AASCIT Communications
Volume 2, Issue 3
April 30, 2015 online
ISSN: 2375-3803

American Association for Science and Technology

N-PAC: Privacy-Aware Access Control with Negotiation Process in the coming Ubiquitous Environments

Hyun-A Park Digital Contents Research Center, Konkuk University, 120 Neungdong-ro, Gwangjin-gu, Seoul, Korea

June Young Ahn Digital Contents Research Center, Konkuk University, 120 Neungdong-ro, Gwangjin-gu, Seoul, Korea

Keywords

Privacy, Personal Information, Self-Determination, Self-Control, Negotiation, Encryption, Daily Life Service

Although future computing technologies have been rapidly developed and it has provided diverse social services to users, there are ongoing issues for users in safety. This paper deals with the privacy problems in future-centric computing environments. In daily life, as users are increasingly participating in various social contexts, some researchers have developed a facility to commence daily life service with wearable computing technologies. This makes it possible for users to store all their daily events or the collected data using their devices. These data can be shared with other people or some service providers only if the user agrees. However, the problem is that there are some potential risks about privacy in the cases of inter-domain web service usage or sharing their data with others. As the solution, the authors propose a new method, privacy-aware access control through negotiation process (N-PAC). This method enables a user to accomplish self-determination and self-control of personal information in the coming ubiquitous computing environments.

Introduction

The Ubiquitous Computing Environments is forthcoming. The environments can be represented as "5 ANYs - anyone, anytime, anywhere, anynetwork, anydevice". Ubiquitous Computing Technologies require that all of the computers, computerized devices, and sensors are connected through Internet or wireless/wired networks. People can use invisibly embedded or incorporated technologies within their own real life without any limitations over time and space. These kinds of technologies enable people to realize their ideas by sharing or taking advantage of their various resources through connected networks. Dailylifeservice is one of the most representative trends to show how people achieve their ideal thoughts in reality by collaborative computing technologies. However, there are still some problems including security and privacy in the mass-market-scale ubiquitous services and applications. To find the solutions for these problems, some researchers have worked daily life service with wearable computing technologies.

In daily life, as users are increasingly participating in various social contexts, the researchers have tried to develop a facility to communicate, to share items and to manage today's complex lifestyles. This makes it possible for users to store all their daily events or collect data using their devices, for example, SMS, photos, call, movie, e-commerce information, web service log and usage information, location information, documents, media, battery charge, personal schedule, and so on. This kind of system deals with a personal lifetime store and it considers every digital media and data. Through the internet, the stored data are transferred to each user's personal database, and stored and managed as a personal history with the passage of time. The data can be shared with other people or some service providers, only if the user wants.

Here is the problem; keeping the connection with networks all day long and storing all their events mean that users are always monitored and exposed to others over the networks. Especially, in the cases of inter-domain web service usages or sharing their data with others, there are some potential risks about privacy. A server manager or unauthorized accesses can

abuse or misuse the data in their personal devices or personal database without users' consents. In this paper, the solution for these problems is proposed as privacy-aware access control through negotiation process (N-PAC). With this method, users can achieve self-determination and self-control of personal information in the coming ubiquitous computing environments. The application is the architecture designed by the previous MobiLife project's service which is connected to wearable computing researches of todays.

Related Work and Contribution

In a variety of perspectives, many works for privacy preserving techniques in data management system have been researched. P3P(Platform for Privacy Preferences), was developed by W3C(World Wide Web Consortium), provides a way for a web site to encode its data-collection practices in a XML format known as a P3P policy [17]. It provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personal information but it does not provide a mechanism to make sure sites act according to their stated policies. Hippocratic databases was introduced as systems that integrates privacy protection within relational database systems [1]. A Hippocratic database uses privacy metadata which consist of privacy policies and privacy authorizations stored in two tables. The policies and authorizations associate with each attribute and each user the usage purpose(s).

In purpose-based access control by Byun et al. [4, 5], they proposed an access control model for privacy protection based on the notion of purpose. They defined purpose and introduced the concepts of intended purpose and access purpose. They proposed a method for determining access purposes, which uses the notions of role attributes and conditional roles. However, purpose management introduces a great deal of complexity at the access control level. In another aspect, [16] introduced an alternative privacy access control mechanism that is not based on purpose. It defined the intended purpose of personal information as a chain of acts on this type of information. The chain represents a syntactical form of controlling access (acts in general) to personal information.

Mun et al. [14] provided policy-based access control mechanism for the personal information directory system. The proposed person-wise access control model allows the information subjects to control access to their own information according to their policy. The model takes the strategy to encrypt each attribute for each individual with different keys and to endow the decryption keys for the allowed attributes to the information users according to the information subjects' policy.

