WEB NOTARY SYSTEMS FOR PRIVACY KEEPING E-COMMERCE

Manen Ying, Yahiko Kambayashi, Kai Cheng
Graduate School of Informatics, Kyoto University, Kyoto, Japan
{yme,yahiko,chengk}@kuis.kyoto-u.ac.jp

Yanchun Zhang
School of Computing University of Tasmania.
Hobart, Tasmania 7001, Australia
yan@utas.edu.au

Abstract We propose a web notary system to support privacy keeping E-Commerce over the Internet. A web notary system can be seen as a trusted third-party enhanced with value-added services. With a web notary system, customers can provide privacy protected information and requests to the system instead to various online shops. The system can then search its information repository in an intelligent way on behalf of the customers and provide personalized services. In this paper, we develop a novel privacy control model based on hierarchy of privacy groups. We also design a method for efficient customer-provider matchmaking. A prototype system has been developed to demonstrate our proposals.

Keywords: Electronic commerce, web notary system, privacy, personalization, matchmaking.

1. Introduction

Recent advances in Internet and Web technology have enabled the rapid development of e-commerce or commerce activities over the Internet. Business companies and organizations began to develop e-business models and systems such as e-shops, e-brokers, e-auction, virtual communities, collaboration platforms, third market places, value chain integration/service, and trusted and specialized information services [2, 3].

When users keep shopping over the Internet, however, they will often leave some personal information behind and consequently may get many irrelevant e-mails or advertising information. Users may worry about the misuse of credit

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35658-7_21
R. Meersman et al. (eds.), *Semantic Issues in E-Commerce Systems*

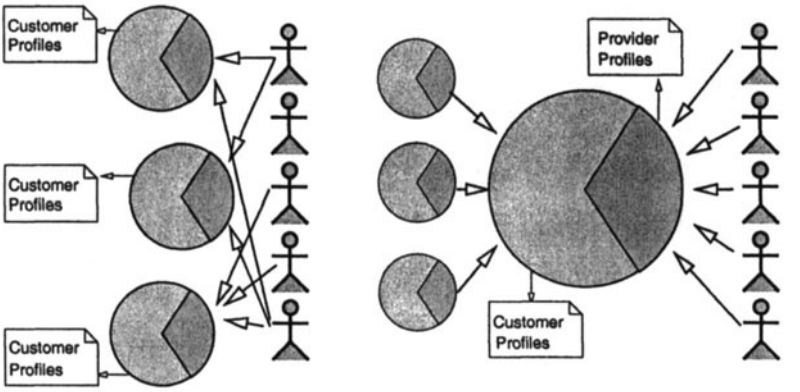


Figure 1. Web Notary System As A Trusted Third-Party Providing Value-Added Services

card information given online, selling or sharing of personal information by site owners, and the prevalence of cookies that track online activity. On the other hand, as providing private information is often a necessary way to obtain better information and services, many users are willing to provide their personal information to a trusted body who not only can protect sensitive information from misusing but also can provide personalized services based on user profiles.

In this paper, we propose a web notary system (WNS) to support users' e-commerce activities and to protect the users' privacy. In the notary system, user's profiles are maintained to provide personalized services, to guide the design of a web view, to speed up the search and filter information for the user. Figure 1 shows the scenario of shopping before and after deploying a shared web notary system, which connects providers and customers and keeps customers' privacy information secret. A web notary system also acts as an information repository that provides a basis for customer relationship management, supporting efficient customer-provider matchmaking and social recommendation.

The rest of this paper is organized as follows. In the next section, we shall discuss the general design goal of a web notary system based on analysis of privacy-profit tradeoffs. In Section 3, we shall develop a flexible privacy control model that supports privacy policy inheritance and overwriting. Section 4 presents an efficient approach for customer-provider matchmaking based on privacy-protected transaction data for both customers and providers. Section 5 describes a prototype implementation of a WNS based on database technology. Section 6 reviews related work and Section 7 concludes the paper.

2. Privacy-Profit Tradeoffs in E-Commerce

Privacy is one of the major concerns of online customers when they decide to conduct online shopping. A recent report [7] from Statistical Research has found that 67% of Internet users typically abandon web sites when they are asked to give personal information. Over half of those polled said they were very concerned about the misuse of credit card information given online, the selling or sharing of personal information by site owners, and the prevalence of cookies that track online activity. In most cases, more profit often means more risk of privacy invasion.

