SS-RBAC: Secure Query Processing Model for Semantic Sensor Networks

Dongwon Jeong[1], Hyejin Jeong[1], and Young-Sik Jeong[2]

[1]*Dept. of Informatics & Statistics, Kunsan National University,*
San 68, Miryong-dong, Gunsan, Jeollabuk-do, 573-701 Korea
{djeong, xhyejin86x}@kunsan.ac.kr

[2]*Dept. of Computer Engineering, Wonkwang University,*
344-2 Sinyong-Dong, Iksan, Jeollabuk-do, 570-749 Korea
ysjeong@wku.ac.kr

Abstract

This paper proposes a novel secure query processing model for semantic sensor networks. A semantic sensor network (SSN) is a sensor network which includes semantics of sensory data and context information, and relationships between the semantics. In brief, SSN is an extension of the current Sensor Network (SN) and realized by using Semantic Web (SW) technologies. Although various researches have been activated on SSN, there is little activity on how to access data in semantic sensor networks in safe. This paper proposes a new access control model for secure query processing under semantic sensor networks. The proposed security model is based on RBAC (Role-Based Access Control) and enables secure access control of ontology for SSNs.

1. Introduction

With the growth of Semantic Web (SW) technology, various research areas such as Grid computing, Sensor Network (SN), Geographical Information System (GIS) have been adopted the SW technologies [1-3]. Semantic Sensor Network (SSN) is an extension of the current SN in which sensor data and context information are given semantics, i.e., well-defined meanings. To do this, the SW technologies such as the Resources Description Language (RDF) are used [4-6]. Until now, most of researches on SSN have been focused on metadata management, integration, visualization, reasoning, data fusion, and so on [7-15]. Even though security issue is very important in the SSN environment, little attention has been given to this issue.

This paper proposes a security model for the SSN environment. The proposed model is based on RBAC (Role-Based Access Control) and the model is named SS-RBAC, Secure query processing model for Semantic Sensor Networks based on RBAC.

Why is our proposal based on the RBAC model? As already mentioned, SSN is an extension of the current SN using SW technologies. For example, for describing metadata (semantics, meanings) of sensory data and context information, RDF can be used. The description is formed as an ontology. The ontology is stored to a storage system, and one of ontology storage systems used in the SW field can be chosen. Many storage systems have been developed to store Web ontologies [16-20]. A remarkable point is that most of storages systems are based on relational database model. It means an ontology built for a SSN is naturally stored into a relational database management system. The security model of relational database is also based on RBAC. Therefore, the SS-RBAC model is designed based on RBAC.

2. Preliminaries

This section describes key notations used in this paper and RDF model. A set of notations in Table 1 is defined to formally describe content of this paper.

Table 1. Definition of notations

Notations	*Description*
N	*A set of nodes; includes URIs; might be subjects and objects*
E	*A set of edges (arcs); corresponds to predicates in RDF graphs*
L	*A set of literals, constant values*
S	*A set of subjects,* $S = \{s_1, s_2, ..., s_n\}$
s_i	*One of subjects,* S; $s_i \in S$
O	*A set of objects,* $O = \{o_1, o_2, ..., o_n\}$
o_i	*One of objects,* O; $o_i \in O$
P	*A set of predicates,* $P = \{p_1, p_2, ..., p_n\}$
p_i	*One of predicates,* P; $p_i \in P$
T	*A set of tables in a relational database*
t_i	*One of tables,* T; $t_i \in T$
$t_i.f_j$	*a field of the table* t_i
V	*A set of views,* $V = \{v_1, v_2, ..., v_n\}$
R	*A set of roles,* $R = \{r_1, r_2, ..., r_n\}$
U	*A set of users,* $U = \{u_1, u_2, ..., u_n\}$
C	*A set of classes,* $C = \{c_1, c_2, ..., c_n\}$
c_i	*One of classes,* C; $c_i \in C$
I	*A set of individuals,* $I = \{i_1, i_2, ..., i_n\}$
i_k	*One of individuals,* I; $i_i \in I$

3. SS-RBAC

This section describes the concept of our approach, access types, and conceptual model for SS-RBAC.

3.1. Our approach

SS-RBAC is based on relational database security model, and it means that RDF ontology storages based on relational model are used for managing a semantic sensor ontology including sensory data, context information, concepts, and relationships of a SSN.

The relational database model is based on RBAC and physically establishes security policies using GRANT operator. The relational security model supports the concepts such as privilege, role, and user group. Using the concepts, we can define fine-grained security policies for the semantic sensor ontology.

