Purpose Based Access Control for Privacy Protection in E-Healthcare Services

Lili Sun, Hua Wang, Jeffrey Soar
University of Southern Queensland, Toowoomba, Australia 4350
(sun, wang, jeffrey.soar)@usq.edu.au

Chunming Rong
University of Stavanger, N-4036, Norway
chunming.rong@uis.no

***Abstract*—Information privacy is a major concern in many areas and none more so than in healthcare. E-healthcare is the use of web-based systems to share and deliver information across the internet. The design of proper models for authorization and access control for e-Health system services is necessary in a large health service. Usage control has been considered as the next generation access control model with distinguishing properties of decision continuity. It has been proven to be efficient to improve security administration with flexible authorization management. Usage control enables finer-grained control over usage of digital objects than that of traditional access control policies and models. In this paper, we have enriched the research for usage access control with purpose extension that is able to be applied in the field of medical information system or e-Healthcare system. This work provides a foundation for developing appropriate security solutions for organizations' secure digital information and will contribute to higher security in the medical information systems.**

***Index Terms*—Privacy, Access control, Purpose, e-Healthcare services**

I. INTRODUCTION

Today E-healthcare informatics is increasing the demands on healthcare providers for more effective healthcare services for their consumers and providing health information to guide consumers accessing the information which they need. Patients are increasingly able to check their own health records, access healthcare information and buy prescription medicines online. The online healthcare information system provides many advantages when used for improved access, collaboration and data sharing among healthcare providers, patients, and researchers. Therefore, considering the highly personal and potentially destructive nature of medical data, it comes with significant risks to the confidentiality, integrity, and availability of such information. This coming explosion of information will be stored in massive data centres around the world and will provide access to healthcare records for patients, insurers, doctors, pharmacies, and institutions. The rapid growth in information technology and database systems has greatly increased the need for better privacy protection. Privacy is becoming a major concern for consumers and enterprises. In general, access control is used for permitting access to resources according to their identities authentication and associated privileges authorization [11]. Access control has been considered as a major issue in information security community since the beginning of the information security discipline. Developing proper models for authorization and access control for the electronic patient record (EPR) is essential to a wide range use of the EPR in large health organizations [1, 10]. However, as an access control solution must keep the confidentiality of EPR data, it is important to address access policy early on in the development of any health system [10]. The *Guidelines Under Section 95 of the Privacy Act 1988* in Australia set the current standard for the protection of privacy in the conduct of medical research involving human participants in Australia. They provide a framework in which medical research involving personal information obtained by Commonwealth agencies should be conducted, to ensure that such information is protected against unauthorised collection or disclosure http://www.nhmrc.gov.au/publications/synopses/e26syn.htm). With internet usage for research of medical information on the rise [20], the traditional view of access control model should be extended with an enterprise wide privacy policy for managing and enforcing of individual privacy preferences [10].

Usage access control is a new access control model extending traditional access control models in multiple aspects [5]. The term "usage" means usage of rights on digital objects. The main different properties of usage control with traditional access control models are continuity of access decision and mutability of subject attributes and object attributes [12]. Continuity is another decision factor in access control management. In traditional access control, authorization is assumed to be done before access is allowed (pre). However, it is quite reasonable to extend this for continuous enforcement by evaluating usage requirements throughout usages (ongoing).

In order to protect data privacy, the notion of purpose plays a major role in access control models and an

doi:10.4304/jsw.7.11.2443-2449

appropriate metadata model was developed to support such privacy based access control models [3, 4]. Purpose is the reasons to collect or to access private data in access management systems. A subject releases his data to the custody of an enterprise while consenting to the set of purposes for which the data is used [8]. Adopting purpose are the fundamental policies for private information concern with which data object is used for what purposes. For example, our clinic partners may access patients' information for research. Patients' information is used for the purpose of research. The traditional view of access control model should be extended with an enterprise wide privacy policy for managing and enforcing of individual privacy preferences [1]. In this paper we propose usage access control requirements models to include purpose in e-Healthcare systems.

