resource supplied by the customer agent to the coordination agent. This is shown in Fig. 5 as information flow #3.

Upon validation, there is implicit trust between the customer knowledge domain and the focal enterprise, and the remainder of the order processing eBusiness processes are conducted by the focal enterprise, The coordination agent has access to the customer order resource and from examination of the resource and the process description infers the next set of activities required and invokes the appropriate agent to fulfill roles required to complete the eBusiness process. Upon completion of any activity by any agent, control is transferred back to the coordination agent to invoke the next agent to fulfill a role that performs an activity that has appropriate permissions for a resource. This is shown in information flows #4 and #5 in Fig. 5. Here, we point out that the information flows #4 and #5 depicted in Fig. 5 are repeated based on eBusiness process descriptions available to the coordination agent. The coordination may require that a human agent be invoked, or called upon, to fulfill a role, such as order approval, by performing the activity GetOrderApproval. Here, the verified order resource permits the activity GetOrderApproval to write to the resource. The order approval role, performed by the management human agent, is permitted to perform this activity.

An interesting interorganizational case is when the coordination agent (of the focal firm) makes a request (as part of executing a part of a business process) to the focal firm security agent for a role(s) that performs activities over resources owned by a value net partner(s). This is where access is needed to local resources, owned by a partner, that need to be shared with agents from the focal firm in the context of a distributed business process to fulfill the requirements of the customer of the value net. This is shown in information flow #6, Here, the focal firm security agent in turn requests for a role(s) from the value network partner security agent where the role(s) can perform activities over resources owned by the value net partner. This exchange is brokered through and monitored by the security agent of the focal enterprise. Here, we point out that the local resources of the value network partner, and the individual activities that are allowed on them, remain within the realm of the value network partner knowledge domain. The security agent requests a role from the value network partner security agent. The requested role allows activities to be performed within the value network partner knowledge domain coordinated by resources, owned by the partner organization, which specify the permissions, within the value network domain. This allows for maintaining the local autonomy, authorization, and integrity of the resources of the organization while fulfilling the contractual service-level agreements of the value network partner. The coordination agent of the focal enterprise invokes the next agent in the eBusiness process description to fulfill roles to execute the eBusiness process. Upon completion of the eBusiness process, the coordination agent sends control back to the security agent of the focal enterprise. This is shown in Fig. 5 as information flow #7. The security agent, responsible for all interorganizational communication and role requests, communicates with the customer agent representing the customer business enterprise and provides the resources generated from completion of the business process by the focal enterprise. This is shown as flow #8 in Fig. 5. We present a generic agent interaction model and matching in DL in Appendix for the interested reader.

VI. RELATED WORK

In Section II, we presented the theoretical foundations of this work positioned in eBusiness processes and workflows, ontologies and ontological analysis, and semantic Web technologies. Atluri *et al.* [4] address the problem of interorganizational eBusiness workflows using a "Chinese wall" security model for decentralized workflows, where agents utilize modular organizational and process knowledge. Ahn *et al. [1]*, [2] discuss the application of RBAC principles to an existing Web-based workflow system using a role server for allocation of roles to users. Kang *et al.* [27] examine access control for interorganizational workflows through mechanisms for monitoring assignments of roles to agents to conduct workflow activities using monitor servers and access control matrices.

Steimsek *et al.* [59] describe access control systems for Web-based knowledge management systems using resource description framework (RDF) meta-data to enforce access control policies. Bhatti *et al.* [8] present XML-based specifications for Web services document security that incorporates models of the essential RBAC elements and their mappings. Van der Aalst and Kumar [63] present an XML-based schema definition to support of interorganizational workflow using XRL. Ricci *et al.* [51] present virtual enterprises and workflow management as agent coordination issues. Lee *et al.* [35] discuss the relevant problem of secure knowledge management in the semantic Web. Kumar and Wainer [32] discuss an approach to utilize meta-models and process descriptions of interorganizational workflows as a means of control and coordination • for handling exceptions in WFMS. To the authors' knowledge, research presented in this paper is one of the first attempts at the conceptualization and analysis of a secure semantic eBusiness process.