As for privacy policy negotiation, Hatakeyama and Gomi [11] introduced a means for providers to be able to confirm privacy policies before an attributes exchange takes place and to determine what kinds of attributes to exchange and how to manage these attributes. In other papers related to privacy policy negotiation, [8] extends the previous session level data privacy methods by adding transaction level data privacy. The method generates session privacy policy based on the provider's and consumer's privacy preferences in distributed environments.

In almost all of the previous papers, access control rules are setup based on purpose, intent, or policy at first time. However, the data for some goal can be used for other purpose. They cannot cover all the cases and had many difficulties for users to make a self-determination or self-control of their personal data. Even if it has negotiation or dynamic process, it is too abstract and conceptual.

In this paper, the authors take the application with daily life service for future computing environments. Based on this service, the authors accomplish privacy-aware access control by adding negotiation protocol and encrypting data under the classified level. PAAC (privacy aware access controller) is introduced as a kind of TTP, so that all the accesses to user's information should pass through PAAC. Negotiation is also processed by PAAC.

Moreover, these properties enable our proposed method N-PAC (Privacy-Aware Access Control through Negotiation) to make self- determination and self-control of personal data.

Application Scenarios

In this section, the application scenario is addressed as daily life services such as MobiLife project. The projects about daily life services are succeed to wearable computing technologies of these days. The application, MobiLife Integrated Project in IST-FP6 (September 2004-December 2006) was to bring advances in mobile applications and services within the reach of users in their daily life by innovating and deploying new applications and services based on the evolving capabilities of the 3G systems and beyond. The project addressed the problems related to different end-user devices, available communication networks, interaction modes, applications and services with a strong user-centric view [18].

The privacy problems caused by the services are the authors' main concerns. Especially, in this paper, the authors model the solution using MobiLife service as the application scenario. The architecture of MobiLife is as follows [20].

- Privacy and Trust Function (PTF)
  - Ensuring privacy and trust through specifying a Trust Engine and defining privacy policies, including Storage/Management
  - Inspects every interaction involving user data and allows or denies the access to the data based on the specified policies
- Personalization Function (PF)
  - Profile Manager with well-defined interfaces to manage user and group-related profiles and preferences
  - Enables adaptation of mobile services and applications according to personal and group needs and interests
  - Service-specific user/group profiles can be created manually or via profile learning (part of CAF Reasoning Function)
  - Profiles are the basis for building sophisticated, service specific recommender systems
- Context Awareness Function (CAF)
  - Handles raw, interpreted and aggregated context data
  - Context Management Framework (CMF), Personal/Group Context Function (PCF/GCF), Reasoning Function (RF)
  - Context Management Framework (CMF):
    - Defines representation, exchange, interpretation and reasoning of raw context data from various sources
    - Determines the situation of a user and/or a group entity
- User Interface Adaptation Function (UIAF)
  - Make services available through multiple devices and modalities
  - Device Gateway Function (DeGan): Handles devices and capabilities
  - Device and Modality Function (DeaMon): Fusion of user input and fission of application output, content adaptation features
- Group Awareness Function (GAF)
  - Group Management Function: Management of group lifecycle aspects
  - Group Evolution System: Automatic creation and deletion of groups
- Service Provisioning Function (SPF)
  - Stores service information: description, properties, semantics, etc
  - Management of user-service profiles
  - Advertises applications proactively to users/groups, without any user/group request or interaction
- Service Usage Function (SUF)
  - Service Discovery, Service Composition and Service Execution
- Operational Management Function (OMF)
  - Performs operational management of applications and service, and related configuration of resources
  - Covers data collection processes

The Construction of N-PAC (Privacy-Aware Access Control Through Negotiation)

- The parts which relates privacy in MobiLife are Privacy and Trust Function (PTF) and Personalization Function (PF). The construction of N-PAC (Privacy-Aware Access Control through Negotiation) is for accomplishing these functions.

The Components of N-PAC

N-PAC has four main parties as follows;.

MA (Mobile user agent). Instead of a user, a mobile user agent does everything related to daily life using their mobile phone.

PAAC (Privacy-Aware Access Controller). PAAC is a kind of TTP (Third Trust Party) and protects users' privacy. This manages users' secret keys, implements encryption and decryption of users' data, registers users' privacy policies, and evaluates and negotiates users' privacy policies with service providers'/ PIR ' policies.

SP (Service provider)/ PIR (personal information requestor). This party requires disclosing of users' data for enabling web services or sharing users' data. It negotiates privacy polices with PAAC.

