User customizable Privacy-preserving Search Framework for Personalized Web Search

Koramutla Rajesh 1, Prof. R. Suresh 2

1 MTech (cse), Chadalawada Ramanamma Engineering college, Tirupati, JNTUA
2 Professor & Head of the Department, Chadalawada Ramanamma Engineering college, Tirupati, JNTUA

Abstract-Searching is one of the common tasks performed on the Internet. Search engines are the basic tool of the internet, from where one can collect related information and searched according to the specified query or keyword given by the user, and are extremely popular for recursively used sites. The information on the web is growing dramatically. The users have to spend lots of time on the web finding the information they are interested in. Today, the traditional search engines do not give users enough personalized help but provide the user with lots of irrelevant information. In such case, personalized web search (PWS) has demonstrated its effectiveness in improving the quality of various search services on the Internet. However, evidences show that users’ are not willing to disclose their private information during search has become a major barrier for the widespread use of PWS. This paper gives information about privacy protection in PWS applications that model user preferences as hierarchical user profiles. This paper proposes a PWS framework called SECURITY that can adaptively generalize profiles by queries while respecting userspecified privacy requirements. It aims at providing protection against a typical model of privacy attack.

Index Terms-Privacy protection; personalized web search; SECURITY framework

1. INTRODUCTION

The web search engine is the most important portal for ordinary people looking for useful information on the web. However, users generally experience failure and get improper results when search engines return irrelevant results that do not meet their real intentions. A typical search engine provides similar set of results without considering of who submitted the query. Therefore, the requirement arises to have personalized web search system which gives outputs appropriate to the user as highly ranked pages. Personalized web search (PWS) is a general category of search techniques which aims to provide better search results, according to individual user needs. So, for this user information has to be collected and analyzed so that the perfect search results required for the user behind the issued query is to be given to the user. The solution to this is Personalized Web Search (PWS). It can generally be categorized into two types, first is click-log-based methods and second is profile-based ones. The click-log based methods are simple and straightforward: This method performs the search based upon clicked pages in the user’s query history. Although this method has been demonstrated to perform consistently and considerably well [2], it can only work on repeated queries from the same user, which is a strong limitation and restricted for certain applications. In contrast, profile-based methods improve the search experience with complicated user-interest models generated from user profiling techniques. Profile-based methods can be proved more effective for almost all sorts of queries, but are reported to be improper under some situations. [1]. Although there are reasons and considerations for both types of PWS techniques, the profile-based PWS has proved its more effectiveness in improving the quality of web search recently, with increasing usage of one’s personal and behavioral information to profile its users, which is usually gathered implicitly with the help of query history [2], [3], [4], browsing history [5], [6], click-through data, [2] bookmarks, user documents [2], and so on. Unfortunately, such type of collected personal data can easily reveal a entire scope of user’s private life. Protecting privacy issues arising from the lack of protection for such data, for example the AOL query logs scandal, not only raise panic among individual users but also downs the data publisher’s enthusiasm in offering personalized service. In fact, privacy concerns have become the major barrier for wide use of PWS services.
2. BACKGROUND

To protect user privacy in profile-based PWS, researchers have to consider two important and contradicting issues during the search process. The first issue is that, they attempt to improve thesearch quality with the personalization utility of the userprofile. On the other hand the second issue is, they need to hide the privacy contents existing in the user profile to place the privacy risk under control. Sometimes people are willing to compromise privacy if the personalization by supplying user profile to the search engine yields better search quality. In an identical situation, significant gain can be obtained by personalization at the expense of only a small (and less-sensitive) portion of the userprofile, namely a generalized profile. Thus, user privacy can be protected without compromising the personalized search quality. In general, there is a compromise between the search quality and the level of privacy protection achieved from generalization.

Unfortunately, the previous works of privacy preserving PWS are far from optimal. The problems with the existing methods are explained in the following observations:[5]

1. The existing profile-based PWS do not support runtime profiling. A user profile is typically generalized for only once offline, and used to personalize all queries from a same user indiscriminately. Such “one profile fits all” strategy certainly has drawbacks given the variety of queries. It is proved that Profile-based personalization may not even help to improve the search quality for some ad hoc queries, though exposing user profile to a server has put the user’s privacy at risk. A better approach is to make an online decision on:
   a. whether to personalize the query (by exposing the profile) and
   b. what to expose in the user profile at runtime.