The remainder of this paper is organized as follows: Section 2 provides a brief overview usage control model, and continuity properties. Purposes are also introduced in this section. Section 3 shows our proposed authorization models for usage control using purpose scheme. It includes *pre-Authorizations, ongoing-Authorizations, pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing-Conditions* six models. Section 4 presents usage access control architectures based on purpose in e-Healthcare services. Section 5 reviews the differences between the work in this paper and others related works. Finally, Section 6 concludes the paper.

II. Related Technologies

A. Usage Control

In this section we briefly review the general ideas of usage control and its authorization models. The traditional access control method normally deals only with authorization decisions on users' access to target resources. The usage control is a generalization of access control. It enriches and refines the access control discipline in its definition and cover obligations, conditions, continuity (ongoing controls) and mutability [21]. There are eight core components in the usage control model: subjects, subject attributes, objects, object attributes, rights, authorizations, obligations, and conditions (see Figure 1). The authorization, obligations and conditions are components of usage control decisions.

In the usage control model, the authorization rule permits or denies the access of a subject to an object based on subject and object attributes. Obligations are performed by subjects or by the system. Conditions are system environment restrictions. In the usage control model, subjects and objects are familiar concepts with traditional access control. Subject and object attributes can be used during the access decision process. Subject attributes are identities, group names, roles, memberships, security clearance, and so on. Objects are entities that subjects hold rights on, whereby the subjects can access or use objects. For instance, in an e-Healthcare system, doctors, nurses and physicians can be subject. A patient's medical records are objects. Rights are privileges that subjects can hold on objects. The authorizations of rights require associations with subjects and objects. A right represents the access of a subject to an object, such as read or write.

Authorizations, obligations and conditions are decision factors used to check and determine whether a subject should be allowed to access an object. Obligations and conditions are new concepts that can resolve certain shortcomings that have been in traditional access controls. In general, the authorization of most traditional access controls are assumed to be done before access is allowed. However in the usage control model it extends this for continuous enforcement. Authorizations may require updates on subject and object attributes. The process of continuity properties in usage control model consists of three phrases, before usage, ongoing usage and after usage. To enforce control decisions, we have two different types: pre-decision and ongoing-decision. For mutability, there are three kinds of updates: pre-update, ongoing-update, and post-update. Therefore, Authorizations can be either pre-authorization (preA) or ongoing-authorization (onA). Pre-authorization is performed before authorization is required to the access. But ongoing authorization may be performed during the access, such as when a patient medical record in a hospital is periodically checked while the access is in progress.

Obligations are requirements that a subject must perform before (pre) or during (ongoing) accesses. An example of a pre-obligation is the requirement that a patient must provide some contact and personal information before seeing a doctor. The requirement that a user has to keep previous medical records while he has some health test is an example of an ongoing obligation. Conditions are decision factors that depend on environmental and system-oriented requirements. Subject and object attributes can be used to select which condition requirements have to be used for a request.

Based on the involvement of three decision factors: authorizations, obligations, and conditions, we have six possible cases as a model for usage control: pre-Authorizations, ongoing-Authorizations, pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing-Conditions.

In order to use usage access control technique, one has to consider that the purpose of an individual in requesting access is not included in usage access control [10]. Individuals may want to have access to different information for different purposes. Therefore, the type of access they get should change depending on their purpose. For instance, a physician may require access to a patient's information. His/her purpose can be to give a prescription to the patient or to complete the patient's profile. In first case, the system can give read access to the physician. In the second case, the physician should also be able to add or change the patient's profile as well.

