PSP:A Mechanism Protecting Privacy by Providing Personal Data Management and Usage Services

Han Wang, Ling Zhang
Yan Shan University
China
wanghan@ysu.edu.cn, zhangling90@foxmail.com

ABSTRACT: *A critical challenge for privacy preserving is to enable internet users to exert some control over their personal data and meet the needs of websites to use personal data in reasonable business procedures. Privacy problem is becoming rather serious in an increasingly digital society especially for countries where necessary legal and regulation systems for personal data protection have not been well established. Thus we presented PSP (Privacy Service Provider) mechanism as an adjunct. Different from legislation and self-regulation which protect privacy by passively restricting the collection and usage of personal data, PSP protects privacy by actively providing personal data management and usage services. Internet users store their personal data in PSP and fulfill basic management like modification and access control. Instead of collecting personal data themselves, websites could get access to the personal data usage services provided by PSP including user authentication, advertising, and data analysis. Any processing on users' privacy data will be recorded for feedback service. The design model of PSP was analyzed as well as the possible implementation of services provided to both internet users and websites.*

Keywords: Privacy, Personal Data Management, Privacy Preserving, Privacy Control, Personal Data Usage

Received: 19 November 2015, Revised 23 December 2015, Accepted 8 January 2016

1. Introduction

In spite of the many convenience brought by internet services, several challenges are hindering its further development, among which privacy security stands out [1]. Usually internet users have to provide some personal data to websites in order to enjoy internet services. Personal data, such as age, gender, E-mail address and telephone numbers, are useful for websites in fulfilling transactions, optimizing operations, driving sales and marketing [2]. Properly used personal data can contribute to both parties, while the fact is that personal data is being misused and abused in a serious extent. Personal data may be collected without consent and being sold or dispatched with unknown third parties [3]. This certainly will increase the privacy risk faced by internet users since they usually have limited right in controlling the storage, distribution and usage of their personal data.

Personal data is playing an increasingly important role for websites to stay competitive in a world of big data [4]. Internet users as well are paying more attention to their privacy security. A Pew Internet Project survey found that 85% of adults believed it was "very important" for them to control access to their personal information [5]. And according to [6], 82% of online users have refused to give personal information and 34% have lied when asked about their personal habits and preferences. Privacy concern will influence both internet users and websites, which makes the conflict between personal data management and usage a major

difficulty in privacy protection, especially in countries where necessary legal or regulation systems are not well established.

With the purpose of balancing the interest of internet users and websites, we propose the PSP (Privacy Service Provider) mechanism, providing security personal data management and usage as services for both parties.

Internet users can get their personal data security stored in PSP and fulfill basic management like modification and access control. Access control enables internet users to set personalized privacy protection level on different kinds of personal data according to their preference. Personal data usage services for websites including user authentication, advertising and data analysis are designed based on Web Service Architecture (WSA), so that websites can access the services by using XML (eXtensible Markup Language) based SOAP (Simple Object Access Protocol), just like using the function in their own applications. Any processing on users' privacy data will be recorded for the feedback service so that the use of personal data can be under control of internet users themselves.

PSP central design goal is to provide a second choice for both internet users and websites so that internet users can enjoy the internet services with no need to provide personal data directly to various kinds of websites, and websites can get what they need from PSP rather than collecting personal data themselves. This mechanism is novel in that PSP provides users a convenient way to actively control and to know what's going on with their personal data, and websites can access the personal data usage services rather than the original data stored in PSP, which saves personal data from being dispatched to store in various websites and necessary privacy preserving can be enforced.

The rest of this paper is organized as follows: Section 2 presents the literature review about related work. In Section 3 we present the design of mechanism model assumed in this work. Section 4 and 5 describe the possible implementation of services offered by PSP to internet users and websites. Section 6 gives a feasibility study and finally the future work and conclusion are presented in Section 7 and 8 respectively.

2. Literature Review

2.1 Personal Data

"Personal Data" is a term that may be used in a slightly different manner by different people. According to Sweeney [7] personal data of internet users can be classified into three categories from a privacy viewpoint:

(i) identifying attributes, information that can be used to identify or locate a unique person;

(ii) confidential attributes, which contain private information that an individual typically does not want revealed, such as salary and sexual orientation; and

(iii) quasi-identifier attributes, which are normally not considered as confidential by individuals, such as age, gender, race, education, and occupation. However the values of these attributes can often be used to match the values of identifying attributes from different data sources, resulting in disclosure of individual identities.