Our work addresses issues that are similar to those addressed by Gudes *et al.* [18], [19] and Wainer *et al.* [64]. Gudes and Tubman [18] use an "alter-ego" paradigm to specify static policy constraints and dynamic authorization using autonomous objects. This was based on their previous work in developing models and specifications for workflow security presented in Gudes *et al.* [19]. In our architecture, role can only be assigned through security agents of respective firms, thus maintaining tight control over how role(s) are assigned. This also preserves complete local control over locally owned resources while allowing partner organizations to access needed resources in a timely and efficient manner. This is possible as all partner organizations share and use the same ontologies to express SAC requirements. Additionally, since agents are able to perform inferencing based on the ontologies and expressed knowledge, our architecture can grow and cope with the dynamic nature of business enterprises. For example, if two roles are in conflict, security agents can infer such conflicts from the ontologies and expressed knowledge in OWL-DL. By having system security administrators who can modify, override, and/or create new mappings between agents and BusinessEnterprise and between activity and resource, our proposed system is dynamic and can cope with the changing requirements of business. Our proposed framework and architecture for secure semantic eBusiness process for secure knowledge management using DL formalism for theoretical soundness and OWL-DL for practical implementation is one of the first attempts in the literature.

VII. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Our proposed framework on a secure semantic eBusiness process integrates three streams of research, namely: 1) eBusiness process; 2) authorization and RBAC; and 3) ontology, DLs, and semantic technology. In this paper, we presented an ontological analysis of an eBusiness process and identified a set of central concepts that are essential to modeling the eBusiness process, In addition, we presented an ontological analysis of RBAC and showed the development of a set of central concepts critical to modeling access control requirements of the eBusiness process. Our framework used DL formalism for theoretical soundness. This forms the basis for the development of machine interpretable knowledge representation in OWL-DL format. We utilized an eBusiness process example to illustrate the development of a semantic architecture that utilizes multiagent systems and the W3C-recommended OWL incorporating reasoning and inferencing mechanisms based on the DL formalism presented. This represents the holistic view of conceptualization, the analysis of a secure semantic eBusiness process framework, and architecture for interorganizational eBusiness processes.

Information and knowledge resources are inherently distributed within and across organizations. Innovation and discovery rest upon the ability of organizations to share and use information that is owned and made available by partner organizations in the information and knowledge-sharing network [41]. Security concerns must be balanced with competitive requirements for collaboration and forming virtual partnerships. The development of information and security architecture from the business process perspective brings the added benefit of a much needed SAC framework for eBusiness process implementations that incorporate secure management of knowledge in interorganizational eBusiness processes.

APPENDIX

AGENT INTERACTION FOR SECURE SEMANTIC eBUSINESS PROCESS AND MATCHING IN DLs

A. Preliminary Notions of DLs

DLs are a family of logic formalisms for knowledge representation. All DLs are endowed with syntax and semantics, which is usually model theoretic. The basic syntax elements of DLs are concept names, role (relationships among concepts) names, and individuals (instances). Intuitively, concepts stand for sets of objects, and roles link objects in different concepts. Individuals are used for special named elements belonging to concepts. Basic elements can be combined using constructors to form concept and role expressions, and each DL has its distinguished set of constructors. Every DL allows one to form a conjunction of concepts, usually denoted as $\bigcap$; some DLs also include disjunction U and complement $\neg$ to close concept expressions under Boolean operations.

More formally, a semantic interpretation is a pair $I = (\Delta, \cdot^I)$, which consists of domain Δ and the interpretation function $\cdot^I$ that maps every concept to a subset of Δ [5]. We assume that different individuals are mapped to different elements of Δ, i.e., $a^I \neq b^I$. This restriction is usually known as unique name assumption (UNA).