Figure 1 illustrates the conceptual model for SS-RBAC proposed in this paper. A current SN consists of several types of data as follows [8]:

- Sensory data: states acquired from sensors

- Context information: Information in which the sensory data is generated; physical properties of sensor nodes such as time, position, data types, and so on.

However, a SSN additionally includes metadata containing the both types of data. The metadata refers to concepts and relationships between concepts. Figure 3 shows an example of semantic sensor ontology for SSN in [7].

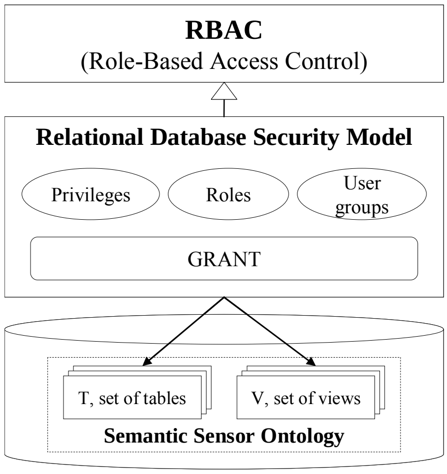


Figure 1. Conceptual model for SS-RBAC

In Figure 2, VideoSegment_1 is a sensory data and BwayAt42nd is a context data describing the location of the traffic camera "Traffic Camera 10036-1". "Traffic Camera 10036-1" is one of instances (Individuals) the class "FixedPositionTrafficCamera" and "hasSegmentWidth" is a relationship between "Audio Segment" and "xsd:duration" corresponding to a subject and an object in RDF graph.

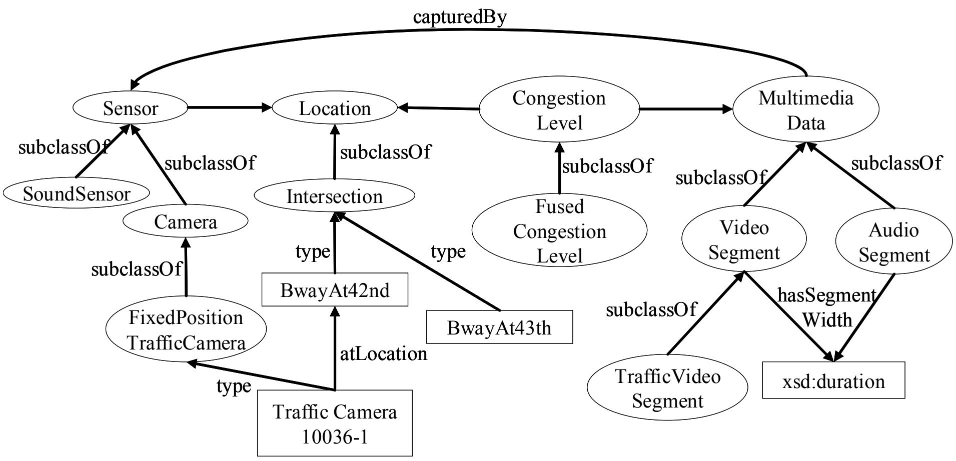


Figure 2. A semantic sensor ontology example

3.2. Access types

In Figure 2, a SSN contains sensory data, context information, concepts, and relationships. These types of data are built as an ontology. The ontology is stored into a storage based on relational database model, and thus the access control of the ontology is accomplished on the database storing the ontology.

As a result, access types of users could be classified into four classes as follows [21]:

- Class-I: whole data in a table (Table level)
- Class-II: all data in specific fields (Column level)
- Class-III: all data in specific tuples (Row level)
- Class-IV: random data (Cell level)

3.3. Definition of SS-RBAC

Before defining SS-RBAC, the relational database model is first briefly defined as follows.

Definition 1 (Relational Database) A relational database is denoted by 2-tuple Ř= (T, V), where:

- T is a set of base tables storing initially a given sensor ontology,
- V is a set of views including a set of data in the base tables.

In fact, the relational model can be defined in detail, but this paper defines it with the two components, i.e., tables, views, which are key components in the SS-RBAC model proposed in this paper.

SS-RBAC is defines as follows.

Definition 2 (SS-RBAC) SS-RBAC is denoted by 4-tuples Ŝ = (Ř, R, U, Δ), where:

- Ř is a relational database containing sets of tables and views,
- R is a set roles,
- U is a set of users,
- Δ is a set of operations to define roles, create views, evaluate authorities, and assign policies to users.