PDM (Personal database manager). As a kind of semi-trusted party, PDM just manages personal database and implements PAAC's requests.

The Processes of N-PAC

Registration

All data are classified into 4-levels;

- Level 1: Not sensitive data. These data don't need to be encrypted.
- Level 2: Sensitive data. These data need to be encrypted but not to be negotiated by PAAC.
- Level 3: High sensitive data. These data need to be encrypted and negotiated by PAAC.
- Level 4: Top secret. These data should be encrypted only by user's secret key so that only the user can request and decrypt them. These data should not be negotiated and disclosed.

All mobile users register their privacy policies on each service to PAAC in advance. A user can determine which attributes can be disclosed. For this, one of the above 4-levels is assigned to all attributes of each table.

But, this process is provided as option. It means that there are two choices. One is that a user can choose what he wants by himself. The other is that a user can follow in advance setup classification under EU guideline or some other privacy rules. It can be updated and added as needed.

PAAC should keep each user's policy table like Table 1, where T_i means the table for service i and A_{ij} means j-th attribute of service i. If each table T_i has its attributes A_{ij}, it is expressed as: $T_i=(A_{i1}, A_{i2}, A_{i3,\ldots}, A_{ij})$

Table 1. *Policy Table of User_1*

	Level 1	Level 2	Level 3	Level 4
T_1 (service 1)	A_{11} A_{12}, A_{16}	A_{13}, A_{15}	A_{14}	A_{17}
T_2 (service 2)	A_{23}, A_{26}	A_{21}	A_{22}, A_{25}	A_{24}
……..	……..	……..	……..	……..

Data Processing

According to a user's policy, MA encrypts the data belonging to level 2, 3, and 4. In N-PAC, there are two kinds of keys, K_2 and K_3. K_2 is the shared key between a user and PACC in advance. K_3 is the key generated by a user. We explain the encryption method as one example with T_1 (service 1) in Table 1. E means efficient encryption function and D means efficient decryption function.

- Level 1: Let these data be in plaintexts.
- Level 2: $E_{k2}(A_{13})$, $E_{k2}(A_{15})$
- Level 3: $E_{k2}(E_{k3}(A_{14}))$
- Level 4: $E_{k3}(A_{17})$

The data stored in MDB are transferred to PDB through wireless network once a day or by certain period. All data of a user are stored in PDB (personal database, Lifeblog) time by time, and day by day, i.e., according to the order of time.

Privacy Policy Evaluation

When a user wants to be provided with something from different domain service or a PIR requests to share with the user's data, at first PAAC evaluates a user's privacy policies with SP or PIR's privacy policies. For more simple explanation, we consider just the case of SP. The following 3 conditions can be expected;

$$\bigcup P_{SP\_T_i} \subseteq P_{MA\_T_i\_L_1} \cup P_{MA\_T_i\_L_2} \quad (1)$$

If the condition satisfies with this formula, then PAAC implements Action Process, where P_{SP_Ti} is service provider's privacy policy on service table T_i. $\bigcup P_{SP\_T_i}$ means all the attributes which a SP wants to be disclosed on the user's data T_i. P_{MA} is mobile user agent's privacy policy and $P_{MA\_T_i\_L_1}$ means the attributes which a mobile user agent wants to be in plaintexts on service table Ti. Therefore, the above formula means that all the data which a service provider wants to share with on service table T_i are included to the disclosing attributes without negotiation process. This time, in Final Process, PAAC needs to decrypt the attributes of L_2 and replies with the attributes of L_1 and the decrypted attributes of L_2.

From next, the conditions are $\bigcup P_{SP\_T_i} \not\subset P_{MA\_T_i\_L_1} \cup P_{MA\_T_i\_L_2}$.

$$P_{SP\_T_i} \subseteq P_{MA\_T_i\_L_3} \quad (2)$$

This condition is that some attributes which a SP wants to know belong to the user's attributes of *Level 3*. Then, PAAC starts to implement Negotiation Process.

$$P_{SP\_T_i} \subseteq P_{MA\_T_i\_L_4} \quad (3)$$

This condition is that some attributes which a SP wants to know belong to the user's attributes of Level 4. Then, PAAC sends the message that the attributes cannot be disclosed, to the SP. If the SP accepts this message under the user's policy, PAAC starts Action Process. If not, the access trial is over.

Negotiation Process

If the privacy policy evaluation satisfies with condition 2, PAAC gets to start Privacy Policy Negotiation Process.