Roles can be combined with concepts using existential role quantification and universal role quantification. Other constructs may involve counting, as number restrictions. Many other constructs can be defined, increasing the expressive power of the DL up to *n*-ary relations. Expressions are given semantics by defining the interpretation function over each construct.

The interpretation of constructs involving quantification on roles needs to make domain elements explicit. Concept expressions can be used in inclusion assertions, and definitions, which impose restrictions on possible interpretations according to the knowledge elicited for a given domain. Definitions are useful to give a meaningful name to particular combinations. Sets of such inclusions are called terminological box (TBox). The semantics of inclusions and definitions is based on set containment: an interpretation I satisfies an inclusion $C \subseteq$

D if $C^I \subseteq D^I$, and it satisfies a definition $C = D$ when $C^I = D^I$. A model of a TBox *T* is an interpretation satisfying all inclusions and definitions of *T*.

DL-based systems usually provide two basic reasoning services.

1) Concept satisfiability: given a TBox *T* and a concept *C*, does there exist at least one model of *T* assigning a nonempty extension to *C?*

2) Subsumption: given a TBox *T* and two concepts *C* and D, is C more general than *D* in any model of *T?*

In DL-based systems, it is commonly accepted that fixed terminology problems are overcome if terms (concepts) have a logical meaning through an ontology [36]. The main deficiency in using fixed terminologies (without logical connection among the terms or concepts) in expressing terms related to describing BusinessEnterprise, agent, role, activity, and resource is in losing common shared meanings of these concepts in our universe of discourse. Hence, by modeling our universe of discourse using DL, based upon ontological analysis, ensures that a common ontology containing concepts BusinessEnterprise BE, Agent AG, Role RL, Activity AC, and Resource RS is established as a TBox *T* in DL. DL.-based reasoning services can now be applied to this TB ox *T*.

In DL,complex concepts are constructed using concept constructors and atomic concepts and DL roles (relationships). In our case, DL roles are the properties that associate concepts with other concepts. For example

Agent ⊆ (≥ 1 Represents · BusinessEnterprise) ∧
(≥ 1 Fulfills • Role).

In our notation, we have

AG ⊆ (≥ Represents · BE) ∧
(≥ 1 Fulfills · RL).

Additionally, we have

BusinessEnterprise BE = (BE1, BE2, BE3, . . ., BE_n) and
Agent AG = (AG1, AG2, AG3, … , AG_n) and
Role RL (RL1, RL2, RL3, …, RL_n) and
Activity AC = (AC1, AC2, AC3, … , AC_n) and
Resource RS = (RS1, RS2, RS3, …, RS_n)

Where *n* is finite.

In an open system, such as ours, we assume *a priori* that the human agent (System Security Administrator) will authenticate Agent AG with BusinessEnterprise BE and represent such authentication in the BE-Agent OWL-DL Repository, Additionally, the System Security Administrator will assign Activity AC appropriate permission to access Resource RS. This openness allows our system to grow and change with the changing requirements of the BusinessEnterprise BE.

B. Generic Agent Interaction for Security

To illustrate how the DL model of our system provide-’ security features in our architecture, we consider two scenarios.

Scenario I: This scenario deals with how a Role is assigned to a requesting Agent by the Security Agent. In this scenario, it is assumed that both the requesting Agent AG 1 and the Security Agent SAG I belong to the same BusinessEnterprise BE. This is essentially an internal assignment of Role to an internal Agent.

We consider that Agent AG1 needs to perform Activities AC10 and AC11 in the process of executing some part of a business process, and even though this Agent AG1 has been assigned other Roles, those Roles do not cover ACIO and AC11. In this case, the Agent AG1 sends a request to the SecurityAgent SAG 1 for Role that once assigned to Agent AG 1 will allow this agent to fulfill its activities. We illustrate this by considering the following steps.

1) Agent AG1 sends request to SecurityAgent SAG I for Role that covers Activities AC10 and AC11.

2) SecurityAgent SAG1 needs to perform a match (using matching algorithm presented in this Appendix) on RL to see if RL contains a Role RL$^{\sim}$ that covers Activities AC10 and AC11 .