On the other hand, for service or merchandise providers, user profiles, including shopping history, are precious information for market targeting and service personalization. Thus, providers are willing to offer profit as a tradeoff to those who can provide their personal information. Privacy-profit tradeoffs are necessary not only for providers but also for customers as providing private information of their own is often the only way to obtain worthwhile benefits.

2.1. Privacy-Profit Tradeoffs for Customers

The privacy-profit tradeoffs for customers can be roughly divided into two groups: *personal information* and *transaction information* as shown in Table 1. Personal information refers to those that can be used to identify a customer, for instance, name, facial photograph, (home or affiliation) address, sex distinction, incomes etc. Personal information is necessary for obtaining better special offers or extra benefits, however, if misused there are risks of privacy invasion. Firstly, personal information can be misused for delivering unsolicited commercial advertisements; Secondly and more importantly, when pieces of customer information are linked through such identification information, it will be unavoidable for customers to prevent privacy from invasion.

Transaction information is on shopping activities (history) of each customer including time, merchandise item and provider (i.e. online shop) involved in each transaction. Transaction information can be used for analysis of preferences and associations of customers' shopping activities so as to create a basis for market targeting and personalized services. When transaction information for a given customer is linked over time, it can be used for monitoring customer activities that may imply serious privacy problems.

The Safeway Club Card [1] is a good example for illustrating privacy-profit tradeoffs of customers. To obtaining a Safeway Club Card, users are required to provide their private information including name, address, phone number, e-mail address, birthdate etc. The Safeway Club then records information regarding the purchases made with each Safeway Club Card to help them provide members with personally tailored coupons, special offers and other information.

Privacy items		Risk	Profit
Personal Information	Name	Misusing	Direct Communication
	Photograph	Misusing	Personality Recognition
	Sex Distinction	Sexual Harassment	Targeted Services
	Marriage	Sex Troubles	Targeted Services
	Birthday	Age Be Public	Targeted Services
	Address	Unsolicited Visits	Home Delivery
	IP Address	Access Monitoring	Adaptable Services
	e-mail	Unsolicited Adv. Mails	Easy Contact
	Phone Number	Unsolicited Calls	Easy Contact
	Incomes	Burglary/Theft/Troubles	Matched Services
Transaction Information	Time	Activity Monitoring	Efficient Matchmaking
	Provider Info	Activity Monitoring	Efficient Matchmaking
	Price/Discount Info	Unsolicited Promotion	Recommendation
	Credit Card No	Link to Personal Info	Convenient Payment
	Merchandise	Unsolicited Promotion	Discount

Table 1. Privacy-Profit Tradeoffs for Customers

One limitation of current E-Commerce solutions is that personal information and transaction information of customers scatter over various sites so that both full control and full utilization of such sensitive but valuable information become impossible. Web notary system is just for dealing with this problem, which provides flexible control of private information as well as customer/provider support based on efficient provider-customer matchmaking.

2.2. Privacy-Profit Tradeoffs for Providers

Similar to (online) customers, providers (or online shops) also have their own privacy issues. Privacy issues of providers are related with so-called "commercial secrets" that include promotion policies, sales records, and customer information. Table 2 lists typical tradeoffs for online service/merchandise providers (except customer information that is basically the same as listed in Table 1). The profit for providers means the benefit they can obtain when privacy items are shared by other providers. The risk column indicates the possible loss when privacy items being misused by their competitors respectively.

Promotion policies are major privacy information for providers, which are often kept as commercial secrets. Information in this category include pricing policy, discount rates, special offers and advertising strategies. Releasing such information may lead to loss in competition if misused by competitors. However, it is also necessary to advertising such information to potential customers as well as commercial partners to attract customers and to facilitate cooperations between partners. Such cooperation exist between homogeneous

Privacy items		Risk	Profit
Promotion Policies	Pricing Policy	Lose Competition	Pricing Cooperation
	Discount Rates	Lose Competition	Discount Cooperation
	Special Offers	Lose Competition	Offer Cooperation
	Advertising Strategies	Bad Adv. Effect	Advertising Enhancement
Sales Records	Time	–	Overall Activity Analysis
	Prices	Price Competition	Overall Price Analysis
	Customer	Lose Customer Share	Overall Customer Targeting
	Merchandise	Lose Better Sales	Efficient Matchmaking

