Privacy-Preserving Online Monitoring Framework for e-Health Applications

Youna Jung
Department of Computing and Information Sciences
Virginia Military Institute
Lexington, Virginia, United States
e-mail: jungy@vmi.edu

Abstract— **Many e-health applications track how they are used by patients to enable and validate their effectiveness. While online monitoring can improve the accuracy and quality of e-health applications, there is the potential of serious privacy violations. As e-health applications use online monitoring services, sensitive health data could be exposed to not only the healthcare providers but also the monitoring service providers against wishes of a user. To prevent privacy loss during online monitoring, in this paper, we propose a privacy-preserving online monitoring framework, in short PPoM, that helps providers and users of e-health applications specify their own policies and enforce user privacy policies in systematic manner. To support medical staff and users who do not have enough knowledge and skills on Information Technologies (IT), the PPoM framework provides intuitive and automatic tools that enable non-IT administrators and users to generate privacy policies, enable administrators to automatically insert monitoring code into their e-health applications, and control outgoing messages sent from users' browsers.**

Keywords-e-health application; online monitoring; privacy protection; framework.

I. INTRODUCTION

Online monitoring and analytics are essential techniques to evaluate and enhance the performance of online applications. They help the online service providers improve the usability of their applications by collecting user/usage data and analyzing the performance of applications [1][2]. In general, there are three different approaches to online user monitoring: 1) log file analysis on the server side, 2) proxy-based monitoring, and 3) use of monitoring scripts provided by online monitoring/ analytics services on the client side [3]. In this paper, we focus on the third approach because it is widely used and requires less time and effort to collect, analyze, and visualize user/usage data.

Online monitoring and analytics services, such as Google Analytics [4] and Adobe Analytics [5] have been widely used in a variety of online application areas, such as e-health [6], e-commerce [7], information retrieval [8], and so on. These monitoring/analytics services enable the tracking and recording of user actions and characteristics, such as mouse clicks, frequency of use of an application, time spent in a particular page, media viewed, page navigation sequences, content entered into a textbox, location information, whether a mobile device is being used, and so on.

Among various online application areas, we focus on the healthcare and wellness domains because e-health applications are becoming ingrained into the everyday life of many people. According to Eysenbach [9], e-health is an emerging field at the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. It is an umbrella term that includes a variety of online healthcare applications and systems that use information technologies, such as e-Learning for healthcare, e-Diagnosis, e-Prescribing and online health interventions. By using advanced information technologies, including electronic data management and rich interaction skills, e-health applications are capable of 1) providing personalized services, 2) reducing healthcare cost, 3) ensuring easy access regardless of time and place, 4) ensuring consistent quality of services over time, 5) enabling automated data collection/analysis, and 6) demonstrating the potential for having more honest self-reporting by patients [11]. Many e-health applications have been used for online healthcare education [10], healthcare research [11] and recruitment of its participants [12], collecting healthcare data for research or national healthcare purposes, and conducting healthcare interventions to facilitate disease prevention, disease self-management, and health promotion [13].

Most e-health applications provide several of the following functionalities: 1) self-assessment or self-profiling to recognize individuals' health-related status and in turn provide personalized messages and/or healthcare services, 2) continuous communication with patients/users using interactive tools such as online trackers, and 3) wide dissemination of information related to health and safety, presented in text and/or multimedia format. To accomplish the purposes of e-health applications, on one hand, detailed monitoring is critical to confirm that e-health applications are used correctly and to validate their efficacy. In order to do so, e-health applications must collect detailed, and often identifiable, user data including health information. On the other hand, the protection of user privacy is however critical since e-health applications often deal with very sensitive private data, including health status, medical records, and family health histories. Control over the sharing of this information is of the utmost importance and urgency because indiscriminate monitoring, if inconsiderate of user privacy, may result in private health data being used for unwanted purposes and/or shared with unknown people [1][14][15]. In case of e-health applications, even generic usage data can be damaging if disclosed. For example, disclosure of the login frequency into an online treatment application for substance

 ISBN: 978-1-61208-424-4

abuse can unintentionally reveal a user's medical status. Consequently, it is urgent and critical for research to examine how we can simultaneously achieve these two important yet opposing goals -- monitoring identifiable user data while protecting user privacy.