3) If yes

a) if there is a match found, then SAG1 returns Role RL$^{\sim}$ to Agent AG1 and updates the Agent—Role OWL-DL Repository that Agent AG) has been assigned Role RL$^{\sim}$. End.

4) If no

a) SecurityAgent SAG 1 needs to perform a match on AC to see if AC contains Activities AC10 and AC11.

b) If yes

i) if there is a match found for each Activity A10 and All, then SAG1 creates a new Role RL1011 and updates Role RL and assigns Role RL1011 to Agent AG 1 and updates the Agent—Role OWL-DL Repository that Agent AG1 has been assigned role RL$^{\sim}$. End,

c) If no, then exception occurs to notify the Security System Administrator to create proper permission for Activity AC10 and AC11 to access their corresponding resources. Notify Agent AG1 to wait until role becomes available.

Scenario II: This scenario presents security across different partner BusinessEnterprise.

Agent AG1 from BusinessEnterprise (Focal Enterprise) BEI needs to carry out activities Al and A2 from partner BusinessEnterprise BE2 and activities A10 and All from partner BusinessEnterprise BE3.

Clarification: Activities Al and A2 needs AccessPermission to resources RS 1 and RS2 owned by registered partner BE2. Therefore, the local security agent LSA2 of BE2 has control over these activities. Similarly, activities A10 and All need AccessPermission to resource RS 10 and RS 11 owned byBE3. Therefore, the local security agent LSA3 of BE3 has control over these activities. The coordination agent CA of the focal firm will make a request, on behalf of other agents, to the focal firm security agent for a role(s). that permits activity to access resources from partner organizations. Here, we assume BE1 represents the focal firm.

In this scenario, coordination agent AG1 (of BE1) requests focal firm (BE1) security agent (SAG1) for a role(s) so that activities Al and A2 from BE2 and A10 and All from BE3 can be performed.

Step 1) The focal firm (BE1) security agent (SAG1) contacts the local security agent LSA2 for BE2 for a role allowing activities Al and A2 and contacts local security agent LSA3 of BE3 for a role allowing activities A10 and All from BE3.

Step 2) LSA2 of BE2 performs matching on the local role repository to find a role R12 that fulfills activities Al and A2 having AccessPermission to resources RS 1 and RS2 owned by BE2. LSA2 then transfers this role to the focal firm security agent SAG1 that then assigns role R12$_{BE2}$ to agent AG1. The focal firm security agent also updates the global agent—role profile OWL repository with this new role R12 being assigned to agent AG1.

Step 3) Similar to step 2 above, LSA3 of BE3 after performing matching to find role R1011 for activities A10 and All requiring AccessPermission to resources RS 10 and RS 11 owned by BE3. LSA3 then transfers this role to the focal firm security agent SAG1 that then assigns role $R1011_{BE3}$ to agent AG1. The focal firm security agent also updates the global agent—role profile OWL repository with this new role $R1011_{BE3}$ being assigned to agent AG1.

Step 4) Both security agents LSA2 and LSA3 have monitoring (read and query) access to the global agent—role profile OWL repository to make sure that no improper access has been granted.

This process of assigning Roles only through Security Agents of respective firms maintains tight control over how the Roles are assigned. This also preserves complete local control over locally owned resources while allowing Partner organizations to access needed resources in a timely and efficient manner. This is possible as all Partner organizations share and use the same Ontologies to express SAC requirements. Additionally, since agents are able to perform inferencing based on the ontologies and expressed knowledge the system can grow and cope with the dynamic nature of business enterprises. For example, if two roles are in conflict, Security Agents can infer such conflicts from the Ontologies and expressed knowledge in OWL-DL. By having System Security Administrators who can modify, override and or create new mappings between Agents and BusinessEnterprise and between Activity and Resource, our proposed systems is dynamic and can cope with the changing requirements of business.

