iGuard: A Personalized Privacy Guard System for Cloud Service Usage on Mobile Devices

Chien-Wei Hu
Institute of Computer and Communication Engineering,
National Cheng Kung University,
Tainan, Taiwan
chienwei@nature.ee.ncku.edu.tw

Hewijin Christine Jiau
Department of Electrical Engineering,
National Cheng Kung University,
Tainan, Taiwan
jiauhjc@mail.ncku.edu.tw

Kuo-Feng Ssu
Department of Electrical Engineering,
National Cheng Kung University,
Tainan, Taiwan
ssu@ee.ncku.edu.tw

***Abstract*—Users encounter privacy threats when they use cloud services through mobile devices. A user leaves a large amount of usage data on the server sides. Leaving a single piece of usage data on the server side may seem harmless to user's privacy, but if usage data is all taken together, the sensitive information can be leaked. To detect privacy leakages, various privacy measurements have been proposed. However, it's not easy for the user to find suitable privacy measurements because he does not have the background knowledge. Moreover, the user also does not know what is available to be used for protecting his privacy when he finds privacy leakages. In this work, iGuard, a personalized guard system for cloud service usage on mobile devices, is provided. iGuard provides a customized privacy measurement plan which fits in the user's personal situation. The plan is executed to detect possible privacy leakages when the user is using cloud services. To resolve the leakages, iGuard also provides workable privacy protection strategies. The user can apply one of the strategies and see its effect on the privacy measurement results. According to the results, the user can tune his strategy continuously until he is satisfied with the results. By continuously tuning, the user can manage the privacy-utility trade-offs of using cloud services.**

Keywords–privacy measurement; privacy protection.

I. Introduction

Users enjoy all kinds of conveniences provided by cloud services through mobile devices anytime and anywhere. Cloud services enable users to access all kinds of data and use various software on the Internet. In 2014, twelve percent of the EU population used cloud services for document editing. The proportion was even higher (23%) among the population aged 16-24 [1]. But the truth is that cloud service providers are also interested in tracking user information, e.g., user preferences, personality traits, and relationship statuses. Privacy threats increase when users access cloud services through mobile devices. Mobile devices are equipped with various sensors to collect users' contextual information, such as geolocation information. When a user performs an operation on a cloud service, not only data that the user enters into the cloud service but also contextual information is sent to the cloud service. The cloud service gets more data than the user inputted manually, but the user does not know what the cloud service gets additionally. Besides, leaking a single piece of usage data to the cloud service may be harmless to user's privacy. But a user's profile, such as his routines and preferences, will be revealed if all the usage data on the server side is aggregated and further analyzed.

The revealed user information is collected further and reused without the user's awareness and permission [2]. The management of user data on cloud services might not be trustworthy [3]. Cloud service providers might use user data for various purposes, or sell the data to others who need to perform data aggregation. More user information might eventually be mined for all kinds of purposes, and the user will not have any control over those purposes. In fact, the user has the right to know what can be revealed from his usage data, but cloud service providers do not respect this right, still collecting user information without notifying the user. If the user wants to be aware of data leakages from his usage data, he must apply appropriate privacy measurements on the usage data by himself. A privacy measurement focuses on a kind of usage data and detects a specific user privacy leakage from the data. There are various privacy measurements available currently. For example, the privacy measurement proposed by Liao et. al [4] can be used to detect leakages of the user's transportation routines from Global Positioning System (GPS) data. Even though the user does not expose any GPS data to the cloud service, another privacy measurement proposed by Valkanas and Gunopulos [5] can be used to detect user's location information leakages from general textual information on social network services. A user has his own combination of cloud services in use and personal privacy preferences. Among all these different privacy measurements, the user has to select privacy measurements that fit in his situation and performs the privacy measurements on suitable timing. However, the user may not have the background knowledge to select and perform the privacy measurements. A general user knows how to operate a cloud service, but he may not know the usage data that will be sent to the cloud service, let alone the privacy measurements that are available for detecting privacy leakages. Even though the user discovers a privacy leakage, he may not have the knowledge to avoid the privacy leakage while keeping using the cloud service.

