International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184, Volume 5, Number 3 (June 2016), pp.170-176

http://www.meacse.org/ijcar

ABSEP3S- An Agent Based Security Engine for Privacy Preserving in Personalized Search

AnuSharma[1], Ali T. Al-khwaldeh[2] and Aarti Singh[3]
[1&3]MMICT&BM, MMUniversity, Ambala, India
[2] Philadelphia University, Amman, Jordan

Abstract

Web personalization is the most debated topic of research these days. Due to ample scope of opportunities for business and individual usage, research community is putting in more and more efforts towards identifying interests of an individual and providing onlyrelevant information to users. However this leads to continuous monitoring and analysis of one's web surfing activities which is undesired for users.Privacy preservation has become animportant issue to deal with in personalized search environment. Sematic web technologies and intelligent software agents are playing important role towards automation of various tasksin web personalization. This work presents a novel method for protecting user's privacy using Elliptical Curve Cryptography (EEC) technique deployed through intelligent software agents. Further, this method further blocks unauthorizedthird party access of information stored in user logs of servers. Software agents are deployed considering the number of users and size of information been searched being autonomous they can increase the efficiency and scalability of the system.

Keywords: Web personalization, privacy preservation, search security, ECC, Software Agents.

1 Introduction

There is a growing increase in the amount of the information available on internet. Web search engines are generally used to find the information from web. But most of the users experience dissatisfaction regarding the search engine ability tounderstand their real intention while displaying the results. Personalized web search provides a solution to this problem by organizing the search results according to the user preferences and context. So, it is required to make available the user personal information on web. Exposing the personal information on public domain raises manyprivacy concerns. This personal information is also used by organizations to promote their product, brands and services directly from the server, without taking permission from the user.Thus, many users are reluctant to share and provide their personal information to web search engines. There is a trade-off between the effectiveness of web search results and level of details provided by the user. Detailed user profile leads to better search results while abstract user profile leads to less relevant results.

Many users are ready to share the information for better services and offers. But others are more concerned about the privacy of their personal information. Privacy preservation has become an important aspect to be taken care of while developing personalized search environment. Pseudo-identity, group identity, no identity and no personalinformation techniques are used for maintaining the privacy of user. Existing work in this area has been discussed in literature review. Analysis of literature has highlighted the use of semantic web and agent technology in this area. Autonomous intelligent agents provide an important technology for accomplishing privacy preservation in web personalization. It is expected that usage of intelligent software

agents in web search will enhance the efficiency, scalability of search engines along with complete automation of tasks involved in the process.

The present study is undertaken with the aim to solve the various privacy issues in web search by partitioning the user profile into public and private through agent oriented mechanism for complete automation of various tasks. A novel concept of encrypting the private data at server side is introduced to block the unauthorized access by third party vendors. This paper is organized into five sections. Section two gives literature survey and motivation of undertaking current research. Section three describes the proposed framework and the algorithmic detail of the proposed work is given in section four. Section five gives the conclusion and future direction of research work.

2 Related Work

This section briefly describes the work in area of preserving the privacy in this information filled world. Many authors have contributed to the survey of privacy issues in recommender systems [1], collaborative filtering [2] and user's perception on personalization efficiency ([3], [4], [5]). One of the important threats to privacy is to identify the user back from the available privately held collection on personal data. A solution to this problem has been given by [6] named k-anonymity whereby a persons is not distinguished from at least k-1 individual in a database.

A distinction and definition of four levels of privacy protection is given by [7]withanalysis of various architectures for personalized search. At the simplestlevel firstmethod is the use of pseudo identity which replaces the identity with single or group of users. But it still leaves the other information about user on server. In level two of privacy protection search engine builds a group profile rather than the individual profile. A proxy server may be used for interactions with search engine by many users or obfuscation of query term may be used to achieve this level of privacy protection. No information about user is available at server side in third level security and it is not possible to aggregate any information about user even at group level.This can be achieved by using anonymous network. But some information like user's original query is still stored on server. Best level of privacy is when no information about user is available on server. It involves the use of cryptographic techniques. A scalable way to create a hierarchical user profilehasbeen proposed by [8]. They have also proposed to two parameters for specifying the content and degree of details of profile information that is to be exposed to the search engine. But incorporation of privacy preservation leads to compromise in quality of search results. So, the better approach would be to expose the information related to the specific query. This aspect has been considered by [9] who have proposed a framework that can adaptively generalize profiles by queries while respecting user-specified requirement. This work can be further strengthened by adding background knowledge and richer relationships among topics.An attempt to quantify the privacy of user profiles have been made by [10] using KL divergence as a measure. The concept of Homomorphic encryption to encrypt the server in such a way that neither an eavesdropper nor an untrusty admin could access the search words and the profile is given by [11].

