International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 1 Issue 6, October 2014

Confidential User Query Profile Construction for Personalized Web Search

Ms. P. Sudhaselvanayaki
II Year M.E(CSE)
Shree Venkateshwara Hi-Tech Engg College, Gobi
mahe11191@gmail.com

Dr. T. Senthil Prakash
Professor & HOD
Shree Venkateshwara Hi-Tech Engg College, Gobi
jtyesp@yahoo.co.in

Ms. V. Karthikeyani
II Year M.E(CSE)
Shree Venkateshwara Hi-Tech Engg College, Gobi
karthikeyani.vn@gmail.com

ABSTRACT- *Web site structures are altered to improve the user navigations. Web personalization method reconstructs the page links with reference to the traversal path and profile of a particular user. User information are collected and analyzed to fetch the user intention behind the issued query. User customizable Privacy-preserving Search (UPS) is used to generalize profiles by queries with user privacy requirements. Greedy discriminating power algorithm (GreedyDP) is used to maximize the discriminating power of the user profiles. Greedy Information Loss (GreedyIL) is used to minimize the information loss in user profiles. GreedyIL algorithm achieves high efficiency than the GreedyDP algorithm. The Personalized Web Search (PWS) scheme is enhanced to control topic relationship based expert attacks. The User customizable Privacy-preserving Search (UPS) model is enhanced to resist query session based attacks. Query generalization is performed with query priority values. Anonymization and topic taxonomy models are used to improve the personalization process.*

Index Terms: *User customizable Privacy-preserving Search, Greedy discriminating power algorithm, Greedy Information Loss, Query generalization*

1 INTRODUCTION

Web Mining, which focuses on automatically discovering information and knowledge through the analysis of Web contents, Web structure and Web usages. Since the Web is huge, heterogeneous and dynamic, automated Web information and knowledge discovery calls for novel technologies and tools, which may take advantage of the state-of-the-art technologies from various areas, including machine learning, data mining, information retrieval, database and nature language processing.

The Web itself and the search engine indices contain information about the documents. Documents have different types of relationships among themselves. Hyperlinks add depth to documents, providing the multi-dimensionality, which characterizes the Web. Documents have an address, a URL, which represents a logical location on a server, which may provide information about the relationship of this document to other on the server. Also, there is a relationship to other documents on the Web unknown to the document, the search engine index may discover such relationships. Web mining is a huge, interdisciplinary and very dynamic scientific area, converging from several research communities such as database, information retrieval, and artificial intelligence especially from machine learning and natural language processing.

The user may wish to synthesize a web page for different individuals from the available set of web pages. Individuals have their own preferences in the style of the contents and presentations while interacting with the web. The information providers like to create a system responds to user queries by potentially aggregating information from several sources, in a manner which is dependent on the user.

2 RELATED WORKS

In this section, we overview the related works. We focus on the literature of profile-based personalization and privacy protection in PWS system.

I Profile-Based Personalization

Previous works on profile-based PWS mainly focus on improving the search utility. The basic idea of these works is to tailor the search results by referring to, often implicitly, a user profile that reveals an individual information goal. We review the previous solutions to PWS on two aspects, namely the representation of profiles, and the measure of the effectiveness of personalization.

Many profile representations are available in the literature to facilitate different personalization strategies. Earlier techniques utilize term lists/vectors or bag of words to represent their profile. Most recent works build profiles in hierarchical structures due to their stronger descriptive ability, better scalability, and higher access efficiency. The majority of the hierarchical representations are constructed with

existing weighted topic hierarchy/graph, such as ODP, Wikipedia [5] and so on. In our proposed UPS framework, we do not focus on the implementation of the user profiles. Actually, our framework can potentially adopt any hierarchical representation based on taxonomy of knowledge.

As for the performance measures of PWS in the literature, Normalized Discounted Cumulative Gain (nDCG) is a common measure of the effectiveness of an information retrieval system. It is based on a human graded relevance scale of item-positions in the result list, and is, therefore, known for its high cost in explicit feedback collection. To reduce the human involvement in performance measuring, researchers also propose other metrics of personalized web search that rely on clicking decisions, including Average Precision (AP), Rank Scoring and Average Rank. We use the Average Precision metric, proposed by Dou et al. [1], to measure the effectiveness of the personalization in UPS. Our work is distinguished from previous studies as it also proposes two predictive metrics, namely personalization utility and privacy risk, on a profile instance without requesting for user feedback.

