A Design of Onto-ACM(Ontology based Access Control Model) in Cloud Computing Environments

Chang Choi
Chosun University
Gwangju, Republic of Korea
enduranceaura@gmail.com

Junho Choi
Chosun University
Gwangju, Republic of Korea
xdman@paran.com

Byeongkyu Ko
Chosun University
Gwangju, Republic of Korea
byeongkyu.ko@gmail.com

Kunseok Oh
Gwangju Health College
Gwangju, Republic of Korea
okseok@ghc.ac.kr

Pankoo Kim*
Chosun University
Gwangju, Republic of Korea
pkkim@chosun.ac.kr

Abstract

There are a lot of security issues in cloud computing service environments such as virtualization, distributed big data processing, serviceability, traffic-handling, application security, access control, authentication, cryptography and etc. Especially, data access using various resources needs authentication and access control model for integrated management and control in cloud computing environments. Cloud computing service provides a differentiated service according to component of security policy because a permitted limit of service provider and user are different. RBAC(Role-Based Access Control) and C-RBAC(Context-Aware Role Based Access Control) do not suggest effective and practical solution using dynamic access control method by manager and user. Therefore, new dynamic access control model needs to make up for the weakness of existing problems according to cloud computing characteristic. In this paper, we propose Onto-ACM(Ontology Based Access Control Model) for dynamic access control. Onto-ACM is a semantic analysis model for permitted limit of service provider and user. This proposed model is the intelligent context-aware access model for applying the proactive security level of resources access using context information ontology modeling and reasoning engine.

Keywords: access control model, cloud computing, ontology reasoning, semantic analysis model

1 Introduction

There are a lot of security issues in cloud computing service environments such as virtualization, distributed big data processing, serviceability, traffic-handling, application security, access control, authentication, cryptography and etc. Especially, data access using various resources needs user authentication and access control model for integrated management and control in cloud computing environments[8, 15, 17].

Cloud computing service provides a differentiated service according to component of security policy[11] because a permitted limit of service provider and user are different. For example, subject of IaaS is a system and network manager. And object divides into user account, network resource, system resource and etc. Nowadays, subject and object classified by service such as IaaS, PaaS, SaaS and etc. are using

Journal of Internet Services and Information Security (JISIS), volume: 2, number: 3/4, pp. 54-64

*Corresponding author: Chosun University, No. 8111, Computer Engineering, 309, Pilmun-daero, Dong-gu, Gwangju, 501-759 Rep. of Korea, Tel: +82-62-230-7799

DAC(Discretionary Access Control), RBAC(Role-Based Access Control) and ABAC(Attribute-Based Access Control) in cloud computing environment.

Particularly, access control model is the most frequently used method for insider intrusion[3, 4, 21] detection and prevention. Generally, insider intrusion detection and prevention system is used RBAC(Role-Based Access Control) and C-RBAC(Context-Aware Role Based Access Control) models[6, 19]. However, RBAC is impossible for dynamic access control because context-aware elements do not include. C-RBAC does not ensure privacy protection and integrity because security level between objects is not considered. Also, C-RBAC doesn't defend the information spill by legal act using objects related works. Recently, Proposed delegation model do not suggest effective and practical solution of security problem such as information spill and etc. Therefore, new dynamic access control model needs to make up for the weakness of existing problems according to cloud computing characteristic[6, 7, 5, 9].

In this paper, we propose Onto-ACM(Ontology Based Access Control Model) for dynamic access control. Onto-ACM is a semantic analysis model for permitted limit of service provider and user. This proposed model is the intelligent context-aware access model for applying the proactive security level of resources access using context information ontology modeling and reasoning engine.

2 Access Control Model based on Ontology in Cloud Computing Environment

2.1 Proposed Frameworks

There are several requirements for detail and dynamic access control in the cloud computing and they are as follows:

(1) User role delegation by changing permissions can be dynamic and partial delegation.

(2) Authorized role Constraints can consider for dynamic access control.

(3) Object, condition, obligation of data access can consider for information protection of database.

(4) Data access as the need can be refused.

(5) Access control by location and equipment need.

(6) The most important factor is a misuse prevention of access right.