To enable e-health applications to conduct trustworthy user monitoring without concern for loss of privacy, in this paper, we propose a new Privacy-Preserving online Monitoring (PPoM) framework. In the PPoM framework, online monitoring services collect user/usage data based on users' policies and users can verify user/usage data being monitored and strictly enforce user policies on the client side. The rest of this paper is organized as follows. In Section II, the requirements for secure online monitoring in e-health applications are identified. In Section III, PPoM framework is proposed and the overall architecture is described. For better understand of practical use, in Section IV, operation flows and example use cases are described in detail. In Section V, evaluation plans are presented. Section VI reports on the related work. The conclusions and future work are presented in Section VII.

II. LIMITATIONS AND REQUIREMENTS

A. Limitations

Existing online monitoring approaches on e-health applications have two major problems, as follows:

1) Lack of systemactic methods to verify and enforce privacy policies mutually agreed by users and providers: To protect user privacy during online monitoring, a user needs to specify his/her preference in data disclosure while the administrators of an e-health application specify their privacy policy describing what kinds of user data might be monitored, what those data are used for, who those data will be shared with, and how user data are maintained. Users and administrators can specify their policies using policy languages such as P3P [19] and WS-XACML [20]. Once a user agrees to an application's policies, the enforcement of agreed policies has been primarily relied on the honor system [16] within the application without any external verification process. To ensure user privacy, the federal Health Insurance Portability and Accountability Act (HIPAA) [17] stipulates that a healthcare component must not disclose protected health information to another component (HIPAA 164.105.(a)(ii)) with only a few exceptions (HIPAA 164.512). However, it is difficult to expose violations of HIPAA regulations within e-health applications in existing approach. If a provider embeds monitoring code and/or third-party data-collecting ads in its webpages, private data can easily be released regardless of users' wishes. Although this is an obvious violation of HIPAA rules, there are no solutions to systematically detect the application's fraud and prevent user data from undesirable use and disclosure.

To protect user privacy from undesirable use, some online applications anonymize/de-identify user data by deleting identifiers in original data but such anonymized data can often be re-identified/de-anonymized [18]. It is hence not enough to hide user identifiers and we need a new method not to share critical information based on user preferences. In addition, anonymization might not be applicable to some e-health applications that require identifiable user data for personalized services. Without a strong enforcement method, many users are unlikely to consent to online monitoring.

2) Need for professional IT knowledge and skills: At present, professional IT knowledge is needed for developing e-health applications with appropriate privacy-preserving monitoring. For example, to specify privacy policies of an e-health application, an application administrator must understand privacy policy languages, such as P3P [19] or WS-XACML [20] and be able to precisely specify the application's policy in that language. In addition, to use an online monitoring service, the administrator must understand the client-side monitoring code (e.g., in JavaScript), and be able to manually insert privacy-preserving code into the original source code (possibly using different languages) for each web object or webpage being monitored. Hence, administrators of e-health applications need to understand at least one language to integrate privacy-preserving monitoring into applications. This is however an impractical expectation for many non-IT administrators, such as doctors, nurses, health educators and communicators. Not only for non-IT clinical staff who manage e-health applications but also for average users who use e-health applications, it is difficult to exactly specify privacy policies and enable their applications/browsers to protect user privacy. The lack of IT knowledge of administrators and users of e-health applications significantly increases the need for easy-to-use tools for a privacy-preserving framework.

B. Requirements

Towards trustworthy and highly usable online monitoring in e-health applications, the following requirements should be satisfied:

1) For strict enforcement of user privacy policies

- Online monitoring services that are aware of user privacy policies rather than application policies.
- Verification methods to ensure that an application complies with policies mutually agreed by providers and users on user side.
- Enforcement methods to protect user privacy on user side in case of privacy violation during online monitoring.