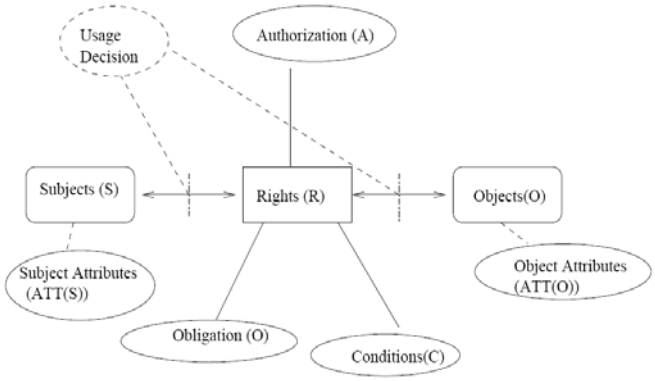

Figure1. Components of Usage Control Model

B. Purpose

A privacy policy mainly concerns with which data is used for which purposes. As the purpose directly dictates how accesses to data items should be controlled, therefore, purpose plays a central concept in many privacy protecting access control models [15]. In common business environment, purposes naturally have a hierarchical relationship among them, such as generalization and specialization relationships. Purposes can be organized according to the hierarchical relationships to simplify the management of purposes [15]. Purpose hierarchy is added to the models where purposes are defined to be mutually exclusive. Purpose hierarchies are similar to asset hierarchies, where the upper levers include general purposes and lower levers include more specific ones. For the following example in Figure 2, the *given treat* purpose is in upper lever, *write prescription* and *refer patients to do X-ray text* purposes are in lower lever. Any policy that applies to the *given treat* purpose, the same set of policies would apply to both *prescription* and *refer patients to do X-ray text* purposes.

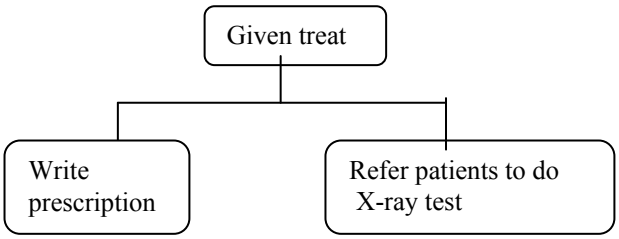

Figure2. Purpose hierarchy example

III. ACCESS PURPOSE AUTHORIZATION IN THE USAGE ACCESS CONTROL MODEL

In this section we consider authorization models for access purpose adopting usage control using E-healthcare services. For treatment purposes, patients' medical information can be accessed by doctors, nurses, physicians, or others who are involved in the patients' care or departments of the healthcare organization. For example, a doctor treating an operation for a patient may need to know if the patient has diabetes because diabetes may slow the healing process. At the same time, the dietician should know if the patient has diabetes as that appropriate meals can be arranged.

As already discussed, usage access control includes components such as subjects, objects and obligations. The purpose involved extended usage model includes the following components: Suppose there is a set of *S* for subjects, a set of *O* for objects, a set *Pu* for purposes, a set of *R* for rights, a set of *A* for authorizations, a set of *B* for obligations and a set of *C* for conditions. Subject s can do operation ops on a set of objects for any purpose. Below, we demonstrate how to apply the UAC model with purpose extension to the healthcare system.

$\forall$ s$\in$SUBJECTS, subject_users(s) $\subseteq$ $\emptyset$

s = "Doctor" $\in$ subject_users(s)

op1 = review, op2 = write, {op1, op2} $\in$ *OPS*

o1 = Patient's General Information

o2 = Patients' history and progress report

{o1, o2} $\in$ object (o)

pu1 = Adding information

pu2 = Review patient' history before giving treatment

{pu1, pu2} $\in$ PURPOSES

Based on the requirements we have six possible cases as a model for usage control: pre-Authorizations, ongoing-Authorizations, pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing-Conditions. Depending on the access requirements on the objects in the real world, it is possible to utilize more than one case. In this paper, we consider only the cases consisting of Authorizations, Obligations or Conditions alone with pre or ongoing decisions. Meanwhile we focus on developing the usage control models for the access documents with purpose. We assume that a usage request exists on a purpose target object. Decision-making can be done

either before (pre) or during (ongoing) exercise of the requested right. Decision-making after the usage has no influence on the decision of current usage

1). Usage control for pre-Authorization Model (UCMpreA)

In a pre-Authorization usage control model, the decision process is performed before access is allowed. The following illustrations of usage decision that can be expressed on the objects are made in pre-authorizations.