Onto-ACM(Ontology Based Access Control Model) offers the security mechanism of application and system based on context-aware technology in cloud computing environment. Figure 1 is the system architecture of Onto-ACM. Onto-ACM is consists of context-aware Security Manager for context-aware security service, Context Analysis Engine for selection, analysis, integration and providing of context-aware information, Access Control Module for composition and management function of security policy based on context-aware and Communication Interface for composition and management interface of security policy. Access Control Module requires security policy and context information for user authentication and access control by request for user access from context Analysis Engine in Onto-ACM. Also, Access Control Module provides security policy related access control and context information. Finally, Ontology reasoning process is performed using integration of context information in Access Control Module. Context Analysis Engine permits the system access through conform of security policy and context condition. Ontology Handler provides the location of all the resources that can be accessed based on role and context information. This method be limited the access of resources through access policy in cloud computing environment.

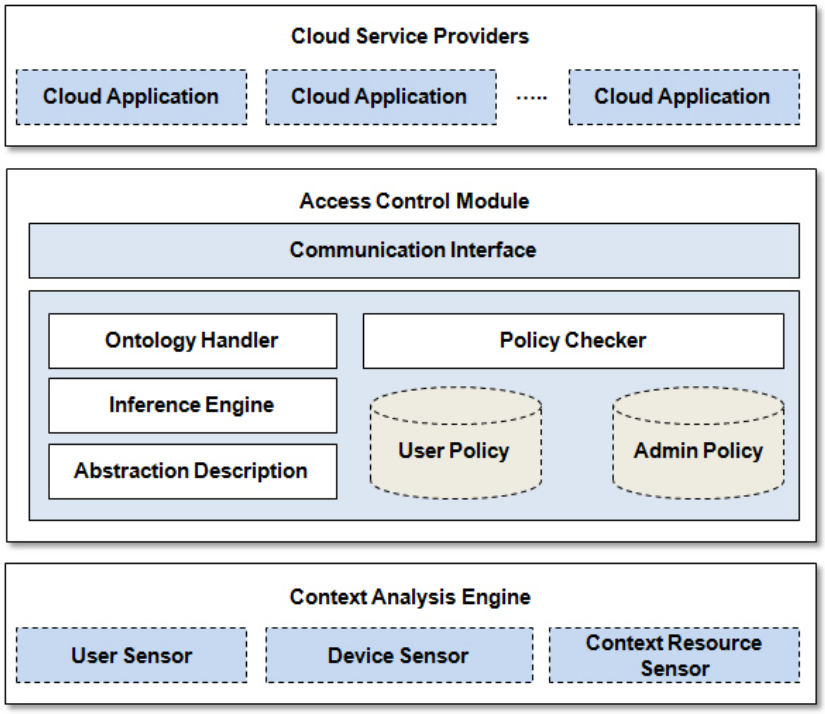

Figure 1: Onto-ACM Framework

- `Context Analysis Engine`
  – Context Analysis Engine manages gathering and management of context information for security service based on context-aware in cloud computing environment. Also, this engine sends query to Access Control Module through query creation for information gathering.

- `Access Control Module`
  – Access control Module manages security service such as user authorization, access control, context information and etc. in cloud computing environment. Onto-ACM provides security service such as user identification, authorization, access control and etc. for using application through Context Analysis Engine. Also, this module performs security service for authorization and access control based on providing context information from Context Analysis Engine.

- `Inference Engine`
  – Access Control Inference Engine performs access control function for proposed context-aware access control system. Inference Engine is consists of authorization service, permission service, context information ontology and etc. Each module performs management of security policy and right access control by access request of information resources through inference based on active user role and context role.

- `Ontology Handler`
  – Ontology Handler manages context information ontology through data processing for context information repository and authorization service from user access. Context information ontology includes the transaction list for access demand and the rule of approval information for permission of each transaction. Also, context information ontology uses OWL(Ontology Web Language) for context information gathering and analysis. Inference Engine performs reasoning of access control policy.

- `Policy Checker`
  – Policy Checker performs subject's identification, management and processing of context information. Also, Policy Checker provides dynamically allocated service based on user role through getting additional information and analysis of the policy approach using access location, access time and the spatial area. Finally, Policy Checker performs access control decisions through comparative analysis of the current user active role, situations that are currently active and security policy.

