Chapter XIII

Trustworthy Data Sharing in Collaborative Pervasive Computing Environments

Stephen S. Yau, Arizona State University, USA

Abstract

Collaborative Pervasive Computing Applications (COPCAs) can greatly improve the investigative capabilities and productivity of scientists and engineers. Users of COPCAs usually form groups to collaboratively perform their tasks using various computing devices, including desktop computers, pocket PCs, and/or smart phones, over Mobile Ad hoc Networks (MANET), LAN, and the Internet. These users usually share various types of data, including research ideas (documents), experimental and statistical data (numerical data, graphics, stream audio/video). A very important issue for sharing data in Collaborative Pervasive Computing Environments (COPCEs) is trustworthiness. To support trustworthy data sharing among groups of users of COPCAs, secure group communication, trustworthy

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

shared data discovery, flexible access control mechanisms, effective data replication, data quality assurance mechanisms, *and* intrusion detection mechanisms *are needed. In this chapter, the challenges, current state-of-the-art, and future research directions for trustworthy data sharing in COPCEs are presented. In particular, discussions will be focused on research issues and future research directions for* trustworthy shared data discovery *and* flexible access control *in service-based COPCAs.*

Introduction

Collaborative Pervasive Computing Applications (COPCAs), such as collaborative research and development environments, can greatly improve the investigative capabilities and productivity of scientists and engineers in many fields. Users of COPCAs usually form groups (or teams) to collaboratively perform their tasks. The collaborations are supported by the users' computing devices, such as desktop computers, pocket PCs, and/or smart phones, over various networks like Mobile Ad hoc Network (MANET), LAN, and the Internet. Users of COPCAs usually need to share various types of data, including research ideas (documents), experimental and statistical data (numerical data, graphics, stream audio/video). Data sharing among various groups of computing devices is one of the most important requirements for COPCAs because data sharing is required for efficient and effective group collaboration. For example, the status of each group member often needs to be shared for group collaboration, and all group members often need to share the same view of certain data when they collaborate on certain tasks.

During the past several years, research on mobile and pervasive data management has generated many useful results for managing and sharing data in pervasive computing environments. A significant trend in designing large-scale information systems in heterogeneous pervasive computing environments, consisting of multiple organizations, is utilizing Web services and emerging Semantic Web technology to improve interoperability and greatly enhance automated data composition/integration. However, most research focuses on how to improve the efficiency of discovering, accessing, distributing, and/or updating shared data. A critical issue, trustworthiness of data sharing in COPCEs, has not attracted much attention among researchers.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Data sharing in COPCEs has the following trustworthiness requirements: (a) flexible and adaptive access control to shared data, (b) secure and reliable shared data discovery, (c) secure and private data retrieval/delivery, (d) authentication of group member devices, (e) scalable and lightweight group key management, (f) detection of attacks and malicious users, (g) high availability of shared data, (h) shared data quality assurance, and (i) inference prevention. Development of effective mechanisms to satisfy these requirements is challenging due to the following reasons:

1. The mechanisms must be lightweight due to the severe resource constraints of pervasive computing devices.
2. The mechanisms must be highly and dynamically scalable due to the possible large variable number of pervasive computing devices in collaboration.
3. The mechanisms must be able to transparently support the device mobility due to high mobility of pervasive computing devices.
4. The mechanisms must be capable of performing runtime adaptation based on the situation; that is, they must be situation aware due to vulnerable and unstable wireless networks, and the pervasive ephemeral computing environments. We consider a *situation* as a set of past contexts of individual devices relevant to future device actions, and a context is any instantaneous, detectable, and relevant condition of the environment, device, or user (Yau, Wang & Karim, 2002).

Substantial research has been done in the areas of secure group communication (Berket & Agarwal, 2003; Chiang & Huang, 2003; Lazos & Poovendran, 2003; Yau & Zhang, 2004), effective data replication (Guy et al., 1998; Ratner, Popek & Reiher, 1999), and intrusion detection mechanisms (Kyasanur & Vaidya, 2002; Zhang, Lee & Huang, 2003). Results from these research efforts can be applied to address the requirements (c) through (g) in COPCEs. Novel techniques for data quality assurance [Requirement (h)] and inference prevention [Requirement (i)] in trustworthy data sharing in COPCAs need to be developed to further improve the trustworthiness of shared data. Due to limited space, the research on these aspects will not be covered in this chapter.