Table 2. Privacy-Profit Tradeoffs for Providers

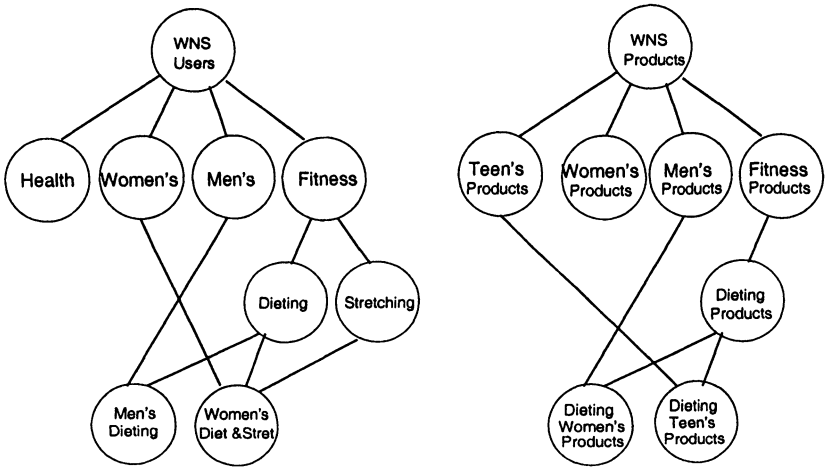
providers, such as automobile sellers, as well as between heterogeneous but related providers, such as automobile sellers and toy makers that produce toy cars. As models of best sales may differ from maker to maker, exchanging information between them may benefit them from each other, although there is a tradeoff between the benefit and competition loss.

Sales records are transaction information collected at each E–Commerce site. Up to date, such information are generally kept for use only by each site without sharing among other sites. On one hand, sales records include useful commercial secrets such as best sales, customer identification, and business showings and actual pricing information that should be well protected from releasing. On the other hand, sharing information of this kind after sensitive information being hidden is also a fair trading for obtaining similar information from other sites. Based on these information, a provider can obtain a complete view of shopping activities for better market analysis and service improvement.

Based on the above analysis, we know privacy–profit tradeoffs are important and necessary for both customers and providers in E-Commerce activities. However, in current E–Commerce environment, such tradeoffs can only take place in each web site independently. Users do not know who can trust and how to prevent their private information from misuse. In addition, independently managed private information is not possible to use for sales or services improvement and market targeting. Web notary system is developed to deal with these problems. First, to facilitate privacy protection, we develop a hierarchical privacy control model that support privacy policy inheritance and overwriting. Second, to facilitate deal attainment, we propose an efficient scheme for customer–provider matchmaking.

3. Privacy Control Model

It is important to provide users (either customers or providers) with capability to control what parts of and how their private information will be used in



(a) Privacy groups for WNS users

(b) Privacy groups for products

Figure 2. Hierarchy of Privacy Groups

a web notary system. To do this, we allow both individual users and privacy group to define their own privacy policy. The web notary system then checks and enforces privacy policies for all of them involved in each e-commerce session. In this section, we develop a privacy control model that enables flexible privacy control while providing personalized services. Our model is based on hierarchy of privacy groups for both WNS users and products (merchandise). Individuals or lower level groups can define their own privacy policy that overwrites general ones inherited from ancestor groups on the upper levels.

3.1. Hierarchy of Privacy Groups

When a user subscribing to a web notary system, he/she can choose to join one or more privacy group, an organization of users that share common interest and privacy concerns. By default, all users belong to the *WNS users* privacy group. Privacy groups form a hierarchy in which a lower level group automatically *inherit* the privacy policy from their ancestor groups. Let $G = \{g_1, g_2, \cdots, g_n\}$ be the set of groups in our question. We define $\preceq$ as the *inheritance* relation between two groups such that:

1 if $g \in G$ then $g \preceq g$;

2 if $g_i, g_j, g_k \in G$ and $g_i \preceq g_j, g_j \preceq g_k$ then $g_i \preceq g_k$;

3 if $g_i \preceq g_j$ and $g_j \preceq g_i$ then $g_i = g_j$.