An attempt to use multi-agent approach for privacy preserving in recommender systems by utilizing fundamental features of agents such as autonomy, adaptability and the ability to communicatehave been made by [12]. The proposed protocol could be extended in order to keep the recommendations themselves as private.A Secure Multi Agent Information Filtering (SMAIF) system based on agents to overcome information filtering challenges is proposed by [13].An approach for ensuring truthfulness of agents for open, dynamic and heterogeneous multi-agent systems is given by [14].A cryptography based approach for security in multi-agent systems is proposed by [15].

Critical analysis of literature reveals that there is a scope of applying agent based techniques for handling the privacy at server side. Also, no study seems to apply software agents for authentication of third party before accessing any user information. The unique contributions of this study are:

- Using separate software agent for each user for controlling privacy as well as security at client-side
- Mechanism for establishing the trust and reputation of various user software agents to avoid any malicious software to act as bogus user agent
- Providing a secure mechanism for transferring the user profile information to third party

Next section describes the detailed framework named, ABSEP3S, along with the description and functionality of each agent.

3 ABSEP3S- An Agent Based Security Engine for Privacy Preserving in Personalized Search

The core idea of privacy preserving using this approach is to allow the user to secureinformation under his profile by encrypting it through intelligent agents. User is provided with the complete authority whether he wants to encrypt his queries or not based on the sensitivity of the data. User queries are generally of two types – normal and sensitive. Sensitive queries are protected both at the client and server side by encrypting them using Elliptical Curve Cryptography (ECC) technique. ECC technique ([16], [17]) is a public key cryptosystem that besides using much smaller key sizes is able to provide a competitive security edge as that of other strong encryption algorithms. Most attractive feature of ECC is its relatively short operand length compared to that of RSA and also it is based on discrete logarithm in finite fields. ECC can provide various security services in the form of key exchange, communication privacy through encryption, authentication of sender and digital signatures to ensure message integrity([18],[19]). The state diagram for the proposed framework is given below:

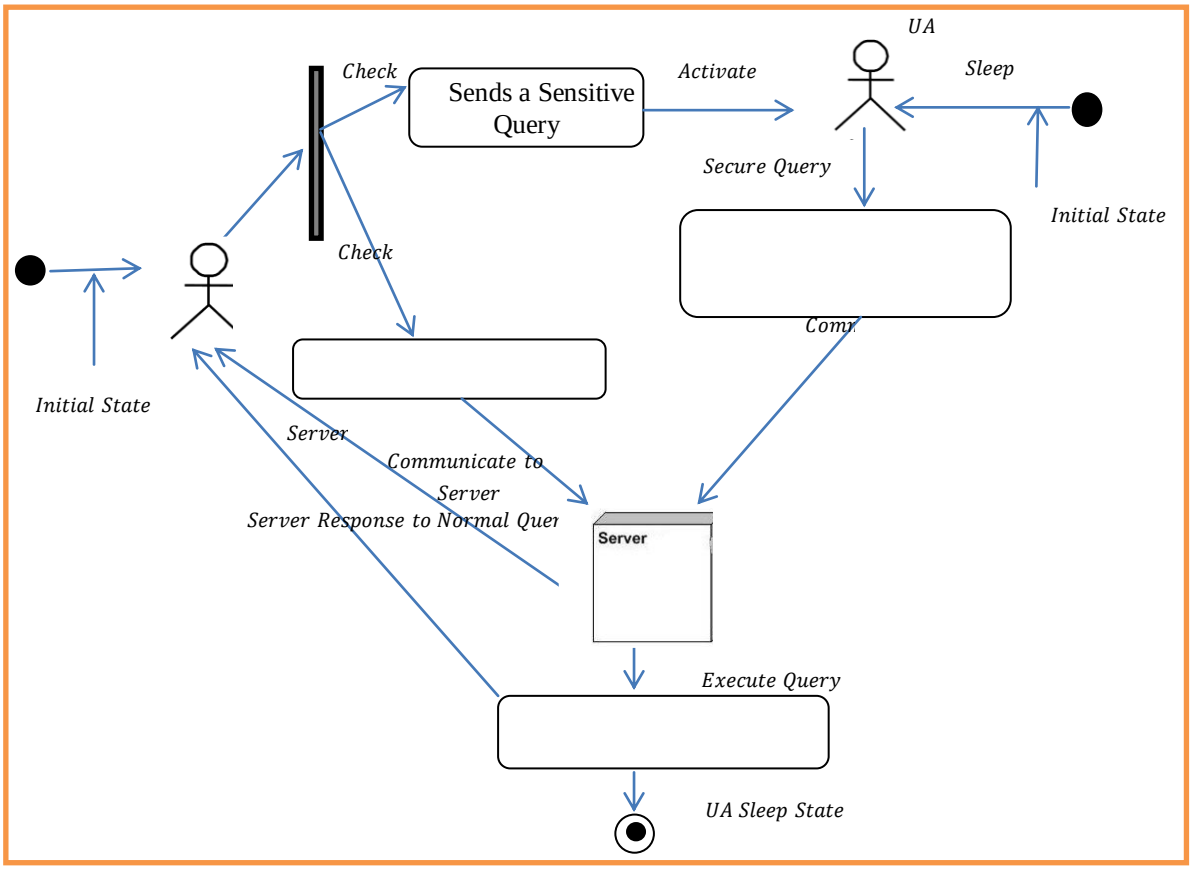

Figure 1: State Diagram for Agent Based Privacy Preservation in Personalize Environment

In the proposed technique every user account has a dedicated user agent (UA) associated with it. UA is responsible for getting set of asymmetric keys for the user. For this purpose every UA gets registered to a Central Certificate Authority (CCA). CCA authenticates the agent and then issues a trust certificate (TC) containing agent-id, set of its elliptical curve public key,private key and validity period of the keys. CCA makes

use of ECC key generation algorithm for generating public and private keys of the agents. The set of public and private keys are given to UA which further passes it to the user. User issues a command to UA for destroying its private key, purpose of removing private key from UA is to secure the encryption keys from any malicious attack on the agent. Now only the user has the set of private, public keys issued by CCA and UA only has the public key of the user, which if gets leaked cannot cause much harm to user or its data stored on the server. Thus, each user hasits private key and the associated public key is kept with UA for future use. Figure 2 given below illustrates the agent registration process with CCA.

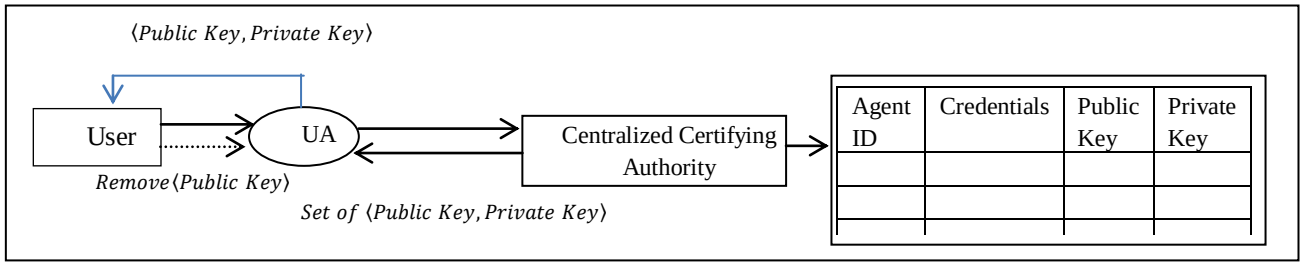

Figure 2: User Agent Registration Process for Privacy Preservation

The flow diagram in Fig. 3 shows the flow diagram of proposed algorithm.