The UCMpreA model consists of the following components: *S, O, R, ATT(S), ATT(O)*, and usage decision Boolean functions *preA* on *O*, respectively, where *S, O, R,* represent Subject, Object and Rights required on the objects. *ATT(S), ATT(O),* represent attributes of subjects and objects respectively. *preA* is predicates about authorization functions. *Pu* is the access purposes as mentioned before.

allowed (s, o, pu, r) $\Rightarrow$ *preA(ATT(s), ATT(o), pu, r),*

In this example this predicate indicates that if subject *s* is allowed to access the objects *o* with right *r* based on purpose *pu,* then the indicated condition *preA* must be true.

The *UCMpreA* model provides an authorization method on whether a subject can access objects by the purposes. The *allowed(s, o, pu, r)* predicate shows that subject *s* can access the object *o*. At this process, the object data is assumed as private information which is restricted to access. For example, A doctor (*s*) responsible for a patient has the permission to review and change (*op1*, *op2*) the patient's General information and Patients' history, progress report (*o*). That is provided that the purpose (*pu*) of reviewing or changing the above information falls in one of these categories: Adding information, Review patient' history before giving treatment.

2). Usage control for ongoing Authorizations Model (UCMonA)

A usage control model for ongoing-Authorizations model is used to check ongoing authorizations during access processes. In this model, usage requests are allowed without any 'pre' decision making.

The *UCMonA* model has the following components: *S, O, R, ATT(S)* and *ATT(O),* as before, and ongoing usage decision functions *onA* on *O*. *onA* is used to check whether *s* can continue to access or not.

allowed (s, o, pu, r) $\Rightarrow$ *true*,

stopped (s, o, pu, r) $\Rightarrow$ $\neg$ *onA(ATT(s), ATT(o), pu, r)*,

The access of subject s to o is terminated if the ongoing authorization *onA* is failed.

In this model usage decision Boolean functions are *onA* instead of *preA*. During this process the requested access is always allowed as there is no pre-authorization all the time. *allowed (s, o, pu, r)* is required to be true, otherwise ongoing authorization should not be initiated. Ongoing authorizations are active throughout the usage of the requested right, and some requirements are repeatedly checked for a continued access. These checks are performed periodically based on time or event. In the process when attributes are changed and requirements are no longer satisfied, stopped procedures are performed. Stopped *(s, o, pu, r)* indicates that right *r* of subject *s* on object is revoked and the ongoing access terminated. For example, a limited number of simultaneous usage, suppose only a team physicians (three physicians) can access the information about the patient object *o* simultaneously. If a fourth physician requests access and passes the pre-authorization, one physician within the group access is terminated. While this is a case of ongoing authorizations, it is important that the certificate should be evaluated in a *pre* decision.

Apart from these two models there are pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing-Conditions access control models. pre-Obligations model introduces pre-obligations that have to be fulfilled before access is permitted. Ongoing-Obligations model may have to be fulfilled periodically or continuously. Conditions models define that certain restrictions have to be satisfied for usage. The pre-conditions model has to be used before requested rights can be exercised. Ongoing-Conditions model requires conditions to be satisfied while rights are in active use. In practice, the six models pre Authorizations, ongoing-Authorizations, pre-Obligations, ongoing-Obligations, pre-Conditions and ongoing-Conditions may need to be combined for an access control. We obtain an authorization method for the objects by checking users' (subjects') authorizations, obligations and conditions with continuity properties.

The following algorithm is based on these models and introduces how to manage a document access control when a user (subject) applies to access an object with purpose *pu* and right *r*. Since the authorization process can remove some parts of the input object, the output may not satisfy some particular objects, which are required by most applications. In this case, the access will be denied.