C. Matching in DLs

Matching has been defined in the literature [36] as follows.
Given A and *C* are atomic concepts in DL TBox *T*, the tvpes of matches are defined as follows.

- Exact: If concepts *A* and *C* are equivalent concepts, then one calls the match Exact; formally, $A \equiv C$.

- PlugIn: If concept *C* is a subconcept of concept A, then one calls the match PlugIn; formally, $C \subseteq A$.

- Subsume: If concept *C* is a superconcept of concept *A*, then one calls the match Subsume; formally, $A \subseteq C$.

- Intersection: If the intersection of concept *A* and concept *C* is satisfiable, then one calls the match Intersection to distinguish it from Disjoint, where the concepts are completely incompatible

- Disjoint: Otherwise, one calls the match Disjoint; that is, $A \cap C \subseteq^{\perp}$.

Degrees of the match are organized on a discrete scale. Exact matches are clearly preferable over other types of matches because there cannot be any ambiguity in terms of who is allowed to perform which activity and access which resource in a security architecture.

The pseudocode for matching concept *C* with concept *A* in the repository was adapted from [36] as

```
doMatch (Requested Concept C) {
   forall Concepts of Type C (which is A) in the Repository do {
      globalDegreeMatch = Exact
      degreeMatch = matchDegree(Input as Ranges of Properties of Concept C, Input as Ranges of Properties of
      Concept A)
      if (degreeMatch < globalDegreeMatch)
         globalDegreeMatch = degreeMatch
      storeResult (Current Requested Concept  C, globalDegreeMatch)//for later analysis to see match failed
      return no-Match)//no matches found in the Concept Repository for the Requested
   //Concept C
      otherwise, return matching concept A
      storeResult (Current Concept C, globalDegreeMatch, matched concept)
}
matchDegree (C, A) {
   if concept-equivalent (C, A) return Exact
   if concept-subsumes (A, C) return Plugln
   if concept-subsumes (C, A) return Subsume
   if concept-subsumes (: C, A) return Disjoint
   return Intersection
}
```

REFERENCES

[1] G. Ahn, R. Sandhu, M. Kang, and J. Park, "Injecting RBAC to secure a web-based workflow system," *in Proc. RBAC,* Berlin, Germany, 2000, .4, pp. 1-10.

[2] G. H. Ahn and R. Sandhu, "The RSL99 language for role-based separation of duty constraints," in *Proc. 4th ACM Workshop Role-Based Access Control*, Fairfax, VA, Oct. 1999.

[3] K. S. Anand and H. Mendelson, "Information and organization for horizontal multi-market coordination," *Manage. Sci,*, vol. 43, no. 12, pp. 1609-1627, Dec. 1997.

[4] V Atluri, A. C. Soon, and P. Mazzoleni, "Chinese wall security for decentralized workflow management systems," *J. Cornput. Secur.,* vol.12, no, 6, pp. 799-840,2004.

[5] F. Baader, D. Calvanese, D. McGuinness, D. Nardi, and P. E Patel-Schneider. Eds., The *Description Logic Handbook: Theory, Implementation and Applications,* Cambridge Univ. Press, Cambridge, U.K., 2003

[6] A. Baru and A. Kumar, "Research commentary: Workflow management systems in e-business," *Int Syst. Res., vol.* 13, no. 1, pp. 1-14, Mar. 2002.

[7] T. Berners-Lee, J. Hendler, and O. Lassila, The semantic web," *Sci. Amer.*, vol. 284, no. 5, pp. 34-43, May 2001.

[8] R. Bhatti, E. Bertino, A. Ghafoor, and J. B. D. Joshi, "XML-based specifications for web services document security," *Computer, vol.* 37, no. 4, pp. 41-49, Apr. 2004.

[9] G. Boella and L. van der Torre, "Attributing mental attitudes to roles: The agent metaphor applied to organizational design," in *Proc. ICEC*, 2004, pp. 130-137.

[10] A. Borgida, "Description logics in data management," *IEEE Trans. Knowl. Data Eng.*, vol. 7, no. 7, pp. 671-682, Oct. 1995.

