International Journal of Smart Home
Vol. 9, No. 5 (2015), pp. 61-72
http://dx.doi.org/10.14257/ijsh.2015.9.5.07

User Privacy Framework for Web-of-Objects based Smart Home Services

Muhammad Ansar Latif[1], Farman Ullah[1], Hynwoo Lee[2], Won Ryu[2] and Sungchang Lee[1,*]

Department of Information & Communication, Korea Aerospace University, Korea
Department of Smart Screen Convergence Research, ETRI, Daejeon, South Korea
[*]sclee@kau.ac.kr

Abstract

This paper presents user privacy framework for web-of-objects based smart home services to control the release of personally identifiable information (PII) in smart home environment. The ubiquity of smart home enables smart home users and third parties to access home devices and data from any location at any time. The ubiquitous and pervasiveness improves the user comfort level, but also makes user PIIs highly prone to leakage. We propose Smart Home Web of Object User Privacy (SWOPR) architecture to protect and control the release of user PIIs according to the user consent. We suggest an architecture that integrates the RESTful framework, ISO/IEC-29101, and XACML/Ontology; the integration is not supported in existing systems. The SWOPR introduces Smart Home Web of Objects Privacy Controller (SWOPC) and Privacy Processor (SWOPP) nodes. SWOPC controls the process of collection of PIIs from users to the release of his PIIs to others. SWOPP provides PIIs processing functions such as anonymization and encryption under the control of SWOPC. The proposed privacy framework architecture is simple, lightweight and has high performance. We also present service scenarios to acquire the user PIIs, consents and release of PIIs to others.

Keywords*: User Privacy; Smart Home; Web of Objects; RESTful; Privacy Controller; Privacy Processor*

1. Introduction

The phrase smart home was first coined in the 1990s [1]. The next generation smart home environment will be ubiquitous, pervasive, and perceptual. The pervasive systems without user interaction support will not exist, and the system which is difficult to use, obtrusive and subject to risks, will not be used by users for their benefits [2]. Smart home embeds computing capabilities, networking and telecommunication interfaces in the home appliances in order to facilitate everyday life and to enable users to control their home devices from any location and at any time. The pervasive and ubiquitous smart home environment provides high-level interactivity to the smart home user and also to the service providers such as smart energy management, remote health monitoring etc., to provide intelligent services. Figure 1 shows a conceptual overview of the smart home environment and shows that home data and devices can be accessed through various devices and communication interfaces from any location and at any time. The smart home improves the comfort level of the people by acquiring different context information and the service providers use these contexts for various decisions to provide services. The contexts in smart homes are people-centric and contain user sensitive information and their acquisition and release raises the issues of privacy and security. The paper focuses on how to control the acquisition and release of user personal

ISSN: 1975-4094 IJSH

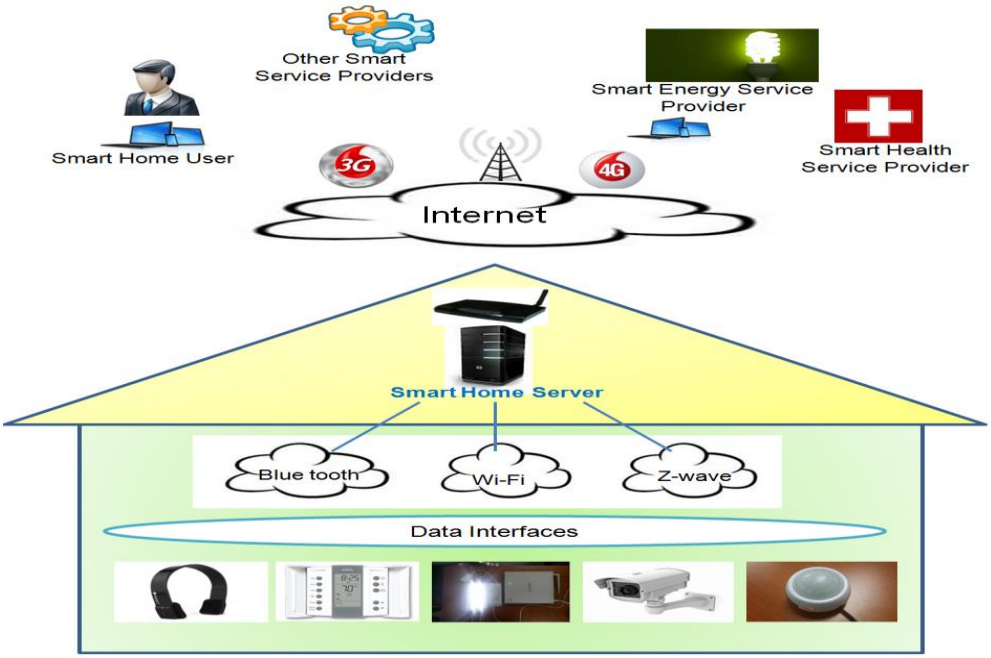

Figure 1. Smart Home Pervasive Environment

information to an SWO user, third party user, or even to any application program. In order to scrutinize and control the disclosure of sensitive information to inherently un-trusted parties in smart home environment, we present Smart Home Web of Objects Privacy (SWOPR) architecture.

