PPM: Privacy Policy Manager for Home Energy Management System

Mohammad Shahriar Rahman[1]*, Anirban Basu[2], Toru Nakamura[3], Haruo Takasaki[4], and Shinsaku Kiyomoto[4]
[1]*University of Liberal Arts, Dhaka, Bangladesh*
shahriar.rahman@ulab.edu.bd
[2]*University of Sussex, UK*
a.basu@sussex.ac.uk
[3]*ATR, Kyoto, Japan*
tr-nakamura@atr.jp
[4]*KDDI Research Inc., Saitama, Japan*
{ha-takasaki, kiyomoto}@kddi-research.jp

Abstract

The smart grid has been a popular technology for the power grid system. In order to optimize the power supply and distribution, and to provide personalized services by service providers, the consumption data is collected from the smart meters through Home Energy Management Systems (HEMS). However, privacy concern has been a major issue for personal data utilization. This paper introduces a new personalized services architecture for HEMS service providers. Under this architecture access control for private information is separated from data storage by using a user's customized privacy policy. Also, the architecture supports user-driven privacy policy management. The Privacy Policy Manager (PPM), a major component, has been designed for this purpose. PPM provides the following functionalities: privacy policy management, information flow control, and recording the flows.

Keywords: Home Energy Management Systems, Privacy Policy, Personalized Services, Management

1 Introduction

Carbon emission reduction and energy conservation, while improving the quality of life of the citizens, are global challenges for protecting the environment. In order to reduce home energy consumption and encourage practicing energy conservation at the household level, the Japanese government has taken initiatives to develop smart house technology leveraging Home Energy Management System (HEMS). As an emerging next-generation electrical power grid technology, the smart grid has the capability of generation, distribution, and consumption of electrical power in an adaptive and optimal manner. The HEMS, being a part of the smart grid system at the consumers' end, utilizes smart meters for data collection from domestic appliances for using the collected data to optimize power supply and its distribution. HEMS is a crucial component of smart house technology as it helps to avoid wasting energy and reducing energy costs. HEMS is connected to various household devices like smart electric meters, air conditioners, water heaters, and others. It thus provides a platform for connecting devices from multiple vendors in order to

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 9:2 (June 2018), pp. 42-56
*Corresponding author: Department of Computer Science and Engineering, University Liberal Arts Bangladesh, Dhaka-1209, Bangladesh. Tel: +88-(0)2-9661255, Web: https://ulab.edu.bd/academics/faculty-list/profile/193/

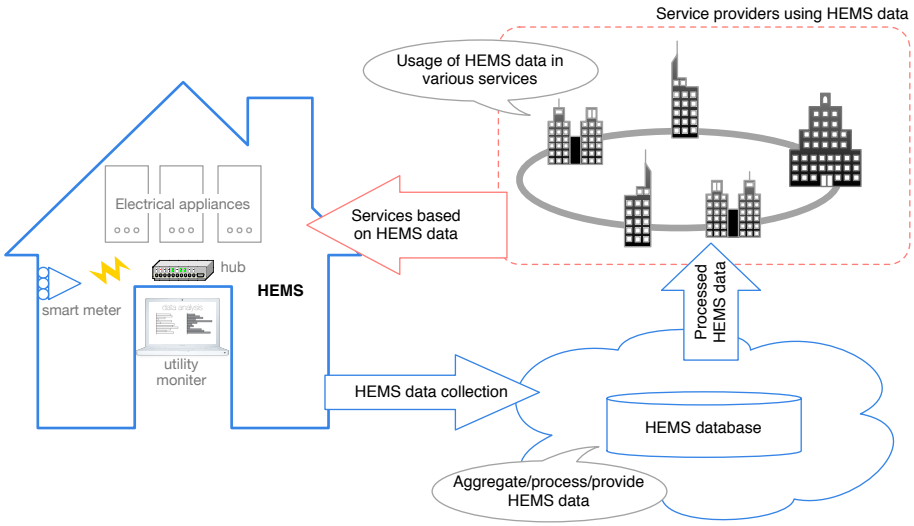


Figure 1: HEMS Data Management

facilitate them with widespread use. It is possible to "view" the electricity and gas consumption data as a useful and visible information through the installation of HEMS. Also, it allows to automatically control HEMS-compatible home appliances leading to optimized utilization of renewable energy. An overview of the HEMS data management environment is depicted in Fig. 1. Also, in order to providing more convenience and realizing a comfortable society with new personalized services which utilizes HEMS data, development of a huge HEMS information platform has been envisaged that ensures a privacy friendly environment for data utilization.

For personalized services' users of online web services as well as offline real services, breach of privacy has been a serious concern. Especially, as Online-to-Offline (O2O) has emerged as a new category of commercial services, there has been a growing concern of privacy because of growing trend of collaborations among such services. Users have shown their concerns over the cases when they are channeled to services which they were unaware of - particularly with the services without prior relationship. It has been suggested by some research results [1, 2] that users' private information is leaked through the internet ads which are personalized with private data. On the contrary, it has been discussed that raising privacy awareness assists users to deal with context-aware services without causing unintentional privacy breach [3].

The amount of task required to check and maintain privacy policies [4] is another point of concern. It is imperative that before using a particular service, users check and accept the privacy policies set by the service which is displayed by the provider of that particular service. For each service a set of privacy policy is prepared by the service provides. This, in turn, compels users to often check on a huge number of privacy policies. Moreover, the fact that users are not allowed to decide or customize the privacy policies for their own makes the management of privacy policy troublesome for them. A user cannot use a service if he/she does not accept the privacy policy of that service.