[11] V. Choudhury, "Strategic choices in the development of interorganizational information systems," *Inf. Syst. Res.*, vol, 8, no. 1, pp. 1-24, Mar. 1997,

[12] R. Cummings, "The evolution of information assurance," *Computer*, vol. 35, no. 12, pp. 65-72, Dec, 2002.

[13] Y. Doz and G. Hamel, *Alliance Advantage.* Boston, MA: Harvard Bus, School Press, 1998.

[14] J. Dyer, *Collaborative Advantage: Winning Through Extended Enterprise Supplier Networks.* New York: Oxford Univ. Press, 2000.

[15] M. S. Fox, M. Barbuceanu, M. Gruninger, and J. Lin, "An organization ontology for enterprise modeling," in *Simulating Organizations: Computational Models of Institutions and Groups,* M. Prietula, K. Carley, and L. Gasser Eds, Menlo Park, CA: AAAI/MIT Press, 1998, pp. 131-152.

[16] B. N. Grosof and T. C. Poon, "Sweet deal: Representing agent contracts with exceptions using semantic web rules, ontologies, and process descriptions," *Int. J. Electron. Commer,*, vol. 8, no. 4, pp. 61-97, Summer 2004.

[17] V. Grover and T. H. Davenport, "General perspectives on knowledge management: Fostering a research agenda," *J. Manage. Inf. Syst.*, vol. 18, no. 1. pp. 5-22, Summer 2001.

[18] E. Godes. and A. Tubman, "AutoWF-A secure web workflow system using autonomous objects," *Data Knowl. Eng.*, vol. 43, no. 1, pp. 1-27, Oct. 2002.

[19] E. Godes, M. S. Olivier, and R. P, van der Riet, "Modeling, specifying and implementing workflow security in cyberspace," *J. Comput, Secur.,* vol. 7, pr. 287-315,1999,

[20] N. Guirtriss, "Formal ontology, conceptual analysis and knowledge representation." *Int, J. Human-Comput. Stud.,* vol. 43, no. 516, pp. 625-640, Nov. 995.

[21] C. Hamel, "Competition for competence and inter-partner learning with international strategic alliances," *Strateg. Manage. J.,* vol. 12, pp. 83-104, Summer 1991.

[22] C. Holsapple and M. Singh, "Toward a unified view of electronic commerce, electronic business, and collaborative commerce: A knowledge management approach," *Knowl. Process Manag.,* vol, 7, no. 3, p. 159, Jul./Sep) 2000.

[23] A. W. Holt, H. R. Ramsey, and J. D. Grimes, "Coordination system technology as the basis for a programming environment," *Electr Commun.,* vol. 57, no. 4, pp. 308-314,1983.

[24] I. Horrocks, P. F. Patel-Schneider, and F. van Hannelen, From SHIQ and RDF to OWL: The making of a web ontology language," *Web Seman.: Sco., Serv. Agents World Wide Web, vol.* 1, no. 1, pp. 7-26,2003.

[25] I. Horrocks and P. F. Patel-Schneider, "Optimizing description logic subsumption," *J. Log. Comput.,* vol.-9, no. 3, pp. 267-293, Jun. 1999.

[26] S. D. Ramchurn, D. Huynh, and N. R. Jennings, "Trust in multiagent systems," *Knowl. Eng. Rev.,* vol. 19, no. 1, pp, 1-25,2004.

[27] M. H. Kang, J. S. Park, and J. N. Froscher, "Access control mechanisms for inter-organizational workflow," in *Proc. SACMAT,* Chantilly, VA, 2001, pp. 66-74.

[28] R. Kishore, R. Sharman, and R. Ramesh, "Computational ontologies and information systems: I, Foundations," *Commun, Assoc, Inf. Syn.,* vol. 14, no. 8, pp. 158-183,2004.