Privacy is the right and the ability of individuals to exercise control over the collection, use, and disclosure of their personal identifiable information (PII) to other individuals. The PIIs can be biographical, biological, transactional, location or any other information that can be used for tracing or distinguishing the user identity [3]. The smart home user can take the benefits of various services such as smart home green environment, remote patient monitoring, smart energy control, etc., by providing consents about the release of his PIIs. In the Smart Home Web of Objects Privacy (SWOPR) architecture, we introduce the Privacy Controller (SWOPC) to collect the user PIIs data with other sensory data, the user privacy preferences, and consents about releasing user PIIs through a web interface. The introduced Smart Home Web of Objects Privacy Processor (SWOPP) will provide privacy functions such as anonymization of user data and encryption of user sensitive PIIs data under the control of SWOPC. The propose SWOPR framework ensures the PIIs of the users remain protected while releasing sensitive information in the smart home pervasive computing environment. The framework uses the RESTful URIs concept to acquire the smart home sensors data, including PIIs and consents of users.

In the smart home ubiquitous environment, the heterogeneous sensing devices and the services applications that use the sensor data often join or leave the network environment. Representational State Transfer (REST) [14] architecture style enables interoperability in Smart Home Web of Objects Architecture (SWOA). RESTful is flexible to equip more and more diverse heterogeneous devices, resources and communication protocols to improve user satisfaction [4]. The REST architecture leverages the integration of devices in the smart home environment and is more appropriate for resource-constrained, ad-hoc environments as it is a simple and flexible protocol that guarantees loose-coupling of resources [5]. REST architecture style based applications and services can coexist and interoperate with legacy systems such as SOAP-based interfaces. These properties of REST architecture style pose a challenge for dealing with privacy protection in a smart home environment. In the paper, we propose eXtensible Access Control Markup

Language (XACML) based policies to protect the user PIIs in the SWOA pervasive environment. XACML models promote a common language and interoperability between control implementation by various service providers [6]. In this paper, XACML represents smart home user privacy policies and its access control. The attributes associated with a smart home user or resource inputs into the decision point of XAMCL and evaluates whether a given user may access a given resource in a particular way. We use the Role-based Access Control (RBAC) model and also the semantic web ontologies to create fine granular access control mechanism for the smart home data access.

The rest of the paper is organized as follows: Section 2 is an overview the related work about smart home and privacy concerns in the pervasive ubiquitous environment. Section 3 introduces the smart home web of objects user privacy framework. The services scenarios based on the proposed framework are introduced in section 4. Finally, we conclude the paper in section 5.

2. Background and Related Works

The Smart Home and ubiquitous computing coined at the end of the 20th century [7] [8]. Jiang et al. [9] surveyed the smart home research and provided the definition of smart home and the smart devices. The reviewed research is mostly focused on the Bluetooth, Infrared and Radio frequency. At the beginning of the 21st century, projects have been launched at various research centers to introduce the concept of home networking of devices and equipment for a better quality of living. The Techno House in Japan provided an E-health care home system for elderly and disabled persons [10], the Georgia Research Alliance project of The Aware Home [11] addressed the challenges facing in the development of human activity recognition in the physical environment, and the Microsoft Easy Living [12] provided the prototype architecture for building intelligent environments that facilitate interaction of people with computers and devices making computing more accessible and pervasive. These systems, mostly focused on the internetworking of home devices, have very limited capabilities of accessing data outside of the home. In recent years, the focus of the smart home research is to merge the computing capabilities in every home physical device to enable it as part of the Internet of Things (IoT) and Web of Things (WoT). The web capabilities provide application layer support to build a flexible application and flexible services. Macro Aiello [13] proposed SOAP-based Web services architecture for the interaction of the heterogeneous devices in the smart home pervasive environment. In the smart home environment, the interaction, joining and leaving of devices and applications is so frequent that they need a light-weight protocol compared to SOAP, which uses a message envelope. The REST Web-based smart home services frameworks have been proposed due to its light-weight and resource-oriented architecture style [15, 16, 17]. Mostly these systems focused on the services oriented architecture and do not consider the user privacy. In the paper, we propose privacy aware smart home web of object architecture.