In this work, iGuard, a personalized guard system for cloud service usage on mobile devices, is proposed. According to the user's personal situation, his combination of cloud services in use and privacy preferences, iGuard selects appropriate privacy measurements for the user. iGuard collects usage data sent to the cloud services and triggers corresponding privacy measurements on suitable timing for detecting possible privacy leakages. If privacy leakage is detected, the user will receive a warning from iGuard. iGuard provides privacy protection strategies for the user. The effect of the applied protection strategies is reflected in the results of the privacy measurements so that the user can improve his strategies continuously based on the results. Contributions of this work are outlined as follows.

1) In this work, user-centric privacy protection is provided. The user-centric privacy protection focuses on personal privacy measurements and customized privacy protection strategies. The personal privacy measurements detect critical privacy threats, and the customized privacy protection strategies help mitigate the threats.
2) iGuard, a system that implements the user-centric privacy protection, is provided. As types and amount of user data collected by cloud services increase, demands of new privacy measurements also increase to provide comprehensive user privacy protection. iGuard takes the extension of privacy measurements into consideration, and is flexible for adding new privacy measurements.

The remainder of this work is organized as follows. In Section II, an overview of related work is provided. The user-centric privacy protection is illustrated in Section III. Details of the iGuard system is described in Section IV. In Section V, two case studies of using iGuard are provided. Finally, this work is concluded in Section VI.

II. Related Work

Privacy leakages caused by using cloud services have been identified in previous work. Chairunnanda et. al [6] indicated that users' identities were constructed from their typing patterns. Liao et. al [7] showed that users' daily activities and movements were identified from raw GPS data collected by mobile devices. Ferrari et. al [8] observed that users' mobility patterns in an urban environment were extracted from their participation in social networks. Valkanas and Gunopulos [5] demonstrated that user's location information was exposed from general textual information about their surroundings in social networks without using a GPS-enabled device. Murukannaiah and Singh [9] indicated that users social circles could be identified by bringing together contextual information and users' online social interactions. These work provides various privacy measurements on different privacy leakages. iGuard utilizes suitable privacy measurements and makes privacy measurement plans for users according to their personal settings.

Protection strategies that alleviate the identified privacy leakages are also proposed. Stenneth and Yu [10] used a trusted thirdparty server as the mediator between user devices and cloud services, and applied the k-anonymity technique to hide identifications of the user devices. Zhang et. al [11] used noise data to obfuscate cloud services. The authors generated noise service requests and injected these requests into real customer service requests. The noise service requests' occurrence probabilities were identical to customer service requests so that cloud service providers could not distinguish them from customer service requests. Customers' privacy was consequently protected. Ren et. al [12] partitioned data into data fragments and stored them to different cloud services. Beresford et. al [13] created a modified version of the Android operating system that allowed users to 'mock' access to the resources of user devices for cloud services. Guha et. al [14] proposed the Koi platform which avoided leaking privacy-sensitive information by masking low-level lat-long information from applications. Kasai et. al [15] proposed a service provision system that selected the best-working services for users according to the minimal personal information provided by the users. Among all these privacy protection strategies, iGuard provides users the ones that solve their identified privacy leakages. Users can select the preferred one and apply it for protecting their privacy.

III. User-Centric Privacy Protection

A user uses cloud services through the mobile device to solve daily problems, and the combination of cloud services in use varies from person to person. Furthermore, information exposure that causes "privacy leakage" to a user also varies from person to person, since the definition of "sensitive information" is different for every user. Some users take their political views as sensitive information but others do not. Some users mind revealing their home addresses, but others do not. Every user has his own sensitive information list describing personal information that should not be exposed to others. As a result, iGuard applies user-centric privacy protection to take the user's personal situation into consideration. The process of the user-centric privacy protection is shown in Figure 1. Details of each step of the process are described as follows.

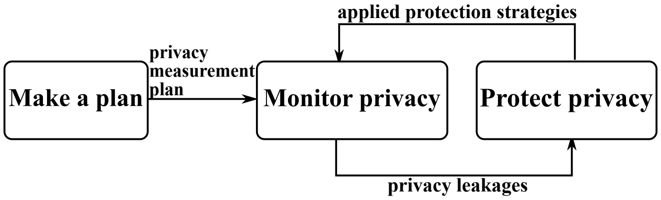


Figure 1. The user-centric privacy protection process.