2) For practical use by non-IT users and staff

- User-friendly interfaces to intuitively specify privacy policies and monitoring objects.
- Automatic generation of privacy policies for e-health applications.
- Automatic conversion of existing e-health applications to privacy-preserving applications in which privacy-aware monitoring code is embedded.

 ISBN: 978-1-61208-424-4

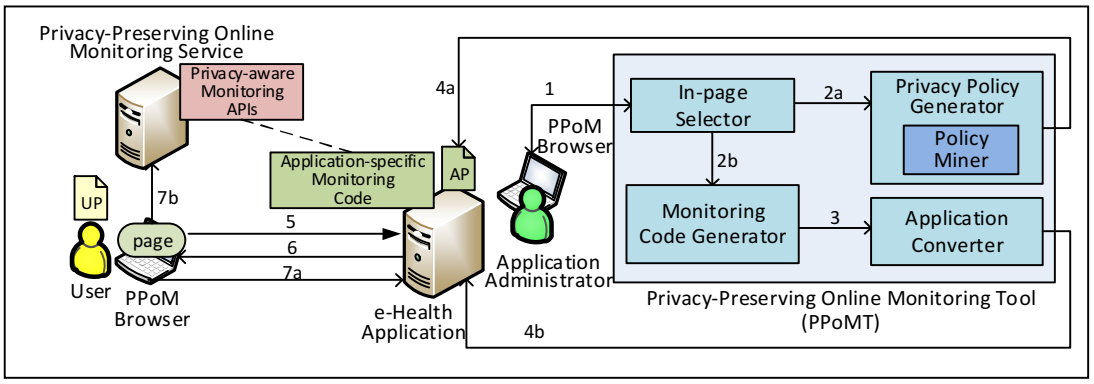

Figure 1. Overall architecture of PPoM framework.

III. OVERALL ARCHITECTURE

To fulfill the requirements described above, in this paper, we propose a new PPoM framework that rigorously protects user privacy by referring user policies and enforcing them on user side. For convenient and easy adoption by e-health application providers, PPoM includes easy-to-use tools for users and providers. The overall architecture of PPoM framework is shown in Figure 1. The detailed descriptions for each component are following:

A. PPoM Service

The problems of existing online monitoring services are twofold. First, users are forced to choose between two options: opt-in or opt-out, and not allowed to choose data to be monitored in fine-grained level. Second, user data are collected based on the decision of providers. Once a user gives consent to monitoring (opt-in), all user activities on the web objects in which monitoring code is embedded are captured regardless of users' privacy preferences. None of existing services considers users' privacy preferences during monitoring.

To address the issue of ignorance of user preferences during monitoring, we propose a PPoM service that gathers only authorized user/usage data that users allow to monitor. By specifying privacy policies, users determine which data can be monitored. User policies will be then enforced by a trustworthy third-party monitoring service, the PPoM service. Using the PPoM service, e-health applications can guarantee effective protection of user privacy by providing a way to enforce user policies in a systematic manner rather than simply providing a written agreement. The concrete enforcement framework assists both monitoring services and e-health applications in building better reputations and accelerates active participation in e-health applications without concerns about privacy leakage. In addition, it can be used to compel and enable e-health applications to obey HIPAA regulations.

B. Privacy-Preserving User Browser

If an e-health application is trustworthy and both users and administrators can correctly specify their own policies, then existing approach may be able to guarantee secure online monitoring. However, this protection presumes the application's honesty and the user's ability to specify privacy policies precisely. Let us assume that an e-health application publishes untrusted policies that differ from its actual monitoring behavior. Once user's policies and the application's policies are matched, a user will start interaction with the dishonest application and his browser will send unconsented data to the application.

However, user privacy must be protected even if a user is exposed to untrustworthy parties, such as indiscriminate monitoring/analytics services that conduct online monitoring in violation of user privacy, naïve applications that do not have their own privacy policies or dishonest applications that write and/or enforce their policies dishonestly. To address the above security requirement, we propose a PPoM-enabled web browser (in short, PPoM browser) as a user-side protection. For easy adoption, we plan to implement a browser extension that enables existing browsers (e.g., Explorer and Chrome) to perform following tasks:

1) It presents all user data being monitored by online monitoring service(s) in web pages: A PPoM browser displays all monitoring data and recipients of data on the screen by analysing source code of web pages.