Pearson [8] meant by this term privacy sensitive data which inaddition includs two categories:

(i) usage data: data collected from computer devices such as browsing history;

(ii) unique device identities: information that might be uniquely traceable to a user device like IP addresses.

In this study, we intend to enable internet users to actively manage their personal data rather than passively submit personal information to various websites, and meet the needs of websites in using personal data meanwhile. Thus from a different viewpoint of usage, personal data can be claisified into three categories: (i) personal data that used to pass the authentication, such as member name and password; (ii) personal data that used to fulfill transaction or achieve communication, such as telephone number and E-mail address; and (iii) personal data mainly used in data analysis process to support management and operation of websites, such as gender, occupation, and education.

2.2 Data Processing Security

In order to achieve processing security in data mining and data publishing related with personal data, a large amount of research has been dealt with privacy preserving technologies to minimize the privacy leakage and potential risks in data processing procedures [9,10].

Technologies based on distorting usually add noise to the original data or swap to achieve disturbance but keep some statistical features. Restricted data dissemination can guarantee the privacy risk under acceptable range. Data anonymity protects personal identity by using aggregation and swap. Encryption hides sensitive data and makes great contributions to security in distributed environment.

Privacy Preserving Data Mining (PPDM) is a new branch of data mining and is gaining its popularity in a world where personal data can be considered to be one of the most important assets for internet venders. PPDM aims to protect privacy during the procedure of data mining, the technologies discussed above are broadly used in PPDM to achieve privacy preserving. Since data on the internet are increasing rapidly and more internet venders need to integrate and share some of their data for better use, many research focus on privacy preserving data mining algorithms for distributed data, including clustering, classification and association rule mining when the data are vertically or horizontally distributed on two or more parties [11].

On one hand, implementation of privacy preserving technologies can help improve the privacy dilemma; On the other hand, the price in efficiency, data accuracy and business cost brought by those technologies is certainly not appealing to websites [12]. Technologies for privacy preserving seem like black box for internet users who still have no actively control on their personal data processings. PSP mechanism intends to make it possible to improve the effect of privacy protection techniques by using them broadly in personal data usage services with user control, since the original personal data would be stored in PSP only.

2.3 Access Control

Access control means concrolling the right that who could access the personal data and which kind of personal data can be shared. Mao et al. [13] propose to store users' identification data in a trusted third-party who is responsible for the authentication of users so that websites have no right to use those data without consent. Bélanger et al. [14] restrict service providers' access to personal data of children on the internet by including a trusted third-party to match the demand of service providers and the collectable personal data set by parents both in P3P format.

OAuth protocol is an open standard for authentication, it provides a method for websites (referred to as "relying party") to access resources stored on OAuth service provider on behalf of a resource owner (referred to as "end-user") [15]. OAuth-based systems make it possible for end-users to login without creating a new account and relying party can collect information about their users that they otherwise might not have been able to collect, even with lengthy registration forms. OAuth-based systems are becoming more and more popular in an integration oriented internet environment. But users indeed do not know exactly what kinds of resources are being shared with relying party even though there do exists a grant process, as Egelman posited that users habitually misunderstanding or ignoring the consent dialogs which fail them in noticing the disclosures diverging from their expectations [16].

Access control may have difficulty in controlling the degree to restrict the collecting behavior. Since storing too much personal data in various websites will increase the privacy risk, however, some reasonable requirements related with users' personal data would be deprived or over-constrained reversely. The question remains to be how to maximize internet users' control over their personal data and meet the needs of websites at the same time. The design of providing personal data usage services to various websites inspired us to propose the PSP mechanism.

3. PSP Mechanism

3.1 PSP Mechanism Design Model

The PSP mechanism model assumed in this work has three main players: Internet user (IU), websites providing various kinds of services to users (SP) and (Privacy Service Provider) PSP. Fig. 1 outlines the mechanism design model and sketches the interaction among the three parties.

