International Journal of Control and Automation
Vol. 11, No. 3 (2018), pp.1-12
http//dx.doi.org/10.14257/ijca.2018.11.3.01

Access Rights Management based on User Profile Ontology for IoT Resources Authorization in Smart Home

Israr Ullah, Faiza Tila and DoHyeun Kim

Computer Engineering Department, Jeju National University, Republic of Korea
israrullahkk@yahoo.com, faizakhan797@gmail.com, kimdh@jejunu.ac.kr

Abstract

Recent development in information and communication technologies has paved the way for IoT. Connected things are getting popular and transforming industries, manufacturing, health care, education, security, business and life style everywhere. In this paper, we present the access rights management scheme based on user profile ontology to facilitate access management in our existing semantic indoor IoT system. The proposed scheme supports multi-user access with assigned rights and roles. Additional, we develop the access rights management module based on user profile ontology in order to effectively organize and manage access to the system resources i.e. sensor and actuators. This work can be instrumental in provisioning safeguard against security vulnerabilities as only authorized user can have access to designated resources.

Keywords*: Internet of Things (IoT), access management, ontology, semantic*

1. Introduction

Internet of Things (IoT) is designed to attach a small communicating device with everything that we want to monitor or control using Internet. The IoT device may be sensing device that collect some desired information or it can be an actuating device that can accept commands to perform some desired task. IoT devices have limited communication, computation and battery power and lightweight protocols are designed for efficient resource utilization over Internet *e.g.* CoAP protocol [1]. IoT Systems have tremendous capabilities and applications. In the recent past, many giant manufacturing and development organizations have made investment in this technology to realize its potential. Many projects are initiated to address different aspect of IoT based systems. Internet of Things (IoT) is the future technology enabling connectivity of things (smart things) for development of Intelligent monitoring and control system. IoT offers lots of useful applications in many different domains *e.g.* industry, transportation, health, energy management, smart homes *etc.*

To realize the IoT vision, we need to overcome certain challenges that needs careful consideration and well-planned solutions. In the future connected world, security and privacy of the user and things will be a major concern which not only demands technological solutions but also serious and careful legislation. From environmental perspective, green globe of tomorrow demands efficient utilization of resources to have minimal impact on the environment. Among the technical challenges includes, protocols device naming and identity, resource discovery and interoperability *etc.* In IoT world, where things are connected and accessed via internet, devices and services interoperability is highly desirable. There need to be an enabling technology that shall help devices to exchange and share data in an understandable fashion. Development of semantic IoT systems helps in meaningful representation of the system for efficient information sharing and discovery.

Received (November 14, 2017), Review Result (January 19, 2018), Accepted (January 16, 2018)

ISSN: 2005-4297 IJCA

First, we briefly describe the design of our existing semantic IoT based system and its architecture. Existing semantic IoT system captures information about sensors, actuators, and combines the same with location information using modular ontology based components. The system is used by different users having different roles (*i.e.* admin, contributors, and guest *etc.*) but user information is not captured in the existing system.

This paper is an extension of our previous work presented in [2]. We have developed a semantic IoT system for Indoor environment monitoring and control. Existing system captures information about sensors, actuators and combines the same with location information. The system is used by different users having different roles (*i.e.* Admin, Contributor, Guest *etc.*) but user information is not captured in the existing system and hence focus of this work.

Rest of the paper is organized as follows; Section 2 presents the summary of related research with a brief description of our previous work. Section 3 presents modified system design and proposed user profile ontology. Section 4 covers implementations details with demo results and discussion. Towards the end, we conclude this paper with an outlook to our future work in Section 5.

2. Related Work

IoT is assumed to be the future technology and many big companies and vendors are actively investing in this area to grad their market share. Today, we have IoT devices from many different companies, each having its own set of protocols and standard interfaces for communication. Devices and services interoperability becomes a major concern in fulfilling the dream of connected world. There need to be an enabling technology that shall help devices to exchange and share data in an understandable fashion. Development of semantic IoT systems helps in meaningful representation of the system for efficient information sharing and discovery. In the following lines, we briefly present the summary of related research contributions made in this direction.

Ontology is a useful medium for knowledge representation and sharing in computing world [3]. Many different ontology structures are developed as standard representation of knowledge concerning to a particular domain. Like in other fields, efforts are made to develop ontologies in IoT domain for better representation and understanding of the shared data and resources. For instance, SSN ontology is developed for annotating sensor and sensors data [4]. Likewise, linked data [5] is used for publishing sensor data [6] and discovery [7], and semantic sensor observation services (SemSoS) [8] are few applications based of semantic technologies in IoT domain. Ontology development is the keystone for building semantic IoT systems. Purpose of having semantic component in IoT system is two fold (a) to represent connected devices information in way that shall also capture the relationship among them for further exploitation (b) to have convenient and shared representation of knowledge collected from heterogeneous sources in order to have a shared and common view of overall system. W. Wang *et al.* have expressed the utility of ontology in IoT based system for performing tasks like service composition and discovery [9]. The authors in [10] presented an ontology for automated deployment of application in heterogeneous IoT environment. A road-map for application of semantic technologies in IoT is presented in [11] to demonstrate how semantic web can be instrumental in addressing associated challenges in conventional IoT systems. A research study presented in [12] illustrate utility of semantic technologies in overcoming device heterogeneity problem. Integration of systems using RFID manufactured by different vendors with different data formats was made possible by defining an ontology for RFID system.