II Privacy Protection in PWS System

Generally there are two classes of privacy protection problems for PWS. One class includes those treat privacy as the identification of an individual. The other includes those consider the sensitivity of the data, particularly the user profiles, exposed to the PWS server.

Typical works in the literature of protecting user identifications try to solve the privacy problem on different levels, including the pseudo identity, the group identity, no identity, and no personal information. Solution to the first level is proved to fragile. The third and fourth levels are impractical due to high cost in communication and cryptography. Therefore, the existing efforts focus on the second level. Both [8] and [2] provide online anonymity on user profiles by generating a group profile of k users. Using this approach, the linkage between the query and a single user is broken. In [3], the useless user profile (UUP) protocol is proposed to shuffle queries among a group of users who issue them [9]. As a result any entity cannot profile a certain individual. These works assume the existence of a trustworthy third-party anonymizer, which is not readily available over the Internet at large. Viejo and Castell_a-Roca [4] use legacy social networks instead of the third party to provide a distorted user profile to the web search engine. In the scheme, every user acts as a search agency of his or her neighbors. They can decide to submit the query on behalf of who issued it, or forward it to other neighbors. The shortcomings of current solutions in class one is the high cost introduced due to the collaboration and communication.

The solutions in class two do not require third-party assistance or collaborations between social network entries. In these solutions, users only trust themselves and cannot tolerate the exposure of their complete profiles an anonymity server. In [12], Krause and Horvitz employ statistical techniques to learn a probabilistic model, and then use this model to generate the near-optimal partial profile. One main limitation in this work is that it builds the user profile as a finite set of attributes, and the probabilistic model is trained through predefined frequent queries. These assumptions are impractical in the context of PWS. Xu et al. proposed a privacy protection solution for PWS based on hierarchical profiles. Using a user-specified threshold, a generalized profile is obtained in effect as a rooted subtree of the complete profile. Unfortunately, this work does not address the query utility is crucial for the service quality of PWS. For comparison, our approach takes both the privacy requirement and the query utility into account.

A more important property that distinguishes our work from is that we provide personalized privacy protection in PWS. The concept of personalized privacy protection is first introduced by Xiao and Tao Privacy-Preserving Data Publishing (PPDP) [11]. A person can specify the degree of privacy protection for her/his sensitive values by specifying “guarding nodes” in the taxonomy of the sensitive attribute. Motivate by this, we allow users to customize privacy needs in their hierarchical user profiles.

Aside from the above works, a couple of recent studies have raised an interesting question that concerns the privacy protection in PWS. The works in [1], [6] have found that personalization may have different effects on different queries. Queries with smaller click-entropies, namely distinct queries, are expected to benefit more from personalization, while those with larger values are not. Moreover, the latter may even cause privacy disclosure. Therefore, the need for personalization becomes questionable for such queries. Teevan et al. [6] collect a set of features of the query to classify queries by their click entropy. While these works are motivative in questioning whether to personalize or not to, they assume the availability of massive user query logs and user feedback. In our UPS framework, we differentiate distinct queries from ambiguous ones based on a client-side solution using the predictive query utility metric.

This paper is an extension to our preliminary study reported in [7]. In the previous work, we have proposed the prototype of UPS, together with a

greedy algorithm GreedyDP to support online profiling based on predictive metrics of personalization utility and privacy risk. In this paper, we extend and detail the implementation of UPS [10]. We extend the metric of personalization utility to capture our three new observations. We also refine the evaluation model of privacy risk to support user-customized sensitivities. Moreover, we propose a new profile generalization algorithm called GreedyIL. Based on three heuristics newly added in the extention, the efficiency and stability of the new algorithm outperforms the old one significantly.

3 PRIVACY PRESERVED PERSONALIZED WEB SEARCH

The web search engine has long become the most important portal for ordinary people looking for useful information on the web. Users might experience failure when search engines return irrelevant results that do not meet their real intentions. Such irrelevance is largely due to the enormous variety of users' contexts and backgrounds, as well as the ambiguity of texts. Personalized web search (PWS) is a general category of search techniques aiming at providing better search results, which are tailored for individual user needs. As the expense, user information has to be collected and analyzed to figure out the user intention behind the issued query.

The solutions to PWS can generally be categorized into two types, namely click-log-based methods and profile-based ones. The click-log based methods are straightforward— they simply impose bias to clicked pages in the user's query history. Although this strategy has been demonstrated to perform consistently and considerably well [1], it can only work on repeated queries from the same user, which is a strong limitation confining its applicability. In contrast, profile-based methods improve the search experience with complicated user-interest models generated from user profiling techniques. Profile-based methods can be potentially effective for almost all sorts of queries, but are reported to be unstable under some circumstances [1].