In this chapter, we will focus on the current state-of-the-art research issues and future research directions for addressing requirements (a) and (b). In particular, our discussion will emphasize the Web service-based information systems

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

mentioned earlier due to increasing popularity and deployment of service-based systems.

Current State-of-the-Art

As mentioned in the last section, our discussion will emphasize Web service-based information systems in pervasive computing environments. In these Web service-based information systems, shared data is published in the form of Web services and can be accessed by users through well-defined service interfaces. Hence, the trustworthiness of shared data in these information systems relies on the trustworthiness of services for data sharing. In this section, we will briefly review the state-of-the-art in the following three aspects related to the trustworthiness of services for data sharing: service specification languages, service discovery/matchmaking, and access control. Although much research has been done on service specification languages (Andrews et al., 2003; Atkinson et al., 2002; Della-Libera et al., 2002; OASIS 2003b, 2004; W3C, 2001, 2004b), service discovery (Balazinska, Balakrishnan, & Karger, 2002; Chen & Kotz, 2003; Czerwinski et al., 1999; Paolucci et al., 2002, 2003; Stoica et al., 2001; Trastour, Bartolini & Gonzalez-Castillo, 2001), and access control (Bell & LaPadula, 1976; Johnston, Mudumbai & Thompson, 1998; Pearlman et al., 2002; Sandhu & Samarati, 1994; Sandhu et al., 1996; Zhang & Parashar, 2003), the results either cannot be applied to COPCEs due to the reasons (1) through (4) discussed in the last section, or do not incorporate trustworthiness.

Service Specification Languages

To facilitate generation, publishing, discovery, and usage of services for data sharing, a service specification language is needed to specify the semantic description of the data to be shared, the access interfaces to be provided, and the access control policies for the shared data.

Currently, several service specification languages are widely used such as Web Service Description Language (WSDL) (W3C, 2001) and Business Process Execution Language for Web Services (BPEL4WS) (Andrews et al., 2003), or have become more popular such as OWL-S (formerly DAML-S) (W3C,

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

2004b). However, WSDL and BPEL4WS specify the interfaces of services and cannot specify the semantics of the shared data. Furthermore, for specifying security policies, WSDL and BPEL4WS rely on WS-Security (Atkinson et al., 2002) and WS-SecurityPolicy (Della-Libera et al., 2002) to satisfy the basic requirements of message integrity, confidentiality, and single-message authentication for Web services. But, it is very difficult to specify declarative access control policies using WS-Security and WS-SecurityPolicy. Other notable languages for specifying security policies include SAML (OASIS, 2004) and XACML (OASIS, 2003b). SAML is an XML-based security language for exchanging authentication and authorization information, but it puts too much burden on services to gather the evidence needed for policy decision. XACML provides schema and namespaces for access control policies, but its semantics are implicit and cause ambiguity when interpretations differ. Although OWL-S can be used to specify the semantic description of the data to be shared, it does not have the notations and structures to specify the access control policies for the shared data. Therefore, these service specification languages can hardly be used to specify services for trustworthy data sharing.

Service Discovery/Matchmaking

Before a published data service can be used by users, it must first be found by users. The process of finding a published data service based on users' requests is known as *service discovery* or *matchmaking*. To facilitate effective data sharing in COPCEs and ensure trustworthiness of information systems, the service discovery in COPCEs must satisfy at least the following requirements:

1. **Intelligent:** The data service discovery must be intelligent; that is, the service discovery should be based on the service semantics rather than the service interface.
2. **Secure:** Access control must be enforced when the service discovery is performed to prevent services from being discovered by untrustworthy or malicious users.
3. **Lightweight:** The shared data service discovery must be lightweight to maximize the battery lifetime of mobile devices.
4. **Robust:** The service discovery must be fault-tolerant to avoid single point of failure.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