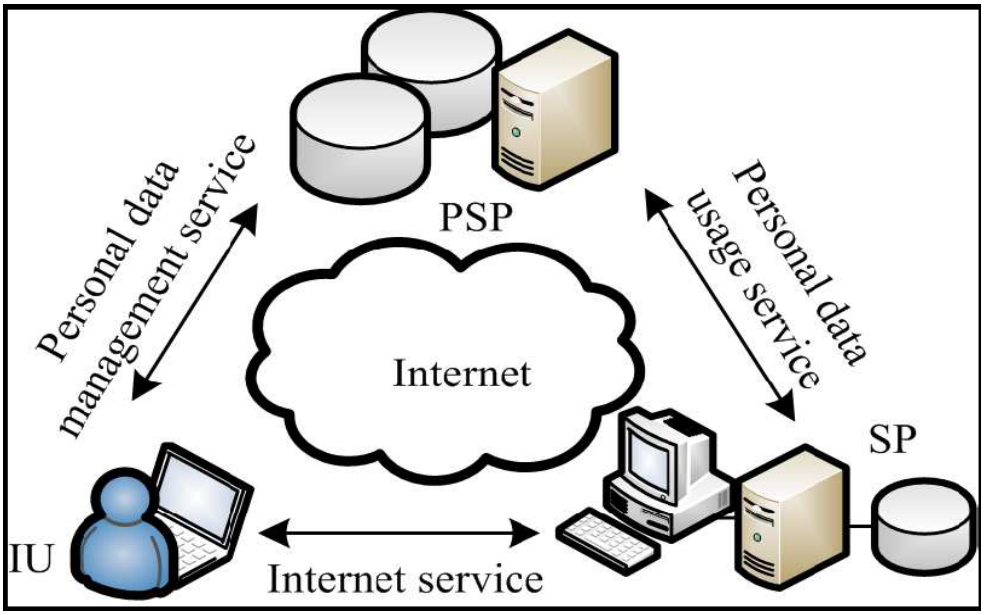

Figure 1. The design model of PSP mechanism

Instead of providing personal data directly to various kinds of SP, IU submit their personal data to PSP after registration. PSP then provides personal data usage services to SP, the services are designed to protect benefits of both IU and SP. When needed, SP could access the privacy data usage services from PSP. The basic framework design of PSP is shown in Fig.2. USI is the User Service Interface where IU can fulfill registration and basic privacy management services; SPI is the Service Provider Interface where SP can get registered and validated. WSM is the Web Service Module that contains services for SP related with personal data of IU.

Web Service Architecture is used here to provide services without worrying about the various kinds of platforms which the applications of SP may be built on, since the SOAP is used as the communication protocol. With UDDI (Universal Descryption, Discovery and Integration) being used to store the descryption about services that can be provided by Web Service application, and WSDL (Web Service Descryption Language) documents containing all the information needed to know if the services are to be called, the client application can use the services just like using the common functions in ther own applications.

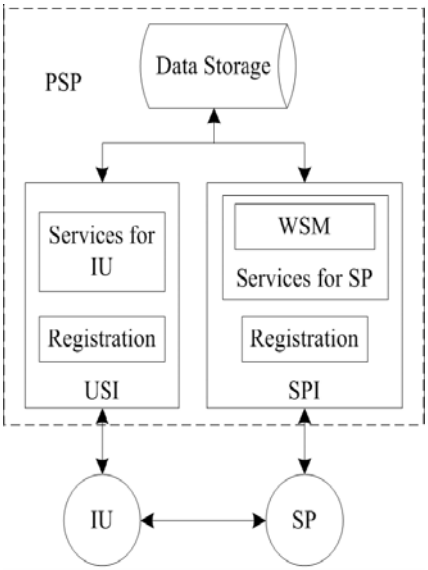

Figure 2. PSP basic framework design

3.2 Interface for IU

IU submits their identification data to PSP and applies for registration through the USI. If the authentication is successful IU will become a member of PSP and receive the unique identification number: UID, which will act as the key parameter for SP to use personal data usage services. When personal data is needed in an internet service, IU can provide SP with the UID. SP then could apply for corresponding services by submitting the UID so that PSP can specify whose personal data this application is correlated with.

After registration, IU could store and manage their personal data through USI. PSP provides IU with a full control on their personal data including what information is stored, who can access to those data and how the information is being processed and used. We shall discuss the services for IU in the next section.

3.3 Interface for SP

SP can get the right to use the SPI after necessary certification to get the unique client credential so as to apply for services related with the personal data from WSM. Their applications are processed by PSP according to the privacy access levels set by IU. It is the fact that most SP may not be incentive and capable enough to fulfill security storage and processing in terms of personal data that necessitates the presence of PSP. We intend to meet the needs of SP without disclosing original personal data or keep it compliance with demands of IU. WSM thereby exists to provide the usage services related with IU's personal data. The interaction between SP and WSM is shown in Fig.3.