Privacy protection in pervasive environments is a major concern for users that has grown commensurately with the growth of Smart Home Environment. The multi-screen smart devices enable users to access data from anywhere and at any time [18]. Users have very dynamic and rich interactions with the smart home environment and as a consequence privacy concerns arise. In 2011, the International Organization for Standards and the International Electro-technical Commission (ISO/IEC) separated the security and privacy standards into two and introduced ISO/IEC-29000 to define common privacy terminologies, actors and their roles in the processing of PII [19]. The ISO/IEC-29101 [20] provided the architectural overview and components of the PIIs' collection and processing system. Bagues et al. [21] provided SOAP-based user centric smart home privacy framework to support users roaming freely in the smart home environment and focused on how a user can build up trust into inherently un-trusted services in ubiquitous environment. The mechanism of hiding power usage consumption because it may contain

sensitive information is provided in [22]. Efthymiou et al. [23] provided the anonymization algorithm to anonymize the frequent patterns in smart metering data. The work in [24] proposes a privacy framework for patients in Healthcare providers called SPOC that help patients in protecting and monitoring personal health information (PHI) in pervasive environment. SPOC processes and computes PHI during m-Health care emergency with minimal privacy disclosure. In this paper, we propose user consent and role-based access to the user PIIs.

In the last decade, the merging of computing and communication technologies changed the accessibility of physical devices. The Web enabled capabilities of the devices can overcome the limitation that the user has to be within boundaries of the smart home environment. The Web services can be categorized as Big Web services (WS-*) and RESTful Web Services [15]. REST has emerged as a predominant web service model that has mostly displaced WSDL-based interface design because it is considerably more simple to use [25]. Romero [3] proposed the architecture of home monitoring systems leveraging the REST architecture style to integrate multi-scale systems exhibiting heterogeneous communication capabilities and protocols to improve user satisfaction. Comparison of REST and SOAP for ubiquitous environments is presented and shows the REST architecture style services along with semantic web is flexible and scalable in such environments [17] [26]. In [27] architecture is developed on top of OSGi framework that embeds a semantic model of smart home system, achieving semantic interoperability and dynamic integration of highly heterogeneous devices and services. The access control policy gives smart home owners control over the way users can access their devices.

3. The Proposed Smart Home Web of Objects User Privacy Framework

In this section, we introduce the proposed Smart Home Web of Objects User Privacy (SWOPR) framework and its component details to protect the smart home user PIIs in the pervasive environment. The Web of Objects (WoO) is a layered approach that provides the interoperability between heterogeneous devices and enables the collection of data in a distributed environment from territory isolated devices. The Web capabilities in the physical devices enable smart home users and third party service providers to access any smart home devices from any location. The ubiquity of the smart home environment may lead to privacy breaches and leaks. In this paper, we propose a smart home privacy aware architecture by introducing the Smart Home Web of Objects Privacy Controller (SWOPC) and Smart Home Web of Objects Privacy Processor (SWOPP). We adopt the concept of ISO/IEC-29101 and the RFC 2753 [28] to ensure the protection of user PIIs in the smart home pervasive environment. The scope of the paper is that it briefly introduces the privacy framework in the WoO REST based smart home and a short introduction to smart home architecture. Figure 2 shows the proposed SWOPR framework architecture to protect the user PIIs and disclose information to other users and third party service providers with the consent of the SWO user. In the architecture, the devices are classified as legacy devices that do not have the web interface (support of HTTP and CoAP protocol) and SWO devices that have the HTTP or CoAP capabilities. We protect the user PIIs in the smart home environment by protected access; collect the user consents about his PIIs including the PIIs collected from sensors as context information such as user location, IP address etc. to disclose to other users. The