[29] R. Kishore, H. Zhang, and R. Ramesh, "Enterprise integration using the agent paradigm: Foundations of multi-agent-based integrative business information systems," *Decis. Support Syst.,* 2006, to be published.

[30] M. Klein, D. Fensel. F. van Harmelen, and I. Horrocks, "The relation between ontologies and XML schemas," *Electron. Tmns. Artif. Intell.,* vol. 6, no. 4, pp. 65-94,2001.

[31] -, "The relation between ontologies and XML schemas," *Linkiip. Electron. Artic. Comput. Inf Sci.,* vol. 6, no. 4,2001.

[32] A. Kumar and J. Wainer, 'Meta workflows as a control and coordination mechanism for exception handling in workflow systems," *Decis. Support Syst.,* vol. 40, no. 1, pp. 89-105,2005.

[33] A. Kumar and J. L. Zhao, "Dynamic routing and operational controls in workflow management systems," *Manage. Sci,,* vol. 45, no. 2, pp. 253- 272, Feb. 1999,

[34] A. Kumar, W. M. P. van der Aalst, and H. M. W. Verbeek, "Dynamic work distribution in workflow management systems: How to balance quality and performance?," *J. Manage. Inf Syst.,* vol. 18, no. 3, pp. 157-193, 2002.

[35] .1. Lee, S. J. Upadhyaya, H. R. Rao, and R. Sharman, "Secure knowledge management and the semantic web," *Commun. ACM,* vol. 48, no. 12, pp. 48-54, Dec. 2005.

[36] L. Li and I. Horrocks, "A software framework for matchmaking based on semantic web technology," *Int. J. Electron. Commen,* vol. 8, no. 4, pp. 39-60,2004.

[37] T. Malone and K. Crowston, "The interdisciplinary study of coordination," *ACM Comput. Surv,,* vol. 26, no, 1, pp. 87-119, Man 1994.

[38] T. W. Malone, K. Crowston, G. A. Herman, Eds,, *Organizing Business Knowledge: The MIT Process Handbook,* MIT Press, Cambridge, MA, 2003.

[39] T. W. Malone, K. Crowston, J. Lee, B. Pentland, C. Dellarocas, G. Wyner, J. Quimby, C. S. Osborn, A. Bernstein, G. Herman, M. Klein, and E. O'Donnell, "Tools for inventing organizations: Toward a handbook of organizational processes," *Manage. Sci.,* vol. 45, no. 3, pp. 425-444. Mar. 1999.

[40] S. Mcllraith, T. C. Son, and H. Zeng, "Semantic web services," *IEEE Inrell. Syst..* vol. 16, no. 2, pp. 46-53, Mar./Apr. 2001.

[41] T. Mukhopadhyay and S. Kekre, "Strategic and operational benefits of electronic integration in B2B procurement processes," *Manage. Sci.,* vol. 48, no. 10, pp. 1301-1313, Oct. 2002.

[42] K. Neville and P. Powell, "The interrelationship between security and knowledge management," in *Proc. SKM,* Buffalo, NY, 2004, pp. 155-160.

[43] A. Newell, "The knowledge level,"Artif *Intel., vol.* 18, no. 1, pp. 87-127, Jan. 1982.