Services can be registered in UDDI and the necessary introduction about the services, for instance, the type and meaning of the parameters and return value, are stored in WSDL documents. Websites can check the service list from UDDI to discover the service they need and call the service in their own application by using SOAP. And the goal for SP to securely use IU's personal data when the data is remotely stored in PSP can be achieved with imlementation of privacy preserving technologies.

4. Service For IU

4.1 Privacy Control

IU can choose what kind of personal data to be stored and deleted by PSP provided that all the information necessary for identification is confidential. IU can edit the personal data when some information has changed such as telephone number or address. Still there are some kinds of information such as social security number and gender that can't be modified unless re-authentication is supported so that the accuracy and accountability are guaranteed for other personal data usage services.

4.2 Personalized Privacy Protection

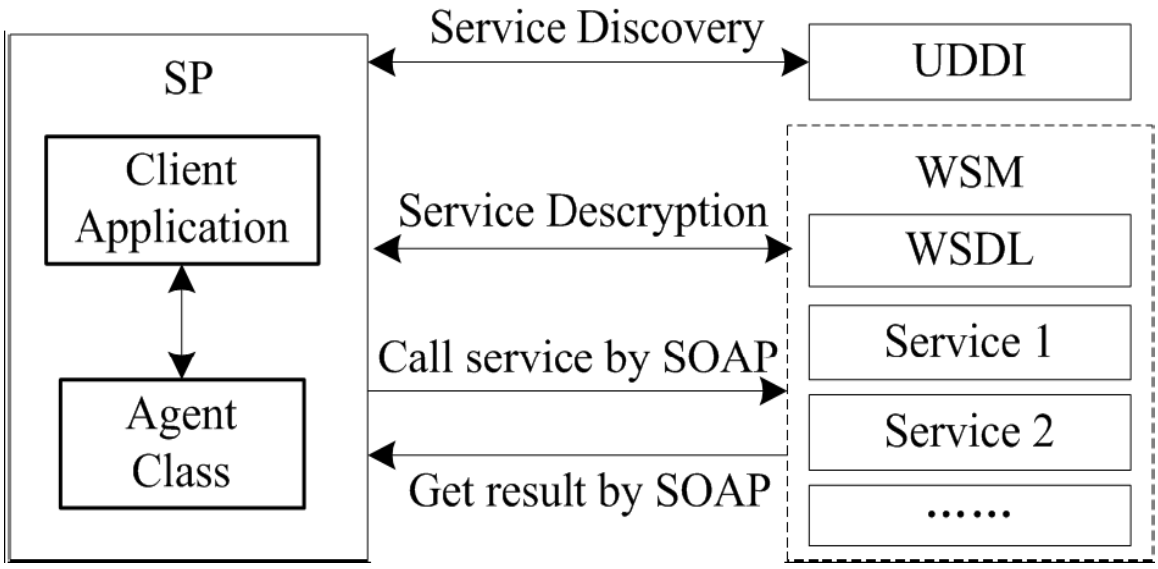

Figure 3. Interaction between SP and Web Service Module

For each kind of personal information submitted to PSP, IU can set different safeguard level. Itani et al. [17] proposed three access levels: Full trust, Compliance-based trust and No trust. In our case it can be extended as follows:

(a) Access to all SP: Original data of this level is available for SP without further notification and configuration.

(b) Access to trusted SP: Only trusted SP specified by IU can access to the information at this level.

(c) Access to none: No SP could get this kind of information unless further notification and consent is given by IU.

(d) Default level: For original data that may not be accessed by other websites, PSP provides a default choice to provide basic anonymity and security protection before it can be used or accessed.

It is essential to make it clear that the safeguard level is effective in personalized privacy protection in case that the personal data of a particular IU is needed by SP. When the group data is being asked by SP with no risk of disclosing individual identification, such as the age distribution of a group of IU, PSP will process the data set to ensure that there is no privacy leakage risk.

4.3 Privacy Feedback

It is a basic right for IU to know who has used their personal information and how the data has been processed and shared. PSP can achieve this by recording the service applications sent by SP and archive the information for IU to check. IU can only access those archives related with her own personal data and check whether the processing on the data is adhere to the safeguard level. The feedback service can effectively relieve the privacy concern and help building confidence of IU for internet service security.

5. Service For SP

The personal data of IU is most widely used by SP for user authentication, communication and data analysis. As we may not envisage all the personal data usage services for SP, this section presents technologies and models exists that can be used to provide or help to achieve the services above as basic implementation examples.