There are pros and cons for both types of PWS techniques, the profile-based PWS has demonstrated more effectiveness in improving the quality of web search recently, with increasing usage of personal and behavior information to profile its users, which is usually gathered implicitly from query history browsing history click-through data bookmarks user documents and so forth. Unfortunately, such implicitly collected personal data can easily reveal a gamut of user's private life. Privacy issues rising from the lack of protection for such data, for instance the AOL query logs scandal not only raise panic among individual users, but also dampen the data-publisher's enthusiasm in offering personalized service. In fact, privacy concerns have become the major barrier for wide proliferation of PWS services.

The UPS (User customizable Privacy-preserving Search) 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. UPS consists of a nontrusty search engine server and a number of clients. Each client 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 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. UPS is distinguished from conventional PWS in that it 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. Our main contributions are summarized as following:

- We propose a privacy-preserving personalized web search framework UPS, which can generalize profiles for each query according to user-specified privacy requirements.
- Relying on the definition of two conflicting metrics, namely personalization utility and privacy risk, for hierarchical user profile, we formulate the problem of privacy-preserving personalized search as Risk Profile Generalization, with its NP-hardness proved.

- We develop two simple but effective generalization algorithms, GreedyDP and GreedyIL, to support runtime profiling. While the former tries to maximize the discriminating power (DP), the latter attempts to minimize the information loss (IL). By exploiting a number of heuristics, GreedyIL outperforms GreedyDP significantly.
- We provide an inexpensive mechanism for the client to decide whether to personalize a query in UPS. This decision can be made before each runtime profiling to enhance the stability of the search results while avoid the unnecessary exposure of the profile.
- Our extensive experiments demonstrate the efficiency and effectiveness of our UPS framework.

4 PROBLEM STATEMENT

User information are collected and analyzed to fetch the user intention behind the issued query. User customizable Privacy-preserving Search (UPS) is used to generalize profiles by queries with user privacy requirements. Two Greedy algorithms are used to generalize the user query profiles. Greedy discriminating power algorithm (GreedyDP) is used to maximize the discriminating power of the user profiles. Greedy Information Loss (GreedyIL) is used to minimize the information loss in user profiles. GreedyIL algorithm achieves high efficiency than the GreedyDP algorithm. An online prediction mechanism is provided for deciding whether personalizing a query is beneficial. Utility of personalization and the privacy risk of exposing the generalized profile metrics are used to analyze the system. The following drawbacks are identified from the existing system.

- Inefficiency in domain expert based attack control
- Session based query attacks are not handled
- Query weightage is not considered
- Utility measure is not optimized

5 USER CUSTOMIZABLE PRIVACY-PRESERVING SEARCH (UPS) PROCEDURES

In this section, we present the procedures carried out for each user during two different execution phases, namely the offline and online phases. Generally, the offline phase constructs the original user profile and then performs privacy requirement customization according to user-specified topic sensitivity. The subsequent online phase finds the Optimal δ-Risk Generalization solution in the search space determined by the customized user profile.

The online generalization procedure is guided by the global risk and utility metrics. The computation of these metrics relies on two intermediate data structures, namely a cost layer and a preference layer defined on the user profile. The cost layer defines for each node $t \in H$ a cost value $cost(t) \geq 0$, which indicates the total sensitivity at risk caused by the disclosure of t. These cost values can be computed offline from the user-specified sensitivity values of the sensitive nodes. The preference layer is computed online when a query q is issued. It contains for each node $t \in H$ a value indicating the user's query-related preference on topic t. These preference values are computed relying on a procedure called query topic mapping. Specifically, each user has to undertake the following procedures in our solution:

1. offline profile construction,
2. offline privacy requirement customization,
3. online query-topic mapping, and
4. online generalization.

Offline-1. Profile Construction. The first step of the offline processing is to build the original user profile in a topic hierarchy H that reveals user interests. We assume that the user's preferences are represented in a set of plain text documents, denoted by D. To construct the profile, we take the following steps:

1. Detect the respective topic in R for every document $d \in D$. Thus, the preference document set D is transformed into a topic set T.
2. Construct the profile H as a topic-path trie with T, i.e., H = trie(T).
3. Initialize the user support $sup_H(t)$ for each topic $t \in T$ with its document support from D, then compute $sup_H(t)$ of other nodes of H with (4).