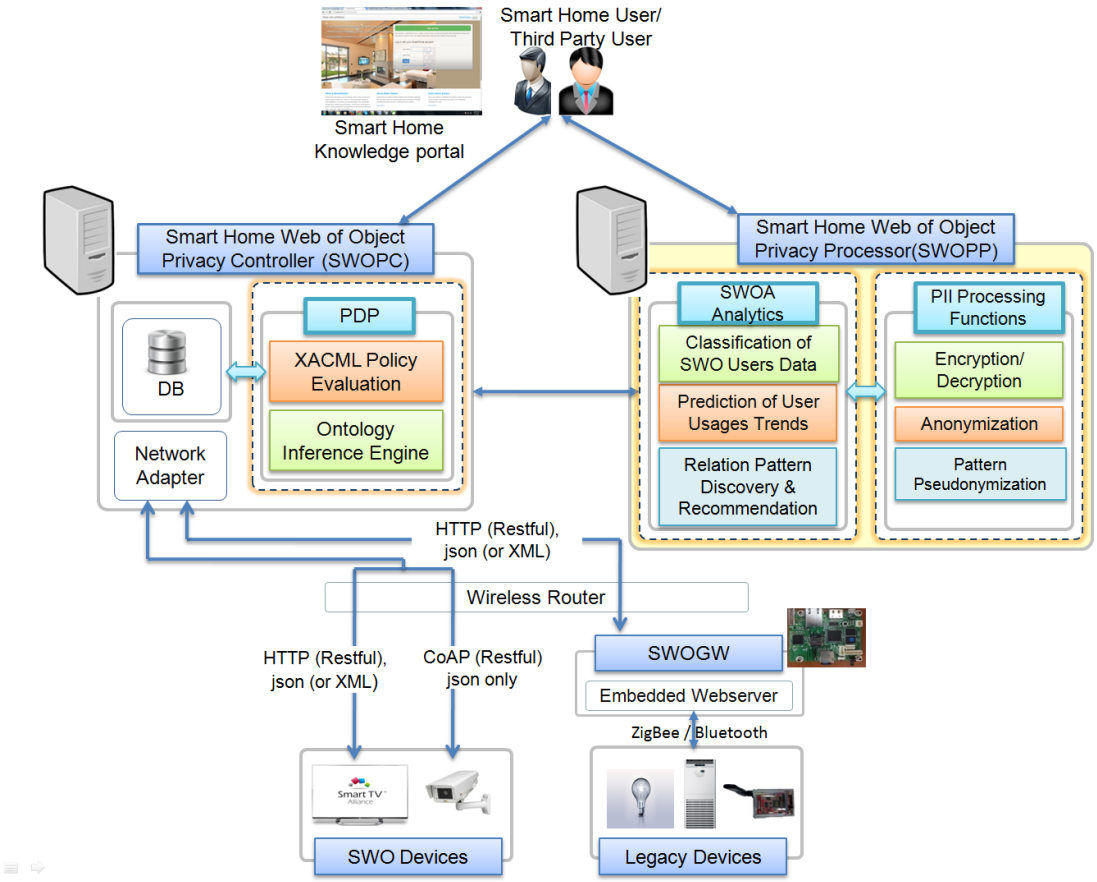

Figure 2. Smart Home Web of Objet User Privacy (SWOPR) Framework Architecture

Framework has been Developed using the Java RESTful Spring Framework, Aspect Oriented Programming, the XACML ALFA, and the SQL. We Will Briefly Explain the Introduced Components in the Following Subsections.

3.1 Smart Home Web of Objects User Privacy Controller (SWOPC)

The SWOPC acts as a central control unit to collect the user information (user data), the resource information (sensors data), its events/context data, the consents and policies etc., and to protect data from unwanted use. The SWOPC controls the data flow among users and the service providers in the smart home environment. Figure 3 shows the detailed architecture of the proposed SWOPC. The SWOPC provides a web based smart home knowledge portal to acquire the user information, resources/sensors registration and consents collection about the disclosure of user's PIIs to different service providers and other SWO users. The Policy Administration Point (PAP) provides the interface to generate, edit, or delete the policies (XACML policies) for various smart home services. In the paper, the proposed SWOPR evaluation manager provides the tools to evaluate and match the privacy policies according to the user provided consents.

The Policy Enforcement Point (PEP) receives the request from a third party user or other SWO users. The PEP converts the request in XACML and sends it to the Policy Evaluation Manger. The Policy Decision Point (PDP) in the evaluation manager evaluates the

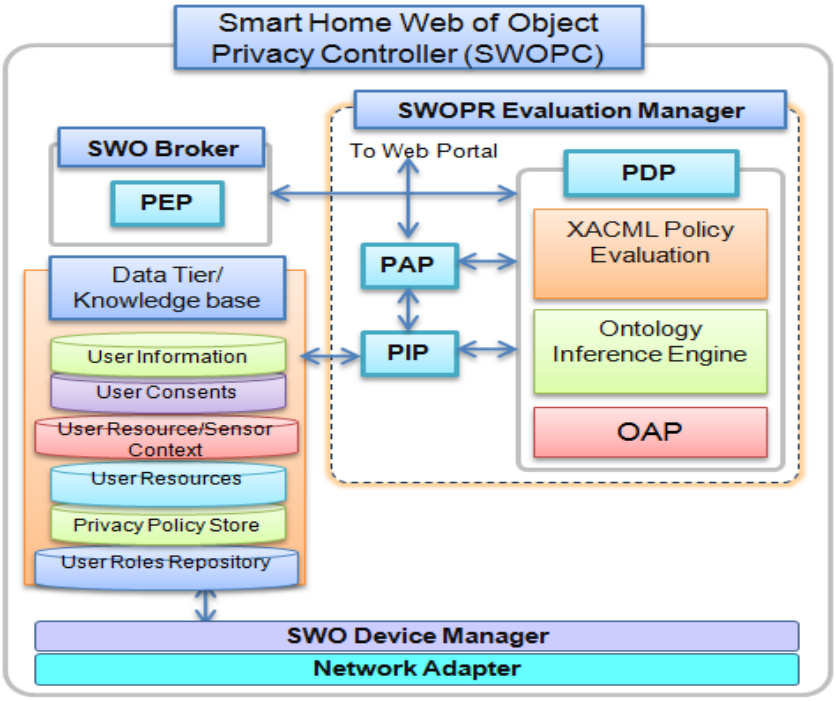

Figure 3. Smart Home Web of Objet User Privacy Controller (SWOPC)

request according to the privacy policies and the user consents, and sends a reply to the PEP which is either 'deny', 'permit' or 'permit with constraints'. If the response is 'permit with constraints', the PEP directs the Smart Home Web of Objects Privacy Processor to process the PIIs in the response message according to the constraints.