Figure 3 shows the overall SS-RBAC framework. In this figure, an ontology is given and parsed and store into the selected storage. Before the process, access control policies are established and reflected to the given ontology. The overall process for defining security policies is as follows:

(1) Creating user groups
(2) Creating roles
(3) Creating views
(4) Assigning roles to users or user groups
(5) Evaluating the defined security policies

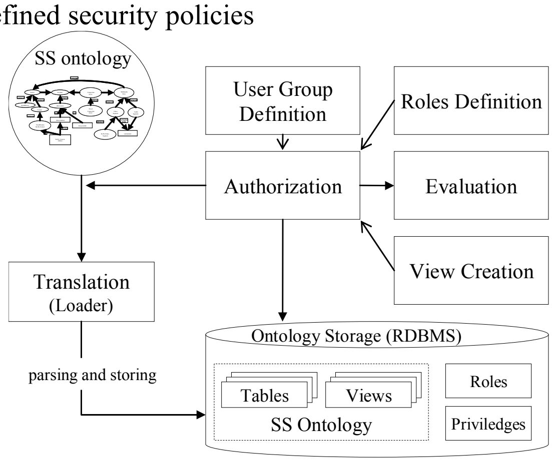


Figure 3. SS-RBAC framework

3.4. Defining processes of security policies

SS-RBAC is based on relational database security model, and thus the overall defining process of security policy is deeply similar to the process of relational databases. First, a security manager selects objects, i.e., data set to be permitted or not. After the selection, a role is created, and proper privileges are assigned to the role. The created role is assign to users or user groups and a security policy is created. Figure 4 illustrates the overall process.

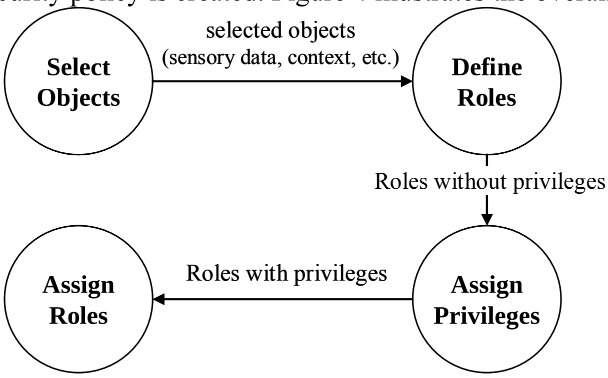


Figure 4. The key processes to define security policies

4. Evaluation

This section describes the concept of our approach, access types, and conceptual model for SS-RBAC.

4.1. Experimental environment

In this paper, the Jena storage is used for the implementation of SS-RBAC. Jena is one of representative frameworks for developing Semantic Web tools, system, applications, and services. Jena provides a storage model based on relational database.

Various security rules for evaluation are defined, and different authorities are assigned to each user considering the access control levels, i.e., table-level, column-level, row-level, and cell-level.

4.2. Evaluation

We conducted an experiment with the aforementioned experiment environment. The experimental item is about the precision of access control. In other words, we check the proposed security model can support a secure query processing on the semantic sensor ontology or not. In the experiment, valid data sets have been returned to users according to the security policies. This evaluation also enables the verification of the policy generation algorithm.

SS-RBAC is based on relational database security model. It provides many advantages and key good points are summarized as follows:

- Ease of use: Relational database is much familiar to users. Therefore, SS-RBAC also supports the characteristic.

- High stability: For several decades, the relational database and its security model have been validated and verified. Hence SS-RBAC also provides the same advantage.
- Finer-grained access control: Relational database provides the mechanism to control access at table level and row level. For the secure ontology query processing is required a finer-grained access control. SS-RBAC can define finer-grained security policies.

5. Conclusion

This paper introduced a security model for secure query processing of semantic sensor ontology. The proposed model is named SS-RBAC, which is based on relational database security model. The conceptual model, framework, and process have been described. This paper also showed an evaluation. The proposed security model, SS-RBAC provides many advantages such as ease of use, high stability, and finer-grained access control support.