5.1 User Authentication

User authentication happens when IU need to apply for some services from SP. PSP can act as an agent for SP to validate the identification of IU so that SP can trust IU to be an honest customer. The authentication now can be achieved with no need to create a new account or submit additional personal information by using protocol such as OAuth. In our case, PSP is acting as the OAuth service provider, while SP is the relying party who needs to use internet users' personal data stored in PSP. The authentication procedure of PSP is shown in Fig. 4.

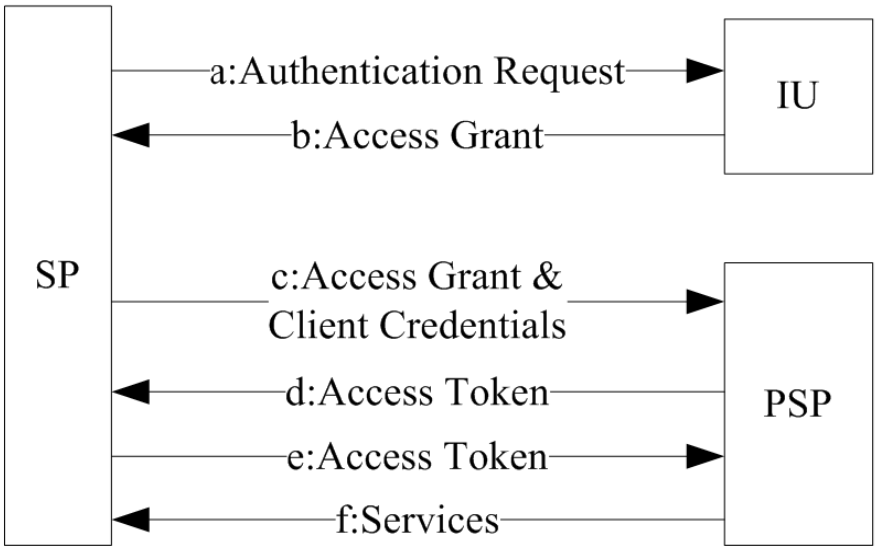

Figure 4. Procedure of authentication based on OAuth protocol

(a) SP requests authorization from IU. The authorization request can be made directly to the IU or preferably indirectly via PSP as an intermediary.

(b) SP receives an access grant, which is a credential representing IU's authorization.

(c) SP requests an access token by authenticating with PSP and presenting the access grant and the credential of SP.

(d) PSP authenticates the client and validates the access grant, and if valid, issues an access token.

(e) SP requests services from PSP and authenticates by presenting the access token.

(f) PSP validates the access token, and if valid, serves the request.

5.2 Communication

In order to communicate with consumers or send advertising information to lower the search cost and increase sales, many establishments resort to junk email and SMS spam since they can be precision-targeted, responded to instantly, and unbelievably cheap. SP can easily obtain unprocessed email addresses and telephone numbers, which brings problems to IU who may frequently accept messages and emails which are often permanently deleted before reading, since most of the content sent by SP are not appealing to the recipients. Though the cost to send solicitations is minimal, it can be harmful on the reputation of SP.

Admediation [18], an advertising business model, proved to be popular in solving the problem of spam. It works by matching the content of emails with the preferences set by consumers, and offering option to consumers to opt-out. With Admediation the volume and content of emails sent to consumers can be limited, and the response rates can be raised since they can target consumers more precisely. Xu et al. [19] proposed to protect security of email address by generating temporary address information and using it during the interaction between internet users and websites.

PSP provides us with a mechanism that is compatible with the models above. PSP can offer IU services to set temporary telephone numbers and email addresses that mapping with their real information. Also IU could provide different SP with different temporary information instead of the real ones. If IU does not need the content sent by certain SP or the service needed to get in touch with SP is over, the particular temporary information to which the SP has access can be deleted so that the temporary information owned by the SP would become invalid. In this way, only the information with consent can be sent to IU and no real personal data would be disclosed to SP.

5.3 Data Analysis

Analysis of data is a process of inspecting, cleaning, transforming, and modeling data with the goal of discovering useful information, suggesting conclusions, and supporting decision making. Data analysis has multiple facets and approaches, encompassing diverse techniques in different situations.

In PSP model, if SP need to know the descriptive statistical features about users only based on their personal data, such as the average of age, the distribution of gender and occupation, the results can be calculated by PSP and sent back to certain SP who applys for the service. Taking the gender distribution service as an example, PSP has already registered and implemented the gender distribution service. The service procedure of gender distribution is shown in Fig.5.