2) It allows a user to decide which usage and his/her data can be disclosed: A PPoM browser inspects data types, data values, and destinations of all outgoing message according to user policies. If it detects malicious monitoring that violates user policies, it alerts a user to unauthorized monitoring. For example, if the user decides to disclose his/her medical history to a first-party (e.g., an e-health application website), then a PPoM browser only allows outgoing messages to the e-health application and blocks other messages to other entities (such as ad companies or social networking sites) even if the application does not have its own privacy policy or inserts monitoring code to collect his/her medical history data.

3) It refines the user's privacy policies based on updated user preferences: If a user' privacy policies are naïve or incorrect, the proposed approach based on user policies cannot protect user privacy successfully. However, It is very difficult for average users to specify precise privacy policies because it is hard to understand the correlation between description of user data in privacy

 ISBN: 978-1-61208-424-4

policies and web objects in web pages. To enhance the proposed PPoM framework, a PPoM browser allows users to refine their preferred policies by intuitively selecting what user/usage data can be monitored in web pages.

C. *Privacy-Preserving Online Monitoring Tool*

As pointed out in Section II. A, it is difficult for non-IT administrators to have professional IT knowledge and skills that necessary for trustworthy online monitoring. In this paper, we propose the PPoM Tools (PPoMT) to help health professionals. PPoMT enables non-IT clinical staff to specify privacy policies for their healthcare applications, and/or to easily convert their applications into privacy-preserving applications that analyze user/usage data without violating user privacy. While motivated by the needs of non-IT administrators, this tool could also improve the efficiency of developers who are required to insert monitoring code into their applications. The PPoMT consists of four individual tools: the In-page Selector, the Monitoring Code Generator, the Privacy Policy Generator, and the Application Converter. The detailed explanations for each tool are following:

1) In-page Selector: It is a server-side software module that is capable of generating modified webpages that have user-friendly interfaces for selection of web objects to be monitored and corresponding policies and delivering user selections to the Privacy Policy Generator and the Monitoring Code Generator. It sends modified webpages to the PPoM browser of an administrator. By clicking on web objects that are displayed in the PPoM browser (e.g., a button, link, text, image, or video), the administrator can select which objects to monitor without any IT knowledge and skills. Additionally, he can declare corresponding privacy policies.

2) Monitoring Code Generator: It generates privacy-aware monitoring code by receiving an administrator's selection on monitoring objects and associated privacy policies from the In-page Selector. The generated code will be varied depending on monitoring services.

3) Privacy Policy Generator: It helps non-IT administrators who may be unfamiliar with online privacy policy languages publish privacy policies for their own applications. Using the Policy Miner, it derives the privacy policies for a given application by analyzing all monitoring objects and corresponding privacy policies that are selected by the administrator.

4) Application Converter: It helps non-IT administrators to update source code of an existing application by assisting them in inserting the privacy-aware monitoring code generated by the Monitoring Code Generator. Once the code modifications are made, an administrator needs to deploy the modified source code in their server.

IV. PRIVACY-PRESERVING MONITORING USING PPOM

In this section, we explain how PPoM protects user privacy during online monitoring and supports non-IT administrators and users by describing operation flows and example use cases from the point of view of administrators and users.

A. *For online healthcare providers*

Let us assume that Alice, a medical doctor, administrates an e-health application that assesses the impact to people following exposure to traumatic events. To trace patients' activities and collect health-related data, Alice wants to conduct online monitoring on her applications, but it is impossible for her to use existing online monitoring services due to lack of IT-related knowledge.