In [5] it was discussed that the self-management model of privacy policy fails to achieve the required goals. Such model has been pushed beyond its limits since the existing privacy law significantly depends on the privacy self-management model. The authors clarified the questions relevant to giving consent to a privacy policy as: (1) development of a reasonable perspective to consent taking into account the decision making process of humans regarding personal data, (2) development of more meaningful privacy rules. Through some experiments, authors in [6] show that there exists knowledge gap among individuals

regarding technical and legal framework for privacy protection during confirmation of privacy policy. The authors observe that even the individuals with significant awareness face several difficulties while attempting to protect their own private information. Another research [7] showed that a lot of users were unaware of the terms related to technical and legal aspects of privacy. Also, it was proposed in [8] that an individual's understanding of privacy threats and relevant technologies for protecting their privacy is rather insufficient.

Privacy Preferences Project (P3P) [9, 10] is a platform that allows user agents to automatically retrieve and interpret the privacy practices that are expressed in a standard format by the websites. User agent modules, as provided by the project, permit site practices to be informed to the users and to automatically take decisions based on those practices as and when needed. However, due to complex policy definitions, online and offline services [11] do not use it in practice, although modules for privacy matching can be found in some browsers. Moreover, the module is considered for implementations on web browsers only.

In our work, we propose an architecture designed for personalized services. We also suggest solutions to privacy problems arising from those services. Under this architecture, data storage and access control are separated from each other depending on a privacy policy. This architecture also allows user-controlled management of privacy policy. A module named Privacy Policy Manager (PPM) for HEMS is the major component of this platform that provides functionalities to support privacy policy management.

2 Towards Privacy-Preserving Personalized Services

We discuss the background of our work and shed light on the issues that arise in designing the architecture in this section.

2.1 Privacy Perception on HEMS Platform

The motivation to design a privacy-preserved personalized services is stemmed from the results of an online survey that was conducted over the HEMS users who have been living in greater Tokyo area, central Japan, Fukuoka, Shizuoka and Fukushima prefectures. Out of 14000 HEMS users, 6648 users responded to the questionnaire sent to them during the months of August and September in 2015. Contents of the questionnaire were concentrated on the following privacy-related matters: (1) features checked by a user while sharing private information, (2) whether a certain set of information is considered sensitive for user's privacy, (3) how a user feels if HEMS raw data is used by third-parties, (4) how a user feels if third-parties get access to estimate its life-cycle data from HEMS raw data, (5) which process is preferred by the user for anonymizing user's attributes, (6) how a user feels regarding the trade-off between quality of service and privacy. Fig. 2 summarizes the survey results. Briefly, respondents are edgy to share their personal identifiable information, they are inclined to check the data sharing platform's features before taking any decision on sharing their private data and they choose privacy protection over quality of service.

As the survey results imply, it was necessary to devise a platform for the users to allow them to handle sharing, accessing and usage policies of their perosnal data that are to be collected by HEMS devices. Hence we decided to design such a platform in this paper.

2.2 Personal Data Service

To support a user-focused transparent architecture having the ability to control information flow, a personal data vault has been proposed in [12]. An appropriate individual has complete access to this vault, which is essentially a secure container. Capturing and storing personal data streams are decoupled from

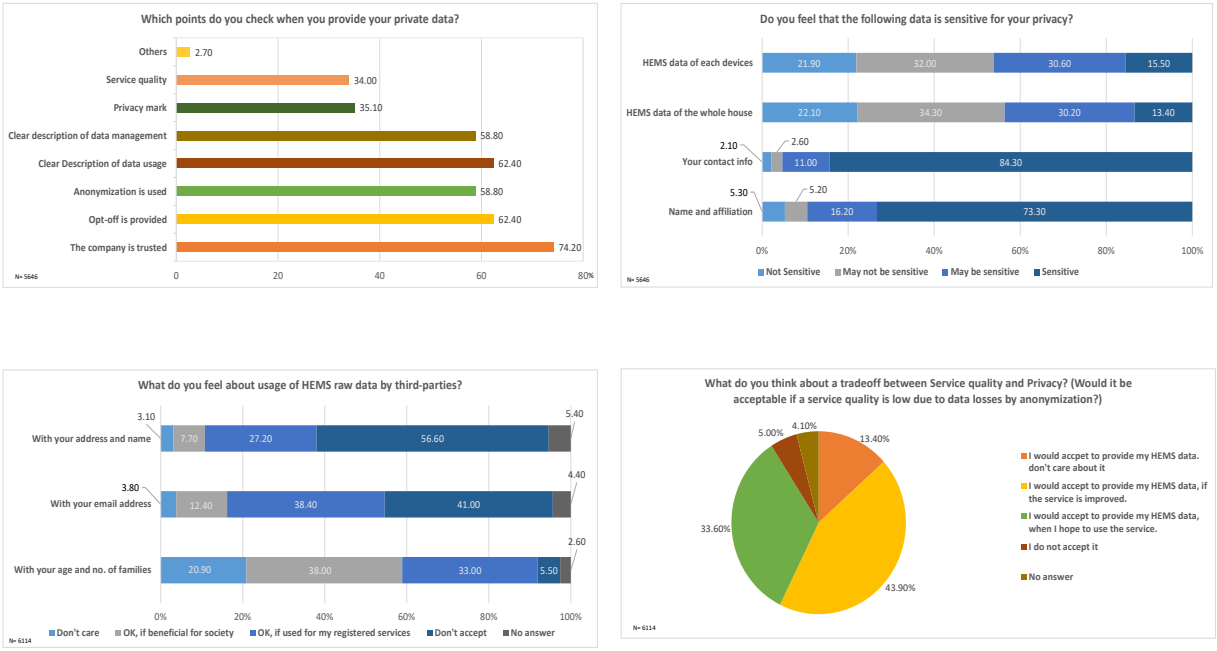


Figure 2: Results of Survey on Privacy in HEMS

the functionality related to sharing of that data. The individual is then facilitated by the personal data vault to selectively share a subset of the data with different services. There exist several platforms for managing such personal data vaults. A user can enforce controlled push and informed pull functions through the personal data vault. Since such platforms are managed by various companies, an individual is bound to trust the entity which is providing service though the platform. The idea behind Personal Data Service (PDS) is introduced to address this problem. Also, a number of research projects have come up with tools to realize individual-centric management of private information.