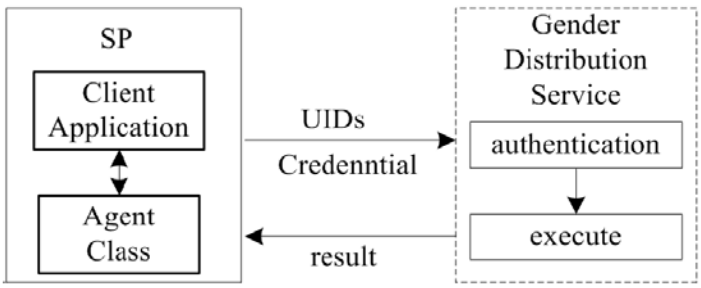

Figure 5. Procedure of gender distribution service

• SP call the service in WSM sending the set of user identifiers *UIDs* = {uid_1, uid_2, ...} and client credential as parameters to PSP;

• PSP authenticates SP based on the credential;

• If the authentication is successful, PSP executes the service being called and gets the distribution information of specified users;

• PSP sends the result back to SP, or a fail message will be sent if SP fails the authentication.

One different case is that SP might need to integrate the data of both sides to find useful knowledge. Data mining is a particular data analysis technique that focuses on modeling and knowledge discovery for predictive rather than purely descriptive purposes. Data mining services offered by PSP are to satisfy SP's demand of finding implicit, previously unknown, and potentially useful information over the personal data of IU in joint their service records and ensure privacy security of IU at the same time. Since the personal data of IU and their service information are stored in PSP and SP respectively, which belongs to vertically partitioned data as is shown in Fig.6. The situation facing PSP thereby belongs to the field of VPPDM (Vertically partitioned Privacy Preserving Data Mining).

PSP				
UID	Age	Gender	Education	...
uid1	24	M	11th	
uid2	37	M	Masters	
uid3	21	F	12th	
uid4	43	M	Bachelors	
...				

SP		
UID	Items	TID
uid3	bread,milk	2
uid2	milk,beer	1
uid1	Tea, beer,...	4
uid4	book,tea	5
...		

Figure 6. Data distribution model in PSP mechanism

There is a rich literature on VPPDM most of which focus on classification, clustering, and association rule mining. Dansana et al. [20] represented how CART algorithm can be used for multi parties in vertically partitioned environment. Secure sum and secure size of set intersection protocols are used for security purpose. Gangrade et al. [21] proposed an approach for the problem of privacy preserving three-layer naïve bayes classification over vertically partitioned data. Ni Weiwei et al. [22] proposed an efficient density-based clustering algorithm DDBSCAN for vertically distributed datasets. Vaidya et al. [23] present a two-party algorithm for efficiently discover frequent item sets with minimum support levels, without either site revealing individual transaction values. Poovammal et al. [24] developed a simple technique of transforming the sensitive data. Experiments showed that this approach was able to achieve cent percent utility for any type of mining task as compared to the original table.

Current study can solve the problems facing PSP with data mining services to some extent. But the situation in our study may be somewhat special since data analytics in relation with the personal data of IU are usually used to support CRM, marketing, decision making and so on. With respect to the commercial privacy of SP, PSP should have no right to access the final results of the data mining procedure. So the duty now for PSP is to achieve data mining tasks with vertically distributed data sets while keeping privacy of both IU and SP, and ensuring that only SP can obtain the final analytic results. In this sense some algorithms proposed may not be suitable such as [25], since PSP knows exactly which IU belongs to SP. Additionally, in order to guarantee enough initiation for SP, for example SP may need to change the minimum support threshold frequently to update interesting association rules. This can hardly be met by algorithms requiring a data center to gather the distributed data and undertake all mining tasks taking into account the communication cost. All in all, it remains to be further studied how to improve the data analytic services to balance proper benefits of both IU and SP.

6. Feasibility Study

As open and sharing have already become main trends of the internet nowadays, many internet giants are providing open platforms based on OAuth protocol such as Facebook, Sina, Tencent and so on, which makes it more acceptable for third-party websites to retrieve what they need from an open platform rather than collecting personal data from internet users directly. The problems discussed in this paper are useful for increasing privacy security of data sharing in current open platforms. In this sense the OAuth-based open platforms have in fact token the critical step for PSP in practice by providing personal data authentication services to internet users. In another way, technologies about OAuth protocol, Web Service, VPPDM, encryption and data distorting also provide PSP with technical supports in implementing the usage services related with personal data.