Many IoT based application are tailor-made and designed for a particular problem. Internet of Things Environment for Service Creation and Testing (IoT-EST) project is focused on the development of a flexible environment where services can easily be customized to fit the user requirement [13]. Semantic models are developed to build reusable components to solve the problem of integration and interoperability. They have developed a framework for testing and designing shared IoT services and semantic layer is used to facilitate collection and integration of information from diverse sources. Another important contribution is made by IoT-A project [14]. They have developed an architecture to address the interoperability challenge and have designed technical standards for various interfaces and protocols related to IoT. They have used a set of ontologies based on the SSN and OWL-S [15] ontology for entities, resources, devices and services in the IoT system to capture their associations and enable shared knowledge representation across the systems. Several implementations for real-life scenarios are demonstrated to realize the potential of the proposed IoT system.

3. Access Rights Management based on User Profile Ontology for IoT Resources Authorization

Existing system captures information about sensors, actuators and combines the same with location information. The system is used by different users having different roles (*i.e.* Admin, Contributor, Guest *etc.*) but user information is not captured in the existing system. This work is focused on development of ontology for users and incorporates the same in existing system to manage access to the resources.

User profiling is commonly employed nowadays to enhance usability as well as to support personalization, adaptivity and other user-centric features. Our objective is to utilize user profile ontology for controlling access to the resources in semantic IoT environment. For this purpose first, we explored existing literature for a suitable ontology so that we can use/extend/adopt the same for our requirement to serve the purpose. We found two ontologies that closely related to our work/need. The Organization ontology has been developed and standardized within the W3C Government Linked Data working group and has recently become a full W3C recommendation [16] but this is more general and comprehensive. Ontology-based access rights management [17] was found more relevant and specific to our need and hence we adopted the same for our semantic indoor IoT system.

Existing semantic IoT system for Indoor environment monitoring and control captures information about sensors, actuators and combines the same with location information using five main modules (a) Sensor provider module holds information and data about registered sensors and provide an access middleware to the upper layer applications. (b) Actuator provider module holds information about registered actuators and accept commands from upper layer applications for execution on desired actuators. (c) GIS provider service combine the location information data with sensor and actuators to display them over map at their corresponding locations. Users can assign regions, building, floors, rooms *etc.* to the IoT devices in the network. (d) Application server sit in the middle between client applications and system support layers. Client requests are redirected towards corresponding application provider for onward processing on IoT devices. (e) Registry serves as the central repository for the whole system. Sensor, actuator and GIS provider publishes their corresponding resources information to the registry which are then queried by application server when desired by client applications. Figure 1 shows the updated structure of system key component's interactions. User profile provider ontology component is added to existing system for incorporating user profile based access management to system resources.

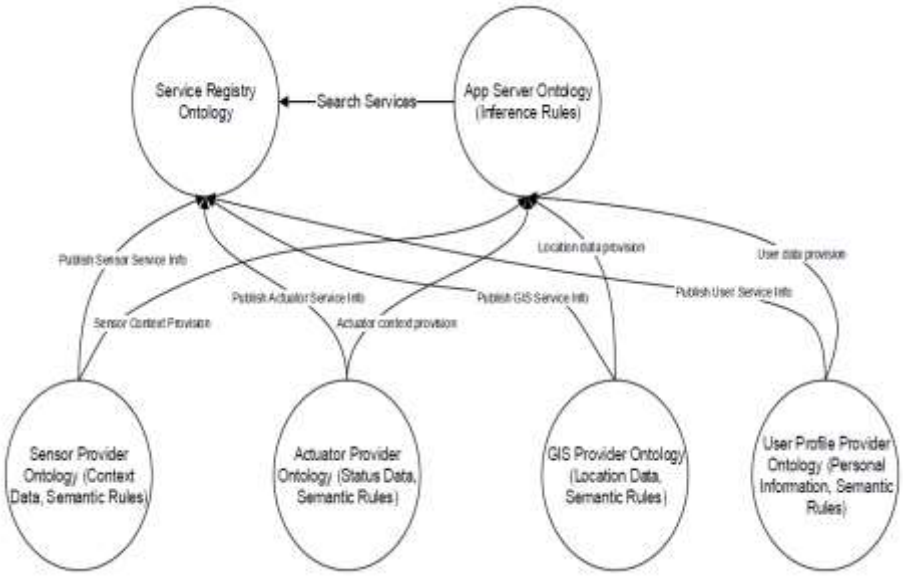

Figure 1. Modified Structure of System Key Component's Interactions for Access Rights Management

User profile provider component publishes the user profile information to services registry which is then queried by application server. User profile information are also shared with application server to support customization and personalization. Furthermore, application server provide controlled access to authorized resources to user via client application.