There is one open question in the above process—how to detect the respective topic for each document $d \in D$. We present our solution to this problem in our implementation.

Offline-2. Privacy Requirement Customization. This procedure first requests the user to specify a sensitive-node set $S \in H$, and the respective sensitivity value sen(s) > 0 for each topic $s \in S$. Next, the cost layer of the profile is generated by computing the cost value of each node $t \in H$ as follows:

1. For each sensitive-node, cost(t) = sen(t);
2. For each nonsensitive leaf node, cost(t) = 0;
3. For each nonsensitive internal node, cost(t) is recursively given by (1) in a bottom-up manner:

$$cost(t) = \sum_{t' \in C(t,H)} cost(t') \times \Pr(t' \mid t) \quad (1)$$

Till now, we have obtained the customized profile with its cost layer available. When a query q is issued, this profile has to go through the following two online procedures:

Online-1. Query-topic Mapping. Given a query q, the purposes of query-topic mapping are 1) to compute a rooted subtree of H, which is called a seed profile, so that all topics relevant to q are contained in it; and 2) to obtain the preference values between q and all topics in H. This procedure is performed in the following steps:

Topics in T (Eagles)	Rel.
Top/Arts/Music/Artists	23
Top/Sports/American football/NFL/Philadelphia Eagles	14
Top/Science/Biology/Animals/Birds/Raptors/Eagles	7
Top/Society/Military/Aviation/Aircraft/Figters/F-15	4

1. Find the topics in R that are relevant to q. We develop an efficient method to compute the relevance's of all topics in R with q. These values can be used to obtain a set of non overlapping relevant topics denoted by T(q), namely the relevant set. We require these topics to be non overlapping so that T(q), together with all their ancestor nodes in R, comprise a query-relevant trie denoted as R(q). Apparently, T(q) are the leaf nodes of R(q). Note that R(q) is usually a small fraction of R.

2. Overlap R(q) with H to obtain the seed profile G_0, which is also a rooted sub tree of H. For example, by applying the mapping procedure on query "Eagles," we obtain a relevant set T(Eagles) as shown in Table 5.1. Overlapping the sample profile with its query-relevant trie R(Eagles)gives the seed profile G_b, whose size is significantly reduced compared to the original profile.

The leaves of the seed profile G_0 form a particularly interesting node set the overlap between set T(q) and H. We denote it by $T_H(q)$, and obviously we have $T_H(q) \subset T(q)$.

Then, the preference value of a topic $t \in H$ is computed as following:

1. If t is a leaf node and $t \in T_H(q)$, its preference pre $f_H(t,q)$ is set to the long-term user support $\sup_H(q)$[3], which can be obtained directly from the user profile.

2. If t is a leaf node and $t \notin T_H(q)$, pre $f_H(t,q) = 0$.

3. Otherwise, t is not a leaf node. The preference value of topic t is recursively aggregated from its child topics as

$$\text{pre } f_H(t,q) = \sum_{v \in C(t,H)} pref_H(t', H).$$

Finally, it is easy to obtain the normalized preference for each $t \in H$ as

$$\Pr(t \mid q, H) = \frac{pref_H(t,q)}{\sum_{t' \in TH(q)} \Pr efH(t',q)} \quad (2)$$

Note that the first step computes for each t 2 T(q) a relevance value with the query, denoted by relR(q). These values can be used to model a conditional probability that indicates how frequently topic t is covered by q:

$$\Pr(t|q)=\Pr(t|q,R)= \frac{rel_R(t,q)}{\sum_{t' \in T(q)} rel_R(t',q)} \quad (3)$$

Though this probability is not used in this procedure, it is needed to evaluate the discriminating power of q and to decide whether to personalize a query or not.

Online-2. Profile Generalization. This procedure generalizes the seed profile G0 in a cost-based iterative manner relying on the privacy and utility metrics. In addition, this procedure computes the discriminating power for online decision on whether personalization should be employed.

6 CONFIDENTIAL USER QUERY PROFILE CONSTRUCTION FOR PWS

The Personalized Web Search (PWS) scheme is enhanced to control topic relationship based expert attacks. The User customizable Privacy-preserving Search (UPS) model is enhanced to resist query session based attacks. Query generalization is performed with query priority values. Anonymization and topic taxonomy models are used to improve the personalization process. The system is designed to protect the web personalization scheme with attack controlling mechanism. Privacy is ensured with anonymization methods. Query optimization process is use to improve the query values. The system is divided into six major modules. They are query log analyzer, user profile construction and query generalization using GreedyDP, query generalization using GreedyIL, personalized search process and attack controller.