- **Step 1. Make a plan.** Privacy monitoring is performed according to a customized privacy measurement plan, which is made based on the user's personal situation. The privacy measurement plan is the base to ensure the user's privacy when he is using cloud services. The privacy measurement plan defines the privacy measurements which should be applied and the timing of triggering these privacy measurements. Selection of the privacy measurements is based on
  1) the type of cloud services in use,
  2) the type of usage data that is sent to the cloud services, and
  3) the user's sensitive information list.

  A privacy measurement does not need to be triggered in real time when the user is using a cloud service. It can be a summary of user operations in a period of time, e.g., a day or several hours. The frequency of applying a privacy measurement is decided according to the user's preference and characteristics of the privacy measurement.

- **Step 2. Monitor privacy.** When the user is using a cloud service through the mobile device, usage data sent to the cloud service should be evaluated for privacy concern. In this step, corresponding privacy measurements are triggered. The privacy measurements take the usage data as input and indicate potential privacy disclosure threats. The user will receive warnings if privacy leakage is detected. He reviews details of the warning and takes further actions for protecting his privacy (step 3).
- **Step 3. Protect privacy.** The user can apply privacy protection strategies to alleviate the privacy leakages. Privacy protection strategies are divided into two categories.
    1) Changing user behavior. Changing the way that a user uses the cloud service will also change the usage data received by the cloud service. The user can thus hide his sensitive information by changing his behavior. For example, a user checks his e-mails most frequently when he is at work. If the user's working hours are detected from his usage frequency, he can confuse the cloud service by using the cloud service as evenly as possible in different time periods of a day.
    2) Applying third-party privacy protection services. There are a variety of privacy protection services available to protect the user's privacy. These services can insert noises to normal usage data [11], use fake data to replace real data [13], or suggest the best-working cloud services that fit the user's privacy requirements to replace the cloud service in use [15]. By applying these privacy protection services, the user can keep his privacy safe while using the cloud service as normally as possible.

  The user can apply more than one privacy protection strategies, and observe their effects on the results of the privacy measurements (step 2). The user can change or adjust the strategies to find one that best fits his personal situation, and balances the trade-offs between cloud service utilities and privacy protection.

IV. iGUARD SYSTEM

The system overview of iGuard is depicted in Figure 2. Components of iGuard are divided into three parts.

1) **Packet collector**. To detect possible privacy leakages, iGuard has to collect usage data which is sent to cloud services. Packet collector is responsible for collecting mobile device packets to further extract usage data from them.
2) **iGuard client**. iGuard client is the interface between the user and iGuard server. It is implemented as an application installed on the mobile device to interact with the user. iGuard client allows the user to review results of the privacy measurements, and send his personal preferences to iGuard server. Once privacy leakage is detected, iGuard client generates instant notification to the user.
3) **iGuard server**. iGuard server consists of four components: plan maker, privacy measurement coordinator, service agent, and strategy suggester. The four components collaborate to complete the whole process of user-centric privacy protection.

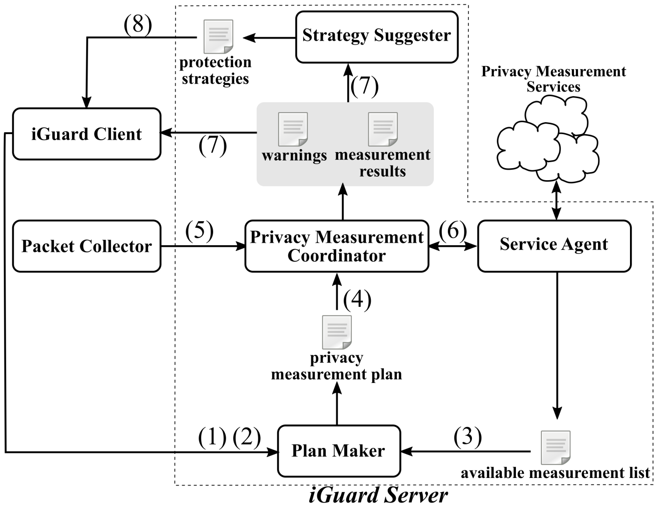


Figure 2. iGuard system overview.

In the following, the ways that the components of iGuard server achieve user-centric privacy protection are illustrated.

A. Make a Plan

Making a personalized privacy measurement plan includes the following three steps.