The PDS platform enables individuals to have control over their personal data. PDS is useful when personal information is shared with friends and other trusted entities. It holds a user's sensitive information (e.g., date of birth, credit card, social security etc.) and provides access control functionality to that user. PDS conceptualizes an individual-oriented model whereby individual's control on accessing personal data is enabled on its device. Access control technique as well as storage of private data are programmed (a web browser, for example) on that device. Users can manage their own information in a secure way and have control on data flows by using PDS. Higgins [13], a browser extension, incorporates components of PDS - allowing browser interactions and web client interactions. Danube [14] is another example of PDS which is designed targeting web services. The VRM project [15] is another example of PDS adaptation that aims for providing a platform as well as tools to realize such services. The project comes up with the following five instructions for the users of privacy enabled services:

- *A user acts as independent actor while entering into relationships with vendors.*
- *A user's data must be integrated by that user.*
- *A user holds the control of the data generated and gathered by that user. In other words, a user must have the permission sharing data in a selective and voluntary manner.*

- *A user should be allowed to declare its own terms of engagement.*
- *A user should have the freedom of expression in terms of its demands as well as intentions which are beyond the control of any particular company.*

However, it is troublesome for an individual that all functions to protect and control the sensitive data must be handled by the data owner. Therefore, an architecture is envisaged that provides better user-friendly experience. Challenges that arise for personalized services based on the points stated above are formalized in the following subsection.

2.3 Challenges for Personalized Services

While personal data services facilitate handling individual's private information, some issues remain with such existing service. We discuss some of the solutions to the problems regarding PDS in this subsection. On the other hand, there are some challenges for devising user-friendly architecture as well. Before going to design such architecture, we briefly discuss the challenges as stated below:

- *Complexity:* Currently the service providers issue privacy policies according to their need for each service. A user has to accept a huge number of conditions stated within various policies prior to start using the services.
- *Flexibility:* Service providers take initiatives to determine the privacy policies. Although users are given choices to select some terms in privacy policies, which include *opt-out*, users are not guaranteed that the terms will fit with users' privacy needs.
- *Availability:* There are restrictions in distributing private information. Personalized services like recommender systems and support services utilize privacy related information. However, the service providers utilize appropriate technologies to distribute information without having to breach privacy. Privacy policy of each service provider is presented by them ensuring that the policies cover the service only from that service provider. Users feel that privacy policies for all services should exist which are common in nature.
- *Assurance:* Users are worried about the service provider's process of managing private information. Ensuring operations integrity and improving the trustworthiness of service providers are significant challenges as private data-driven services grow.

To deal with the above challenges, we propose an architecture in this work.

3 Architecture for Personalized Services

This section introduces our proposed architecture for personalized services utilizing a new concept of personal data service. To address the challenges mentioned earlier, our designed architecture assists an individual to administer its common privacy policies and to reduce the operational complexity at the user end. The architecture carries the following features:

- **Separating Access Control from Policy Management:** The functionality of our proposed personal data service is separated into data storage and access control. The access control part is managed by a trusted entity for supporting individuals to configure suitable privacy policies as well as to control data flows according to the corresponding privacy policies. Designing modules for data storage is out of scope of our work; we assume that each individual manages data storage

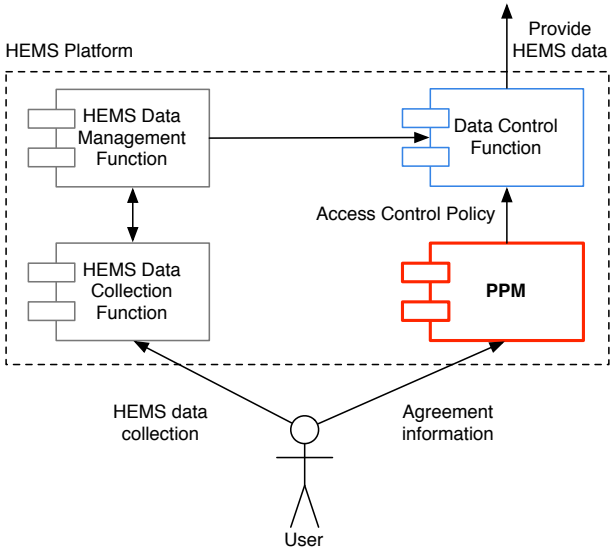


Figure 3: Integration of PPM into HEMS Platform

or it is distributed among some domains. The trusted entity manages the privacy policies so that common policies can be applied to various services.

- **Supporting Policy Management:** One of the features of the architecture is that it supports management of privacy policies set by the individuals. This approach supports to generate a common privacy policy for every individual and make it optimized relying on individual's recommendations.

- **Log Management:** Our architecture utilizes a proxy for managing individuals and service providers. The trusted area of the architecture captures all the communication that takes place through the architecture. It, thus, helps to get the flows of private data verified by the users.