3.1. Access Rights Management based on User Profile Ontology

In our indoor semantic IoT system, roles (admin, guest *etc.*) are assigned to users to support access management to IoT sensors and actuators in smart home environment. Depending upon the user type, various role can be assigned. As a result a set of classes and properties needs to be defined to build ontology to describe the access rights to resources. Our semantic IoT system is system as content management system with only difference that we have sensors and actuators whereas content management system have shared documents. Therefore, we use the same access management ontology as defined in [19] with slight modification *i.e.* we have included a resource class having two sub-types sensor and actuator. Next, we briefly describe the various classes and their properties used in proposed user profile ontology.

Agent is used to express system users and user groups. Agents are assigned roles. Three roles are modeled *i.e.* admin, contributor and guests. Each role have associated list of authorized actions. Currently, six different types of actions are included, others can be added if needed. Figure 2 shows the detailed view of proposed user profile ontology in OntoGraf. It shows the ontology main classes and includes instances of certain classes. Protege view of our user profile ontology for access management is shown in Figure 3. This ontology holds semantic information about users and their group along with authorized action on particular resources. We have imported ontology to application server ontology and using canAccessBy object property, we specify which object can be accessed by certain group.

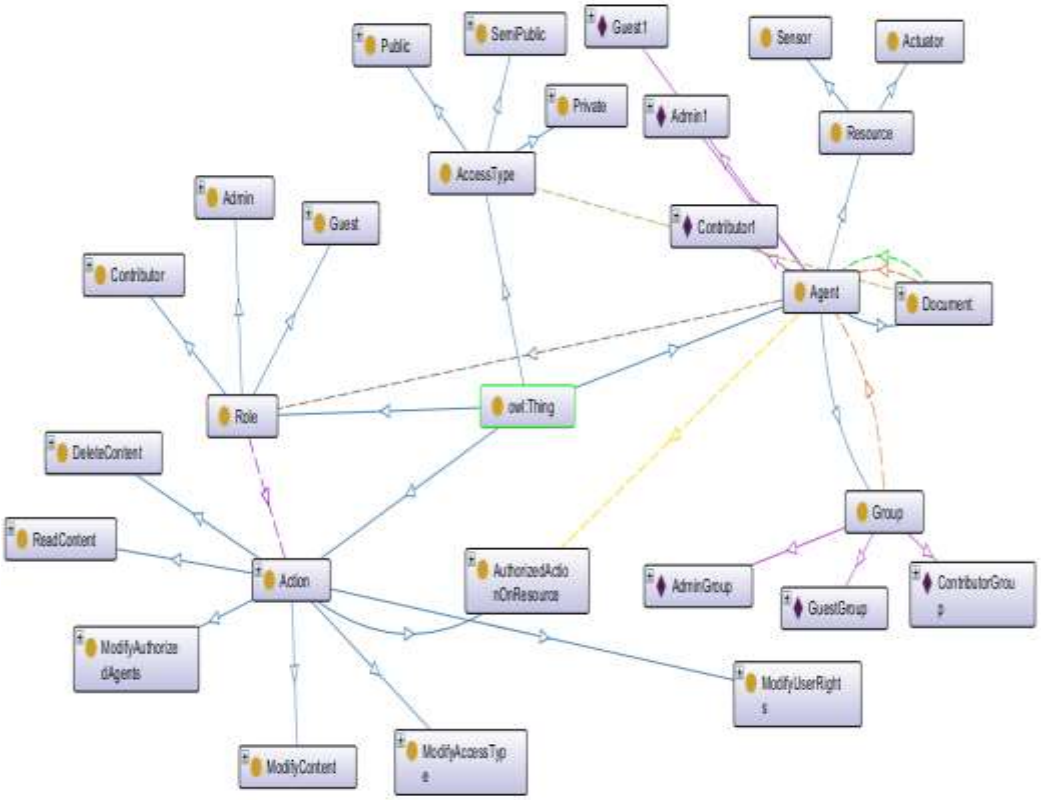

Figure 2. Ontograph View of user Profile Ontology in Protege

Proposed user profile ontology has four main classes under the root class owl:Thing *i.e.* agent, role, action, and accesstype. Agent is used to express system users and user groups. For every user of the system, we will have an instance of agent class. Agents are assigned roles. Three roles are modeled *i.e.* admin, contributor and guests. Each role have associated list of authorized actions. Depending upon the role assigned to the user, access the system resources can be controlled. Currently, the system support only seven different operations on resources which are captured by sub-classes of action class. With every resource in our system, first we define what kind of operation can be performed on it which is controlled by AuthorizeActionOnResource operation that enable what kind of actions can be associated with a particular resource. DeleteContent operation can delete certain resources information from the system and shall only be assigned to admin users. ModifyAccessType operation can change the access type of resource to make it publicly available, private or semi-public. ModifyAuthorizedAgents operation is used to add or remove agents to have access to a particular resource in the system. ModifyContent operation can change the resources information in the system. ModifyUserRights operation is used to define and update various roles defined in the system to control its access rights. ReadContent operation provide read only access to the system resources which is assigned to all roles by default.