1) **Acquire types of usage data that will be sent to cloud services**. Applications are client-side interfaces for cloud services. Permissions of an application reveal the types of data that will be acquired by its corresponding cloud service. At the beginning, iGuard client collects all the applications installed on the mobile device and their permissions. iGuard client sends the information to plan maker (1). Plan maker analyzes permissions of the applications and gets the types of usage data collected by the cloud services behind the applications. If a new application is installed on the mobile device, plan maker will be notified about the new-installed application and update the privacy measurement plan.
2) **Confirm the user's sensitive information list**. In this step, plan maker checks the user's sensitive information list. A sensitive information list describes a user's personal information that should not be exposed to others. Initially, iGuard client provides a generalized sensitive information list to the user. Once the user tunes the list to get a personalized sensitive information list, plan maker will receive the updated list from iGuard client (2).
3) **Check available privacy measurements**. Plan maker gets the list of available privacy measurements from service agent (3), which is responsible for communicating with third-party privacy measurement services. In the available measurement list, privacy measurements provided by the third-party privacy measurement services are described. For each of the privacy measurements in the list, its type of input

data, focused privacy leakage, and suggested detection frequency are provided. Plan maker selects the privacy measurements, which not only fit in the types of usage data but also can detect leakages of sensitive information. Plan maker then creates a privacy measurement plan, which defines the corresponding privacy measurements and their triggering frequency when the cloud services are used.

After a privacy measurement plan is created or updated, plan maker sends it to privacy measurement coordinator for performing privacy monitoring (4).

B. *Monitor Privacy*

When the user is using the cloud service, mobile phone packets sent to the cloud service are acquired by packet collector. Packet collector can be a component which embeds either in a modified version of the Andriod operating system or in software-defined networking [16]. Packet collector then copies the packets to privacy measurement coordinator (5). Privacy measurement coordinator identifies the cloud service in use and extracts the usage data sent to the cloud service. Privacy measurement coordinator accumulates the usage data until the triggering time of the corresponding privacy measurements specified in the privacy measurement plan comes. To trigger a privacy measurement, privacy measurement coordinator activates the corresponding privacy measurement service through service agent (6). Service agent is responsible for communicating with privacy measurement services. Once it receives measurement results from the privacy measurement service, service agent passes the measurement results back to privacy measurement coordinator. Privacy measurement coordinator keeps the measurement results for user review in the future. If privacy leakages are identified in the measurement results, privacy measurement coordinator will generate warnings to iGuard client and activate strategy suggester (7).

As all sorts of portable devices are invented and widely used, new types of usage data are exposed to cloud services, such as the user's daily amount of exercise and heart rate. Demands for new privacy measurements increase to detect new privacy risks caused by the usage data. To flexibly add new privacy measurements, service agent applies the service-oriented architecture (SOA). Third-party privacy measurement services are assumed trustworthy. They are self-contained units which provide privacy measurement functionality. The mechanism for communication between service agent and privacy measurement services is described in authors' another work [17]. A privacy measurement service can join iGuard by registering to service agent. If a new privacy measurement service successfully registers to service agent, service agent will update the available measurement list. Service agent also updates the available measurement list when a privacy measurement service becomes unavailable. Once the available measurement list is updated, service agent will notify plan maker to update the privacy measurement plan.

C. *Protect Privacy*

The goal of privacy protection strategies is to confuse cloud services so that sensitive user information will not be inferred from the usage data. Strategy suggester collects privacy protection strategies that can work on a specific type of usage data. Taking GPS data as an example, the user can turn off the GPS sensor, change his route, or use a privacy protection service to insert fake GPS data into his usage data. Strategy suggester provides possible protection strategies (8) according to the type of usage data that causes the privacy leakage. Regarding more than one privacy leakages, the user can apply several protection strategies at the same time. The effect of the applied strategies will be reflected in the results of future privacy measurements. The user can tune and change the privacy protection strategies until he is satisfied with the results.