The Policy Information Point (PIP) provides the required information such as the user consents, user resources and their context, and user roles etc., required to PDP for policy evaluation. The PDP evaluates the policies and user consents obligations the XACML Policy evaluation engine, ontology inference engine and OAP.

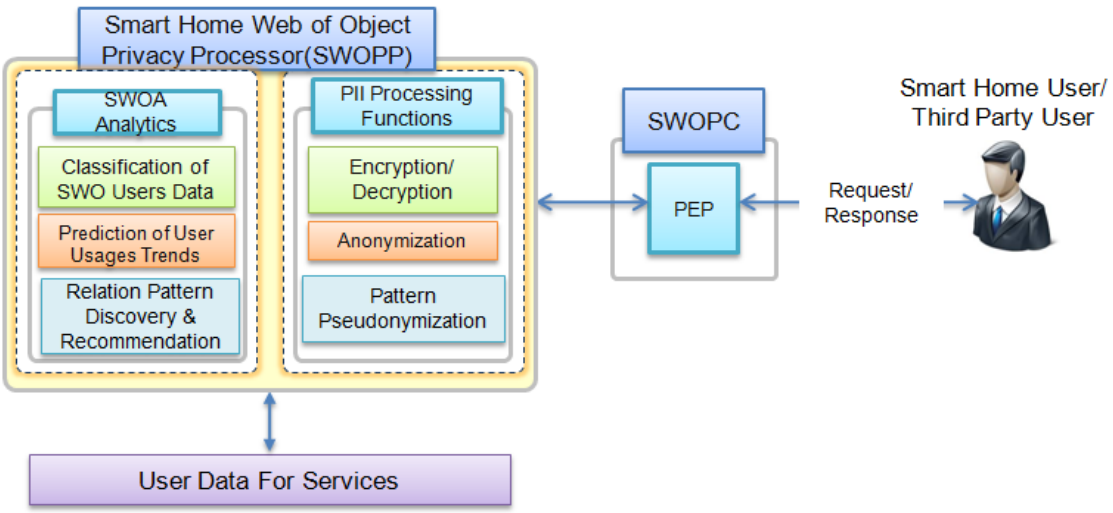

Figure 4. Smart Home Web of Objet User Privacy Processor (SWOPP)

3.2 Smart Home Web of Objects User Privacy Processor (SWOPP)

The Smart Home Web of Objects user Privacy Processor processes the user PIIs according to the permit constraint received from the PEP after the user request evaluation. Figure 4 shows a pictorial overview of the SWOPP architecture. The SWOPP will provide the privacy functions such as anonymization of user PII data, encryption of user sensitive PIIs, and Pattern pseudonymization. The user data request may include the sensitive PIIs data and needs to be protected during the transfer. We use the MD5 128bits to encrypt and decrypt the user sensitive PIIs to protect them during transferring.

The SWO user data may include usage patterns that could reveal the user identity. The pseudonymization scheme introduces arbitrary identifiers in the patterns so that it can be detected. The user request may include a data set of users, so we introduce a k-anonymity scheme to anonymize the users' identities. The SWOPP functions are not the scope of the paper, and we will provide the detail schemes in our future research.

4. The SWOPR Applications Services Scenarios

In this section, we introduce the application procedure from collection user PIIs and registration of devices & services to the disclosure of user PIIs to a third party (other SWO user or service provider). Figure 5 shows the procedure to register user's information, the