Our proposed architecture is as shown in Fig. 3 where the core component is a Privacy Policy Manager (PPM). Privacy policies of an individual and control on the flows of private data corresponding to the policies are managed by the PPM. The PPM is constructed on a trusted party within a domain and the domains are separated. Such domains contain at least one PPM. An individual is required to get its privacy policy registered with a PPM of a domain according to the individual's location. Through the PPM the individual may configure the measures to be taken when access to private information is requested by a service provider whose service breaches the registered policies. For instance, the PPM will seek permission from a user for sharing private information whereas the act of sharing the information violates the user's privacy policy. The architecture also provides inter-communication between PPMs. If a user steps into a different area, it will access a PPM situated in area. In such cases, the PPM of the new area will request the previous PPM for transferring the privacy policy or a permission for sending private information to a service provider.

Notion of Opt-In Domain: Reaching a comprehensive agreement on access and use of private information is conceptualized through "Opt-In Domain". As individuals perceive that their private information might be accessed by unfamiliar services or shared with different service providers than the ones they know of, concerns over privacy breaches have grown significantly among such individuals. However, the service providers face the challenge of availabililty of such information, as discussed earlier. The

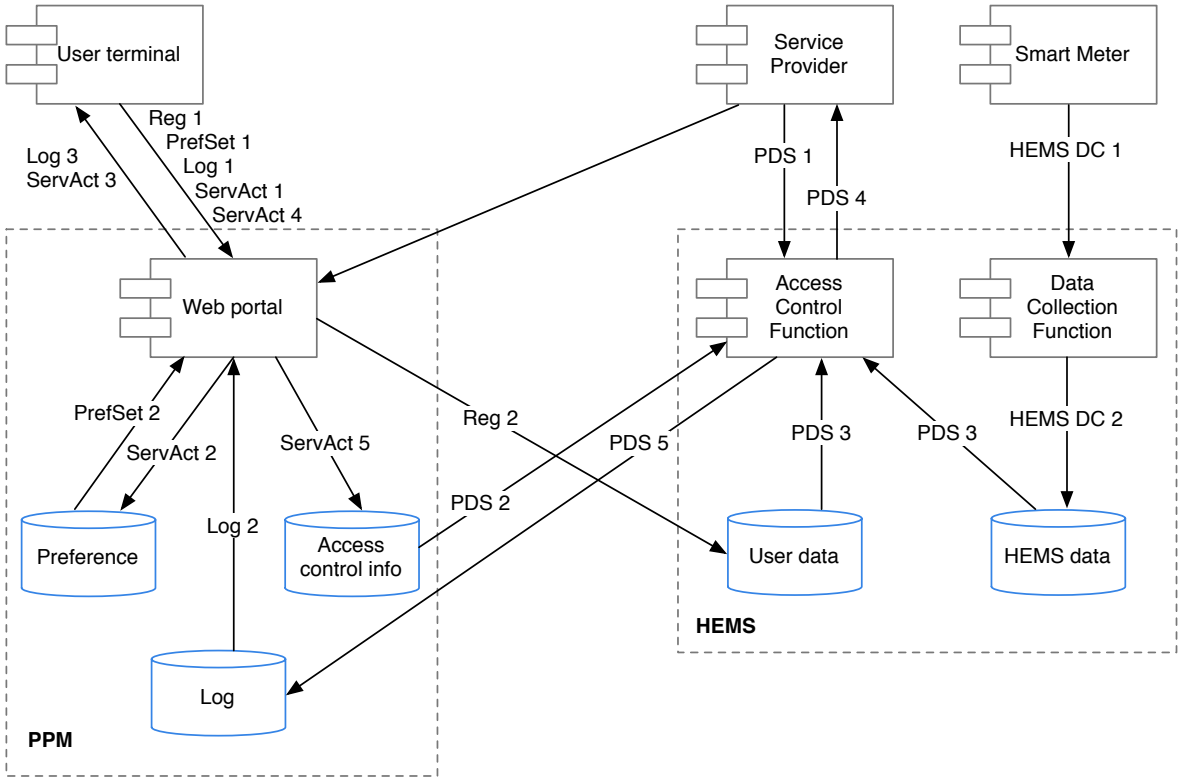


Figure 4: Architecture for Privacy Policy Management

notion of "Opt-In Domain" allows various service providers located in the same domain to use private information. Using private information is confined within a physically- or virtually-defined boundary [1]. Under this notion, a particular privacy policy is set for a certain area or domain by an individual and the service providers are permitted for accessing the individual's private data gathered within the domain. Our architecture satisfies this notion as an extensive agreement is managed by the PPM for the service providers.

4 Privacy Policy Manager

The Privacy Policy Manager (PPM) is the major module of our proposed architecture. Individuals use PPM within their respective domain, and the database of the PPM manages the privacy policy of the individuals. Control of information flow is managed utilizing the privacy policies. ID management is the major task of the PPM, namely authenticating users and managing privacy policy. An holistic of the PPM is shown in Fig. 4. The PPM, similar to a proxy service that includes a mechanism for access control, has the following functionalities:

- Create and Update User Privacy Policy:
  A user-friendly graphical user interface (GUI) should be provided by the PPM for generating privacy policy of a user. Also, there should be a mechanism to frequently update the registered

[1]Note that individuals are more comfortable with a physical boundary as it is clearly defined. We shall analyze individual's acceptance of boundaries by an experiment in future.

privacy policies utilizing service usage records. The functions, f_m and f_w, are defined for managing privacy policy.

- Privacy Policy Checking:
  The PPM checks privacy policy of a user in order to decide on sending private information upon receiving a request from a service provider.