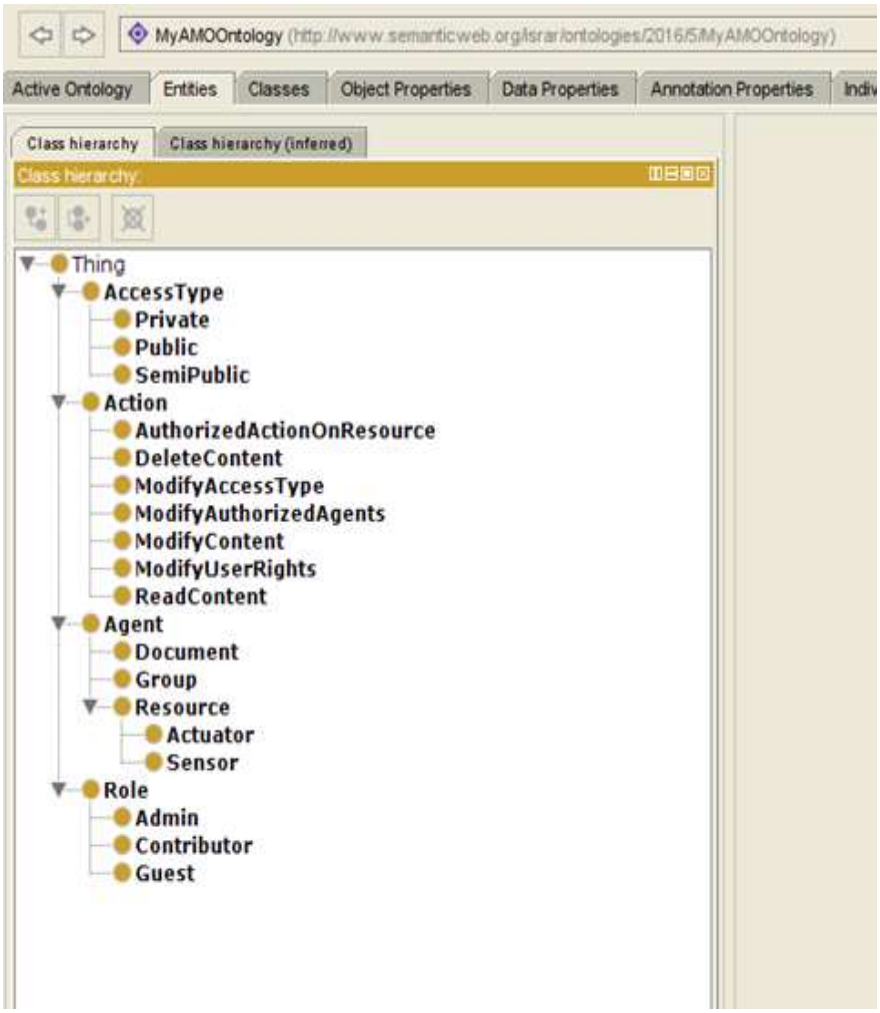

Figure 3. Main Classes of user Profile Ontology as Viewed in Protege

4. Implementation Results of Access Rights Management based on User Profile Service Provider

Semantic user profile service provider is implemented as separate service in the system and its internal components can be viewed as show in Figure 4. It has both user profile database and ontology. It has two information provisioning modules (a) to share individual user information (b) to share information about the registered roles. Roles are assigned to users that specify which kind of operation a particular user can perform. Semantic rights reasoning component is used for inference additional rights of a particular user *i.e.* rights of each user is not hard coded in ontology rather these are discovered on the fly depending upon the user group and assigned roles. A user can be member of one or more groups and can have one or more roles assigned.