Purpose based Algorithm:

Input: Subject s needs to access right on object o with access purpose (pu),
Output: Accesses accept or deny
Method:
1)//Verify UCMpreA
2)**if** *preA(ATT(s), ATT(o), pu, r)* = false
//The process in pre-Authorization is not successful
3)ACCESS denied;
4)**endif**;
// subjects with the access purpose can access the private information
5) ACCESS accepted;
// Verify UCMonA:
6) **if** *preA(ATT(s), ATT(o), pu, r)* = false
// The process in pre-Authorization is failed, don't need further verification.
7) ACCESS denied;
8) **endif**;
// subjects with the access purpose can continue to access the private information
9) ACCESS accepted;

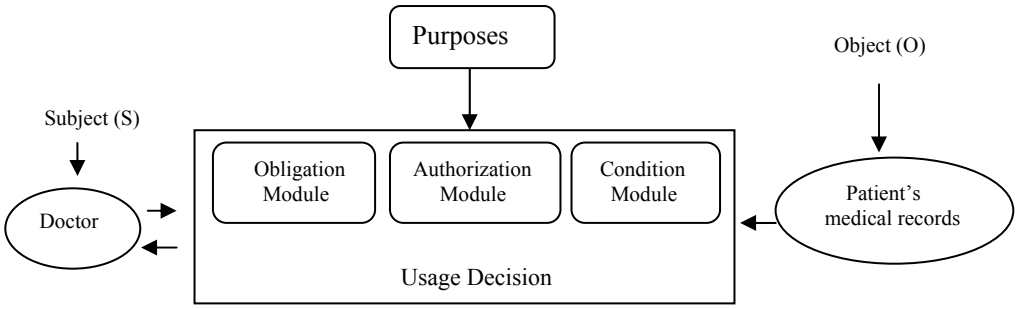

Figure3. UAC Architectures on Access Purpose Authorization

IV. UAC ARCHITECTURES ON ACCESS PURPOSE AUTHORIZATION

In this section, we discuss a structure of UAC architectures based on access purpose authorization. Following Figure 3 shows the implementation layout based on our proposed architecture presented in Section 3. An access control framework consists of Subject, Object, Usage Decision Facility (UDF) and Purposes. UDF includes authorization, condition and obligation decision modules. When a request arrives at the access control, the core UAC is enhanced with the purpose based extension. Once the decision is made either grant or denies the permission to the subject in according with the request will be returned. The condition module is used to make a decision for whether the conditional requirements are satisfied or not. The Obligation module is applied to verify whether obligations have been performed or not before or during the requested usage. The entire messages transported among the services are identified in purpose data.

In order to build a usage access control with the purpose, we must consider the system has to make decision by using access purpose (Pu). In this model, an access decision for the subjects and objects is made based on the access purpose *pu.*

Now we give an example for applying UAC with purpose to the e-Healthcare system. Suppose a medical practitioner, responsible for the patient, can only review the patient's medical record if the medical practitioner wants to give treatment to the patient. However if she/he wants to complete the patient's profile, she/he is able to review and make changes to the patient's medical record. Otherwise, if doctor only wants to discuss the patient's case with others, she/he only can review patient's profile, but cannot make any changes to it. In this example, we can see that it is not possible to define access control without including an entity for purpose.

V. RELATED WORKS

Our work is related to many areas of privacy preserving access control, especially private data management in e-Healthcare system. We also exploit the tremendous work carried out for usage access control which mainly focuses on secure management of data in e-Healthcare.

Recently, Farzad and Yu [8] introduced a role-based access control requirements model with purpose extension. Their work focuses on discussing RBAC with privacy extension and how it overcomes some of problems associated with RBAC. However, our work substantially differs from that proposal. The main differences in our approach are in the following aspects. Firstly, their protocol is based on RBAC and hence it focuses on permissions-role assignment, objects hierarchies and constrains. Our approach is based on usage control, we have analyzed the characteristics of various access authorizations and presented detailed models for different kinds of authorizations. Secondly, their approach does not mention how to update users' permissions on the objects when their conditions or obligations have changed. It is an important state for the data in the Internet since users always alter their conditions or obligations. By contrast, users in our scheme have to pass pre-Authorizations and ongoing-Authorizations as well as pre-Obligations, pre-Conditions and ongoing-Obligations and ongoing-Conditions. This indicates that our method is much more powerful in dynamic environments.