So far, no service discovery techniques can satisfy all these requirements simultaneously. For Requirement (i), there are service discovery techniques (Paolucci et al., 2002, 2003; Trastour et al., 2001) to provide the capability of matching services' semantics. For example, the technique presented in Paolucci et al. (2003) makes use of DAML-S for semantic matching and performs discovery based on Gnutella P2P protocol (Gnutella). However, these techniques do not address Requirements (2) and (4). For Requirement (2), although some existing service discovery techniques such as secure Service Discovery Service (SDS) (Czerwinski et al., 1999) allow control over who can discover and access the services, they make the assumption that service providers can provide a list of the principles that are allowed to access the services, and the access control is based on such a list. This kind of access control is static and not suitable for COPCEs, in which users may be added or removed from the systems dynamically. For Requirements (3) and (4), existing service discovery techniques for Web services, such as Universal Description Discovery & Integration (UDDI) (OASIS, 2003a), DAML-S Matchmaker (Paolucci et al., 2002), and a matchmaking service developed by HP (Trastour et al., 2001), are based on centralized service registries. However, the centralized service registry will be the performance bottleneck when a large amount of service queries need to be processed and cause single point of failure. Hence, these approaches are not suitable for dynamic environments like COPCEs. Other service discovery techniques (Balazinska et al., 2002; Czerwinski et al., 1999; Paolucci et al., 2003; Stoica et al., 2001) developed for P2P computing and ubiquitous computing do not use centralized service registries; hence, they are more dynamic and fault tolerant. However, these techniques have large overhead in service discovery and cannot guarantee the successful discovery of requested services. Yau and Karim (2003, 2004a, b) introduced energy-efficient protocols for situation-aware object discovery in ubiquitous computing environments. Although the approaches by Yau and Karim are not intended for service-based COPCAs, they can be extended to service-based COPCAs.

Access Control

To ensure the proper usage of published data services, access control mechanisms are needed. Access control mechanisms are based on three types of models: Mandatory Access Control (MAC) models (Bell & LaPadula, 1976), Discretionary Access Control models (Sandhu & Samarati, 1994), and Role-Based Access Control (RBAC) models (Sandhu et al., 1996). These

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

models cannot be applied to COPCAs directly because of the following reasons:

- MAC models are based on an assumption that access decisions cannot be decided by the object owner (NIST, 1994). The MAC-based system enforces the access policy over the wishes or intentions of the object owner. But, in COPCAs, the owner of shared data may require making access decisions on the provided data. As security labels of object and subject are relatively static in MAC models, it is difficult to use MAC models to enforce flexible dynamic security policies.
- DAC models need to maintain an Access Control List (ACL) or capability. Due to the large amount of services and clients in a COPCA, it will be very difficult to maintain ACL or capability lists in DAC models. Revoking the granted access rights will also be very difficult.
- RBAC models assume that the User-Role and Role-Permission assignments are relatively static, which may not be the case in the COPCA environments.

To enforce flexible security policies and make access control more usable, Thuraisingham and Ford (1995) introduced a flexible security constraint handling process in distributed database management systems by assigning security levels to the data based on content, context, and time. In COPCEs, data to be shared is often unstructured or semi-structured. Thus, generating flexible access control policies for sharing data based on situations in COPCEs needs further improvement.

Research Issues and Future Research Directions

Based on the discussions on the current state-of-the-art, we will identify the research issues and future research directions in the three aspects (service specification languages, service discovery, and access control) in this section.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Data Service Specification for Trustworthy Data Sharing in Service-Based COPCAs

Data service specification is very important for the operations of service-based COPCAs since all service discovery mechanisms require the knowledge of certain types of service descriptions. In order to achieve trustworthy data sharing in service-based COPCAs, trustworthiness constraints for data services must be included in service specifications. Such service specifications should include at least the following three items:

(a) The description of the data to be shared such as the name of the data source, semantics, type, owner, and location of the data.

(b) The access interfaces to be provided such as query, update, and subscription.