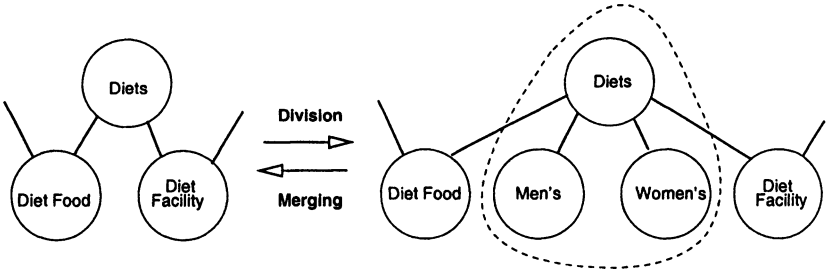


Figure 3. Division and Merging of Privacy Group(s)

In addition to user grouping based on privacy policies, product grouping is also necessary in our privacy control model. This is because some products are themselves very sensitive to any customers who would purchase them, for example, dieting facilities. We define another kind of hierarchy of privacy group that is based on categories of sensitive merchandise.

In Figure 2(a), we give an example hierarchy of privacy groups based on Yahoo!Clubs [2]. Beneath the WNS users group are four subgroups, namely "Health", "Women's", "Men's" and "Fitness". privacy group "Fitness" also has two subgroups "Dieting" and "Stretching". "Men's Dieting" is formed on the basis of two parents "Men's" and "Dieting" so it inherits privacy policy from the two parent groups. Similarly, "Women's Dieting and Stretching" inherits privacy policy from three upper level privacy groups "Women's", "Dieting" and "Stretching". Similarly, Figure 2(b) gives an example for product based hierarchy of privacy groups.

Privacy groups can be added and removed. Adding a new privacy group into current group hierarchy includes the following steps. (1) find existing groups of interest; (2) (aided by system) check profit and privacy policy for each interested group; (3) define specific profit and privacy policy of its own (may overwrite those inherited from its parents). Suppose, for example, we want to add the "Men's Dieting" groups. After searching and browsing of the existing privacy groups, we find there exist two groups that are similar to our interest and after checking profit and privacy policy of these groups, we find some privacy items are not necessary whereas others are not suitable for our case. We can then define our own privacy policy in the form to be presented in next section.

To remove a privacy group, all descendant groups that depend only on this group will also be recursively deleted. For example, to remove the "Fitness" group as in Figure 2, "Dieting" and "Stretching"should be deleted with as both are dependent only on "Fitness". However, neither "Men's Dieting" nor "Women's Dieting and Stretching" should necessarily be deleted as they also depend on other groups.

A privacy group can also be divided or merged with shift of user interest. A privacy group could be divided when interests of members in the group diverge over a long time. As shown in Figure 3, when members of "Diets" diverge in interest with respect to distinct sex, it can be divided into women's and men's groups. Conversely, two or more groups of similar interest could be merged into one as exemplified in Figure 3.

3.2. Definition of Privacy Policy

As mentioned above, users of a web notary system automatically inherit profit and privacy policy from their groups they belong to, however, they can also add new policy as well as overwrite all or part of the inherited one. Similarly, product based privacy groups can protect all customers who purchase a product under a protected group. We provide flexible mechanism for users (both individuals or groups) to specify their own privacy policy and we call the list of users specified privacy policy definitions, called *privacy item*, as *user privacy profile*, stored in the *privacy profile database, or PPDB*. Each item in a profile should be one of the following forms.

- Allow $\langle who \rangle$ $\langle action\_list \rangle$ $\langle data\_list \rangle$
- Deny $\langle who \rangle$ $\langle action\_list \rangle$ $\langle data\_list \rangle$

An *Allow / Deny* privacy item declares $\langle who \rangle$ can/cannot access $\langle data\_list \rangle$, performing $\langle action\_list \rangle$. Here $\langle who \rangle$ can be ALL, a list of user IDs, or a list of group IDs, default is the ID of current group. $\langle action\_list \rangle$ can be READ (read out the value), COUNT, SUM, AVERAGE, MAX, MIN (do aggregation). $\langle data\_list \rangle$ is the data items to be protected, which in fact are attribute names in WNS database. Typical private data include name, postal address, e-mail, telephone number, income, photograph etc.

Note, although privacy policy can be inherited, it can also be replaced or overwritten. The allowed access in an inherited privacy item can be denied by new definition and vice versa. Furthermore, the inherited privacy items can be completely or partially overwritten using one of the following forms: (1) Overwrite ALL; (2) Overwrite ALL EXCEPT $\langle p_i, \cdots, p_j \rangle$; (3) Overwrite $\langle p_i, \cdots, p_j \rangle$. An *Overwrite* privacy item specifies the scope for one to inherit privacy policy from upper level groups. Here p_i, p_j denote specific items inherited from related groups."Overwrite ALL" declares to invalidate all inherited privacy items, which means only the explicitly defined privacy items are valid. "Overwrite ALL EXCEPT $\langle p_i, \cdots, p_j \rangle$" means only inheriting $\langle p_i, \cdots, p_j \rangle$ while invalidating all other inherited privacy items. "Overwrite $\langle p_i, \cdots, p_j \rangle$ " means only invalidating $\langle p_i, \cdots, p_j \rangle$ while inheriting the rest.