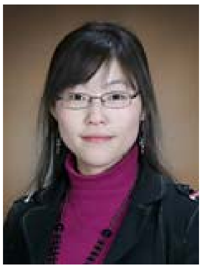
References

[1] T. Berners-Lee, "The World Wide Web: Past, Present and Future," IEEE Computer special issue, 1996.
[2] D. Jeong, J. Son, D.-K. Baik, and L.T. Yang, "View-based Storage-Independent Model for SPARQL-to-SQL Translation Algorithms in Semantic Grid Environment," IEEE Computer Society, The 11th IEEE International Conference on Computational Science and Engineering (CSE'08) - The International Symposium on Pervasive Grid (PerGrid'08), pp. 381-386, Sao Paulo, Brazil, July 16-18, 2008.
[3] J.-D. Kim, H. Shin, D. Jeong, and D.-K. Baik, "Jena Storage Plug-in Providing an Improved Query Processing Performance for Semantic Grid Environment," IEEE Computer Society, The 11th IEEE International Conference on Computational Science and Engineering (CSE'08) - The International Symposium on Pervasive Grid (PerGrid'08), pp. 398-398, Sao Paulo, Brazil, July 16-18, 2008.
[4] W3C, Resource Description Framework, http://www.w3.org/RDF/.
[5] Frank Manola and Eric Miller, RDF Primer, W3C Recommendation, February 10, 2004.
[6] Dave Beckett, RDF/XML Synta specification (Revised), W3C Recommendation, February 10, 2004.
[7] Eric Bouillet, Mark Feblowitz, Zhen Liu, Anand Ranganathan, Anton Riabov, and Fan Ye, "A Semantics-Based Middleware for Utilizing Heterogeneous Sensor Networks," Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, Vol. 4549, 2007, pp. 174-188.
[8] Guangtao Xue, Qunhua Pan, and MingLu Li, "A New Semantic-based Query Processing Architecture," 2007 International Conference on Parallel Processing Workshops (ICPPW 2007), September 10-14, 2007.
[9] Ismail Khalil Ibrahim, Reinhard Kronsteiner, and Gabriele Kotsis, "A semantic solution for data integration in mixed sensor networks," Computer Communications, Elsevier, Vol. 28, No. 13, August 2005, pp. 1564–1574.
[10] Caleb Goodwin, and David J. Russomanno, "An Ontology-Based Sensor Network Prototype Environment," The 5th International Conference on Information Processing in Sensor Networks (Poster), IEEE, Nashville , TN , 2007, pp. 1-2.
[11] Michita Imai, Yutaka Hirota, Satoru Satake, and Hideyuki Kawashima, "Semantic Connection between Everyday Objects and a Sensor Network," Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, Vol. 4273, Semantic Sensor Networks Workshop (SSN'06): A Workshop of the 5th International Semantic Web Conference (ISWC 2006), Athens, Georgia, USA, November 5-9, 2006.
[12] Michita Imai, Yutaka Hirota, Satoru Satake, and Hideyuki Kawashima, "Semantic Sensor Network for Physically Grounded Applications," Proceedings in ICARCV, The 9th International Conference on Control, Automation, Robotics and Vision (ICARCV 2006), Singapore, December 5-8, 2006, pp. 1637-1642.
[13] Lionel Ni, Yanmin Zhu, Jian Ma, Minglu Li, Qiong Luo, Yunhao Liu, S.C. Cheung, and Qiang Yang, "Semantic Sensor Net: An Extensible Framework," In Proceedings of International Conference on Computer Networks and Mobile Computing, Zhangjiajie, China, 2005.
[14] Hideyuki Kawashima, Yutaka Hirota, Satoru Satake, and Michita Imai, "MeT: A Real World Oriented Metadata Management System for Semantic Sensor Networks," In Proceedings of the 3rd International Workshop on Data Management for Sensor Networks (DMSN'06), Seoul, Korea, September 11, 2006, pp. 13-18.
[15] Micah Lewis, Delroy Cameron, Shaohua Xie, and I. Budak Arpinar, "A Semantic Approach to Data Management in Sensor Networks," Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg, Vol. 4273, Semantic Sensor Networks Workshop (SSN'06): A Workshop of the 5th International Semantic Web Conference (ISWC 2006), Athens, Georgia, USA, November 5-9, 2006.