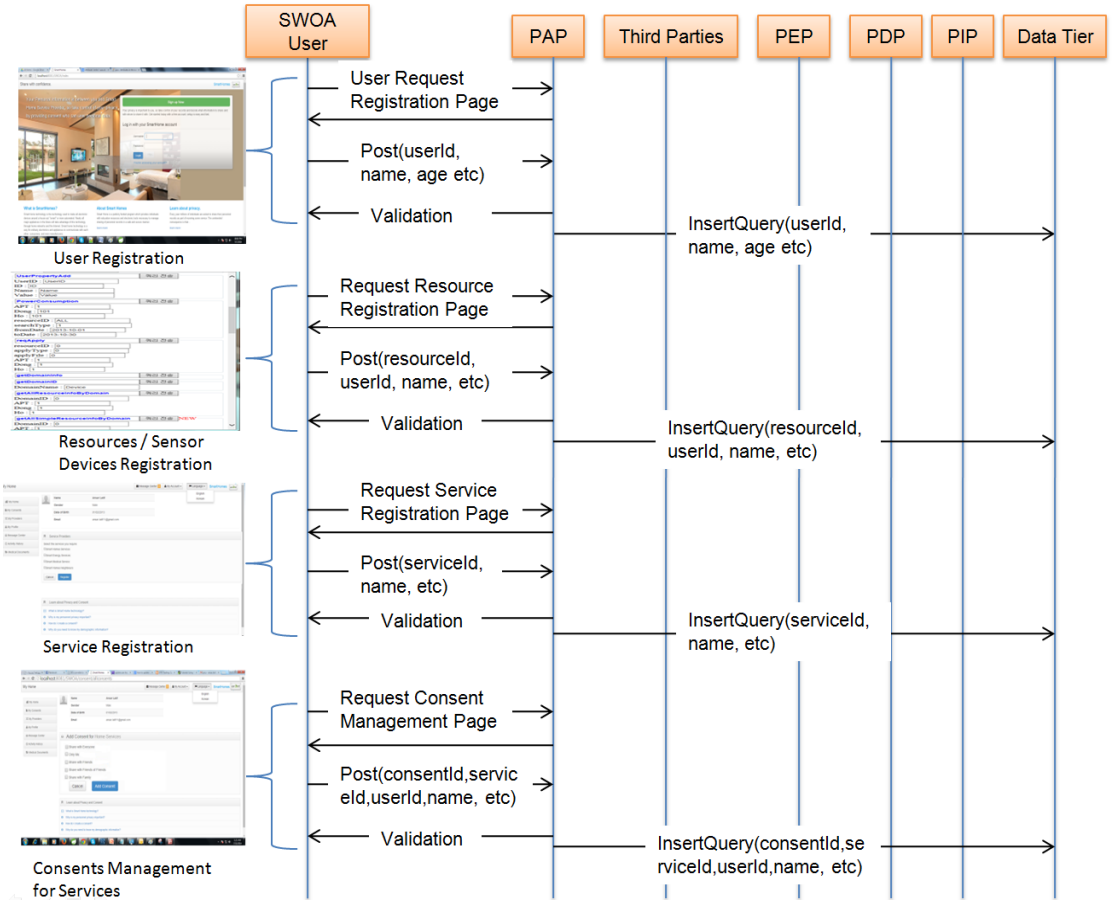

Figure 5. SWO User Profile, Devices/Sensors and Services Registration Procedure

smart home devices/sensors and the services (smart energy management, remote patient monitoring and smart green home). At the start, the user provides his basic information and creates an account. The user login to his account and provides his detailed information, the user registers all his smart home devices, and the user signs up for the services he wants. The user applies the privacy policies and consents about the disclosure of his PIIs to other users and services.

Figure 6 shows the procedure for making requests and for the disclosure of PIIs to a third party user. The third party user (SWO Service Provider) requests the SWO user data by sending a request to the PEP. The PEP intercepts the message and creates an XACML and sends it to the SWOPR evaluation manager to check whether the requested data is permitted to the user or not. The PDP evaluates the user request according to the privacy policies and user consents and obligations to either 'deny', 'permit' or 'permit with some constraints'.