Product based privacy policies are defined in a similar way. There are cases where privacy preserving conflicts with deal attainment. For example, a cus-

tomer in the "dieting" privacy group may not allow others to query her waist size. However, when she wants to buy a suit from a provider, she has to provide this measurement so that the suit can fit her well. To deal with this special case, we provide a choice for WNS users to specify the *priority* between privacy preserving and deal attainment, that is, to specify when a conflict occurs whether to sacrifice privacy for deal attainment or to abandon the deal for preserving her privacy. The third form of privacy definition is:

- Order Privacy | Deal [$\langle Conditions \rangle$]

The $\langle Conditions \rangle$ is defined on the basis of attributes in personal information and transaction information as described in Section 2. Here, Order Privacy defines that privacy is prior to deal (default case). Order Deal tells that deal is prior to privacy. For Order without $\langle Conditions \rangle$, the priority is valid for all cases. If $\langle Conditions \rangle$ are given, the $\langle Conditions \rangle$ will be checked at the first hand. If the result is true, the priority is valid. Otherwise, default priority is used. In the above example, if Order Deal is defined, then the customer chooses to sacrifice her privacy by providing her waist size. Otherwise, she has to give up the deal.

3.3. Privacy Policy Enforcement

Privacy policy enforcement is for checking and enforcing privacy policy while private information being queried. A query has the following form:

- $\langle who, action\_list, data\_list, condition \rangle$

The process of privacy enforcement is as follows. When user $\langle who \rangle$ requests $\langle data\_list \rangle$ with $\langle action\_list \rangle$ and $\langle condition \rangle$, WNS checks if there is privacy restrictions on data access by user $\langle who \rangle$. If there are "Deny" privacy items on the requested data, or some data in $\langle data\_list \rangle$ are not allowed to access by $\langle who \rangle$ using operations in $\langle action\_list \rangle$, WNS will reject to perform such operations and feedback with warning messages. Otherwise if there are "Allow" privacy items on the requested data, that is, the requested data and operations are permitted, WNS will perform as requested and return results to users.

If there is no privacy items on the requested data and the user (individual or group) is descendant of one or more groups, then check the privacy items in the union of privacy items in all parent groups and enforce them as defined. The process will continue until the last group is the WNS users group or there are "Overwrite" privacy items that invalidate some or all inherited privacy policy.

4. Efficient Customer-Provider Matchmaking

As afore–mentioned, private information for customers and providers is important as personalized services and efficient market targeting rely heavily on

such information to identify user preferences. The problems with today's E-Commerce systems are twofold. On one hand, customers shopping online usually feel difficult to find trusted providers that can provide them with high quality products and services. On the other hand, providers are eager to find more loyal customers. Web notary system provide a comprehensive solution to both of these problems. In this section, we will describe an efficient customer–provider matchmaking scheme that is scalable and can support maintaining trust relationships.

Matchmaking is a typical issue in multi-agent cooperation and has been an active field of research [1, 6]. However, as customer–provider matchmaking in a web notary system involves complex user relationships and privacy–profit tradeoffs, our model and algorithm are quite different than the previous work.

4.1. User Relationships in a Web Notary System

Users of a web notary system include online customers and providers. With time lasting, trust/loyalty relationships between customers and providers will form and evolve. Such trust/loyalty relationships combined with online groups create a foundation for fast customer–provider matchmaking. In the following, we use (1) $U = \{u_1, u_2, \cdots, u_m\}$, the set of all customers; (2) $P = \{p_1, p_2, \cdots, p_n\}$, the set of all providers; (3) $C = \{c_1, c_2, \cdots, c_s\}$, the merchandise categories; (4) $M = \{m_1, m_2, \cdots, m_t\}$, the merchandise or the set of all products. Each provider p_i can supply some categories of merchandise:

$$G_i = \{c_{i1}, c_{i,2}, \cdots, c_{i,g}\}$$

Customer–to–customer (C2C) relationships There are a few kinds of relationships between WNS customers. As we have described in Section 3 that each WNS user can join some privacy groups so that they can be protected under privacy policy of those groups. Moreover, as in our real society, we assume each customer has a list of trusted friends and share interest with them. Let

$$F_{c2c}(i) = \{u_{i1}, u_{i2}, \cdots, u_{ik}\}$$

be a friend list of customer u_i. We also assume each friend of u_i has a friend list. As users trust friends of themselves more than friends of others, this *trust relationship* defines an order between each customer and his friends and the distance between two customers in such friendship relation is called *friendship distance.*

$$F'_{c2c}(i) = \{< u_{i1}, 0 >, < u_{i2}, 0 >, \cdots, < u_{ik}, 0 >, \cdots < u_j, d >\}, \quad (d \geq 0)$$

where d in $< u_{ik}, d >$ represents the friendship distance between customer u_i and customer u_{ik}. $d = 0$ indicates direct friendship.

Customer–to–provider (C2P) relationship As customers trust online shops where they have ever bought something much more than those they never reach deal with. In general, the more frequently a provider has been contacted, the more trusted it is. Thus, for each customer u_i, there a list of providers in a non-increasing order of *contact frequency*.

$$F_{c2p}(i) = \{< p_{i1}, f >, < p_{i2}, f >, \cdots, < p_{ik}, 1 >\}, \quad (f \geq 1)$$

where f in $< p_{i1}, f >$ represents the contact frequency between customer u_i and provider p_{i1}.

Provider–to–provider (P2P) relationship Similarly, we assume for each provider p_i there is a list of business partners that trust each other. Let

$$F_{p2p}(i) = \{p_{i1}, u_{i2}, \cdots, p_{ik}\}$$

be a partner list of provider p_i and we assume each partner of p_i has a partner list. The *trust relationship* between a provider and its partners defines an order between providers and the distance between two providers in this partnership is called *partnership distance*.

$$F'_{p2p}(i) = \{< p_{i1}, 0 >, < p_{i2}, 0 >, \cdots, < p_{ik}, 0 >, \cdots < p_j, d >\}, \quad (d \geq 0)$$

where d in $< p_{ik}, d >$ represents the partnership distance between provider p_i and provider p_{ik}. Distance $d = 0$ indicates direct partnership.

Provider–to–customer (P2C) relationship Provider–to–customer (P2C) relationship is inverse of C2P relationship. That is

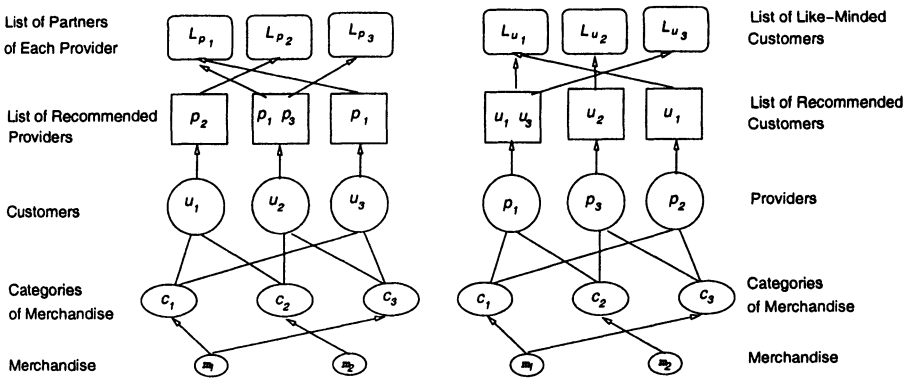
$$F_{p2c}(i) = \{< u_{i1}, f >, < u_{i2}, f >, \cdots, < u_{ik}, 1 >\}, \quad (f \geq 1)$$

where f in $< u_{i1}, f >$ represents the contact frequency between provider p_i and customer u_{i1}.

4.2. Customer to Provider (C2P) Matchmaking

A customer looks for suitable providers that can offer best products or services is called customer to provider (C2P) match as shown in Figure 4(a). In a large scale web notary system, matchmaking, or seeking optimal matches, is difficult and thus scalable methods are necessary. Based on customer–provider relationships maintained in a web notary system, the C2P matchmaking can be carried out very efficiently.