- Storing Records of Service Use:
  One of the core tasks of the PPM is to visualize the flows of private information transfer. All service access goes through the PPM. The PPM stores the whole log of information flow for providing those to users. We introduce a notion of *user consent log search* and explain it in section 4.4.

- Communication with other PPMs:
  The PPM contains a communication function for supporting a roaming user whose privacy policy is attached to some other PPM. The primary task of this function is to inquire the privacy policy or asking for a consent regarding privacy control related to that roaming user. We summarize the protocol in section 4.5.

4.1 Procedure

The PPM performs the job of a proxy which acts as a communication mediator between a user and a service provider. The procedure for an example case of HEMS service use is given below:

1. **User Registration:** A user registers itself through the web portal using its terminal (Reg 1 in figure4). User registration data is stored in the HEMS server (Reg 2 in figure4).

2. **Preference Setting:** A user sets its preferences through the web portal using its terminal (PrefSet 1 in figure4). User preference data is stored in the PPM server (PrefSet 2 in figure4).

3. **Service Activation:** The service activation procedure consists of the following steps:

   (a) A user requests a service from the PPM through the web portal using its terminal (ServAct 1 in figure4).

   (b) The web portal collects the user preferences from the PPM server and the privacy policy/usage contract from the service provider (ServAct 2 in figure4).

   (c) From the ServAct 2, the portal generates a personalized permission request for the user (ServAct 3 in figure4) and the user approves this request (ServAct 4 in figure4).

   (d) The PPM generates access control information of the corresponding service provider and stores in the server (ServAct 5 in figure4). This step allows the service provider to access the user data according to its personalized preferences in later stage.

4. **HEMS Data Collection:** The HEMS platform collects smart meter data through its data collection module and stores in the server (HEMS DC 1 and HEMS DC 2 in figure4).

5. **Providing Data to Service:** The procedure to provide data to service provider consists of the following steps:

   (a) Service provider requests the HEMS platform for data (PDS 1 in figure4).

   (b) The HEMS platform collects the access control information from the PPM through the access control function (PDS 2 in figure4).

(c) The access control function of the HEMS platform collects the user data and HEMS data, and prepares the deliverable data for the service provider according to the personalized preferences of the user (PDS 3 in figure4).

(d) The HEMS platform forwards the deliverable data to the requesting service provider (PDS 4 in figure4).

(e) The HEMS platform stores the log information of the service provider in PPM (PDS 5 in figure4)

6. **Log Request:** Through the web portal, the user requests and receives the log information from PPM (Log 1, Log 2 and Log 3 in figure4)

One may allow an offline batch operation for updating a privacy policy as it would be otherwise excessively burdensome for the PPM to update.

4.2 Creating and Modifying Privacy Policy

The PPM provides the functionalities to create and update privacy policies of users. A user essentially needs to set up an explicit privacy policy ahead of utilizing the service. The PPM of the proposed architecture contains two stages: setting up privacy policy primarily and customize it according to the user's need.

A privacy policy $\mathscr{P}$ in the PPM is defined using a hierarchical structure. Let $P_i \in \mathscr{P}$ $(0 \leq i \leq l_i)$ be the i-th item in the policy, and P_i contains sub-items P_{ij} $(0 \leq j \leq l_{ij})$. If $P_0 = A$, then all items are allowed. Similarly, P_{ij} contains sub-items P_{ijk}. Given an item is A all subsequent sub-items are A. During the primary stage of creating policy, each top-level item is defined with a policy by a user; e.g., $P_1 = A, P_2 = \neg A, P_3 = \neg A, ...$, where A represents "allowed to send", and $\neg A$ represents "not allowed to send". For instance, if P_1 is the policy to access location data of a user's device, this location data is allowed to be shared with other service providers. Therefore, policies for almost every item are initially set to $\neg A$.

For location-based services, the service provider sends a permission description D_x (similar to the description of privacy policy items) as a part of requesting the PPM. The PPM then inspects the privacy policy for location data. For instance, such permission is described as "$D_x = P_{1433}$: Brief location information (town level) for a trust level 3 service provider". Let b_x be a user's response for D_x. If the policy for location data is $P_1 = \neg A$, the PPM checks with the user whether D_x is accepted $(b_x = 1)$ or not $(b_x = 0)$. The location data is sent upon user's permission and the item P_{1433} is added to the privacy policy. Thus, upon modification the policy becomes $f_m(\mathscr{P}, D_x, b_x) = \{P_1 = \neg A, P_{14} = \neg A, P_{143} = \neg A, P_{1433} = A\}$, where $f_m(*,*,*)$ is privacy policy's modification function. The rest of the items, e.g. P_{1432}, are implicitly configured as $\neg A$. It is required that groups of service providers are pre-defined for the sake of privacy policy setting to be accurate and precise. In the above example, "trust level" is used as a basis for grouping. It is defined by an entity (a rating agency, for example) which is deemed trustworthy by the users. Another method would be to identify two groups: service providers who are from the same domain and who are not. Such method is mirrored in "opt-in domain" discussed earlier.

This work also considers a policy recommendation mechanism which can be offered during initial policy design. A user is introduced to a sample privacy policy of a user holding similar profile or to a default setting. Also, recommending modification of privacy policy can be designed on the basis of the policies set by similar users. Kelley *et al.* showed an approach for policy learning that can be controlled by a user. The learning utilizes searches of nearby users to consider modifying user's current policy gradually [16] and implemented it in the people-finder [17]. A similar approach is applied for generating as well as modifying policy in order to minimize the operational complexity at the user end. A master key K_m is used to encrypt the privacy policies which are saved in privacy policy database of the user.