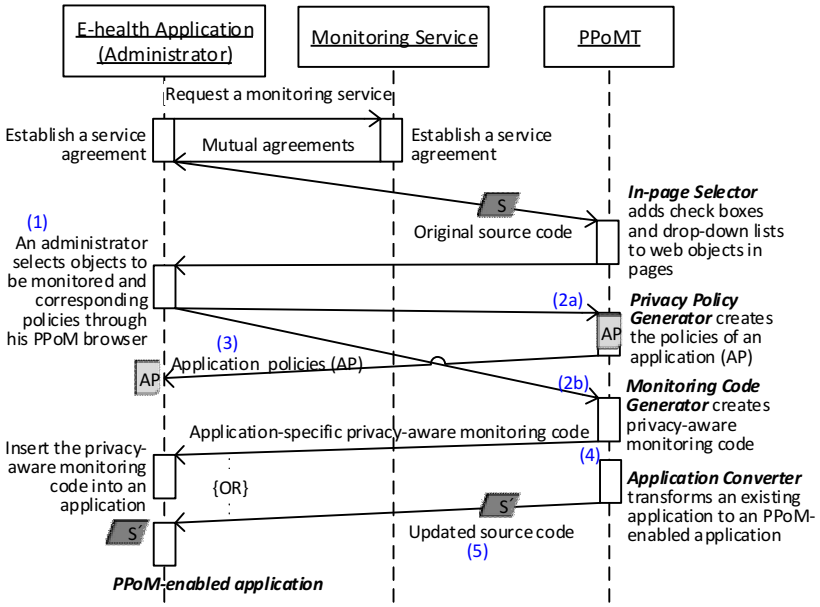

Figure 2. Operation flow of administrators of e-health applications in PPoM.

If she uses the PPoMT, she can easily transform her application into a monitoring-enabled application without any IT knowledge. For better understanding, let us look at its operational flow in detail. First, she needs to upload the source code of her application or enter the URL(s) of the application's webpage(s). Second, she selects objects to be monitored through the user-friendly interfaces generated by the In-page Selector, and specifies corresponding privacy policies (Figure 1.(1) and Figure 2.(2)). Third, her selections are delivered to the Policy Generator (Figure 1.(2a) and 2.(2a)) and the Monitoring Code Generator (Figure 1.(2b) and Figure 2.(2b)). Forth, the Privacy Policy Generator then creates the applications' policies by analyzing selected monitoring data and policies, while the Application Converter (which enables the application to perform privacy-preserving monitoring by inserting monitoring code generated by the Monitoring Code Generator into the original source code (Figure 1.(3) and Figure 2.(4)) produces the updated source code. Fifth, Alice deploys the created application policies (Figure 1.(4a) and Figure 2.(3)) and the updated source code in the application server (Figure 1.(4b) and Figure 2.(5)).

B. *For Users*

Let us assume that Bob is one of Alice's patients. Alice recommends Bob to use her e-health application every week to assess his mental and physical health but he hesitates to use the application due to privacy concern. If Bob uses the PPoM browser, he may want to use an e-health application without privacy loss. Towards this, Bob is first required to specify his own privacy policies and store his policies in his browser before using an e-health application (Figure 3.(1)). His PPoM browser then compares his privacy policies and application policies when he enters a url of Alice's application (Figure 3.(2)). If they match, the application server sends PPoM-enabled pages which privacy-aware monitoring code is embed in (Figure 1.(5)(6) and Figure 3.(3)). As he interacts with the application, the PPoM browser displays all user/usage data being monitored to enable users to verify privacy protection during online monitoring (Figure 3.(4)). If there is no privacy violation, the privacy-aware monitoring code collects only authorized user data according to policies of him specified by him for the sake of himself (Figure 1.(7a)(7b) and Figure 3.(5)). To ensure enforcement of user policies, his PPoM browser blocks outgoing messages that violate his privacy policies on the user side (Figure 3.(6)).