Suppose customer u_i is looking for an online shop that can provides product m_j. The steps for obtaining a C2P matchmaking are as follows: (1) Determine the categories that product m_j belong to, say $H_j = \{c_{j1}, c_{j2}, \cdots, c_{jh}\}$; (2)



(a) Customers look for suitable providers

(b) Providers look for potential customers

Figure 4. Efficient Matchmaking for Customers and Providers

For each contact frequency f from maximum till 1, check $F_{c2p}(i)$, choose the providers that that can provide products in H_j; (3) Unless there is only one provider for a merchandise category, choose a provider offering best price and best services, move the matched products and providers from H_j and $F_{c2p}(i)$ respectively; (4) If there still some products left in H_j, repeat (2)–(4) for next value of f unless $f = 1$; (5) If all providers in $F_{c2p}(i)$ are matched, then obtain a nearest friend of u_i from $F'_{c2c}(i)$ and repeat (2)–(4), unless all friends in $F'_{c2c}(i)$ are checked.

After all matches finished, update $F_{c2p}(i)$ to reflect new contact frequency. At the same time, some new providers may be added into the $F_{c2p}(i)$ with contact frequency $f = 1$. The newly added providers are those introduced by friends of u_i.

4.3. Provider to Customer (P2C) Matchmaking

Conversely, a provider looking for potential customers for advertising and selling some products is call a P2C match as shown in Figure 4(b) The process of P2C matchmaking is similar to that of C2P matchmaking. The difference is that a P2C match may not necessarily result in a deal instead it only obtain a set of potential customers that are most likely to purchase the advertised products or services.

Suppose provider p_i is looking for WNS customers that may purchase product m_j. The steps for obtaining a P2C matchmaking are as follows: (1) Determine the categories that product m_j belong to, say $H_j = \{c_{j1}, c_{j2}, \cdots, c_{jh}\}$; (2) For each contact frequency f from maximum till 1, check $F_{p2c}(i)$, choose

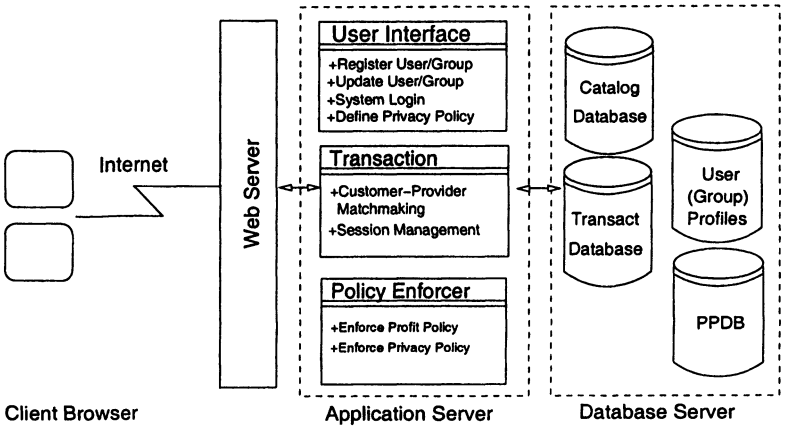


Figure 5. A Reference Architecture of the Web Notary System

the customers that that may be interested in products in H_j; (3) Choose customers that are big–buyers, loyal customers, and put the matched products and customers in advertising list; (4) If there still some products left in H_j, repeat (2)–(4) for next value of f unless $f = 1$; (5) If all customers in $F_{p2c}(i)$ are matched, then obtain a nearest friend of p_i from $F'_{p2p}(i)$ and repeat (2)–(4), unless all friends in $F'_{p2p}(i)$ are checked. After all matches finished, advertise product m_j to all matched customers.

5. A Prototype Web Notary System

To demonstrate our proposal, we are developing a prototype web notary system. Figure 5 illustrates the reference architecture of this system, which consists of database server, application server and web server and client browsers. Most features of this system are implemented as application server modules, including interface management, policy enforcement and transaction management.

A PostgreSQL-based *database server* is used for management of catalogs, privacy profile database (PPDB), user profiles, and transaction records. The data of catalogs are taken from Yahoo!Shopping[3]. Providers are categorized in terms of the category of products they can provide. Categories are taken from Yahoo!Shopping catalogs up to the third level from catalog top. C = {apparel.mens.pants, apparel.mens.atheliticwear, $\cdots$, beauty.skincare.cleanser, beauty.fragrance.womens, $\cdots$}. Customers and privacy groups are associated with their own privacy policy definitions as described in Section 3. For each customer, we maintain a friend list. For each provider, we maintain a partner list. Consider the efficiency of each matchmaking, we assume each list has a limit of length and members of each list will evolve with time.