4.3 User-Friendly Interface for Privacy Policy

A privacy policy is often defined by complicated descriptions which causes bitter user experience with privacy policy management. Two technical issues are considered in this work towards designing a user-friendly privacy policy management: (1) the policy has to be configured easily, and (2) the policy has to be recognized easily. We have already discussed issue (1) in the previous section. Issue (2) is mainly discussed here.

For attaining an easy to understand overview of a policy, it is required that a transformation function $f_w(x,y,z)$ should be utilized for translating the machine-friendly design to a user-friendly design. A multi-level view of a policy is considered to be used in our architecture. At the top level lies the initial view of the policy. When a particular top level item is clicked by a user, the corresponding section of the next layer of the policy is shown. The item describing irregularities to items is to be displayed as well as descriptions of other common items should be shown in a single paragraph. Let d denotes the level of description, and u denotes the preference of a user for a privacy policy view. The function $f_w(*,*,*)$ outputs a privacy view $\mathscr{P}_{view}$ as $f_w(\mathscr{P},d,u) = \mathscr{P}_{view}$. For instance, $f_w(\mathscr{P},d_1,u_k) = \{P_0 = A, P_1 = \neg A, P_2 = \neg A, ..., P_{l_i} = \neg A\}$, where d_1 denotes the highest level of the privacy policy $\mathscr{P}$, and u_k is the user k's preference. In the running example, $f_w(\mathscr{P},d_4 = 143*, u_k = all) = \{P_{1433} = A, others = \neg A\}$, as common items have been integrated. Preference of the user which utilizes the user's requirements and feedback, is used to optimize the policy view for each user.

Description of each item is another point to be considered. A description has to be user-friendly for indicating an item. One effective method is to underline crucial or atypical components of the policy. For instance, when a user agrees to an item which is agreed by many other users, the item is highlighted in green color. If an item contains crucial private data it is highlighted in red when the user comes to an agreement on that item. Designing tools for visualizing privacy policy is an avenue for future research.

4.4 Log Management

Records of private data flows are stored in the database of the PPM. This typically contains date, time and name of the service provider. It also stores the private data carrying similar structures to those defined in the privacy policy, but does not contain private data. The service log DB contains those records. Users use retrieval keys, such as their ID, name of service provider, and type of private data to look into their own records. Appropriate encryption functions have to be used to protect the database against external attackers.

User Consent Log Search: Tasks like tracing or searching user logs is not allowed in the PPM without explicit user consent. User is required to be authenticated for searching the database. Also, the user presents *user secret* to the PPM while getting authenticated. [2] Due to this reason an *offline attacker* (e.g., a curious operator of the PPM) can not successfully search the records of a user. Although there exist various cryptographic tools for private search, those techniques are dependent on heavy computational costs. Therefore, we envisage a lightweight scheme for user consent log search.

4.5 Interoperability Between PPMs

An individual accesses a PPM belonging to a domain and enjoys various services available in that domain. As a generic use case, we consider the scenario whereby an individual accesses a different PPM in another domain. We design a distributed system of PPMs for building PPMs in different domains. The PPM is connected with the service providers of its corresponding domain, but it may neither connect

[2] Any standard authentication protocol can be used for this purpose. Designing an authentication protocol is orthogonal to this work

with the same operating in another domain nor have access to relevant privacy policy data of that service provider. Consequently, users need to use different PPMs for each domain. When a user connects to a PPM from another domain, the new PPM must hand over the user's request to the PPM the user is registered with. The scenario is identical to roaming protocols designed for user authentication. Following four procedures are defined for realizing interoperability:

- Requesting registered PPM for user authentication.
- Downloading privacy policy of a user from it's registered PPM.
- If a user's privacy policy is modified, upload it to the registered PPM.
- Sending service use log to the registered PPM.

Upon successful user authentication, user's privacy policy from registered PPM is downloaded by the new PPM. Privacy policy of the user is revised given that contain permission items those are needed for using the service are not contained in it. The user is asked if the user wishes to allow the permission items. If the user allows, the PPM adds those items to the user's privacy policy. The user privacy policy, after modification, is automatically uploaded to the PPM where the user is registered with, and the newly uploaded policy replaces the old user privacy policy. To realize mutual authentication between the new and registered PPMs, a suitably designed public key infrastructure is required. A private key embedded in the PPM in a secure way. The procedures may have the following general steps:

1. A secure channel between the PPMs is established for executing an authenticated key exchange mechanism that includes mutual authentication with public key certificates; for instance, the ephemeral DH with RSA certificates mode (DHE-RSA) in TLS 1.2 [18] can be a good candidate. A trusted party endorses each PPM and each of them holds a valid certificate. In that manner, a PPM is enabled to authenticate other PPMs for executing the authenticated key exchange mechanism.
2. A PPM communicates with other PPMs using the procedures. All transaction information is protected as it is shared through a secure channel.

5 Related Work

The Privacy Bird [19, 20] is web browser extension that has the ability to retrieve a website's P3P policies automatically. However, it is suggested in [4] that the privacy preference settings offered by the Privacy Bird cause weak user acceptance, which eventually puts the intention for real-world use at risk. Therefore, the authors came up with a proposal of a user-centric privacy preference creator [4] for service providers, incorporating a set up wizard along with a preference summary. In [21], authors introduced a privacy policy checking tool targeting online services. Under this mechanism, privacy policies of users and providers are compared with each other and usability of the service is determined automatically. A technique for detecting differences of privacy settings between user preference and the requirements of a smart phone application is presented in [22]. Privacy Butler [23], a tool for personal privacy management in social network, is proposed for monitoring a user's online presence and trying to make necessary modifications utilizing privacy policy for user's online presence. Although the concept behind the Privacy Butler is almost identical to that of this work, it emphasizes on corrections of contents those are stored at social networking services. Privacy Mirror [24] allows users to see their private information those are available online.