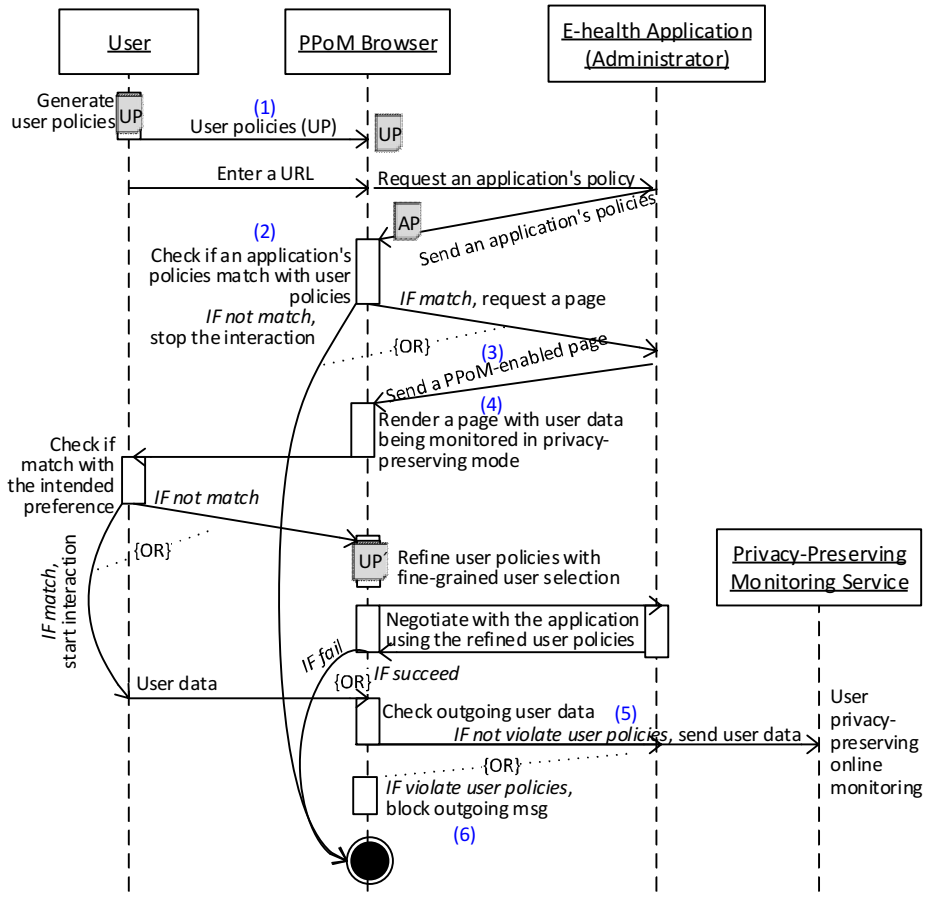

Figure 3. Operation flow of users in PPoM.

V. EVALUATION PLAN

To evaluate the performance of the proposed privacy-preserving monitoring service, we will calculate the ratio of the number of all monitoring data ($a+c$ in Table I) to the number of unauthorized but collected data (c in Table I). In addition, we will also test the successful blockade ratio of the number of messages containing unauthorized data ($g+h$ in Table II) to the number of blocked messages among them (g in Table II). We will plan to test the developed tool, PPoMT, by comparing a user's selections of monitorable data and corresponding privacy preferences with monitoring scripts or source code that generated by PPoMT. To evaluate the correctness of the generated privacy policies, we will create a variety of anticipated privacy policies, use PPoMT to generate privacy policies, and compare the resulting policies with the anticipated policies.

TABLE I. USER DATA MONITORED BY THE PROPOSED PRIVACY-PRESERVING MONITORING SERVICE

	Monitored	**Not monitored**
Allowed	*a*	*b*
Not allowed	*c*	*d*

TABLE II. OUTGOING MESSAGES FROM A PROPOSED USER AGENT

	Sent	**Blocked**
Allowed	*e*	*f*
Not allowed	*g*	*h*

VI. RELATED WORK

A. Provider-side privacy protection for online monitoring

To guarantee secure user monitoring, a few methods have been proposed by providers of online applications and monitoring services. Some third-party advertising companies have voluntarily begun to insert an 'Adchoices' icon into their ads to increase user awareness of online tracking. However, it has been found that the icon was not very effective at making users aware of tracking occurrences [21]. As a middleware approach, Privad [22][23] is proposed to conceal a user's activities from an advertising network by interposing an anonymizing proxy between the browser and the ad network. However, the adoption of a proxy-based middleware may not be a feasible solution to small-size e-health applications because of its huge overhead requirements. In addition, it is useless if an e-health application requires identifiable user data to analyze performance of applications at the individual level.