Previous work we used to focus on using usage access control methods with XML document [16]. In the authorization models, the subjects and objects for access control are elements of XML documents. We did not provide the access control models based on the purpose information, especially in e-Healthcare areas. By contrast, in this paper our work included an extended usage access control model and supports purpose hierarchy and

granularity of data by using access purposes, purpose associated e-Healthcare data system. We provided a rich variety of options that can deal with purpose data. Users can access purpose information with their keys at any time, even when their properties are updated. In our scheme, users have to satisfy pre-Authorizations, pre-Obligations and pre-Conditions as well as ongoing-Authorizations, ongoing-Obligations, ongoing-Conditions.

VI. Conclusions And Future Work

In this paper we presented a purpose-based access control suited for e-Healthcare system. Usage control models provide an approach for the next generation of access control. In usage control we analyse not only decision factors, such as authorizations, obligations and conditions, but also the continuity properties (Ongoing authorization). This paper also illustrates two different kinds of models built for purpose data. The methods presented in this paper can be used to control purpose data in a dynamic environment. It also begins a new application with usage control. This paper represents only a first step for authorization model in purpose data with usage control. Much work is still to be done before these models can be used in practice.

References

[1] Anderson, J., "Security of the distributed electronic patient record: a case-based approach to identifying policy issues", *International Journal of Medical Informatics*, vol. 60, no. 2, pages 11-118, 2000.

[2] "Australian Charter of Healthcare Rights", http://www.health.gov.au/internet/safety/publishing.nsf/Content/PriorityProgram-01

[3] Byun, J.-W., Bertino, E., Li, N., "Purpose based access control of complex data for privacy protection", *'SACMAT'05: Proceedings of tenth ACM symposium on Access control models and technologies. ACM. New York, NY, USA*, pp. 102-110, 2005.

[4] Byun, J.-W., Li, N., "Purpose-based access control for privacy protection in relational database systems", *Technical Report* 2004-52. Purdue University. 2004.

[5] Cao, J., Sun, L., Wang, H., 'Towards secure xml documents with usage control", *Lecture Notes in Computer Science*, 3399, pp. 296-307, 2005.

[6] Cheng, V. S. Y., Hung, P. C. K., 2005. Health insurance portability and accountability act (HIPAA) compliant access control model for web services, International Journal of Healthcare information systems and Informatics, Vol 1, Issue 1, pp. 22-39.

[7] Damiani, E., Paraboschi, S. and Samarati, P., "A fine-grained access control system for xml documents", *ACM Trans. Inf. Syst. Secur*., 5(2):169-202, 2002.

[8] Farzad, F., Yu, E., Hung, P. C. K., "Role-based access control requirements model with purpose extension", http://wer.inf.pucrio.br/WERpapers/artigos/artigos_WER07/Xwer07-farzad.pdf, 2007.

[9] "Guidelines Under section 95 of the Privacy Act 1988", http://www.nhmrc.gov.au/publications/synopses/e26syn.htm.

[10] Hung, P. C. K., "Towards a privacy access control model for e-Healthcare services", *In Proceedings of the third annual conference on privacy, security and trust*, October pp. 12-14, 2005.

[11] Motta, G. H. M. B., Furuie, S. S., "A contextual role-based access control authorization model for electronic patient record", *IEEE Transactions on Information Technology in Biomedicine*, vol. 7, no. 3, pages: 202- 207, 2003.

[12] Park, J., Sandhu, R., "Towards usage control models: beyond traditional access control", *In Proceedings of the seventh ACM symposium on Access control models and technologies*, *ACM Press*, page 57-64. 2002.

[13] Park, J., Sandhu, R., Schifalacqua, J., "Security architectures for controlled digital information dissemination", *In Proceedings of 16th Annual Computer Security Application Conference*, December 2003.

[14] Sandhu, R., Park, J., "Usage control: A vision for next generation access control", *In MMM-ACNS* , 17-31, Springer-Verlag Berlin Heideberg, 2003.