6.1 PSP and Internet Users

From an internet user's perspective, with personal data stored in PSP, internet user thereby has a second choice to only provide personal data to PSP rather than various websites. The ability of internet user to control and manage personal data is maximized. Necessary security can be enforced so that the possibility for websites to misuse or abuse their personal data can be lowered. The problem is that PSP model may be more effective to users who have not breach much of their personal information seriously. While for internet users who have no idea how many websites have already got their personal data since the information they provided to websites may have been shared, sold, or even stolen by unknown parties. Then how could PSP be effective in a situation where many websites have already known the real information. Given the situation above, there are chances that internet users may need services from new service providers, in which case PSP could protect their privacy leakage from becoming further seriously. What's more, in some kinds of services like online shopping the personal data is frequently used which raise the risk of privacy leakage. In this case PSP could provide security privacy services to improve the privacy situation.

6.2 PSP and Websites

From a website's perspective, properly implemented, PSP model can be appealing to websites provided that the services are effective and efficient enough than collecting personal data themselves. While for industry giants such as Amazon and Facebook who by themselves have accumulated scalable valuable personal data, PSP is not contradicted with their own personal data usage procedures.

On one hand, privacy concern would cause data quality and integrity to deteriorate. The services provided by PSP thus can be complementary with those on their websites, since the information on PSP, a trusted third-party, can be much more comprehensive and authentic. On the other hand, PSP provides a framework for current open platforms to enhance their privacy preserving effects in data sharing services. They can all implement the interface for internet users and third-party websites as described above to form a system of privacy service providers just like the system of CA (Certificate Authority) rather than just one service center. In this term they are just acting as the role of PSP and providing privacy services to their customers and website clients.

6.3 Summary

Technical and environmental supports along with obstacles exist for PSP in real-life implementation. Since the quality of services provided by PSP is essential for involving more websites, technologies are important for providing more comprehensive and efficient personal data based services. The simplicity and interoperability is another important feature deciding the feasibility of PSP. Improvement is needed for a system framework design with less cost and better effects.

Privacy risk seems always exist since internet users can be influenced even in situation where the identification is impossible such as online targeting based on the IP-address [26]. In this sense we shall not expect that PSP model can solve all the privacy problems on the internet. While privacy concern is becoming increasingly significant in the increasingly complex internet environment, where cloud computing, mobel internet and other advanced technlogies are driving us to a world of big data, legislation and self-regulation which passively restrict the usage of personal data are not enough for new privacy preserving challenges, an actively personal data management platform confrorming to the trends and demands of new technology is needed as an auxiliary.

With good design of compatibility and scalability, PSP can adapt to the changing environment and provide privacy data management and usage services. Taking cloud computing as an example, the identity information and other privacy sensitive data which are not directly used for cloud service but for authentication and business demands of cloud service providers, can be stored in PSP. Cloud service providers can use these data under control of cloud users so that the privacy concern can be relieved. With less and less websites having intention to collect and misuse personal data, PSP can help improve the privacy situation facing internet users.

7. Future Study

Future study shall pay special attention to the following aspects: (i) In order to attract more websites to support PSP mechanism, we need to achieve finer personal data usage services in terms of cost, effiency, ease of use and scope of contexts. (ii) For better interoperability, common APIs based on web service architecture are to be designed, since the cost of communicating via browser on the internet is much lower; And the design of personal data metadata is essential to facilitate PSP mechanism by providing a common language for interaction. (iii) It's a multi-disciplinary task to achieve the real-life implementation of PSP. Experts and professionals from fields of economic, technology, legislation and socio-political shall cooperate and contribute to this mission.

8. Conclusion

The PSP mechanism proposed in this paper intends to meet the need of both internet users and websites by storing personal data of internet users in PSP and providing related services to both parties. The goal is to provide internet users with a second choice when faced with the demands of submitting personal information to websites so as to actively manage the processing and use of their personal data. Obstacles surely exist for the implementation of PSP mechanism, but it offers us a way to take the usage of personal data under control of internet users themselves, which is becoming increasingly necessary under a rapidly changing internet environment.

References

[1] Li, H., Sarathy, R., Xu, H. (2011). The role of affect and cognition on online consumers' willingness to disclose personal information. *Decision Support Systems,* 51 (3) 434–445.