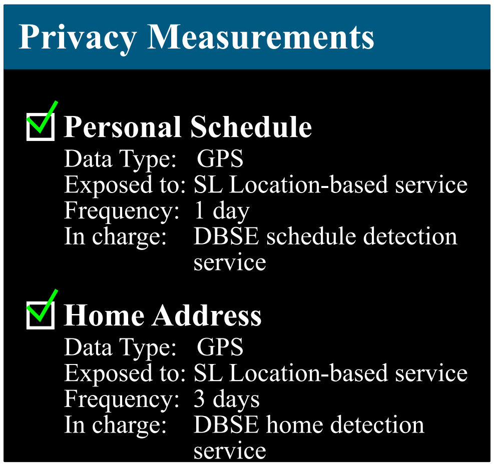
V. Case Studies

GPS data is common in the usage data exposed to cloud services. The case studies demonstrate not only that extra user sensitive information will be leaked from the GPS data, but also the ways that iGuard assists user in detecting the leakages and fixing them. To make the case studies as real as possible, real telecommunications service usage data with user's GPS locations is used to simulate the user's usage data exposed to a location-based cloud service. The telecommunications service usage data is provided by Mr. Malte Spitz, a German Green Party politician and Executive Committee member. He acquired the usage data from his telecommunications service provider. The usage data can be downloaded on ZEIT Online [18]. This data set was collected from August 2009 to February 2010, and contained 30,374 location-based usage data. It is assumed that the location-based service collects the user's GPS locations to provides contextual information for him, such as the weather, traffic conditions, nearby restaurants which are open, etc. It is assumed that this location-based service always runs in the background and collects the user's locations regularly to update the contextual information. The user can also actively query the location-based service for further information. When the user is actively using the location-based service, his locations will be collected more frequently than normal. So, the behavior of the location-based service in collecting the user's GPS locations is close to the telecommunications service. The location-based usage data of the telecommunications service is used to simulate the usage data collected by the location-based service. In the case studies, iGuard is applied to eliminate the privacy issues which result from exposing the user's personal schedules and home address to the location-based service.

At the beginning, iGuard makes the privacy measurement plan, as shown in Figure 3. In Figure 3, two privacy measurements which aim at GPS data are selected. One is for detecting personal schedule leakage, and the other is for detecting user's home address leakage from the exposed GPS data. For each privacy measurement, the type of the target usage data, the cloud service which the usage data is exposed to, the frequency to perform the privacy measurement, and the privacy measurement service which is in charge to perform the privacy measurement are displayed. Currently, those two privacy measurement services are implemented by authors as third-party privacy measurement services. If the user unchecks the box before a privacy measurement, the privacy measurement will not be performed. Results of these two privacy measurements are shown in the following.

A. *Case 1: Personal Schedule Leakages*

Since the location-based service is frequently used in the user's daily life, user's usage frequency reflects his personal



Privacy Measurements

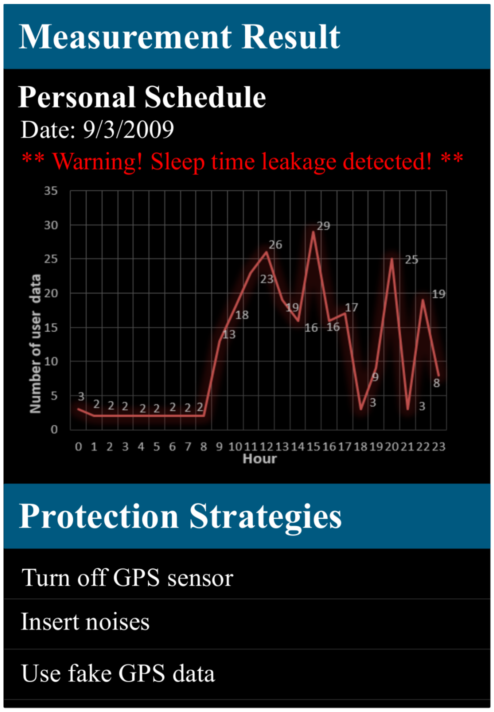
☑ Personal Schedule

Data Type: GPS
Exposed to: SL Location-based service
Frequency: 1 day
In charge: DBSE schedule detection service

☑ Home Address

Data Type: GPS
Exposed to: SL Location-based service
Frequency: 3 days
In charge: DBSE home detection service

Figure 3. The privacy measurement plan.