B. User-side privacy protection for online monitoring

1) Browser-based approaches: To protect user privacy in user side, browser-based approaches have been proposed. Adnostic [24], a browser extension, is capable of behavioral profiling and targeting in users' browsers to select effective ads while not sending user data to third-party ad companies. RePriv [25] enables browsers to conduct user interest mining and only share the resulting encapsulated interests with third-parties. Both Adnostic and RePriv have only focused on targeted advertising and/or personalization but have not considered online monitoring services. As a simple solution to indiscriminate online monitoring, using opt-out cookies and/or a blocked-application list have been recommended. Opt-out cookies are, however, fragile because they can be easily disabled or deleted by a third party [26][27]. Setting a block list in a browser can effectively block malicious applications but currently this approach blocks any listed application in its entirety and does not support fine-grained blocking at the data level.

2) Policy-based approaches: As a policy-based protection approach, Privacy Bird [28] has been proposed. It is a P3P user agent that reads P3P policies of online applications and lets users know whether the application policies and user preferences are matched. If policies are not matched, a bird icon turns red. A user can get information by clicking on a red bird icon. However, Privacy Bird is only able to check the acceptability of application's P3P policies, so users cannot check all user data monitored at the application's data level.

VII. CONCLUSION AND FUTURE WORK

The lack of reliable and effective methods of privacy protection has been the biggest obstacle to the growth of e-Health applications. Without a suitable solution, people keep hesitating to use e-Health applications, even though those applications help users access healthcare services in easy and convenient way at the reduced cost. To address the privacy protection issue above, in this paper, we proposed the PPoM framework that protects user privacy in both the application side and the user side so that secure online monitoring can be guaranteed in the entire process of online monitoring. We believe that PPoM accelerates practical use of e-health applications. Towards this goal, a few challenges need to be pursued in the future:

- Development of the privacy policies to specify preferences on healthcare data in fine-grained level.
- Development of a privacy-preserving monitoring service that protects user privacy based on user policies.
- Development of the PPoM browser and tools.
- Performance tests on the other individual components and an integrated component and a field test associated with actual clinical trials.
- Development of a threat model for PPoM and security test using a threat model.

REFERENCES

[1] J. R. Mayer and J. C. Mitchell, "Third-Party Web Tracking: Policy and Technology," Proc. IEEE Symp. on Security and Privacy (SP '12), IEEE Press, 2012, pp. 413-427, 2012, doi=10.1109/SP.

[2] B. A. Schroeder, "On-line monitoring: A tutorial," IEEE Computer, vol. 28, no. 6, pp. 72-78, 1995.

 ISBN: 978-1-61208-424-4

[3] N. Schmucker, "Web Tracking," SNET2 Seminar Paper (Online), 2011. http://www.snet.tu-berlin.de/fileadmin/fg220/courses/SS11/snet-project/web-tracking_schmuecker.pdf [retrieved: June, 2015].

[4] Google Analytics. http://www.google.com/analytics/index.html [retrieved: June, 2015].

[5] Adobe Analytics. http://www.adobe.com/sea/solutions/digital-analytics.html [retrieved: June, 2015].

[6] M. N. K. Boulos et al., "CAALYX: a new generation of location-based services in healthcare," Int. J. Health. Geogr., vol. 6, no. 1, March 2007, pp. 1-6, doi:10.1186/1476-072X-6-9.

[7] C. Hoelscher and H. Dietrich, "E-Commerce Personalization and Real-Time Site Monitoring," in Designing personalized user experiences in eCommerce, Kluwer Academic Publishers, 2004, pp. 95-117.

[8] C. L. Borgman, S. G. Hirsh, and J. Hiller, "Rethinking online monitoring methods for information retrieval systems: from search product to search process," J. Assoc. Inf. Sci. Technol., vol. 47, no. 7, pp. 568-583, July 1996.