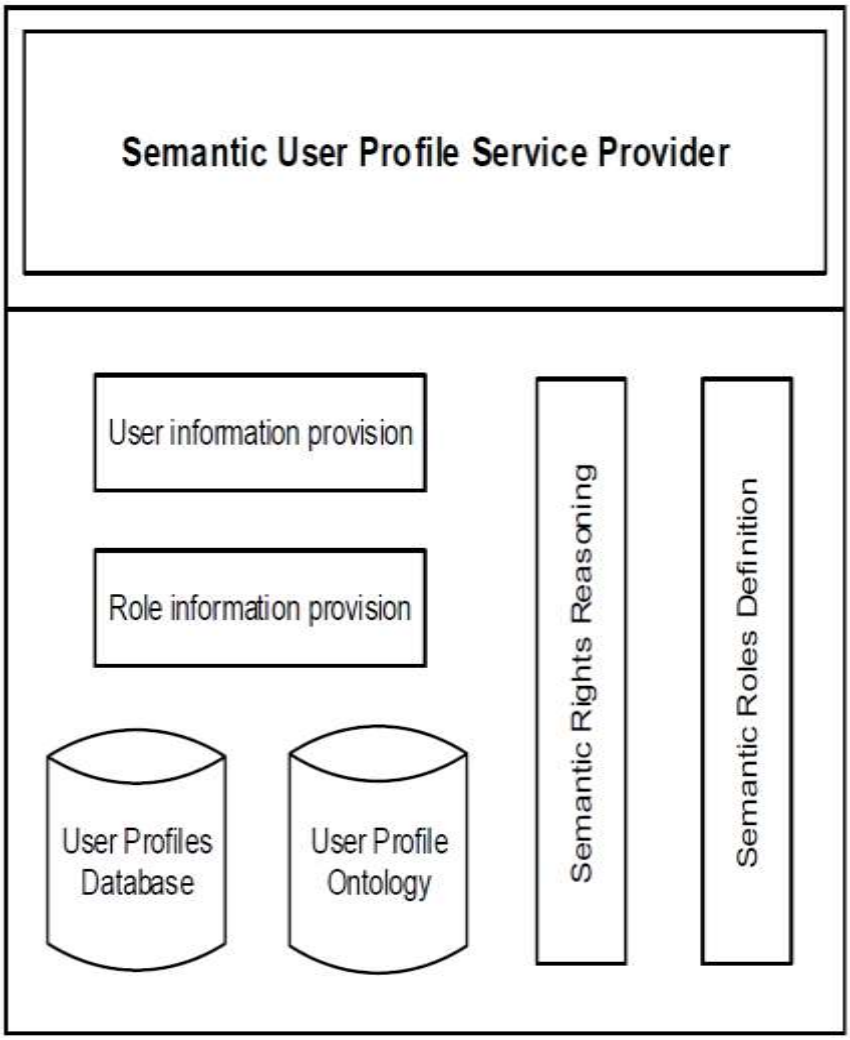

Figure 4. Internal Components of user Profile Service Provider

Users profile service provider module snapshot is given in Figure 5. We can see, it has two main services *i.e.* Semantic provider service which retrieve information from ontology in order to manage access to the resources and content service retrieve user information from database in order to verify user access to the system. SOAP based services are used to support interaction with other system components. Services can be started and stopped at any time using this interface. Execution history of services is also maintained for record keeping and bug tracking. Both services must be in running state, when a user tries to log-in to the system using client application interface.

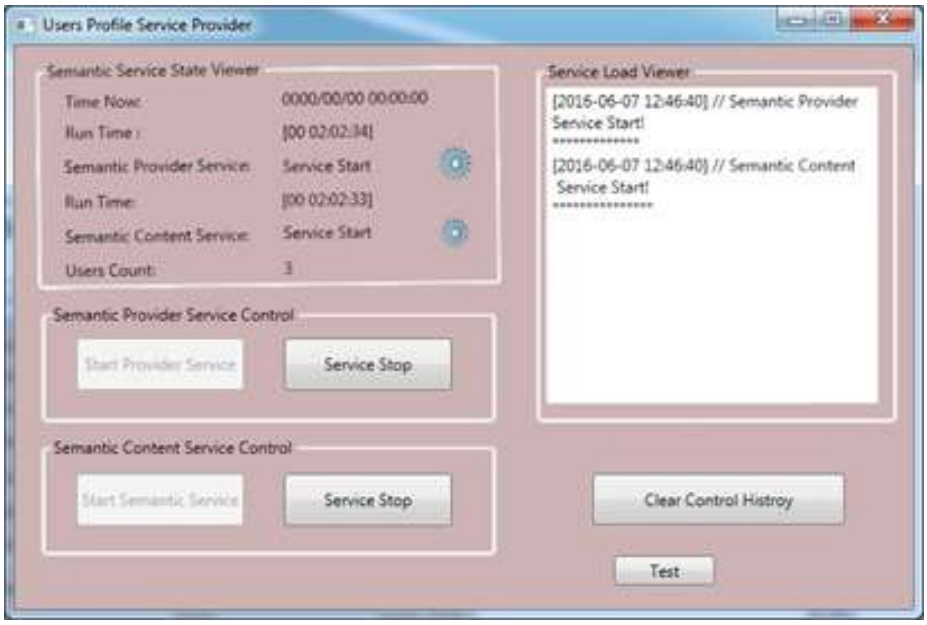

Figure 5. Snapshot of user Profile Service Provider Module

The modified system has now a log in facility which allows only register users to access the application server and any unauthorized access attempt to the system is denied. All registered users are assigned and particular user group and their access to the system resources is controlled to the rights as assigned to the respective group in ontology. The following screen-shots (Figure 6) gives a view of updated client application interface. Valid user name and password is required for successful log-in to the system. After successful log-in, the application server search button is enabled and client application can get access to running application servers.