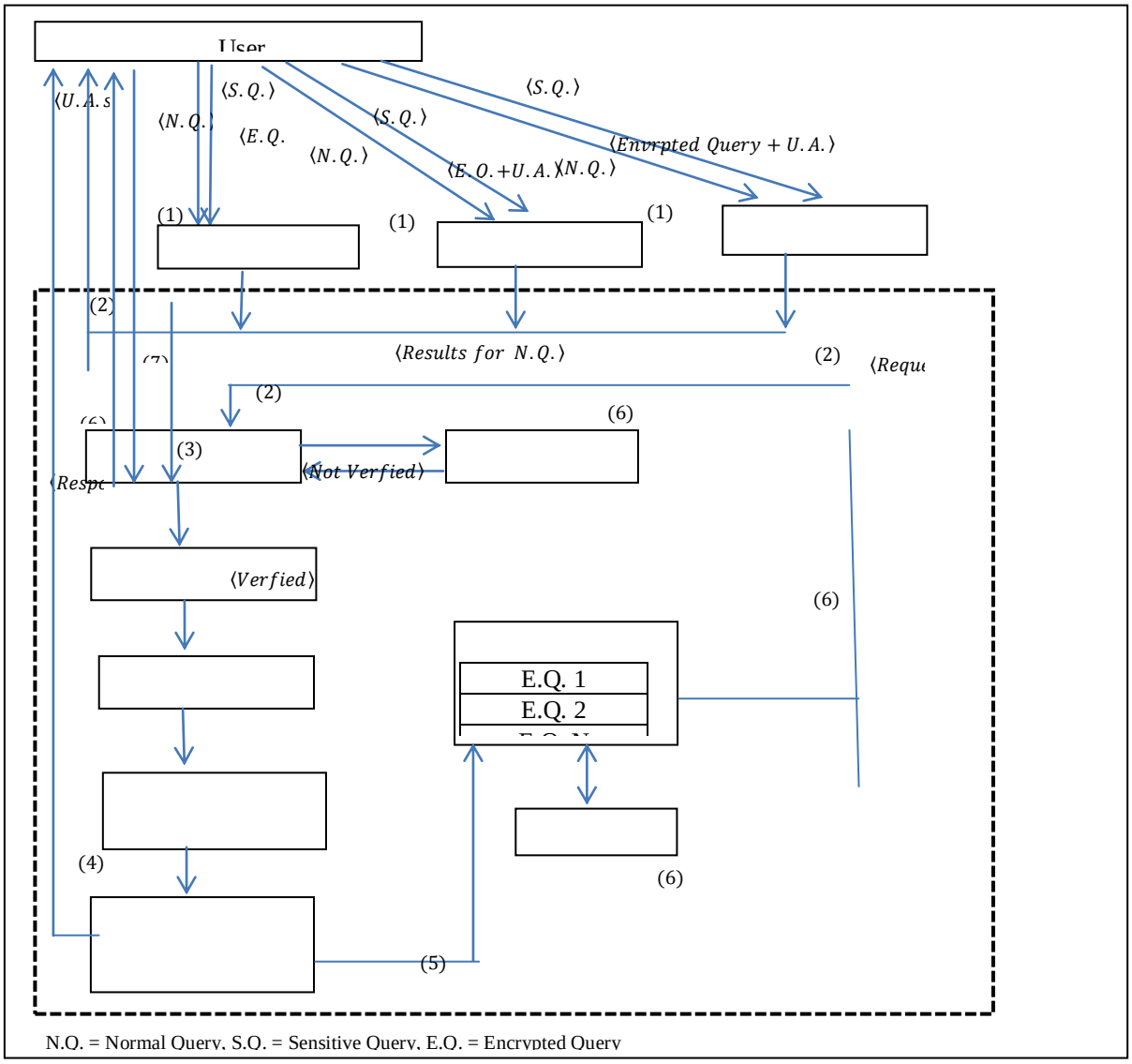

Figure 3: Flow diagram of the proposed framework

1. User sends a search request to the server and specifies whether it is sensitive or not.
2. If the query is not sensitive and the user is willing to share the information with server, then server will execute the search request and send back the normal results to the user.
3. If the query is sensitive then the user will encrypt the message with its private key and UA will migrate from user to server sidealong with encrypted message. The following sub-tasks are performed:
    a. Server will verify the UA. On verification the agent is allowed to access the specified server resources
    b. UA will decrypt the query using public key and server executes this query
4. Results are sent back to user.
5. UA will encrypt the message again and stores them to server usage logs.
6. In case a third party wishes to access the encrypted server usage logs, it sends a request for accessing it to respective UA.
7. This request is sent to UA which sends a message to the user seeking its permission for third party. If the user grants the permission then third party can access the sensitive information else not.

The algorithm for UA is given below:

```
User Agent ()
Input: Query From User (QFU), Query Type (QT)
{
Input (QFU, QT)
IF  (QT==Sensitive)
        Activate.UserAgent()
        UserAgent.SecureQuery(QFU);
        UserAgent.MigrateServer(QFU);
        Server.Authenticate(UserAgent);
        If (Authenticated)
                Decrypt (QFU);
                Search(QFU);
                SendResults(User);
                Encrypt(QFU);
                StoreQFUTo_ServerUsageLogs();
                Sleep();
        End if;
        If (ThirdParty.Request)
                Activate();
                RequestUserForPermission();
                If (allowed)
                        getUserData()
                else
                        AccessDenied()
                End if;
        End if;
Else
        Execute as normal query ();
}
```

Figure 4: Algorithm for User Agent

So, the proposed mechanism aims to control the unauthorized distribution of user data to third party by server without the user consent. The complete process is automated and more efficiency is achieved by using agents.