1. PACC sends the message that the attributes cannot be disclosed to the SP.
2. If the SP accepts this acknowledgement under the user's policy, PAAC starts Action Process.
3. If the SP rejects this, then PAAC sends this message that the SP wants to know the attributes of *Level 3* for a service T_i to the MA.
4. If the MA rejects this acknowledgement under the SP's policy, the access trial is over.
5. If the MA accepts, MA replies to PAAC as "Yes".
6. Then, PAAC requests the attributes to PDM (personal database management) and decrypts the received data of *Level 3* from PDM with the shared key K_2; $D_{k2}(E_{k2}(E_{k3}(A_4)))= (E_{k3}(A_4))$
7. PAAC resends the half decrypted data $E_{k3}(A_4)$ to MA.
8. MA decrypts the data again with K_3 and sends it to PAAC; $D_{k3}(E_{k3}(A_4))= A_4$

9. PAAC starts Action Process.

Final Process

In this process, PAAC implements the final results.

In the case of condition 1, PAAC requests the attributes of $\bigcup P_{SP\_T_i}$ to PDM and decrypts the attributes of L_2; $D_{k2}(E_{k2}(A_3))= A_3$, $D_{k2}(E_{k2}(A_5)) = A_5$. Then, PAAC provides the SP with the user's data which belong to *Level 1* and *2* and the user can be offered something from the SP.

In the case that SP accepts a user's policy in condition 3 or after negotiation process, PAAC provides the SP with the finally selected attributes. Thereafter, the user can be offered something from the SP.

Discussion and Analysis About Privacy

The right of informational self-control is merging with the right of self-determination to a new meaning of freedom, keeping abreast with the trend that more and more of personal belongings are stored in persistent media. The most important thing is that the decision whether we would like to share personal information with others is up to us. If we do not want to reveal personal data, we do not have to. If we wish to remain anonymous, we should be capable of doing so. We should not be observed if we have the desire to be. Considering the rising amount of network-computing, it should be realized that we all have to take measures to enforce our human rights [21].

One of the most important properties of the method N-PAC is self-determination and self-control of personal information. One of the 4 levels for each information is selected by the user himself. According to the classified level, the different encryption module is applied with 2 kinds of keys. But, the data of *level 1* don't need to be encrypted. Because of this different encryption module, even PAAC cannot negotiate or disclose on its own authority. Negotiation is only allowed to level 3 data. Only under user's consent, it is also possible to release data through negotiation because the data are encrypted twice with K_2 and K_3. K_3 is the key which the user only knows and PAAC does not know. The data of level 4 must not be disclosed by no means so they are encrypted with K_3.

Some people may wonder about why we encrypt Level 2 data with two keys K_2 and K_3. It is for preventing others' impersonalization attack. The malicious PDM or attacker can masquerades as PAAC. In the 5^{th} step of negotiation process, if MA accepts, PAAC will implement the 6^{th}, 7^{th} steps. This time, if Level 2 data are encrypted with only the key K_3, MA cannot know who sends $E_{k3}(A_4)$. But, in our negotiation process, Level 2 data are encrypted twice with K_2 and K_3. Even if a malicious attacker tries to masquerade as PAAC, he cannot generate the valid value of $E_{k3}(A_4)$ in the 6^{th} step because he cannot know K_2.

Another specialty of this paper is PAAC as a kind of TTP. All accesses into users' data should pass through PAAC. PDM only has to manage and implement the requests from PAAC. The decryption processes never happen in PDM because PDM does not know any of the encryption keys. Decryption is possible only by the user or PAAC. It can prevent PDM or an external attacker from misusing or abusing users' data. PAAC is an intermediary between a user and a SP/PIR in negotiation process. This privacy policy negotiation process enables users to determine and control their personal information by themselves.

Conclusion

In this paper, the authors highlight the privacy and security problems in the forthcoming daily life services. This paper reminds us the potential risks of privacy in Ubiquitous Computing Environments which are connected through Internet or wireless/wired networks to all of the computers, computerized devices, sensors and so on. The proposed Negotiation Process makes us realize the importance of Privacy-Awareness. Through the whole processes, users can accomplish self-determination and self-control of their information. Finally, N-PAC enables users' data protection to accomplish FIPs (fair information practices).

However, this paper only considers partly approaches with separate concentrations in the application and independent technologies – such as access control, negotiation technology - for coming ubiquitous computing era. Hence, there are limitations and huge challenges to prevent higher risks for users' security and privacy in future computing applications and technologies. Therefore, the security and privacy problems in ubiquitous computing environments also should be managed as an integrated system.