- `Abstraction Description`
  – Abstraction Description performs access control monitoring of user and administrator. Also, Abstraction Description works context information reasoning of access user ambient environment from sensor and equipment.

2.2 Process for context-aware security system

Figure 2 is a sequence diagram of context-aware security system. In this paper, the process of Onto-ACM is as follows:

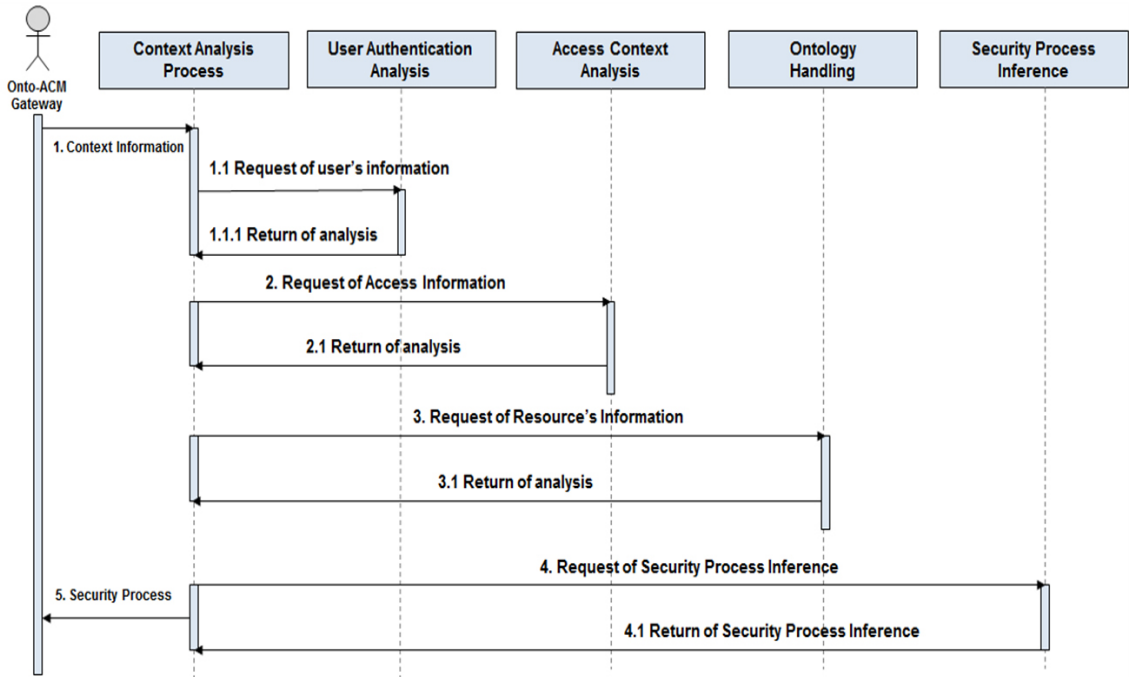

Figure 2: Sequence Diagram of Onto-ACM

- Internal user accesses the Access Control Module for certification processing of resources access. Context Analysis Engine gathers user context information for internal user authorization based on approach for cloud resources. Access Control Module analyzes gathered user context information.

- Also, Access Control Module connects context information ontology repository for user role assignment and access control.

- Access Control Module is required user role information and access policy data from context information ontology repository. Policy Checker of Access Control Module grants access right through user role and access policy for resource access.

- Internal user is required service through acquisition of access right. Access Control Module accesses suitable resources with access right level through role and right of required resources. Context information ontology is used the decision of suitable resources through inference based on user context information, security policy and access control.

3 Context-Aware Ontology based Access Control Policy

3.1 Definition of Onto-ACM Access Control Policy

Owner has to know all kinds of services and owner's information of each service in cloud computing when existing access control methods describe to make the policy by owner because access control methods can make the policy by administrator and owner. Also, administrator has to know each user's information and access status in cloud computing when existing access control methods describe to make the policy by administrator. Therefore, existing access control methods can be difficult to apply because of the large scale system and more users. The proposed Onto-ACM is divided by user policy and administrator policy in this paper. And administrator describes the policy of service and user with special role. Also, owner describes the user-defined policy with access level of information for special object.