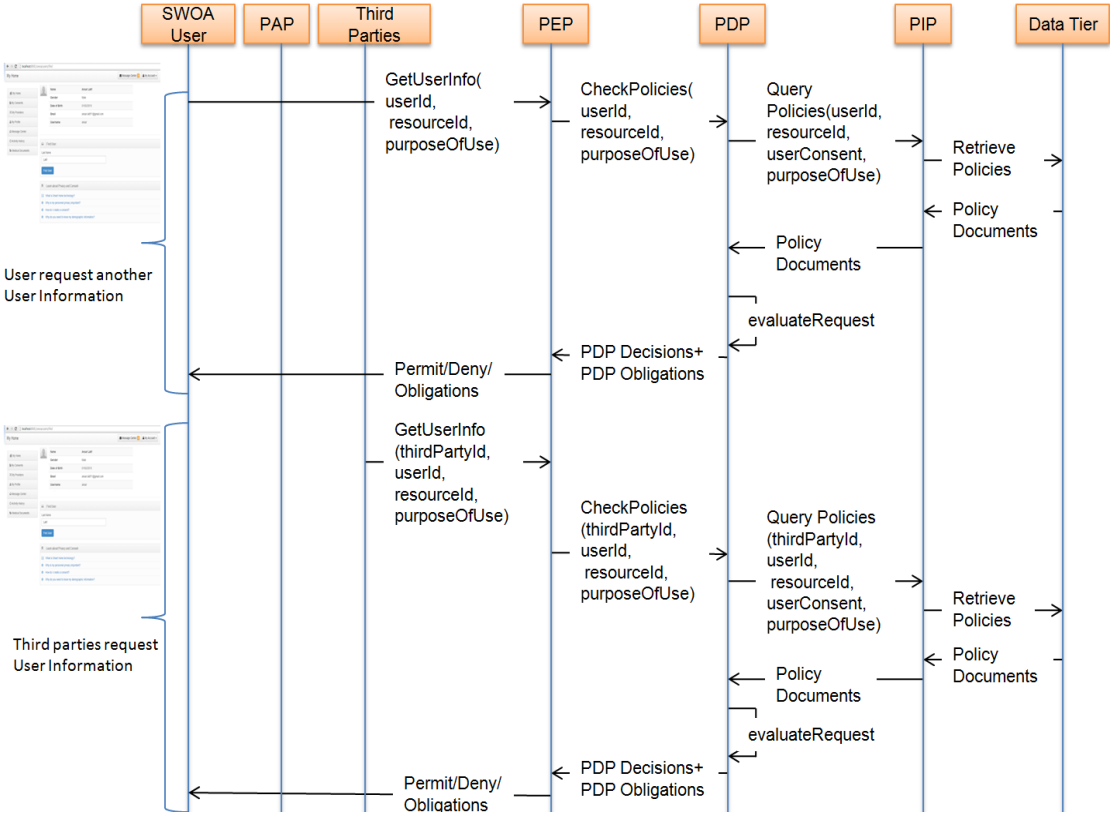

Figure 6. Third Party User Data Request and Disclosure of Data

5. Conclusion and Future Work

In this article, we present the Smart Home Web of Objects Privacy framework to control the collection and disclosure of user personally identifiable information to other user and third party service providers. The smart home pervasive environment, the web and computing capabilities of the physical devices on one side improves the comfort level of users, but on the other side it make the user more prone to having his identity revealed. This paper makes three main contributions. First, we provide a RESTful based Smart Home Web of Object architecture to control the user data and his resources/sensor information, to register for various smart home services, and to provide consents for the disclosure of his data to other users and service providers. Second, we introduce the Smart Home Web of Objects User Privacy Controller (SWOPC) to collect, control and protect the user data by applying various privacy policies; the Smart Home Web of Objects

Privacy Processor (SWOPP) to process the user PIIs according to the 'permit with constraint' received from the controller. The SWOPP provides the functions of encryption of user sensitive information, pseudonymization of the patterns in the user data such as electric/gas usage, and the anonymization of user identity in the data sets. The schemes of the SWOPP are not in the scope of this paper, and we will provide it in our future research. Third, SWOPR supports XACML and Ontology which provide fine grained privacy policies for evaluation at various levels of detail ranging from abstract to more specific. In our future research, we will provide a WoO based Semantic Ontology model for privacy protection in the Smart Home Environment. We also introduce the application service scenarios, from the collection of PIIs to the disclosure of PIIs to other and third party users.

Acknowledgement

This research is supported by the Korean Evaluation Institute of Industrial Technology (KEIT) funded by the Ministry of Trade, Industry and Energy (MOTIE, Korea) [Grant no. 10047233, Development of Smart Home Web of Objects Architecture.

References

[1] K.-K. Du, Z.-L. Wang, and M. Hong, "Human Machine Interactive System on Smart Home of Iot", The Journal of China Universities of Posts and Telecommunications 20, vol. 1, **(2013)**, pp. 96-99.
[2] G. Pallapa, S. K. Das, "Adaptive and context-aware privacy preservation exploiting user interactions in smart environment", Pervasive and Mobile Computing, vol. 12, **(2014)**, pp. 232-243.
[3] Guide to Protecting the Confidentiality of Personal Identifiable Information, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
[4] D. Romero, "RESTful integration of heterogeneous devices in pervasive environments", Distributed Applications and Interoperable Systems. Springer Berlin Heidelberg, **(2010)**.
[5] A. Taherkordi, F. Eliassen, **(2011)**, "Restful service development for resource-constrained environments", REST: From Research to Practice, pp. 221-236.
[6] S. Godik, A. Anderson **(2002)**, "OASIS eXtensible access control 2 markup language (XACML) 3", Tech. rep., OASIS.
[7] M. Brezovan, "An Overview of Smart Home Environments: Architectures, Technologies and Applications".
[8] M.. Weiser, "Some computer science issues in ubiquitous computing", ACM SIGMOBILE Mobile Computing and Communications Review, vol. 3, no. 3, **(1999)**, pp. 12.
[9] L. Jiang, D.-Y. Liu, "Smart home research", Proceedings of the Third Conference on Machine Learning and Cybernetics SHANGHAI, **(2004)**.
[10] T. Tamura, "E-healthcare at an experimental welfare techno house in Japan", The open medical informatics journal, vol. 1, **(2007)**.
[11] C. D. Kidd, "The aware home: A living laboratory for ubiquitous computing research", Cooperative buildings. Integrating information, organizations, and architecture, Springer Berlin Heidelberg, **(1999)**, pp. 191-198.
[12] S. Shafer, "The new easyliving project at microsoft research", Proceedings of the 1998 DARPA/NIST Smart Spaces Workshop, **(1998)**.
[13] M. Aiello, "The Role ofWeb Services at Home", Telecommunications, 2006. AICT-ICIW'06. International Conference on Internet and Web Applications and Services/Advanced International Conference on, IEEE, **(2006)**.
[14] R. T. Fielding, "Architectural styles and the design of network-based software architectures", University of California, Irvine, **(2000)**.
[15] A. Kamilaris, V. Trifa, "HomeWeb: An application framework for Web-based smart homes. Telecommunications (ICT)", 2011 18th International Conference on, IEEE, **(2011)**.
[16] M. Gray and P. Scherer, "Web Services Framework for Wireless Sensor Networks", SERVICE COMPUTATION 2014, The Sixth International Conferences on Advanced Service Computing, **(2014)**.
[17] I Mashal, O. Alsaryrah, "Choices for interaction with things on Internet and underlying issues", Ad Hoc Networks.
[18] J. W. Kim, "Dynamic addition and deletion of device in N-screen environment", Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on. IEEE, **(2012)**.
[19] ISO/IEC 29100, "Information Technology—Security Techniques—Privacy Framework ", international report, ISO/IEC standardization (ISO) JTC 1/SC 27, **(2011)**.