Measurement Result

Personal Schedule

Date: 9/3/2009

** Warning! Sleep time leakage detected! **

Protection Strategies

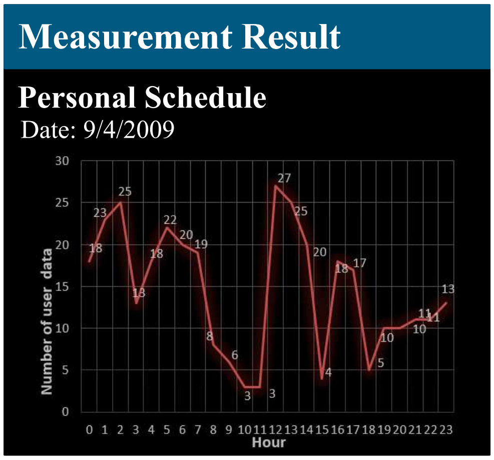
Turn off GPS sensor

Insert noises

Use fake GPS data

Figure 4. The privacy leakage for personal schedule.

schedule, especially the sleep time. The user will not use the location-based service when he is sleeping. A time duration that the usage frequency is steady but relatively low can be the user’s sleep time. This privacy measurement checks the number of usage data transmissions to the location-based service in each hour of a day to find possible sleep time leakages. The privacy measurement is performed once a day and takes usage data of the whole day as the input. In fact, the measurement results of the usage data for each day from August 2009 to February 2010 are similar. The sleep time is leaked almost every day from the usage frequency of the service. In this case study, the usage data on 09-03-2009 is selected as the example to demonstrate the privacy leakage, as shown in Figure 4. In the measurement results, there is a relatively low and steady curve in the time duration 1:00-8:59, which is a hint for the sleep time leakage. Below the measurement results, privacy protection strategies for GPS data are suggested. If the user selects to insert noises to his future usage data to change his service usage frequency, iGuard will suggest corresponding privacy protection services that are available to assist the user in completing the work. In this work, a noise inserting service is implemented to assist user in inserting noises to his usage data. The service inserts noises that are similar to the normal usage data [11]. The new measurement results are show in Figure 5. The measurement results show that the privacy leakage is eliminated by the strategy.



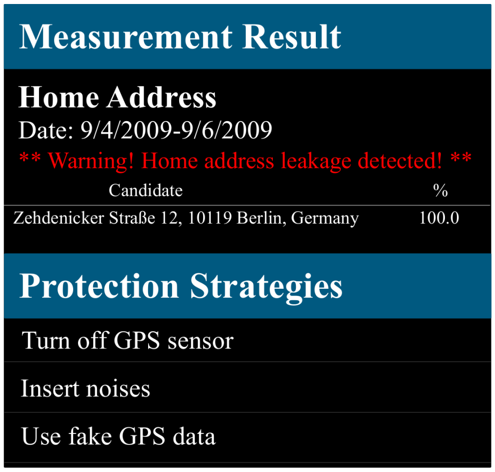
Measurement Result

Personal Schedule

Date: 9/4/2009

Figure 5. The measurement results after a privacy protection strategy is applied.

B. *Case 2: Home Address Leakages*



Measurement Result

Home Address

Date: 9/4/2009-9/6/2009

** Warning! Home address leakage detected! **

Candidate	%
Zehdenicker Straße 12, 10119 Berlin, Germany	100.0

Protection Strategies

Turn off GPS sensor

Insert noises

Use fake GPS data

Figure 6. The privacy leakage for home address.

Most people stay at home to sleep at night. If the user’s locations in sleep time are exposed to cloud services, his home address is likely to be exposed, too. This privacy measurement checks the user’s locations exposed to the cloud service in sleep time for possible home address leakages. The privacy measurement is performed every three days according to the privacy measurement plan. The user is assumed to be sleeping during 1:00 AM to 4:00 AM. The privacy measurement calculates the percentage which the user stays at a location in the period of time. In this case study, the usage data from 09-10-2009 to 09-12-2009 is used as an example to demonstrate the home address leakage, as shown in Figure 6. The measurement results show that the user only stays at one location during the sleep time of these three days. The location can indicate the user's home address. The user can select to insert noises with fake GPS data when he is at home. The fake GPS data is mixed with real ones and the percentage of fake data can even be higher than real data. As a result, the user can mislead the location-based service to wrong home address information so that the home address leakage can be prevented.

VI. Conclusion and Future Work

iGuard plays the role of a mediator, which links available privacy measurements and privacy protection strategies to the user. According to the user's personal situation, iGuard performs customized privacy measurements for the user and suggests workable strategies to protect his privacy. In the user's view, the user will enjoy comprehensive privacy detection and protection as available privacy measurements and protection strategies linked to iGuard extend. In the view of providers for services of privacy measurement and privacy protection, they benefit from increasing users of their services. iGuard creates a win-win situation for both of users and service providers handling privacy issues.