Table 1: Onto-ACM Policy Example

[System Policy] Policy : AdminPolicy, DataOwnerPolicy Permission 1, Permission 2 : Permission Permission : Accept, Reject [Admin Policy] AdminPolicy : Permission 1 Role Action To Access [DataOwner Policy] DataOwnerPolicy : Permission 2 Access Action To Context Data

The role is a particular position and function of user or service in system in table 1. And the advantage of role is to describe the efficient policy because user or administrator does not directly describe the policy. Even if administrator policy permits special service. there can not be the access of special information by role if user does not permit special service.

3.2 Context Information Class

In this paper, Context Information class is consists of Identity Information, Physical Information, Preference Information and etc. Table 2 is the situation of context information.

Onto-ACM defines context information ontology of user and administrator using OWL based on ontology class such as, basic information, resource time, terminal and etc. The figure 3 is a representation of context information classification using ontology classes and properties of the context ontology.

Table 3 is a OWL source code of Onto-ACM context ontology.

Table 2: The Classification of Context Information

Context Information	Example of Context Information
Identity Context Information	User Right and etc.
Physical Context Information	User Location, Terminal, Security Status and etc.
Preference Context Information	System Access Time , Resource Access Time and etc.
Behavioral pattern Context Information	Number of Accesses, Main Commands and etc.
Resource Context Information	Resource Access Right and etc.

Table 3: OWL source code of Onto-ACM context ontology

```
<owl:Class rdf:ID="CloudContext">
<rdfs:hasPhysics rdf:resource="#Physics"/>
<rdfs:hasUser rdf:resource="#User"/>
<rdfs:hasEvent rdf:resource="#Event"/>
<rdfs:hasResource rdf:resource="#Resource"/>
</owl:Class>

<owl:Class rdf:ID="User">
<rdfs:subClassOf rdf:resource="#CloudContext"/>
</owl:Class>

<owl:Class rdf:ID="Admin">
<rdfs:subClassOf rdf:resource="#User"/>

<rdfs:hasHistory rdf:resource="#History"/>
<rdfs:hasDepartment rdf:resource="#Department"/>
<rdfs:hasOption rdf:resource="#Option"/>
<rdfs:hasAdmin-Resource rdf:resource="#Admin-Resource"/>
<rdfs:hasAdmin-Event rdf:resource="#Admin-Event"/>
</owl:Class>

<owl:Class rdf:ID="Admin-Resource>
<rdfs:subClassOf rdf:resource="#Admin"/>
</owl:Class>

<owl:ObjectProperty rdf:ID="System">
<rdfs:domain rdf:resource="#Admin-Resource"/>
<rdfs:range rdf:resource="#Resource"/>
</owl:ObjectProperty>

<owl:Class rdf:ID="Admin-Event">
<rdfs:subClassOf rdf:resource="#Admin"/>
</owl:Class>

<owl:ObjectProperty rdf:ID="User-Create">
<rdfs:domain rdf:resource="#Admin-Event"/>
<rdfs:range rdf:resource="#Event"/>
</owl:ObjectProperty>
```