(c) The trustworthiness constraints for data services such as access control policies (to be discussed later), availability, survivability, and auditability of data services. In COPCEs, these constraints usually vary due to context/situation changes. Hence, the service specifications must also include situation-awareness specifications.

Existing Web service specification languages cannot specify these three items together. Therefore, new specification languages for services for trustworthy data sharing need to be developed. The same languages should also be usable by users to specify their service requests.

A fundamental issue in developing such specification languages is how to model these services for trustworthy data sharing in COPCAs. The current service model of W3C (W3C, 2004a) is not suitable for trustworthy data sharing in COPCAs because it does not include mobility and situation-awareness and has no formal representation for service semantics. A notable ongoing work in SDK WSMO (Web Service Modeling Ontology) working group focuses on the development of an ontology for describing various aspects of semantic Web services, including non-functional properties, capability, interfaces, and ontology mediators to be used by Web services (Fensel & Bussler, 2002; WSMO, 2004). WSMO allows formal definition of real-world semantics based on logical frameworks such as F-Logic (Kifer, Lausen & Wu, 1995) and has identified a set of non-functional properties, including security, reliability, and

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

robustness for semantic Web services. Machine-understandable specification languages can be developed based on WSMO. These languages will enable the automation of service discovery and service composition. However, current WSMO lacks detailed definitions for the non-functional properties and does not consider mobility and situation-awareness either.

Therefore, to develop specification languages for services for trustworthy data sharing in COPCAs, we need to do the following: (1) incorporate mobility and situation-awareness into existing service models, (2) identify a set of trustworthiness constraints for data services and incorporate the models for these trustworthiness constraints into existing service models, and (3) develop machine-understandable languages based on the new service models.

Data Service Discovery for Trustworthy Data Sharing in Service-Based COPCAs

We have previously identified four requirements of service discovery for trustworthy data sharing in COPCAs: (1) intelligent, (2) secure, (3) lightweight, and (4) robust. As mentioned before, no existing service discovery techniques can satisfy all four requirements. The following research issues need to be addressed in order to develop service discovery mechanisms that can satisfy these requirements:

1. **Efficient distributed trust management for secure service discovery.** In COPCAs, users in the same group may be in geographically dispersed locations and need to communicate among themselves through public communication networks. Hence, the service query and response must both be secured to avoid being intercepted and manipulated by malicious agents. Furthermore, access control needs to be considered in service discovery to prevent the system from revealing confidential data services to users without proper privileges. In addition, services need to be authenticated to ensure the trustworthiness of shared data.

   As mentioned before, existing service discovery techniques require centralized certificate management and access control. However, in COPCAs, users may come from various organizations, each of which may have different security policies and require different certificates. Furthermore, centralized certificate management and access control are vulner-

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

able to denial-of-service attacks. Therefore, new techniques for distributed trust management need to be developed and used in data service discovery. It should be noted that introducing security mechanisms into data service discovery will result in larger overhead in service discovery, which is a critical issue to be considered for mobile/embedded devices running on battery power.

2. **Reliability and robustness of service discovery.** As discussed before, service discovery techniques not using centralized registries or indexes are more suitable for COPCAs because they are more dynamic and more robust (avoid single point of failure). This type of service discovery techniques is normally based on multi-casting service queries or creating a direct mapping of services with hosts (e.g., DHT-based service discovery). The latter has better performance but is not suitable for COPCAs since it requires a uniform service-to-host mapping mechanism across the entire system and needs to have the capability to deploy services to different hosts according to the mapping, which is unrealistic in COPCAs involving multiple organizations. The service discovery techniques based on multi-casting service queries can be used in such an environment, but they are not reliable in the sense that they cannot guarantee the discovery of a requested service even if the service exists. However, for COPCAs, we believe that reliable service discovery techniques can be developed based on reliable group communication mechanisms. But, there will be a tradeoff between reliability and performance since reliable group communication will result in more overhead.