[15] Sun, L., Wang, H., "A Purpose Based Usage Access Control Model", *International Journal of Computer and Information Engineering*, 4:1 2010, 44-51.

[16] Sun, L., Li, Y., "Using usage control to access xml database", *International Journal of Information Systems in the Service Sector*, 32-44(1), 2008.

[17] Sun, L., Wang, H., "A purpose based access control in native XML databases", *Concurrency and Computation: Practice and Experience*, DOI: 10.1002/cpe.1717, 2011.

[18] Wang, H., Cao, J., Zhang, Y., "Access control management for ubiquitous computing", *Future Generation Computer Systems journal*, 870-878(24), 2008.

[19] Wang, H., Cao, J., Zhang, Y., "Ubiquitous computing environments and its usage access control", P*roceedings of the First International Conference on Scalable Information System,. ACM Press, Hong Kong, China,* 72-81, 2006.

[20] Williams, J., "Role-based access control models for E-healthcare systems", 2008.

[21] Zhang, X., Park, J., Parisi-Presicce, F., "A logical specification for usage control", *In SACMAT'4. ACM Press*, 2004.

Lili Sun received her PhD degree in computer science from the University of Southern Queensland (USQ), Australia in 2010. She is currently a research assistant at the University of Southern Queensland. Her research interests include databases, Web service and access control for Electronic service system. She has published about 15 articles in international journals and conferences.

Hua Wang is a professor in the University of Southern Queensland. Dr Wang awarded a PhD degree in Computer Science from the University of Southern Queensland in 2004. He has been active in the areas of Information Systems Management, Distributed Database Management Systems, Access Control, Software Engineering and Electronic Commerce. He has participated in research projects on mobile electronic system, Web service, and role-based access control for Electronic service system, and has already published over 100 research papers.

He is the co-editor-in-chief for ICST Transaction on Scalable Information Systems and was an editor of the special issue for International Journal of Security and Networks (IJSN) as well as an Editorial Board Member of The Open Cybernetics and Systemics Journal. He is also a member of the Australian Research Council Network in Enterprise Information Infrastructure.

Prof. **Jeffrey Soar** holds a Personal Chair in the School of Information Systems, Faculty of Business and Law at the University of Southern Queensland. Soar is Director of the Collaboration for Ageing & Aged-care Informatics Research (CAAIR), and founder of the Queensland Smart Home Initiative, and industry research consortium. He is also Honorary Professor at the School of IT and Electrical Engineering at The University of Queensland and Adjunct Professor in the Centre for Research on Ageing at Curtin University. His research interests include informatics for ageing and independent living, smart homes, cloud computing, strategy and policy, benefits realization, organizational change, security and privacy. Prof. Soar has extensive experience in managing research and development projects funded by both industry and funding agencies, such as the Australian Research Council.

Prof. **Chunming Rong** is head of the Center for IP-based Service Innovation (CIPSI) at the University of Stavanger (UiS) in Norway. The CIPSI has the mission to promote cross-fertilization between several research fields to facilitate design and delivery of large-scale and complex IP-based services required by many application areas. He is also visiting chair professor at Tsinghua University and served also as an adjunct professor at the University of Oslo 2005-2009. He spent one sabbatical year as visiting professor at the Stanford University 2009-2010. His research interests include cloud computing, big data analysis, security and privacy. He is co-founder and chairman of the Cloud Computing Association (CloudCom.org) and its associated conference and workshop series. He is member of the IEEE Study Group on Cloud Standard and co-chairs the IEEE Technical Area of Cloud Computing, in TCSC (Technical Committee on Scalable Computing). He is the co-Editors-in-Chief of the Journal of Cloud Computing by Springer. He received award Editor's Choice in Discrete Mathematics in 1999. He coauthored a book titled "Security in Wireless Ad Hoc and Sensor Networks" published by John Wiley and Sons in 2009. Prof. Rong has extensive experience in managing research and development projects funded by both industry and funding agencies, such as the Norwegian Research Council and the EU Framework Programs.