The query log analyzer module is designed to perform preprocess on user query logs. User query profiles are constructed using query keywords. Query

values are generalized under the Query generalization with GreedyDP module. Query values are generalized under the Query generalization with GreedyIL module. Query optimization process is carried out under the personalized search process module. Query session attacks are handled in attack controller module.

I Query Log Analyzer

User query values are maintained under the query log files. User and query details are parsed from the query log data. Redundant log entries are removed from the log information. Optimized query data values are updated into the database.

II User Profile Construction

User profiles are constructed to manage the search behavior of the user. Search history is used in the user profile construction process. Query keywords are updated with the frequency values. Domain information are updated with the search query values.

III Query Generalization using GreedyDP

Anonymization methods are used to provide privacy for user query values. User query values are generalized for privacy preservation. Greedy discriminating power (GreedyDP) algorithm is used for the query generalization process. Generalized query values are updated in the user search history environment.

IV Query Generalization using GreedyIL

Query values are generalized with information lose factors. Greedy Information Loss (GreedyIL) algorithm is used for the generalization process. Data usage is considered in the generalization process. Generalized query keywords are used in the search optimization process.

V Personalized Search Process

Privacy preserved web search is performed in the personalized search process. Query optimization is used to improve the query keywords. Generalized query keywords are used in the query optimization process. Query weight values are used for the query optimization process.

VI Attack Controller

The attack controller is used to control query attacks. Session information are protected to control session based attacks. Topic taxonomy is used for the query optimization and generalization process. Data utilization rate is considered in the attack controlling process.

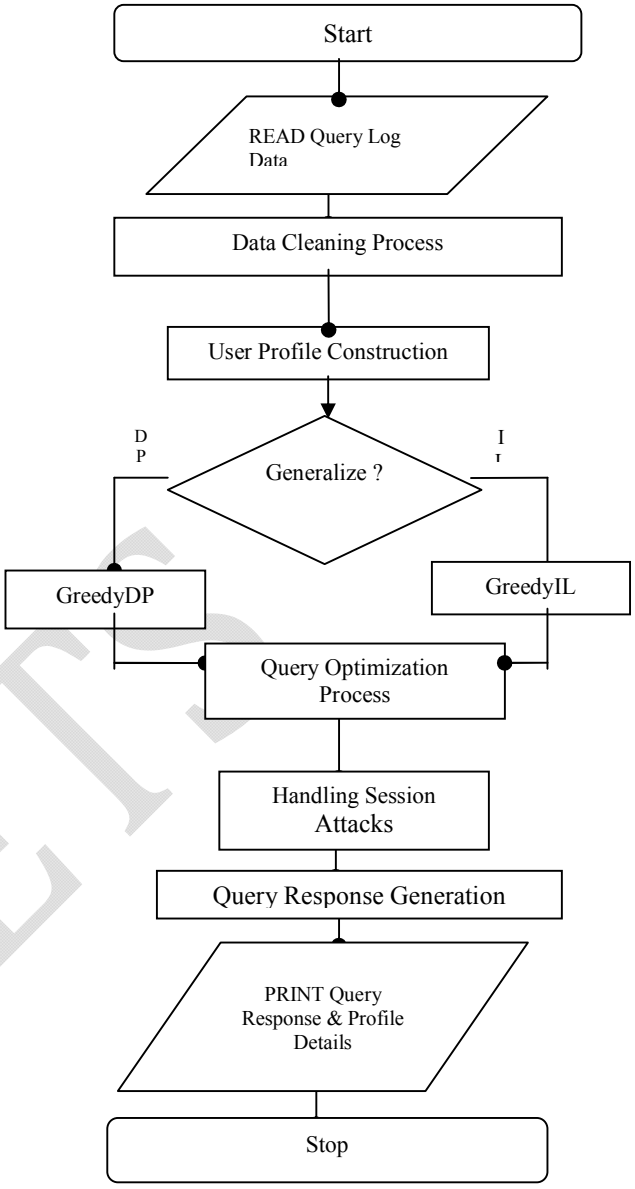

Fig. No:1 Confidential User Query Profile Construction Process

7 CONCLUSION

Personalized web search (PWS) is used to improve the quality of various search services on the Internet. Privacy preserved PWS methods are used to protect the disclosure of personal information in search process. User customizable Privacy-preserving Search (UPS) framework is used to support privacy in search process. The UPS scheme is enhanced with Anonymization and attack resistant methods. Personalization utility is high in the personalized web search scheme. The system reduces the generalization

risk levels. The system increases the attack control rate. Priority based user profile construction process is supported by the system.