In the future, iGuard will be extended for various user devices, such as smart home systems in Internet of Things (IoT), and assist users in managing their privacy for all devices in use. iGuard will provide users a comprehensive protection strategy that considers users' personal preferences and handles all privacy issues caused by using the devices. Thus users can enjoy simple and effective way to keep their privacy while utilizing all services through various devices.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable suggestions that improved this paper. This research was supported in part by the Ministry of Science and Technology of Taiwan under Contracts MOST 104-2221-E-006-158 and MOST 104-2221-E-006-040.

References

[1] H. Seybert and P. Reinecke, "Internet and Cloud Services - Statistics On The Use by Individuals." http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_and_cloud_services_-_statistics_on_the_use_by_individuals, Dec. 2014. [Online; retrieved: Jun. 15, 2016].

[2] K. Shilton, "Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection," *Communications of the ACM*, vol. 52, no. 11, pp. 48–53, Nov. 2009.

[3] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing ," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1 – 11, Jan. 2011.

[4] L. Liao, D. J. Patterson, D. Fox, and H. Kautz, "Learning and Inferring Transportation Routines," *Artificial Intelligence*, vol. 171, no. 5-6, pp. 311–331, Apr. 2007.

[5] G. Valkanas and D. Gunopulos, "Location Extraction from Social Networks with Commodity Software and Online Data," *2012 IEEE 12th International Conference on Data Mining Workshops (ICDMW)*, pp. 827–834, 2012.

[6] P. Chairunnanda, N. Pham, and U. Hengartner, "Privacy: Gone With the Typing! Identifying Web Users by Their Typing Patterns," *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom)*, pp. 974–980, Oct. 2011.

[7] L. Liao, D. J. Patterson, D. Fox, and H. Kautz, "Building Personal Maps from GPS Data," *Annals of the New York Academy of Sciences*, vol. 1093, no. 1, pp. 249–265, 2006.

[8] L. Ferrari, A. Rosi, M. Mamei, and F. Zambonelli, "Extracting Urban Patterns From Location-Based Social Networks," *Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Location-Based Social Networks*, pp. 9–16, 2011.

[9] P. Murukannaiah and M. Singh, "Platys Social: Relating Shared Places and Private Social Circles," *IEEE Internet Computing*, vol. 16, no. 3, pp. 53 –59, May-Jun. 2012.

[10] L. O. Stenneth and P. S. Yu, "Privacy-Aware Mobile Location-Based Systems," *Proceedings of the 1st International Workshop on Mobile Location-Based Service*, pp. 79–88, 2011.

[11] G. Zhang, X. Liu, and Y. Yang, "Time-Series Pattern Based Effective Noise Generation for Privacy Protection on Cloud," *IEEE Transactions on Computers*, vol. 64, no. 5, pp. 1456–1469, May 2015.

[12] P. Ren, W. Liu, and D. Sun, "Partition-Based Data Cube Storage and Parallel Queries for Cloud Computing," *2013 Ninth International Conference on Natural Computation (ICNC)*, pp. 1183–1187, Jul. 2013.

[13] A. R. Beresford, A. Rice, N. Skehin, and R. Sohan, "MockDroid: Trading Privacy for Application Functionality on Smartphones," *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, pp. 49–54, 2011.

[14] S. Guha, M. Jain, and V. N. Padmanabhan, "Koi: A Location-Privacy Platform for Smartphone Apps," *Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation*, 2012.

[15] H. Kasai, W. Uchida, and S. Kurakake, "A Service Provisioning System for Distributed Personalization With Private Data Protection," *Journal of Systems and Software*, vol. 80, no. 12, pp. 2025 – 2038, 2007.

[16] R. Jin and B. Wang, "Malware Detection for Mobile Devices Using Software-Defined Networking," *Proceedings of the 2013 Second GENI Research and Educational Experiment Workshop*, pp. 81–88, 2013.

[17] C.-W. Hu and H. C. Jiau, "Trust Circle: Promoting Collaboration and Data Sharing Between Data Providers and Data Consumers in IoT," submitted for publication.

[18] K. Biermann, "Betrayed by Our Own Data." http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz, Mar. 2011. [Online; retrieved: Jun. 15, 2016].