[16] Z. Pan and J. Heflin, "DLDB: Extending relational databases to support Semantic Web queries," In Workshop on Practical and Scalable Semantic Web Systems, 2nd International Semantic Web Conference (ISWC2003), Springer-Verlag, Lecture Notes in Computer Science, Vol. 2870, Sundial Resort, Sanibel Island, Florida, USA, October 20-23, 2003, pp. 109-113.
[17] J. Broekstra, A. Kampman, and F. v. Harmelen, "Sesame: A Generic Architecture for Storing and Querying RDF and RDF Schema," Springer-Verlag, Lecture Notes in Computer Science, Vol. 2342, June 2002, pp. 54-68.
[18] OWLJessKB: A Semantic Web Reasoning Tool, http://edge.cs.drexel.edu/assemblies/software/owljesskb/.
[19] Jena Semantic Web Framework, http://jena.sourceforge.net/, 2007.
[20] D. Jeong, M. Choi, Y.-S. Jeon, Y.-H. Han, L.T. Yang, Y.-S. Jeong, and S.-K. Han, "Persistent Storage System for Efficient Management of OWL Web Ontology," Springer-Verlag, Lecture Notes in Computer Science, Vol. 4611, July 2007, pp. 1089-1097.
[21] Dongwon Lee, Wang-Chien Lee, and Peng Liu, "Supporting XML Security Models using Relational Databases: A Vision," Lecture Note In Computer Science, Springer-Verlag Berlin Heidelberg, Vol. 2824, Berlin Germany, September 8, 2003, pp. 267-281.

Authors

Dongwon Jeong received his B.S degree in Computer Science from Kunsan National University, Korea, in 1997. He received his M.S. and Ph.D. degree in Computer Science from Chungbuk National University, Korea, in 1999 and from Korea University, Korea, in 2004 respectively. He worked as a full-time instructor, 1999 to 2000 in the Advanced Institute of Information Technology, Korea. He was a Senior Researcher, Jigunet Corporation, from 2000 to 2001. He was a Research Assistant Professor, Korea University, from 2004-2005. He was a Visiting Research Scholar (PostDoc.), School of Information Sciences & Technology, Pennsylvania State University, US, 2005. Now, he is a Professor in the Dept. of Informatics and Statistics, Kunsan National University, Korea from 2005. He was a Committee Member, Data Study Group (SG08.02), Telecommunications Technology Association (TTA), Korea, from 2002 to 2004. He is a Committee Member, Metadata Project Group (PG 606), Telecommunications Technology Association (TTA), Korea, 2004-Present. He is a National Committee Member, Data Management Service, Korean Agency for Technology and Standards (KATS), Korea, 2006-Present. He is an Editorial Board Member, International Journal of Ubiquitous Computing (IJUC), Serials Publications, India, 2008-Present, and an Editorial Board Member (Regional Editor), Asian Journal of Information Management (AJIM), Academic Journals Inc., 2006-Present. He is a Member, IEEE and IEEE Computer Societry, Korea Society for Simulation (KSS), Korea, 2003-Present, Korea Information Science Society, Korea (KIISE), 2001-Present, Korea Information Processing Society (KIPS), Korea, 2003-Present, The Institute of Electronics, Information and Communication Engineers (EIC), Japan, 2004-Present, Korea Society of IT Services (KITS), Korea, 2007-Present, and Korea Society of Computer Information (KSCI), Korea, 2008-present. He was a PC Member or Program/Publicity/General Chair of many conferences and workshops. He is now a General Co-Chair/Steering Co-Chair/Program Co-Chairs of various conferences and workshops. His research interests include Data Integration, Semantic Web, Semantic Sensor Network, Semantic GIS, Semantic Grid, and Security.



Hyejin Jeong received her B.S degree in Informatics and Statistics from Kunsan National University, Gunsan, Jeollabuk-do, Korea, in 2008. She is a Master student in Informatics and Statistics, Kunsan National University, Gunsan, Jeollabuk-do, Korea, from 2008 to current. Her research interests include Database, Semantic Web, Semantic GIS, and Security.

Young-Sik Jeong received his B.S degree in Mathematics, Korea University, Seoul, Korea, in 1987. He received his M.S degree and Ph.D. degree in Computer Science, Korea University, Seoul, Korea, in 1989 and 1993 respectively. He was a visiting scholar, Dept. of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824, USA, 1997, and Dept. of Electrical and Computer Engineering, Wayne State University, Detroit, MI 48202, USA, 2004. He is a Director of Culture Contents Technology Society, from 2006 to Current, an Appraisal Committee of University Industrial Technology Force (UNITEF) for Patents, from 2003 to Current, a Chairman of IEC/TC 108 Korean Agency for Technology and Standards, 2003 to Current, a Committee of IEC/TC 100 Korean Agency for Technology and Standards, from 2002 to Current, and a Korean Committee, ISO/IEC JTC 1/SC 25, from 2002 to Current. He was a PC Member or Program/Publicity/General Chair of many conferences and workshops. He is a Professor, Department of Computer Engineering, Wonkwang University, Iksan, Korea, from 1993 to Present. His interests include Grid Computing, Semantic Grid, Mobile Computing, and e-Learning.