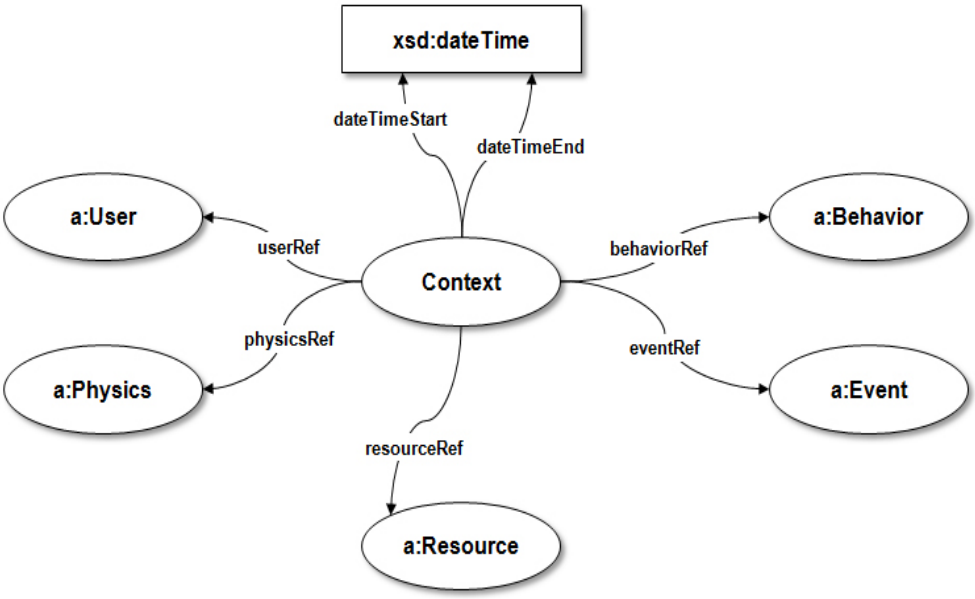

Figure 3: Classes and properties of the Context ontology

3.3 The Context Reasoning in Onto-ACM

The cloud computing user is given the authorization information through inference based on context ontology and Inference processing in Onto-ACM is performed based on Jena inference engine and query processing is performed based on SPARQL. Table 4 is the result of inference by Onto-ACM context ontology.

Table 4: Result of inference by Onto-ACM context ontology

[Result 1]
User ID: ”Admin” [User Permissions: admin. History: everyday]
Client IP: ”203.237.102.11”[Network: LAN, Location: office]
Client Info: ”PC”, ”High” [Device: PC, Battery Status: High]
Resource IP: ”117.16.23.173” [Access Level: Low]
Access Time: ”23::12:11” [Access Time: working]
[Result 2]
User ID: ”user1” [User Permissions: user, History: everyday]
Client IP: ”202.217.112.15”[Network:VPN, Location: Home]
Client Info: ”PC”, ”High” [Device: PC, Battery Status: High]
Resource IP: ”.117.16.23.177” [Access Level: High]
Access Time: ”02:24:32”[Access Time: off]

The obtaining context information is consists of User ID, Resource IP, Client IP, Client Info, Access Time and etc. And, The obtaining context information by user authorization decides handling procedures for security. Even if proposed Onto-ACM is consists of same person and same situation, handling procedures for security is decided different by access time and user location.

4 Related Works

4.1 Role-Based Access Control) model

RBAC(Role-Based Access Control) model[1, 2, 12, 14] is a versatile model that conforms closely to the organizational model used in corporations. RBAC meets this requirement by separating users and roles. Access rights are given to roles, and roles are further assigned to users. Role is a combination of users and privileges[16, 13, 18]. C-RBAC is an extension of traditional role-based access control model that allows security administrators to define context oriented access control policies enriched with the notion of purposes. By adding C-RBAC roles, they extend traditional access control model that helps organizations to know which user can perform what operation on which object with what purpose[20, 19].