Authors in [10, 25, 26] have introduced several languages for describing privacy policies. Backes *et al.* studied a number of comparisons between privacy policies at enterprise level leveraging formal abstract syntax and semantics for expressing contents of various policies [27].

The VRM project [15] aimed to make users the integration points for their own information and to give users the capacity for sharing information selectively, hence the ability to control the way their information is to be utilized by others, and to assert users' own terms of service. This notion relies on Personal Data Service (PDS) and it is fundamentally similar to this work, but their mechanism is an integrated design for access control and data storage.

6 Discussion and Conclusion

This paper presents an architecture for privacy-preserving personalized services and designs a major component - PPM. The PPM provides a platform for managing privacy for the users and plays the role of a proxy for checking private data flow and recording those flows. The concept behind the proposal is delegation of access control and policy management, and the proposed framework relies on the notion of PDS. This framework allows users to get confirmed that the service log database is appropriately used by private information flows. Moreover, our design considers *offline attackers* and ensures that the PPM is secure from such attackers. The PPM achieves availability and flexibility providing a platform for managing common user privacy policies. The PPM also provides mechanisms for policy checking which refers to the common policies. It is believed that users enjoy the freedom of using user-friendly services easily for providing a transparent perspective of data flows and ensuring access control driven by their own privacy policies.

References

[1] S. Guha, B. Cheng, and P. Francis, "Challenges in measuring online advertising systems," in *Proc. of the 10th ACM SIGCOMM conference on Internet measurement (IMC'10), Melbourne, Australia*. ACM, November 2010, pp. 81–87.

[2] A. Korolova, "Privacy Violations Using Microtargeted Ads: A Case Study," in *Proc. of the 2010 IEEE International Conference on Data Mining Workshops (ICDMW'10), Sydney, New South Wales, Australia*. IEEE, December 2010, pp. 474–482.

[3] A. Deuker, "Addressing the privacy paradox by expanded privacy awareness–the example of context-aware services," in *Proc. of the 2009 IFIP PrimeLife International Summer School on Privacy and Identity Management for Life, Nice, France*, ser. IFIP Advances in Information and Communication Technology, vol. 320. Springer, Berlin, Heidelberg, September 2010, pp. 275–283.

[4] J. Kolter and G. Pernul, "Generating User-Understandable Privacy Preferences," in *Proc. of the 2009 International Conference on Availability, Reliability and Security (ARES'09), Fukuoka, Japan*. IEEE, March 2009, pp. 299–306.

[5] D. J. Solove, "Privacy self-management and the consent dilemma," *Harvard Law Review*, vol. 126, pp. 1880–1903, January–February 2013.

[6] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Security & Privacy*, vol. 3, no. 1, pp. 26–33, February 2005.

[7] I. Pollach, "What's wrong with online privacy policies?" *Communications of the ACM*, vol. 50, no. 9, pp. 103–108, September 2007.

[8] C. Jensen, C. Potts, and C. Jensen, "Privacy practices of internet users: self-reports versus observed behavior," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 203–227, July 2005.

[9] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, "The platform for privacy preferences 1.0 (P3P1.0) specification," https://www.w3.org/TR/2002/REC-P3P-20020416/ [Online;

accessed on June 20, 2018], April 2002, platform for Privacy Preferences (P3P) Project- W3C recommendation 16.

[10] L. F. Cranor, "P3P: making privacy policies more useful," *IEEE Security & Privacy*, vol. 99, no. 6, pp. 50–55, November 2003.

[11] A. Pedersen, "P3P - problems, progress, potential," *Privacy Laws & Business International Newsletter*, vol. 2, pp. 20–21, February 2003.

[12] D. Estrin *et al.*, "Participatory sensing: applications and architecture [Internet Predictions]," *IEEE Internet Computing*, vol. 14, no. 1, pp. 12–42, December 2009.

[13] T. E. Foundation, "Higgins, Personal Data Service," *Higgins Home*, 2009.

[14] P. Danube, "Danube, Identity and Communication for Political and Social Innovation," Project Danube Web Page, http://projectdanube.org/[Online; accessed on June 20, 2018], 2010.

[15] D. Searls, "ProjectVRM - Vendor Relationship Management," http://blogs.harvard.edu/vrm/ [Online; accessed on June 20, 2018], 2013, project of the Berkman Center for Internet Society at Harvard University.

[16] P. G. Kelley, P. H. Drielsma, N. Sadeh, and L. F. Cranor, "User-controllable learning of security and privacy policies," in *Proc. of the 1st ACM workshop on Workshop on AISec (AISec'08), Alexandria, Virginia, USA*. ACM, October 2008, pp. 11–18.

[17] J. Lin, G. Xiang, J. I. Hong, and N. Sadeh, "Modeling people's place naming preferences in location sharing," in *Proc. of the 12th ACM international conference on Ubiquitous computing (Ubicomp'10), Copenhagen, Denmark*. ACM, September 2010, pp. 75–84.

[18] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) protocol," IETF RFC 5246, August 2008, https://www.ietf.org/rfc/rfc5246.txt.

[19] L. F. Cranor, M. Arjula, and P. Guduru, "Use of a P3P user agent by early adopters," in *Proc. of the 2002 ACM workshop on Privacy in the Electronic Society (WPES'02), Washington, DC, USA*. ACM, November 2002, pp. 1–10.