[2] Kauffman, R.J., Srivastava, J., Vayghan, J. (2012). Business and data analytics: new innovations for the management of e-commerce. *Electronic Commerce Research and Applications,* 11 (2) 85-88.

[3] Li, X.B., Raghunathan, S. (2014). Pricing and disseminating customer data with privacy awareness. *Decision Support Systems* 59 63–73.

[4] Feijóo, C., Gómez-Barroso, J.L., Voigt, P. (2014). Exploring the economic value of personal information from firms' financial statements. *International Journal of Information Management,* 34 (2) 248-256.

[5] Bélanger, F., Crossler, R.E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly* 35 (4) 1017-1042.

[6] Teltzrow, M., Kobsa, A. (2004). Impacts of user privacy preferences on personalized systems: a comparative study. *Designing Personalized User Experiences in e-Commerce* 315–332.

[7] Sweeney, L. (2002). K-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* , 10 (5) 557–570.

[8] Pearson, S (2009). Taking Account Of Privacy When Designing Cloud Computing Services. *In:* Proc. of ICSE Workshop on Software Engineering Challenges of Cloud Computing, 44–52, 2009.

[9] Fung, B., Wang, K., Chen, R., Yu, P.S. (2010). Privacy-preserving data publishing: a survey of recent developments. *ACM Computing Surveys (CSUR),* 42 (4) 14.

[10] Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., Zhu, M.Y. (2002). Tools for privacy preserving distributed data mining. *ACM SIGKDD Explorations Newsletter,* 4 (2) 28-34.

[11] Li, Y., Chen, M., Li, Q., Zhang, W. (2012). Enabling multilevel trust in privacy preserving data mining. *Knowledge and Data Engineering,* 24 (9) 1598-1612.

[12] Zhou, S.G., Li, F., Tao, Y.F., Xiao, X.K. (2009). Privacy preservation in database applications: a survey. *Chinese Journal of Computers* 32 (5) 847-857.

[13] Mao, J., Li, K., Xu, X.D (2011). Privacy protection scheme for cloud computing. *T sing hua Univ (Sci & Tech)* 51 (10) 1357-1362.

[14] Bélanger, F., Crossler, R. E., Hiller, J. S., Park, J. M., Hsiao, M. S (2013). POCKET: a tool for protecting children's privacy

online. *Decision Support Systems*, 54 (2) 1161-1173.

[15] Internet Engineering Task Force, http://tools.ietf.org/html/rfc6749.

[16] Egelman, S. (2013). My Profile is My Password, Verify Me! The Privacy/Convenience Tradeoff of Facebook Connect. *In Proc. of CHI 2013*, 2369-2378.

[17] Itani, W., Kayssi, A., Chehab, A. (2009). Privacy As A Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. *In:* Proceedings of the 8th IEEE International Conferenceon Dependable, Autonomic and Secure Computing, p. 711 – 716.

[18] Gopal, R. D., Tripathi, A. K., Walter, Z. D (2005). Economic issues in advertising via email: role for a trusted third party?. *Contemporary Research in E-Marketing*, 1, 38-47.

[19] Xu, J. (2011). Research on privacy protection model and methods in network interaction. Beijing, China: Beijing University of Technology.

[20] Dansana, J., Dey, D., Kumar, R. (2013). A Novel Approach: CART Algorithm for Vertically Partitioned Database in Multi-Party Environment. *In:* Proceedings of IEEE Conference on Information and Communication Technologies (ICT) p. 829-834.

[21] Gangrade, A., Patel, R. (2013). Privacy preserving three-layer naïve bayes classifier for vertically partitioned databases. *Journal of Information and Computing Science*, 8 (2) 119-129.

[22] Ni, W.W., Chen, G., Sun, Z. H. (2007). An efficient density-based clustering algorithm for vertically partitioned distributed datasets. *Journal of Computer Research and Development*, 44 (9) 1612-1617.

[23] Vaidya, J., Clifton, C. (2002). Privacy Preserving Association Rule Mining in Vertically Partitioned Data. *In:* Proc. of SIGKDD, p. 639-644. Edmonton.

[24] Poovammal, E., Ponnavaikko, M. (2009). Utility independent privacy preserving data mining on vertically partitioned data. *Journal of Computer Science*, 5(9) 666-673.

[25] Rozenberg, B., Gudes, E. (2009). Association rules mining in vertically partitioned databases. *Data & Knowledge Engineering* 59 378–396.

[26] Schermer, B.W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27 (1) 45-52.