[44] S. Oh and S. Park, "Task-role-based access control model," *Inf. SM.*, vol. 28, no. 6, pp. 533-562, Sep. 2003.
[45] D. O'Leary, "Knowledge management systems: Converting and connecting," *IEEE Intel!. Syst. Their Appl., 'vol, 13,* no. 3, pp. 30-33, May 1998.
[46] M. A. Ould, *Business Processi;s-Modeling and Analysis for Re-Engineering and Improvement.* Chichester, U.K.: Wiley, 1995.
[47] J. S. Park, R. Sandhu, and G. Alin, "Role-based access control on the web," *ACM Trans. Inf Syst. Secur,* vol. 4, no, 1, pp. 37-71, Feb. 2001.
[48] M. E. Porter and V. E. Millar, "How information gives you competitive advantage." *Harvard* BUS. *Rev.,* vol. 63, no. 4, pp. 149-160, Jul./Aug, 1985,
[49] T. S. Raghu, B. Jay araman, and H. R. Rao, "Towards an integration of agent and activity-centric approaches in organization process modeling: Incorporating incentive mechanisms," *Inf. Syst. Res.,* vol. 15, no. 4, pp. 316-335, Dec. 2004,
[50] 1. Ray, P. Ammann, and S. Jadojia, "Using semantic correctness in multidatabases to achieve local autonomy, distribute coordination. ahtl maintain global integrity," Inf, *Sci.,* vol. 129, no. 1-4, pp. 155-195, Nov. 2000.
[51] A. Ricci. A. Omicini, and E. Denti, "Virtual enterprises and workflow management as agent coordination issues," Int. *J. Coop. Inf. Syst., vol.* 11, no. 3/4, pp. 355-379, Sep./Dec. 2002.
[52] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Yournan, "Role-based access control models," *Computer,* vol. 29, no. 2. pp. 38-47, Feb. 1996.
[53] M. Sawhney and D. Parikh, "Where value lies in a networked world," *flaniard Bus. Rev.,* vol. 79, no. 1, pp. 79-86, Jan. 2001.
[54] R. Sikora and M. J. Shaw, "A multi-agent framework for the coordination and integration of information systems," *Manage. Sci., vol. 44,* pt. 2 of 2, no. 11, pp. S65-S78, Nov. 1998.
[55] R. Singh, A. F. Salam,, and L. Iyer, "Intelligent infomediary-based eMarketplaces: Agents in e-supply chains," *Commun. ACM,* vol. 48, no. 6, pp. 108-115, Jun. 2005,
[56] R. Singh, L. S. Iyer, and A. F, Salam, "Semantic eBusiness," *Ira. J. Sernaril. Web Inf. Syst., vol.* 1, no. 1, pp. 19-35, Jam-Mar. 2005.
[57] H. Sped, P. van der Vet, and N, J. Mars, "Runtime and memory usage performance of description logics," in *Proc. KRUSE, 1995,* pp. 13-27.
[58] S. Staab, R. Studer, H. P. Schnurr, and Y. Sure, "Knowledge processes and ontologies," *IEEE Intel!. Syst.,* vol. 16, no. 1, pp. 26-34. Feb. 2001.
[59] G. Stermsek, M. Strembeck, and G. Neumann', "Using subject- and object-specific attributes for access control in web-based knowledge management systems," in *Proc. SKM,* Buffalo NY, 2004, pp. 15-20.
[60] S. Tallman, M. Jenkins, N. Henry, and S. Pinch, "Knowledge, clusters and competitive advantage," *Acad, Manage. Rev,,* vol. 29, no. 2, pp. 258-271, 2004.
[61] J. Tillquist, J. L. King, and C. Woo, "A representational scheme for analyzing information technology and organizational dependency," *Manage. Inf Syst. Q.,* vol. 26, no. 2, pp. 91-118, Jun. 2002.
[62] W. M. P. van der Aalst, "Exterminating the dynamic change bug: A concrete approach to support workflow change," *Inf. Syst. Front.,* vol. 3, no. 3, pp. 297-313,2001.
[63] W, M. P. van der Aalst and A. Kumar, "XML based schema definition for support of inter-organizational workflow," Inf *Syst. Res.,* vol. 14, no. 1, pp. 23-46,2003.
[64] J. Wainer, P. Barthelmess, and A. Kumar, "W-RBAC a workflow security model incorporating controlled overriding of constraints," *Int. J. Coop. Inf. Syst.,* vol. 12, no. 4, pp. 455-485, Dec. 2003.
[65] Y. Wand and R. Weber, "An ontological model of an information system," *IEEE Trans, Softw. Eng.,* vol. 16, no. 11, pp. 1282-1292, Nov. 1990.
[66] WfMC. (1996). *Workflow Management Coalition* [Online]. Available: www.wfnnc.org