[9] G. Eysenbach, "What is e-health?," J. Med. Internet. Res., vol.3, no. 2, 2001.

[10] J. M. Bernhardt and J. Hubley, "Health education and the Internet: the beginning of a revolution," Health. Educ. Res., vol. 16, no. 6, pp. 643-645, 2001.

[11] E. M. Daley, R. J. McDermott, K. R. B. McCormack, and M. J. Kittleson, "Conducting web-based survey research: a lesson in internet designs," Am. J. Health. Behav., vol. 27, no. 2, pp. 116-24, Mar-Apr 2003.

[12] D. F. Duncan, J. B. White, and T. Nicholson, "Using Internet-based Surveys to Reach Hidden Populations: Case of Nonabusive Illicit Drug Users," Am. J. Health. Behav., vol. 27, issue 3, pp. 208-218, May-Jun 2003.

[13] K. E. Evers, "eHealth promotion: the use of the Internet for health promotion," Am. J. Health. Behav., vol. 20, issue 4, pp. 1-7, Mar-Apr 2006.

[14] M. Bilenko and M. Richardson, "Predictive client-side profiles for personalized advertising," Proc. ACM SIGKDD conf. on Knowledge discovery and data mining (KDD '11), ACM New York, 2011, pp. 413-421.

[15] A. McDonald and L. F. Cranor, "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising," TPRC 2010 Social Science Research Network (SSRN), August 16, 2010, pp. 1-31, http://ssrn.com/abstract=1989092.

[16] Wikipedia, "The Honor System," http://en.wikipedia.org/wiki/Honor_system [retrieved: June, 2015].

[17] U.S. Department of Health and Human Services Office for Civil Rights, "HIPAA Administrative Simplification Regulation Text, 45 CFR Parts 160, 162, and 164 amended through March 26," 2013, pp. 1-115, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

[18] P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," UCLA Law Review, vol. 57, pp. 1701-2010, August 2009.

[19] P3P 1.1. http://www.w3.org/TR/P3P11/ [retrieved: June, 2015].

[20] WS-XACML 1.0. http://xml.coverpages.org/Anderson-WS-XACMLv10.pdf [retrieved: June, 2015].

[21] M. Hastak and M. J. Culnan, "Online Behavioral Advertising "Icon" Study," Future of Privacy Forum (online), 2010, http://www.futureofprivacy.org/2010/02/15/online-behavioral-advertising-icon-study [retrieved: June, 2015].

[22] S. Guha, B. Cheng, and P. Francis, "Privad: practical privacy in online advertising," Proc. USENIX conf. on Networked systems design and implementation (NSDI'11), USA, 2011, pp. 169-182.

[23] A. Reznichenko, S. Guha, and P. Francis, "Auctions in do-not-track compliant internet advertising," Proc. ACM conf. on Computer and communications security (CCS '11), New York, 2011, pp. 667-676, doi=10.1145/2046707.2046782.

[24] V. Toubiana, H. Nissenbaum, A. Narayanan, S. Barocas, and D. Boneh, "Adnostic: Privacy Preserving Targeted Advertising," Proc. Symp. on Network and Distributed System Security, March 2010, pp. 1-21.

[25] M. Fredrikson and B. Livshits, "REPRIV: Re-Envisioning In-Browser Privacy," Proc. IEEE Symp. on Security and Privacy, May 2011, pp. 1-15.

[26] P. Leon et al., "Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising," Proc. ACM Conf. on Human Factors in Computing Systems (CHI '12), USA, 2012, pp. 589-598, doi=10.1145/2207676.2207759.

[27] M. Ayenson, D. J. Wambach, A. Soltani, N. Good, and C. J. Hoofnagle, "Flash cookies and privacy II: Now with HTML5 and etag respawning," Social Science Research Network, July 2011, http://dx.doi.org/10.2139/ssrn.1898390.

[28] Privacy Bird, http://www.privacybird.org [retrieved: June, 2015].

 ISBN: 978-1-61208-424-4