[20] L. F. Cranor, P. Guduru, and M. Arjula, "User interfaces for privacy agents," *ACM Transactions on Computer-Human Interaction*, vol. 13, no. 2, pp. 135–178, June 2006.

[21] G. O. Yee, "An automatic privacy policy agreement checker for e-services," in *Proc. of the 2009 International Conference on Availability, Reliability and Security (ARES'09), Fukuoka, Japan*. IEEE, March 2009, pp. 307–315.

[22] D. Biswas, "Privacy policies change management for smartphones," in *Proc. of the 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom'12), Lugano, Switzerland*. IEEE, March 2012, pp. 70–75.

[23] R. Wishart, D. Corapi, A. Madhavapeddy, and M. Sloman, "Privacy Butler: A personal privacy rights manager for online presence," in *Proc. of the 2010 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom'10), Mannheim, Germany*. IEEE, March 2010, pp. 672–677.

[24] M. Bylund, J. Karlgren, F. Olsson, P. Sanches, and C.-H. Arvidsson, "Mirroring your web presence," in *Proc. of the 2008 ACM workshop on Search in social media (SSM'08), Napa Valley, California, USA*. ACM, October 2008, pp. 87–90.

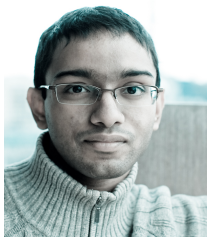
[25] A. Dehghantanha, N. I. Udzir, and R. Mahmod, "Towards a Pervasive Formal Privacy Language," in *Proc. of the IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA'10), Perth, Australia*. IEEE, April 2010, pp. 1085–1091.

[26] K. Bekara, Y. B. Mustapha, and M. Laurent, "Xpacml extensible privacy access control markup langua," in *Proc. of the 2nd International Conference on Communications and Networking (ComNet'10), Tozeur, Tunisia*. IEEE, November 2010, pp. 1–5.

[27] M. Backes, G. Karjoth, W. Bagga, and M. Schunter, "Efficient comparison of enterprise privacy policies," in *Proc. of the 2004 ACM symposium on Applied computing (SAC'04), Nicosia, Cyprus*. ACM, March 2004, pp. 375–382.

Author Biography

Mohammad Shahriar Rahman is currently an associate professor at the University of Liberal Arts Bangladesh. Earlier, he worked as a research engineer at the Information Security group of KDDI Research, Japan. He received his Ph.D. and M.S. degrees in information science from Japan Advanced Institute of Science and Technology (JAIST), in 2012 and 2009 respectively, and B.Sc. in computer science and engineering from University of Dhaka, Bangladesh, in 2006. His research interests include secure protocol construction, privacy-preserving computation and security modeling. He is a member of International Association for Cryptologic Research (IACR). Dr. Rahman has co-authored 40+ research papers and submitted 8 co-authored Japanese patent applications.



Anirban Basu is currently a Visiting Research Fellow at the University of Sussex, UK. With more than a decade of research experience within both academia and industry, Dr. Anirban Basu has co-authored 70+ research papers and submitted about 20 co-authored Japanese patent applications. He holds a Ph.D. in Computer Science (2010) and a Bachelor of Engineering (Hons.) in Computer Systems Engineering (2004) from the University of Sussex. His research is based on a user-centric view of privacy; and computational trust as an information security paradigm in an increasingly knowledge-based connected world. He is particularly active within the IFIP WG 11.11 computational trust management community

Toru Nakamura was born in Hiroshima, Japan, in 1983. He received the B.E., M.E., and Ph.D degree from Kyushu University , Fukuoka, Japan in 2006, 2008, and 2011, respectively. In 2011, he joined KDDI in Tokyo, Japan and in the same year he moved KDDI R&D Laboratories, Inc. (currently Renamed KDDI Research) in Saitama, Japan. Since 2018, he has been with Advanced Telecommunications Research Institute International(ATR), Kyoto, Japan. His current research interests include security and privacy, especially privacy enhanced technology and analysis of privacy attitudes. He is a member of the Institute of Electronics, Information and Communication Engineers(IEICE) and the Information Processing Society of Japan(IPSJ).

Haruo Takasaki was born in Hokkaido, Japan, in 1957. He received the Bachelor of Laws from Tohoku University, Sendai, Japan, in 1980, and Ph.D. degrees in economics from Kyushu University, Fukuoka, Japan in 2018. In 1980, he joined Kokusai Denshin Denwa (KDD, later changed to KDDI) and has a lot of experience in the field of telecommunication. He has moved to KDDI Research, Inc. in 2005. Since then, he has researched in the field of privacy regulation and economics of privacy.He was awarded the journal prize for the articles titled “The Study on User Preferences of Personalized Services An Empirical Analysis Assuming Plurality of Privacy Concerns” from JSICR in 2017. He was certified as Privacy Design Ambassador from Privacy Commissioner of Ontario, Canada, in 2014. He is a member of Japanese committee of ISO/SC27/WG5 and is contributing to standardization of privacy matters.

Shinsaku Kiyomoto received his B.E. in engineering sciences and his M.E. in Materials Science from Tsukuba University, Japan, in 1998 and 2000, respectively. He joined KDD (now KDDI) and has been engaged in research on stream ciphers, cryptographic protocols, and mobile security. He is currently a senior researcher at the Information Security Laboratory of KDDI R&D Laboratories (now KDDI Research, Inc). He was a visiting researcher of the Information Security Group, Royal Holloway University of London from 2008 to 2009. He received his doctorate in engineering from Kyushu University in 2006. He received the IEICE Young Engineer Award and IEICE Achievement Award in 2004 and 2016 respectively. He is a member of JSPS and IEICE.