[20] ISO/IEC 29101 (2013). "Information Technology—Security Techniques—Privacy Architure Framework ", international report, ISO/IEC standardization (ISO) JTC 1/SC 27.
[21] S. A. Bagüés, "Sentry@ Home-Leveraging the smart home for privacy in pervasive computing", International Journal of Smart Home, vol. 1, no. 2, **(2007)**, pp. 129-145.
[22] K. Ohara, "Privacy-preserving smart metering with verifiability for both billing and energy management", Proceedings of the 2nd ACM workshop on ASIA public-key cryptography. ACM, **(2014)**.
[23] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data", Smart Grid Communications (SmartGridComm), First IEEE International Conference on. IEEE, **(2010)**.
[24] R. Lu, X. Lin and X. Shen., "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency", Parallel and Distributed Systems, IEEE Transactions, vol. 24, no. 3, **(2013)**, pp. 614-624.
[25] G. Mulligan and D. Gracanin, "A comparison of SOAP and REST implementations of a service based interaction independence middleware framework", Simulation Conference (WSC), Proceedings of the 2009 Winter. IEEE, **(2009)**.
[26] Y. Liu and K. Connelly, "Realizing an open ubiquitous environment in a restful way", Web Services, 2008. ICWS'08. IEEE International Conference on. IEEE, **(2008)**.
[27] J. E. Kim, "Seamless integration of heterogeneous devices and access control in smart homes", Intelligent Environments (IE), 2012 8th International Conference on. IEEE, **(2012)**.
[28] R. Yavatkar, D. Pendarakis and R. Guerin, "A framework for policy-based admission control", **(2000)**, vol. 1.

Authors

Muhammad Ansar Latif, he received his BS degree from Ghulam Ishaq Khan Institute Topi, Swabi, KPK, Pakistan in 2012. From 2012 to 2013, he joined Digital Spinners Pvt Ltd Islamabad, as Software Engineer. From 2013 to 2014, he was System Maintenance Engineer at Zong HQ, Islamabad, Pakistan. Since 2014, he has joined as graduate student Korea Aerospace University, Goyang, Korea.

Farman Ullah, he did his BSc (2006) in Computer Systems Engineering from University of Engineering and Technology, Peshawar, Pakistan and his MSc (Fall, 2010) in Computer Engineering from Center for Advanced Studies in Engineering, Islamabad, Pakistan. He worked as Telemetry Engineer at Advanced Engineering Research Organization, Pakistan from 2007 to 2011. He is on study leave from COMSATS Institute of Information technology, Attock Pakistan and pursuing his PhD from Korea Aerospace University, South Korea .

Hyunwoo Lee, he received his BS degree in electronics engineering from Hankuk Aviation University, Kyonggi, Rep. of Korea, in 1993 and his MS and PhD degrees in communication and information engineering from Hankuk Aviation University, Kyonggi, Rep. of Korea, in 1995 and 2005. Since 1995, he has been working as a senior researcher in the Broadband Convergence Network Interworking Laboratory, ETRI, Daejeon, Rep. of Korea. He is currently working as the director of the Media Networking Research Section, ETRI.

Won Ryu, he received his BS degree in computer science and statistics from Pusan National University, Busan, Rep. of Korea, in 1983 and his MS degree in computer science and statistics from Seoul National University, Seoul, Rep. of Korea, in 1988. He received his PhD degree in information engineering from Sungkyunkwan University, Kyonggi, Rep. of Korea, in 2000. He is currently working as a Managing Director of the Intelligent Convergence Media Research Department, ETRI.

Sungchang Lee, he received his BS degree from the Kyungpook National University in 1983, received M.S. degree in Electrical Engineering from KAIST (Korea Advanced Institute of Science and Technology) in 1985, and received Ph.D. degree in Electrical Engineering from Texas A&M University in 1991. From 1985 to 1987, he joined KAIST as researcher, where he worked on Image Processing and Pattern Recognition projects. From 1992 to 1993, he was Senior Researcher in ETRI (Electronics and Telecommunications Research Institute), Korea. Since 1993, he has joined the faculty at Korea Aerospace University, Goyang, Korea where he is currently a Professor and School Head in School of Electronics, Telecommunication & Computer Engineering. During 2004-2009, he was the Director of government Project on Intelligent Smart Home Security & Automation Service Technology. In 2009, he was the vice President of IEIE (The Institute of Electronic and Information Engineers), Korea as the Director of Telecommunications Society.