3. **Intelligence vs. efficiency.** As mentioned before, several approaches exist to provide the capability of matching services' semantics to enable intelligent service discovery. The size of service queries in these approaches is bigger than other non-semantic service discoveries since additional semantic information needs to be carried in service requests. However, in COPCEs, devices often communicate over wireless networks and rely on battery power. To what extent the bigger size of service queries will affect the resource consumption (network bandwidth, battery power) is not clear and needs to be investigated. If the size of service request has a big impact on the resource consumption, new data structures and compression algorithms need to be developed to effectively reduce the size of service requests.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Flexible and Adaptive Access Control to Data Services

There is an inherent tradeoff between security and performance. We should not make the system unusable or unmanageable in order to achieve security (Thuraisingham & Ford, 1995). One major research issue here is how to enforce flexible and adaptable access control policies for ensuring security with acceptable performance. The access control mechanism for COPCAs should address the dynamicity of the user activities and the environments of COPCAs. For example, Alice and Bob are two researchers working together on a nuclear research project. When Alice and Bob are in a secure room passed by security inspection, Alice should be allowed to access Bob's shared data services. When Alice is traveling outside, she should not be allowed to access Bob's shared data services.

Context-based access control systems have been studied extensively to provide adaptable access control for distributed and dynamic systems, especially pervasive computing systems. There are two ways to consider context in access control. One is to consider context values as constraints on access right granting. For example, Kumar, Karnik, and Chafle (2002) presented an extended role-based access control (RBAC) model, which includes context filters during the definition of a role to make RBAC sensitive to the context of an attempted operation. Extensive research on temporal constraints has been done on role-based access control (Bertino, Bonatti & Ferrari, 2001; Joshi, 2003). The other way is to consider context values as principals in access control (Corradi, Montanari & Tibaldi, 2004). Access rights are assigned to context values, and if the user/system has certain context value, then the user will have the access rights assigned to those context values. However, the dynamicity of user activity and the multiple domain policy interactions (Bell, 1994) have not been addressed. Therefore, to provide flexible and adaptive access control for COPCAs, we need to address the following research problems:

1. Develop a security policy ontology based OWL-S and integrate the dynamicity of user activity with the dynamicity of computing environments to incorporate situation-aware constraints in existing access control models. It will allow users to specify and enforce more flexible and adaptable access policies for COPCAs.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

2. Develop a situation-aware access policy language based on the OWL-S based security policy ontology to specify access policies for data sharing. Such an OWL-S based language will enhance semantic interoperability of access policies across organizational boundaries.
3. Provide mechanisms for delegation, and policy confliction detection and resolution for sharing data in collaborative device groups.

Summary

In this chapter, a brief overview of data sharing and its trustworthiness requirements in COPCAs has been presented. Due to limited space, our discussions have focused on the two important aspects requiring most investigations: *data service specification and discovery for trustworthy data sharing,* and *flexible and adaptive access control to data services in service-based COPCAs*. The current state-of-the-art research issues and future research directions for *these two aspects* have been presented. The long-term goal of this research should be to develop techniques to enable dynamic, efficient, secure, and reliable data sharing among groups of users in pervasive computing environments to facilitate effective ad hoc group collaboration.

Acknowledgment

This work is supported in part by the National Science Foundation under the grant number IIS-0430565. The author would like to thank Dazhi Huang and Yisheng Yao of Arizona State University for many valuable discussions of the results presented in this chapter.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

References

Andrews, T., et al. (2003, May). Business process execution language for Web services version 1.1. Retrieved May 7, 2005, from *http://www-106.ibm.com/developerworks/webservices/library/ws-bpel/*

Atkinson, B., et al. (2002, April). Web services security v1.0. Retrieved May 7, 2005, from *http://www-106.ibm.com/developerworks/webservices/library/ws-secure/*

Balazinska, M., Balakrishnan, H., & Karger, D. (2002). INS/Twine: A scalable peer-to-peer architecture for intentional resource discovery. *Proceedings of the 1st International Conference on Pervasive Computing,* August (pp. 195-210).

Bell, D.E. (1994). Modeling the "Multipolicy Machine". *Proceedings of the New Security Paradigms Workshop,* August 3-5, Little Compton, RI.