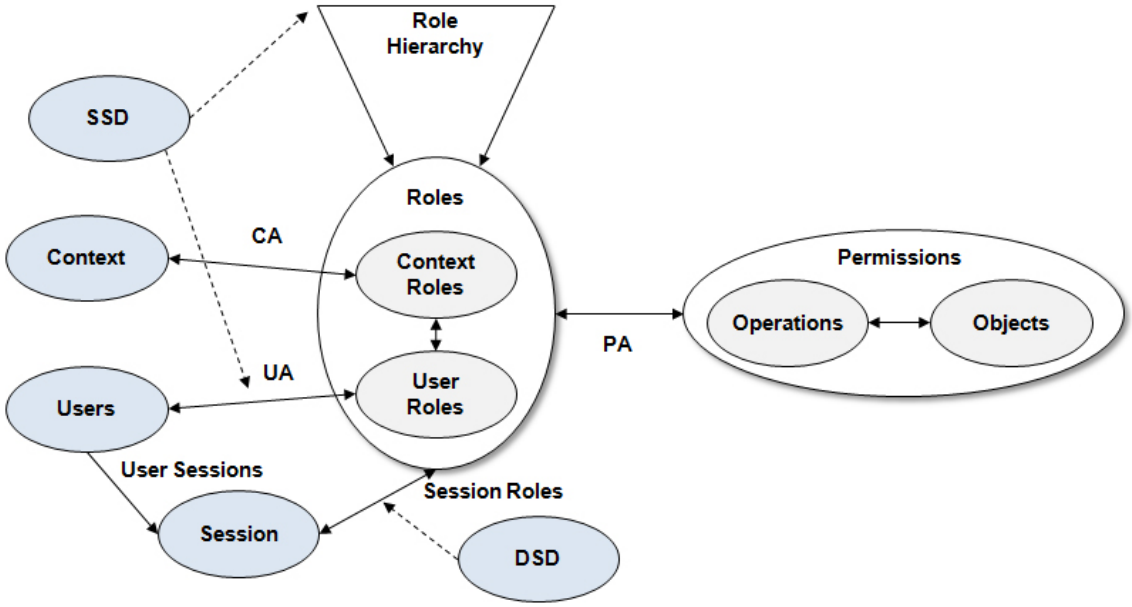

Figure 4: C-RBAC(Context- Role Based Access Control) Model

Figure 4 is a extended C-RBAC model and access control model for security context information based on context-role in ubiquitous computing system. This model is given the additional features of role active/inactive, hierarchy role and etc.

4.2 Context Aware-Task Role Based Access Control

CA-TRBAC(Context Aware-Task Role Based Access Control) is a control access and prevent illegal access efficiently for various information systems in ubiquitous computing environment. CAT-RACS(Context-Aware Task-Role based Access Control System) applied CA-TRBAC, which adds context-role concept tor achieve policy composition by context information and security level attribute to be kept confidentiality of information. It provides security services of user authentication and access control by context-aware security manager, and provides context-aware security services[10].

5 Conclusion

Access control model is the most frequently used method for insider intrusion detection and prevention. Generally, insider intrusion detection and prevention system is used RBAC and C-RBAC models. How-

ever, RBAC is impossible for dynamic access control because context-aware elements do not include. C-RBAC does not ensure privacy protection and integrity because security level between objects is not considered. Also, C-RBAC doesn't defend the information spill by legal act using objects related works. Therefore, new dynamic access control model needs to make up for the weakness of existing problems according to cloud computing characteristic. In this paper, we propose Onto-ACM for dynamic access control and Onto-ACM is a semantic analysis model for permitted limit of service provider and user. we are testing the Onto-ACM using developed prototype and we will build the dynamic access control model based on context information ontology in cloud computing environments. In the future works, proposed model needs to update access right, user role, inference rules, security policy using cloud resources.

Acknowledgements

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2010-0011656) and the Ministry of Education, Science Technology (MEST) and National Research Foundation of Korea(NRF) through the Human Resource Training Project for Regional Innovation.

References

[1] G.-J. Ahn and R. Sandhu. Role-based authorization constraints specification. *ACM Transactions on Information and System Security (TISSEC)*, 3(4):207–226, November 2000.

[2] E. Bertino, P. A. Bonatti, and E. Ferrari. Trbac: A temporal role-based access control model. 4(3):207–226, 2001.

[3] B. M. Bowen, M. B. Salem, , and S. Hershkop. Designing host and network sensors to mitigate the insider threat. *The Journal of Security & Privacy*, 7(6):22–29, December 2009.

[4] D. Cappelli, A. Moore, R. Trzeciak, and T. J. Shimeall. Common sense guide to prevention and detection of insider threats. Software Engineering Institute, CarnegieMellon, January 2009. `http://www.cert.org/archive/pdf/CSG-V3.pdf`.

[5] J. Carneiro, J. Laranjeira, G. Marreiros, C. Freitas, and R. Santos. A context-aware model to support ubiquitous group decision making, 2012.

[6] A. Corradi, R. Montanari, and D. Tibaldi. Context-based access control for ubiquitous service provisioning. In *Proc. of the 28th Annual International Computer Software and Applications Conference (COMPSAC'04), Hong Kong, China*, pages 444–451. IEEE, September 2004.