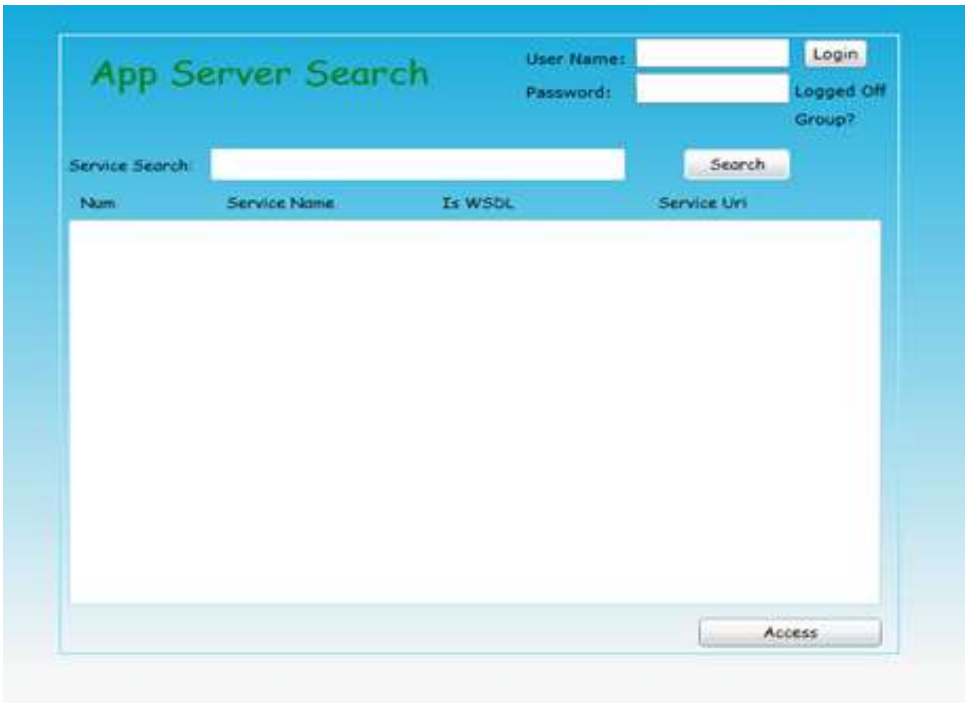

Figure 6. Updated Client Application Interface

4.1. Demo Results

For sake of demonstration, we have connected one temperature sensor and two actuators (*i.e.* fan and light) to our semantic indoor IoT system. For testing purpose, we have defined three user groups *i.e.* admin, contributor and guest. We have registered three users in our system (one in each class). Admin group user has all rights and can view all sensors and actuators. Admin user can also get sensing data and send actuation commands to fan and light. Contributor group user have less rights than admin user. For testing purpose, we only assign access rights to an light actuator *i.e.* he can view light current status and can also send actuation commands to the light *i.e.* turn on/off. The third user belong to guest group and have only access rights to the sensing device *i.e.* he can only query current room temperature but cannot access fan or light. The screen-shots shown in Figure 7, 8 and 9 present each user's view of the same contents. We can see that all users have different view of the same system as they belong to different user groups. Thus access management to the system resources is achieved via user profile ontology in our indoor semantic IoT system.

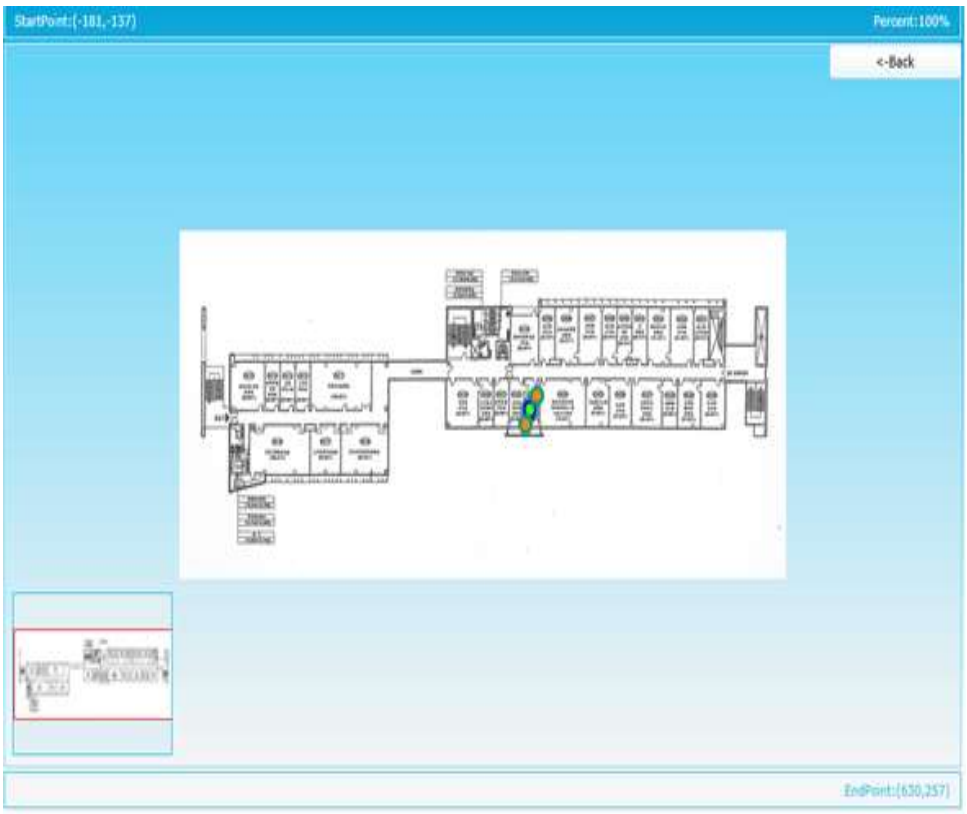

Figure 7. One Sensor and Two Actuators Deployed in 4th Floor as View by Admin User