Bell, D.E., & LaPadula, L.J. (1976, May). *Secure computer system: Unified exposition and multics interpretation* (Tech. Rep. No. ESD-TR-75-306). Mitre Corporation.

Berket, K., & Agarwal, D. (2003). Enabling secure ad-hoc collaboration. *Proceedings of the Workshop on Advanced Collaborative Environments*, June. Retrieved May 7, 2005, from *http://www-itg.lbl.gov/Collaboratories/Publications/Karlo-WACE-2003-final.pdf*

Bertino, E., Bonatti, P.A., & Ferrari, E. (2001). TRBAC: A temporal role-based access control model. *ACM Transactions on Information Systems Security, 4*(3), 191-233.

Chen, G., & Kotz, D. (2003). Context-sensitive resource discovery. *Proceedings of the 1st International Conference on Pervasive Computing and Communications (PerCom'03),* March (pp. 243-252).

Chiang, T.C., & Huang, Y.M. (2003). Group keys and the multicast security in ad hoc networks. *Proceedings of the International Conference on Parallel Processing Workshop*, October (pp. 385-390).

Corradi, A., Montanari, R., & Tibaldi, D. (2004). Context-based access control for ubiquitous service provisioning. *Proceedings of the 28th Annual International Computer Software and Application Conference* (pp. 444-451).

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Czerwinski, S., et al. (1999). An architecture for a secure service discovery service. *Proceedings of the 5th Annual International Conference on Mobile Computing and Networks (MobiCom'99)* (pp. 24-35).

Della-Libera, G., et al. (2002, December). Web service security policy. Retrieved May 7, 2005, from *http://www-106.ibm.com/developerworks/library/ws-secpol/*

Fensel, D., & Bussler, C. (2002). The Web service modeling framework WSMF. *Electronic Commerce Research and Applications, 1*(2).

Gnutella. The Gnutella protocol specification v0.4. Retrieved May 7, 2005, from *http://www9.limewire.com/developer/gnutella_protocol_0.4.pdf*

Guy, R., Reiher, P., Ratner, D., Gunter, M., Ma, W., & Popek, G. (1998). Rumor: Mobile data access through optimistic peer-to-peer replication. *Proceedings of the Workshop on Mobile Data Access,* 254-265.

Johnston, W., Mudumbai, S., & Thompson, M. (1998). Authorization and attribute certificates for widely distributed access control. *Proceedings of the IEEE 7th International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises* (pp. 340-345).

Joshi, J. (2003). *A generalized temporal role based access control model for developing secure systems*. Unpublished Ph D dissertation, Purdue University, West Lafayette, Indiana.

Kifer, M., Lausen, G., & Wu, J. (1995). Logical foundations of object oriented and frame-based languages. *Journal of the ACM, 42*(4), 741-843.

Kumar, A., Karnik, N., & Chafle, G. (2002). Context sensitivity in role-based access control. *ACM SIGOPS Operating Systems Review, 36*(3), 53-66.

Kyasanur, P., & Vaidya, N.H. (2002, August). *Detection and handling of MAC layer misbehavior in wireless networks* (Tech. Rep.). University of Illinois at Urbana-Champaign, Coordinated Science Laboratory. Retrieved May 7, 2005, from *http://citeseer.nj.nec.com/kyasanur02detection.html*

Lazos, L., & Poovendran, R. (2003). Energy-aware secure multicast communication in ad-hoc networks using geographic location information. *Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing,* April (pp. 201-204).

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

NIST. (1994). Security in open systems. *NIST Special Publication SP800-7*. Retrieved May 7, 2005, from *http://csrc.nist.gov/publications/nistpubs/800-7/*

OASIS. (2003a). UDDI version 3.0.1. Retrieved May 7, 2005, from *http://uddi.org/pubs/uddi_v3.htm*

OASIS. (2003b). eXtensible Access Control Markup Language (XACML) version 1.0. Retrieved May 7, 2005, from *http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml*

OASIS. (2004, August). OASIS security assertion markup language (SAML) v2.0. Retrieved May 7, 2005, from *http://www.oasis-open.org/committees/download.php/8778/sstc-saml-conformance-2.0-cd-01.pdf*

Paolucci, M., Kawamura, T., Payne, T.R., & Sycara, K. (2002). Semantic matching of Web services capabilities. *Proceedings of the 1st International Semantic Web Conference (ISWC'02),* June (pp. 333-347).