Application server is implemented using Java Servlet technology. Servlets provide a component-based, platform-independent method for building web-based applications. The interface management module provides interface and process for login, registration (system and groups), privacy policy definition, update and verification. The transaction management module is responsible for management of dynamic information and shopping activities. The first is customer–provider matchmaking, including C2P match and P2C match as defined in Section 4. The second is session management for tracking and guiding the whole process from user login to logout (when finishing a deal or failed out).

The Policy Enforcer is the last module responsible for checking and validating profit policies and privacy policies. The privacy enforcement is implemented on the basis of PostgreSQL active database mechanism (Event–Condition–Action, or ECA rules). As of the writing, PostgreSQL does not support event definition on a column basis, so we only implement simple privacy policies.

6. Related Work

There are papers addressing one or another issue of intelligent search, information filtering, privacy preserving in payment, however, none of them have seriously considered all the above mentioned issues together in a real system. An agent-based auto-negotiation model helps customers to find suppliers and to negotiate a better deal was proposed in [2]. In [5], Schafer et al suggest two technological directions for protecting privacy. The first assumes the business can not be trusted or audited and thus attempts to disguise or scramble personal information. The second direction attempts to automate the negotiation and enforcement of privacy policies. In this direction, the predominant research is the Platform for Privacy Preference(P3P), which aims to provide customers more control over how their information is shared on the web [4]. Our system differs from P3P mainly by shifting focus from solely the customers to both customers and providers.

7. Conclusion

Privacy is a main concern of Internet users when conducting E-Commerce activities but private information is precious information for better services and additional offers. There exist privacy-profit tradeoffs for both customers and providers. However, current E-Commerce solutions failed to provide full support for privacy control as well as to make full use of private information for market targeting and sales improvement.

In this paper we proposed a new approach for protecting user privacy yet retaining advantages of current e-commerce systems. With a web notary system,

customers can leave their personal information to the system, which can provide personalized service to the customers based on the locally available purchasing information of similar customers and semantic relationship between products. The main contribution of this paper is as follows: (1) A comprehensive analysis of privacy–profit tradeoffs involved in E–Commerce; (2) A flexible privacy control model based on the concept of *hierarchy of privacy groups* and privacy policy inheritance and over-witting; (3) A solution for efficient customer–provider matchmaking. In the C2P case where customers seek for ideal providers, match is based on catalog-based product category. In the P2C case where providers try to promote a certain product, match is based on contact frequency of customers and friendship of customers.

There are still some problems to be solved in the future work. First, a successful E-Commerce system should provide guarantee for both security and privacy protection. Incorporating security solution in a web notary system is important. Second, in this paper we have focused on customer's privacy. However, providers privacy is hard to handle. Our future work will include this aspect.

Notes

1. `http://www.safeway.com/club_card.asp/`
2. `http://dir.clubs.yahoo.com/`
3. `http://shopping.yahoo.com/`

References

[1] K. Decker, K. Sycara, and M. Williamson. Middle-Agents for the Internet. In *Proceedings of the 15th International Joint Conference on Artificial Intelligence*, pages 578–583, 1997.

[2] B. Limthanmaphon, Y. Zhang, and Z. Zhang. An Agent Based Negotiation Model Supporting Transactions in EC. In *Proceedings of DEXA'00 Workshop*, London, September 2000. IEEE Computer Society Press.

[3] M. Papazoglou and A. Tsalgatidou. Special issue on information systems support for electronic commerce. *Information Systems*, 1999.

[4] J. Reagle and L. F. Cranor. The platform for privacy preferences. *Communications of the ACM*, 42(2):48–55, February 1999.

[5] J. Schafer, J. Konstan, and J. Riedl. Electronic Commerce Recommender Applications. *Journal of Data Mining and Knowledge Discovery*, January 2001. to appear.

[6] O. Shehory. A Scalable Agent Location Mechanism. In *Lecture notes in Artificial Intelligence, Intelligent Agents VI, M. Wooldridge and Y. Lesperance(Eds.)*, pages 162–174, 1999.

[7] Statistical Research, Inc. Even veteran web users remain skittish about sites that get personal. Press Releases, June 2001. `http://www.statisticalresearch.com/press/pr060701.htm`.

Session III: Process Interoperability