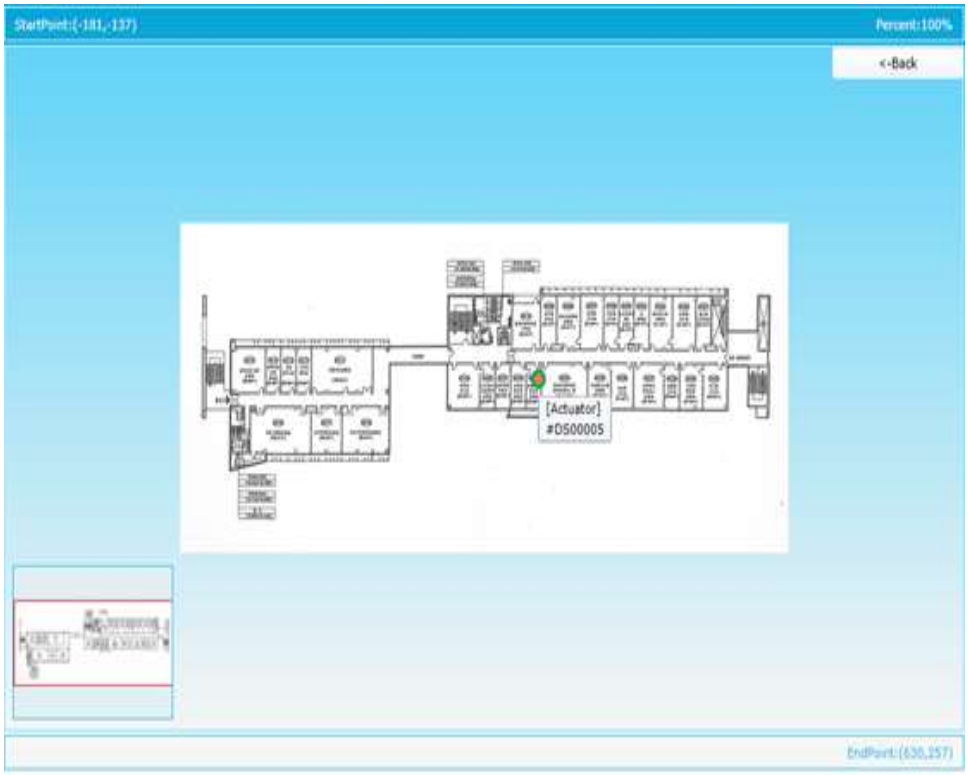

Figure 8. One Sensor and Two Actuators are deployed in 4th floor but Contributor Group User is allowed only to View an Actuator

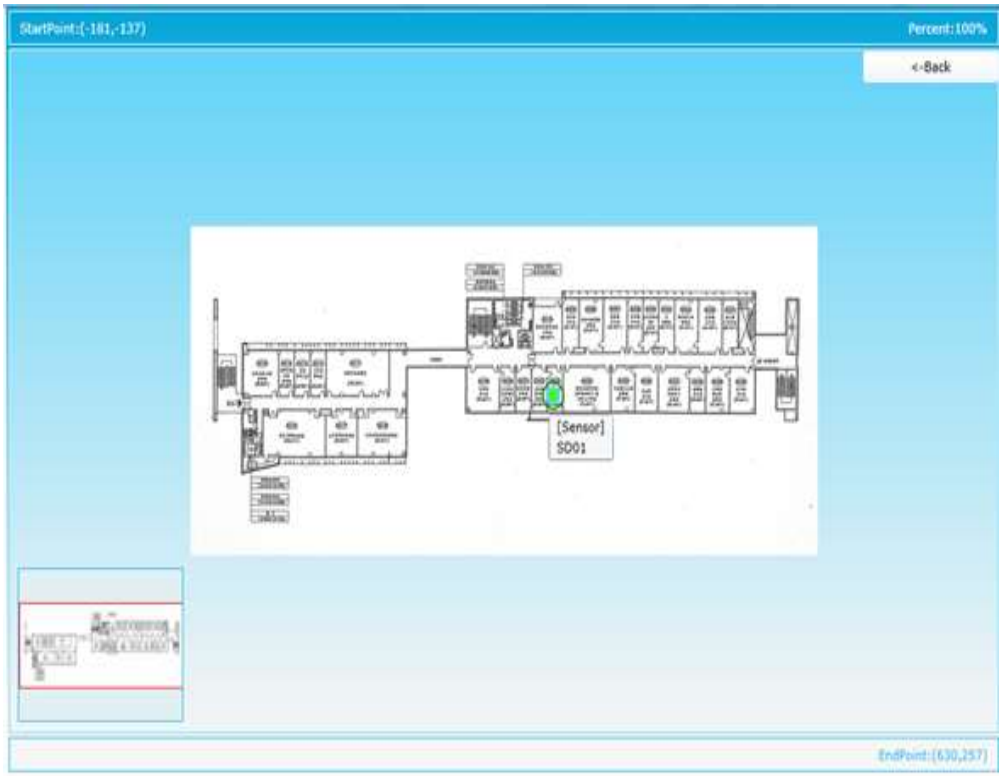

Figure 1. One Sensor and Two Actuators are Deployed In 4th Floor but Guest Group Users Are Allowed Only to View Sensor

5. Conclusion

Existing semantic IoT system is updated by incorporating user profile ontology to manage access to the system resources. The system can be used by different users having different roles (*i.e.* Admin, Contributor, Guest *etc.*) and every group user can have access to allowed system resources. We have incorporated user profile ontology into our semantic indoor IoT system and access management to the system resources is achieved via user profile ontology. Furthermore, this work can be instrumental in provisioning safeguard against security vulnerabilities as only authorized user can have access to designated resources. This work provides a base for future application of deep inferences on the users profile and access control information.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2015R1D1A1A01060493), and this research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2014-0-00743) supervised by the IITP (Institute for Information & communications Technology Promotion), Any correspondence related to this paper should be addressed to DoHyeun Kim.