REFERENCES

[1] Z. Dou, R. Song, and J.-R. Wen, "A Large-Scale Evaluation and Analysis of Personalized Search Strategies," Proc. Int'l Conf. World Wide Web (WWW), pp. 581-590, 2007.

[2] Y. Zhu, L. Xiong, and C. Verdery, "Anonymizing User Profiles for Personalized Web Search," Proc. 19th Int'l Conf. World Wide Web (WWW), pp. 1225-1226, 2010.

[3] J. Castellı´-Roca, A. Viejo, and J. Herrera-Joancomartı´, "Preserving User's Privacy in Web Search Engines," Computer Comm.,vol.32, no. 13/14, pp. 1541-1551, 2009.

[4] A. Viejo and J. Castell_a-Roca, "Using Social Networks to Distort Users' Profiles Generated by Web Search Engines," Computer Networks, vol. 54, no. 9, pp. 1343-1357, 2010.

[5] K. Ramanathan, J. Giraudi, and A. Gupta, "Creating Hierarchical User Profiles Using Wikipedia," HP Labs, 2008.

[6] J. Teevan, S.T. Dumais, and D.J. Liebling, "To Personalize or Notto Personalize: Modeling Queries with Variation in User Intent,"Proc.31st Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), pp. 163-170, 2008.

[7] G. Chen, H. Bai, L. Shou, K. Chen, and Y. Gao, "Ups: Efficient Privacy Protection in Personalized Web Search," Proc. 34th Int'l ACM SIGIR Conf. Research and Development in Information, pp. 615- 624, 2011.

[8] Y. Xu, K. Wang, G. Yang, and A.W.-C. Fu, "Online Anonymity for Personalized Web Services," Proc. 18th ACM Conf. Information and Knowledge Management (CIKM), pp. 1497-1500, 2009.

[9] D. Xing, G.-R. Xue, Q. Yang, and Y. Yu, "Deep Classifier: Automatically Categorizing Search Results into Large-Scale Hierarchies," Proc. Int'l Conf. Web Search and Data Mining (WSDM), pp. 139-148, 2008.

[10] Xueming Qian, He Feng, Guoshuai Zhao, and Tao Mei, "Personalized Recommendation Combining User Interest and Social Circle",IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 7, July 2014

[11] Zheng Lu, Hongyuan Zha, Xiaokang Yang, Weiyao Lin, and Zhaohui Zheng, "A New Algorithm for Inferring User Search Goals with Feedback Sessions" , IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 3, March 2013

[12] A. Krause and E. Horvitz, "A Utility-Theoretic Approach to Privacy in Online Services," J. Artificial Intelligence Research,vol. 39, pp. 633-662, 2010.

Ms. P. Sudhaselvanayaki received the B.E (CSE) degree from the RVS College of Engineering and Technology, Coimbatore, India in 2009-2013 and pursuing ME (CSE) degree in Shree Venkateshwara Hi-Tech Engineering College, Erode, India in 2013-201 5, all in Computer Science and Engineering. She is a Member of Computer Society of India (CSI). Her research interests include Data Bases, Data Mining, and Networks. She published 1 National Conferences, 4 Workshops.

Dr.T.Senthil Prakash received the Ph.D. degree from the PRIST University, Thanjavur, India in 2013 and M.E(CSE) degree from Vinayaka Mission's University, Salem , India in 2007 and M.Phil.,MCA.,B.Sc(CS) degrees from Bharathiyar University, Coimbatore India, in 2000,2003 and 2006 respectively, all in Computer Science and Engineering. He is a Member in ISTE New Delhi, India, IAENG, Hong Kong..IACSIT, Singapore SDIWC, USA. He has the experience in Teaching of 10+Years and in Industry 2 Years. Now He is currently working as a Professor and Head of the Department of Computer Science and Engineering in Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamil Nadu, and India. His research interests include Data Mining, Data Bases, Artificial Intelligence, Software Engineering etc.,He has published several papers in 17 International Journals, 43 International and National Conferences.

MS.V.Karthikeyani pursuing M.E(CSE) degree from Shree Venkateshwara Hi-Tech engineering college, Erode, India in 2014 and B.E(CSE) degree from Nandha College of Technology, Erode, India in 2013. She has attend a National conference on Cloud Security and 2 workshops. Her research interests include Network Security, Data mining.