Paolucci, M., Sycara, K., Nishimura, T., & Srinivasan, N. (2003). Using DAML-S for P2P discovery. *Proceedings of the International Conference on Web Services (ICWS'03)* June (pp. 203-207).

Pearlman, L., Welsh, V., Foster, I., Kesselman, C., & Tuecke, S. (2002). A community authorization service for group collaboration. *Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks* (pp. 50-59).

Ratner, D., Popek, G.J., & Reiher, P. (1999). Roam: A scalable replication system for mobile computing. *Mobility in Databases and Distributed Systems,* 96-104.

Sandhu, R., Coyne, E.J., Feinstein, H.L., & Youman, C.E. (1996). Role based access control models. *IEEE Computer, 29*(2), 38-47.

Sandhu, R., & Samarati, P. (1994). Access control: Principles and practice. *IEEE Communications Magazine, 32*(9), 40-48.

Stoica, I., Morris, R., Karger, D., Kaashoek, F., & Balakrishnan, H. (2001, August). Chord: A scalable peer-to-peer lookup service for Internet applications. *Proceedings of the ACM SIGCOMM'01* (pp. 149-160).

Thuraisingham, B., & Ford, W. (1995, April). Security constraints processing in multilevel secure distributed database management system. *IEEE Transactions on Knowledge and Data Engineering, 7*(2), 274-293.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Trastour, D., Bartolini, C., & Gonzalez-Castillo, J. (2001). A Semantic Web approach to service description for matchmaking of services. *Proceedings of the 1st International Semantic Web Working Symposium*, July. Retrieved May 7, 2005, from *http://citeseer.nj.nec.com/trastour01semantic.html*

W3C. (2001). Web service description language (WSDL) 1.1. Retrieved May 7, 2005, from *http://www.w3.org/TR/wsdl*

W3C. (2004a). Web services architecture. Retrieved May 7, 2005, from *http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/*

W3C. (2004b). OWL Web Ontology Language: Overview. Retrieved May 7, 2005, from *http://www.w3.org/TR/owl-features*

WSMO. (2004, March). Web service modeling ontology (WSMO) standard. Retrieved May 7, 2005, from *http://www.wsmo.org/2004/d2/v0.2/20040306/*

Yau, S.S., & Karim, F. (2003, November). An energy-efficient object discovery protocol for context-sensitive middleware for ubiquitous computing. *IEEE Transactions on Parallel and Distributed Systems, 14*(11), 1074-1084.

Yau, S.S., & Karim, F. (2004a, February). A context-sensitive middleware-based approach to dynamically integrating mobile devices into computational infrastructures. *Journal of Parallel and Distributed Computing, 64*(2), 301-317.

Yau, S.S., & Karim, F. (2004b). An adaptive middleware for context-sensitive communications for real-time applications in ubiquitous computing environments. *Real-Time Systems, 26*(1), 29-61.

Yau, S.S., Wang, Y., & Karim, F. (2002). Development of situation-aware application software for ubiquitous computing environments. *Proceedings of the 26th IEEE International Computer Software and Applications Conference (COMPSAC 2002)*, August (pp. 233-238).

Yau, S.S., & Zhang, X. (2004, December). A middleware service for secure group communication in mobile ad hoc networks. *The Journal of Systems and Software, 76,* 29-43.

Zhang, Y., Lee, W., & Huang, Y. (2003, September). Intrusion detection techniques for mobile wireless networks. *ACM/Kluwer Wireless Networks Journal (ACM WINET), 9*(5), 545-556.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Zhang, G., & Parashar, M. (2003). Dynamic context-aware access control for grid applications. *Proceedings of the 4th International Workshop on Grid Computing (Grid 2003),* November (pp. 101-108).

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.