References

[1] C. Bormann, A. P. Castellani and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes", IEEE Internet Computing, vol. 16, no. 2, **(2012)**, pp. 62-67.
[2] F. Tila and D. H. Kim, "Semantic IoT System for Indoor Environment Control–A Sparql and SQL based hybrid model", Advanced Science and Technology Letters, vol. 120, **(2015)**, pp. 678-683.
[3] N.F. Noy and D. L. McGuinness. "Ontology development 101: A guide to creating your first ontology", **(2001)**.
[4] M. Compton, P. Barnaghi, L. Bermudez, R.L. GarcíA-Castro, O. Corcho, S. Cox and J. Graybeal, "The SSN ontology of the W3C semantic sensor network incubator group", Web semantics: science, services and agents on the World Wide Web, vol. 17, **(2012)**, pp. 25-32.
[5] C. Bizer, T. Heath and T. Berners-Lee, "Linked data-the story so far", Semantic services, interoperability and web applications: emerging concepts, **(2009)**, pp. 205-227.
[6] P. Barnaghi and M. Presser. "Publishing linked sensor data", In Proceedings of the 3rd International Conference on Semantic Sensor Networks, CEUR-WS. Org., vol. 668, **(2010)**, pp. 1-16.
[7] J. Pschorr, C. A. Henson, H. K. Patni and A. P. Sheth, "Sensor discovery on linked data", **(2010)**.
[8] C. A. Henson, J. K. Pschorr, A. P. Sheth and K. Thirunarayan, "SemSOS: Semantic sensor observation service", In Collaborative Technologies and Systems, 2009. CTS'09. International Symposium on., IEEE, **(2009)**, pp. 44-53.
[9] W. Wang, S. De, R. Toenjes, E. Reetz and K. Moessner, "A comprehensive ontology for knowledge representation in the internet of things", In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on., IEEE, **(2012)**, pp. 1793-1798.
[10] K. Kotis and A. Katasonov, "An ontology for the automated deployment of applications in heterogeneous IoT environments", Semantic Web Journal (SWJ), **(2012)**.
[11] I. Toma, E. Simperl and G. Hench, "A joint roadmap for semantic technologies and the internet of things", In Proceedings of the Third STI Roadmapping Workshop, Crete, Greece, vol. 1, **(2009)**.
[12] H. S. Hamza, M. Maher, S. Alaa, A. Khattab, H. Ismail and K. Hosny, "Ontology for Semantic Enrichment of Radio Frequency Identification Systems", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 9, no. 10, **(2015)**, pp. 2251-2256.
[13] S. De, F. Carrez, E. Reetz, R. Tönjes and W. Wang, "Test-enabled architecture for IoT service creation and provisioning", In The Future Internet Assembly, Springer, Berlin, Heidelberg, **(2013)**, pp. 233-245.
[14] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. Van Kranenburg, S. Lange and S. Meissner, "Enabling things to talk", Springer-Verlag Berlin An, **(2016)**.
[15] D. Martin, M. Burstein, J. Hobbs, O. Lassila, D. McDermott, S. McIlraith and S. Narayanan, "OWL-S: Semantic markup for web services", W3C member submission22 **(2004)**, pp. 2007-04.
[16] World Wide Web Consortium, "The organization ontology", **(2014)**.

[17] H.-S. Choi and W.-S. Rhee, "IoT-based user-driven service modeling environment for a smart space management system", Sensors, vol. 14, no. 11, **(2014)**, pp. 22039-22064.

Authors

Israr Ullah, he received his MCS degree from Institute of Computing and Information Technology (ICIT), Gomal University, Pakistan, in 2004. He completed his M.S. in computer science from National University of Computer and Emerging Sciences (NUCES), Islamabad, Pakistan, in 2009. Currently, he is pursuing his Ph.D. studies at Computer Engineering Department, Jeju National University, Republic of Korea. His research work is focused on application of prediction and optimization algorithms to build IoT based solutions. His research interests also include analytical modeling, network simulation and analysis of optimization algorithms.

Faiza Tila, she received her B.Sc. degree in Computer Software Engineering from University of Engineering and technology, Pakistan in 2012. She joined the Mobile Computing Lab. at Jenu National University, South Korea and completed her Master in Computer Engineering in 2016. Her area of interest is semantic web technologies and Internet of things.

Do-Hyeun Kim, he received the B.S. degree in electronics engineering from the Kyungpook National University, Korea, in 1988, and the M.S. and Ph.D. degrees in information telecommunication the Kyungpook National University, Korea, in 1990 and 2000, respectively. He joined the Agency of Defense Development (ADD), from Match 1990 to April 1995. Since 2004, he has been with the Jeju National University, Korea, where he is currently a Professor of Department of Computer Engineering. From 2008 to 2009, he has been at the Queensland University of Technology, Australia, as a visiting researcher. His research interests include sensor networks, M2M/IOT, energy optimization and prediction, intelligent service, and mobile computing.