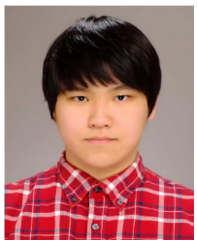
Acknowledgments

This research was supported by the Ministry of Trade, Industry and Energy(MOTIE), KOREA, through the Education Support program for Creative and Industrial Convergence.■

Biography

Hyun-A Park

She received the BS degree from the Department of Mathematics at Korea University, Seoul, in 2003, and the MS and PhD degrees in information security from Korea University, Seoul, in 2005 and 2010, respectively. Currently, she is a researcher with the DCRC at the Konkuk University. Her main research interests include practical retrieval system on encrypted database systems. She is interested in database security, access control, privacy preserving in data mining (PPDM), anonymous communication channel, privacy enhancing technology (PET), and cryptographic protocols.
E-mail: kokokzi@naver.com



June Young Ahn

He is with HCI LAB at Konkuk University in Korea as a master course student. His main research interest is Wearable Computing, HCI (Human-Compuyer Interaction), HAI (Human-Animal Interaction).
E-mail: secpet0305@gmail.com

References

[1] Agrawal, R. Kiernan, J. Srikant, R. and Xu. Y. (2002). Hippocratic databases. In The 28th International Conference on Very Large Databases (VLDB), Hong Kong, China, August.

[2] C.A. Ardagna, E. Damiani, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati. The architecture of a privacy-aware access control decision component. In Proc. of the Construction and Analysis of Safe, Secure and Interoperable Smart devices (CASSIS'05), 2005

[3] P. Ashley, S. Hada, C. Powers and M. Schunter. Enterprise Privacy Authorization Language (EPAL). IBM Research, 2003.

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

[5] J. Byun, E. Bertino, and N. Li. Purpose based access control of complex data for privacy protection, Symposium on Access Control Models and Technologies Proceedings of the tenth ACM symposium on Access control models and technologies , Pages: 102 - 110, 2005

[6] Ann Cavoukian, Genetic Privacy: the right "not to know", Notes for Remarksin 10th World Congress on Medical Law, 1994

[7] Marco Casassa Mont, Siani Pearson, Pete Bramhall, An Adaptive Privacy Management System For Data Repositories, Trusted Systems Laboratory HP Laboratories Bristol, HPL-2004-211 November 18, 2004

[8] Wu, Chen and Potdar, Vidysagar and Chang, Elizabeth (2006) A conceptual framework for privacy policy negotiation in web services, in Furnell, S.M. and Dowland, P.S. (ed), Sixth International Network Conference (INC), pp. 195-202, 2006

[9] Eldin' and Rend Wagenaar, Towards users driven privacy control, Systems, Man and Cybernetics, 2004 IEEE International Conference on, Volume 5, pp. 4673- 4679, 2004

[10] Wolfgang Hommel, An Architecture for Privacy-Aware Inter-domain Identity Management, DSOM 2005, LNCS 3775, pp. 49–60, 2005.

[11] Makoto Hatakeyama and Hidehito Gomi, Privacy Policy Negotiation Framework for Attribute Exchange, W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement,2006

[12] El-Khatib, K., A Privacy Negotiation Protocol for Web Services, Workshop on Collaboration Agents: Autonomous Agents for Collaborative Environments Halifax, 2003.

[13] Kristen LeFevre, Rakesh Agrawal, Vuk Ercegovac, Raghu Ramakrishnan, Yirong Xu, and David DeWitt. Disclosure in Hippocratic databases. In The 30th International Conference onVery Large Databases (VLDB), August 2004.

[14] Hyung-Jin Mun, Keon Myung Lee, and Sang-Ho Lee, Person-Wise Privacy Level Access Control for Personal Information Directory Services, EUC 2006, Springer LNCS 4096, Aug, 01, 2006, pp. 89-96

[15] Q Ni, D Lin, E Bertino, J Lobo, Conditional Privacy-Aware Role Based Access Control, ESORICS 2007, LNCS 4734, pp. 72-89, 2007

[16] Sabah S. Al-Fedaghi, Beyond Purpose-Based Privacy Access Control. In Proc. Eighteenth Australasian Database Conference (ADC 2007), Ballarat, Australia. CRPIT, 63. Bailey, J. and Fekete, A., Eds. ACS. 23-32

[17] P3P (2002). The Platform for Privacy Preferences 1.0(P3P1.0) Specification, The Wolrld Wide Web Consortium, April 16, 2002, http://www.w3.org/p3p/.

[18] http://www.istmobilife.org/index.php?option=com_content&task=view&id=41&Itemid=51

[19] http://www.newsfactor.com/perl/story/20064.html

[20] http://www.ist-mobilife.org/images/stories/architecture%20(wp5).pdf

[21] http://www.acm.org/crossroads/xrds11-2/spa_article.html