[7] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli. *Role-Based Access Control*. Artech House, 2003.

[8] K. Fukushima, S. Kiyomoto, and Y. Miyake. Towards secure cloud computing architecture - a solution based on software protection mechanism, 2011.

[9] W. Han, J. Zhang, and X. Yao. Context-sensitive access control model and implementation. In *Proc. of the 5th International Conference on Computer and Information Technology (CIT'05), Shanghai, China*, pages 757–763. IEEE, September 2005.

[10] J. ho Eom, S.-H. Park, and T.-M. Chung. A study on architecture of access control system with enforced security control for ubiquitous computing environment. *Journal of Korea Institute of Information Security & Cryptology*, 18(5):71–81, 2008.

[11] G. Hughes and T. Bultan. Automated verification of access control policies using a sat solver. *International Journal on Software Tools for Technology Transfer (STTT)*, 10(6):503–520, December 2008.

[12] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor. A generalized temporal role-based access control model. *IEEE Transactions on Knowledge and Data Engineering*, 17(1):4–23, 2005.

[13] T. Kalajainen. *An Access Control Model in a Semantic Data Structure: Case Process Modelling of a Bleaching Line*. PhD thesis, HELSINKI UNIVERSITY OF TECHNOLOGY, May 2007.

[14] N. Li and M. V. Tripunitara. Security analysis in role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, 9(4):391–420, 2006.

[15] X. Li and J. H. A. User-centric method for data privacy protection in cloud computing. In *Proc. of the 2011 International Conference on Computer, Elctrical, and Systems Sciences, and Engineering (ICCESSE'11), Paris, France*, pages 355–358, July 2011.

[16] A. Macfie, P. Kataria, N. Koay, H. Dagdeviren, R. Juric, and K. Madani. Ontology based access control derived from dynamic rbac and its context constraints. In *Proc. of the 11th International Conference on Integrated Design and Process Technology (IDPT'08), Taichung, Taiwan*, pages 226–231, June 2008.

[17] W. Pieters. Representing humans in system security models: An actor-network approach. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JoWUA)*, 2(1):75–92, 2011.

[18] A. J. T. Finin, L. Kagal, J. Niu, R. Sandhu, W. Winsborough, and B. Thuraisingham. ROWLBAC: representing role based access control in OWL. In *Proc. of the 13th ACM Symposium on Access Control Models and Technologies (SACMAT'08), Colorado, USA*, pages 73–82. ACM, June 2008.

[19] M. N. Tahir. C-rbac: Contextual role-based access control model. *Ubiquitous Computing and Communication Journal*, 2(3):67–74, 2007.

[20] C. Zhao, N. Heilili, S. Liu, and Z. Lin. Representation and reasoning on rbac: A description logic approach. *Theoretical Aspects of Computing - ICTAC 2005*, 3722(1):381–393, 2005.

[21] T. A. Zia and A. Y. Zomaya. A lightweight security framework for wireless sensor networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JoWUA)*, 2(3):53–73, 2011.

Chang Choi received a doctoral degree in the Department of Computer Engineering at Chosun University of Korea in 2012. Currently, He is working as a lecturer at the same university. His research interests include semantic information processing, semantic web and Multimedia.

Junho Choi received a doctoral degree in the Department of Computer Seience at Chosun University of Korea in 2004. Currently, He is working as a lecturer at the same university. His research interests include multimedia processing, semantic information processing, ontology engineering and semantic web.

Byeongkyu Ko is a student for the doctoral degree in computer engineering from Chosun University of Korea. He is received a master degree at the same university in 2012. His research interests include web documents classification, semantic information processing and semantic web.

Kunseok Oh received his Ph.D. degrees in Intelligent Information System from Kyushu University , Japan in 2001. He is an associate professor in the Department of Hospital Information Management at Gwangju Health College. His specific interests include web accessibility, semantic information processing and retrieval, multimedia database.

Pankoo Kim received his M.S. and Ph.D. degrees in Computer Engineering from Seoul National University, Korea in 1994. He is a full professor in the Department of Computer Engineering at Chosun University. His specific interests include semantic web techniques, semantic information processing and retrieval, multimedia processing and semantic web.