4 Conclusion and Future Direction of Work

The proposed framework provides a detailed mechanism for handling problem of privacy preserving in personalized search through intelligent software agents.The framework uses a cryptographic approach for storing private user information at server side. To the best of our knowledge no work has provided the facility for storing the user's private information at server side while controlling the unauthorized access by third party.Implementation and testing of the framework in the real world may be taken up in future studies. Further, a comparison and evaluation of various new encryption algorithms may be done to improve the efficiency of the system.

References

[1] A.J.P.Jeckmans,M.R.T.Beye, Z.Erkin, P.H.Hartel, R.L.Lagendijk, Q. Tang, "Privacy in Recommender Systems," in Proc. of Social Media Retrieval, Computer Communications and Networks, Springer Verlag, London, 2013, p. 263-281.

[2] S.Berkovsky, Y.Eytani, T.Kuflik, and F., Ricci, "Privacy-Enhanced Collaborative Filtering," inProc. of PEP05, UM05 Workshop on Privacy-Enhanced Personalization, Edinburgh, Scotland, 2005, p. 75-83.

[3] R. K. Chellappaand R. G.Sin, "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," Information Technology and Management, vol. 6, 2005, p. 181–202.

[4] E.Toch, Y.Wang and F.CranorL,"Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems," User Modeling and User-Adapted Interaction, vol. 22(1), 2012, p. 203-220.

[5] A. Kobsa,B. P. Knijnenburg and B.Livshits ,""Let's Do It at My Place Instead?: Attitudinal and Behavioral Study of Privacy in Client-side Personalization". In Proc. of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14). ACM New York USA, 2014, p. 81–90.

[6] L. Sweeny, "k-anonymity: A model for protecting privacy", International Journal of Uncertainty, Fuzziness and knowledge Based Systems, vol. 10(5), 2002, p. 557 – 570.

[7] X. Shen, B. Tan and C.Zhai, "Privacy Protection in Personalized Search," in Proc. of ACM SIGIR Forum, vol.41(1), 2007, p. 4-17.

[8] Y. Xu, B. Zhang, Z. Chen and K. Wang, "Privacy-Enhancing Personalized Web Search," inProc. of WWW 2007, Banff, Canada, 2007, p. 591-600.

[9] L.Shou, H. Bai, K. Chen and G. Chen "Supporting Privacy Protection in Personalized Web Search", IEEE Transactions on Knowledge and Data Engineering, vol. 26(2), 2014, p. 453-467.

[10] J. Parra-Arnau, D.Rebollo-Monedero and J.Forné, "Measuring the privacy of user profiles in personalized information systems," Future Generation Computer Systems, vol. 33, 2014, p. 53–63.

[11] G. V.Jaison and C. M. Varghese, "Privacy Protection in Personalized Web Search using Homomorphic Encryption," International Journal of Scientific and Research Publications, vol. 5(9), 2015, p. 1-5.

[12] R.Ciss´ee and S.Albayrak,"An agent-based approach for privacy-preserving recommender systems,"in Proc. of the 6th international joint conference on Autonomous agents and multi-agent systems, Article No. 182, ACM , New York, NY, USA, 2007.

[13] PeyraviF. andLatifA.,"Secure Multi Agent Information Filtering," International Journal of Computer Theory and Engineering, vol. 6(3), 2014, p. 240-246.

[14] A.Singh, D.Juneja, A. K.Sharma, "Introducing Trust Establishment Protocol in Contract Net Protocol,"in Proceedings of International Conference on Advances in Computer Engineering, 2010, p. 59-63.

[15] A. Singh, D.Juneja and A.K.Sharma, "Elliptical Curve Cryptography Based Security Engine for Multi-agent Systems Operating in Semantic Cyberspace," International Journal of Research and Reviews in Computer Science (IJRRCS), vol. 2(2), 2011, p. 283-290.

[16] V.SMiller, "Use of Elliptic Curves in Cryptography," in Proc. of Advances in Cryptology-CRYPTO'85, LNCS, vol. 218, Springer-Verlag, 1986, p. 417-426.

[17] N.Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, vol. 48, 1987, p. 203-209.

[18] G.V.S.Raju an R.Akbani," Elliptic Curve Cryptosystem and its Applications" in Proc. of IEEE International Conference on Systems, Man & Cybernetics. vol. 2, 2003, p. 1540-1543.

[19] R. Shanmugalakshmi and M.Prabu, "Research Issues on Elliptic Curve Cryptography and its applications,"International Journal of Computer Science and Network Security, vol. 9(6) , 2009, p. 19-22.