   Until now no previous work has supported such feature.

2. The existing methods do not take into account the customization of privacy requirements. This probably makes some user privacy to be overprotected whereas others insufficiently protected. For example, in all sensitive topics are detected using an absolute metric called surprised based on the information theory, assuming that the interests without user document support are more sensitive.

3. Many personalization techniques require iterative user interactions when creating personalized search results. They usually refine the search results with some metrics which require multiple user interactions, such as rank scoring, average rank [8], and so on. This paradigm is, however, infeasible for runtime profiling, as it will not only pose too much risk of privacy breach, but also demand prohibitive processing time for profiling. Thus, we need predictivemetrics to measure the search quality and breach risk after personalization, without incurring iterative user interaction.

3. RELATED WORK

The above problems are explained in the SECURITY (which means User customizable Privacy-preserving Search) framework.[5] The framework assumes that the queries do not contain any sensitive information, and aims at protecting the privacy in individual user profiles while retaining their usefulness for PWS.

As given in Fig. 1, SECURITY consists of a non-trust search engine server and a number of clients. Each client (user) accessing the search service trusts no one but himself/ herself. The key component for privacy protection is an online profiler implemented as a search proxy running on the client machine itself. The proxy maintains both the complete user profile, in a hierarchy of nodes with semantics, and the user-specified (customized) privacy requirements represented as a set of sensitive nodes.

The framework works in two phases, namely the offline and online phase, for each user. During the offline phase, a hierarchical user profile is constructed and customized with the user-specified privacy requirements. The online phase handles queries as follows:

1. When a user issues a query qi on the client, the proxy generates a user profile in runtime in the light of query terms. The output of this step is a generalized user profile Gi satisfying the privacy requirements. The generalization process is guided by considering two conflicting metrics, namely the personalization utility and the privacy risk, both defined for user profiles.

2. Subsequently, the query and the generalized user profile are sent together to the PWS server for personalized search.

3. The search results are personalized with the profile and delivered back to the query proxy.

4. Finally, the proxy either presents the raw results to the user, or reranks them with the complete user profile.

SECURITY is distinguished from conventional PWS in that
1) provides runtime profiling, which in effect optimizes the personalization utility while respecting user’s privacy requirements;
2) allows for customization of privacy needs; and
3) does not require iterative user interaction

4. ATTACK MODEL

Our work aims at providing protection against a typical model of privacy attack, namely eavesdropping. As shown in Fig. 2, to corrupt Alice’s privacy, the eavesdropper Eve successfully intercepts the communication between Alice and the PWS-server via some measures, such as man-in-the-middle attack, invading the server, and so on. Consequently, whenever Alice issues a query q, the entire copy of q together with a runtime profile G will be captured by Eve. Based on G, Eve will attempt to touch the sensitive nodes of Alice by recovering the segments hidden from the original H and computing a confidence for each recovered topic, relying on the background knowledge in the publicly available taxonomy repository R. Note that in our attack model, Eve is considered as an adversary satisfying the following assumptions:[5]

Knowledge bounded: The background knowledge of the adversary is limited to the taxonomy repository R. Both the profile H and privacy are defined based on R.

Session bounded: None of previously captured information is available for tracing the same victim in a long duration. In other words, the eavesdropping will be started and ended within a single query session.

Fig. 1. System architecture of SECURITY framework

Fig. 2. Attack model representing personalized web search

www.jreecs.com
5. CONCLUSION

The remarkable development of information on the Web has forced new challenges for the construction of effective search engines. This paper provides information on User customizable Privacy preserving Search framework-SECURITY for Personalized Web Search. SECURITY could potentially be adopted by any PWS that captures user profiles in a hierarchical taxonomy. The framework allowed users to specify customized privacy requirements via the hierarchical profiles.

REFERENCES