ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

Hippocratic Database- Persisting privacy in e- banking

Minakshi Memoria, Neha Malik

ABSTRACT

Preserving the private information in the era of web is one of the most challenging issue. Web services (e-health, e-commerce, e-banking) collect data from users and use them for other purposes. Sometimes data is shared with other purposes. Recent advances in Hippocratic databases promise the privacy in e-banking.

This paper tackles the issues in applying Hippocratic database design to e-banking. The solution is proposed at middleware level. Hippocratic database is integrated to APPEL preferences to support the privacy.

Finally implement issues are discussed.

Categories and Subject Descriptors

H.2.0 [**Database Management**]: General – Security, Integrity and Protection.

General Terms

Management, Security, Legal Aspects, Verification.

Keywords

Logging, Privacy, Enforcement, Hippocracy, APPEL

I. INTRODUCTION

E-Banking systems are playing a critical role in today's banking organizations. How to safeguard customers' private information is an important and challenging issue faced by the designer and administrator of e-banking systems. The privacy issue is critical to such systems because most banking data are about individual customers and highly sensitive. Inappropriate disclosures of those data cause privacy breaches to customers, which in turn lead to serious legal and financial consequences to the organization.

At the same time, the privacy issue is particularly challenging in e-Banking systems due to the usually complex design and implementation of such systems. There exist standards and solutions for addressing the privacy issue in general purpose applications. The platform for privacy preferences (P3P) developed by the World Wide Web Consortium (W3C) allows users and websites to declare privacy preferences and policies in a machine-readable format [1]. On the other hand, the Hippocratic Database is a framework for enforcing privacy policies based on database technologies [2]. The integration of P3P and HDB is a natural solution for preserving privacy in e-Banking systems, which forms the basis of our work.

In this paper, we tackle several issues around the integration of P3P and HDB technologies in e-Banking systems. Here, we design architecture for integrating P3P preferences with HDB policies. Customers' preferences specified in APPEL (P3P's language for privacy preferences) are mapped to privacy metadata tables stored in HDB. Employers requesting for private data are authorized against the privacy metadata. Second, we study the principles. We provide a solution based on a redesigned schema. Third, we extend HDB to support the multi-dimensional model. The original design of HDB based on relational database model is not suitable for multidimensional models used in banking data warehouses.

The rest of this paper is organized as follows. First, Section 2 reviews related work. Section 3 describes ten principles foe HDB. Section 4 describes architecture for preserving privacy based on integration of P3P and HDB. Section 5 concludes the paper.

II. RELATED WORK

E-Banking privacy is preserved on the similar basis as in e-health systems. Protecting patients' privacy is a mandatory requirement in most e-Health systems according to privacy

***Minakshi Memoria**, CSE Department., Dronachary College of Engg. Gurgaon, India, 09953679907*
***Neha Malik**, CSE Departmente, Dronacharya college of Engg., Gurgaon, India, 09911147170.*

legislation and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) [3]. Threats to patients' privacy may arise from many aspects of a medical organization. For example, published medical data can lead to attacks on patients' privacy even though the data are sanitized. The concept of *k*-anonymity requires identifying attributes to be generalized such that any real world individual can be linked to at least *k* records in the published data, which is considered a tolerable privacy threat [4]. Privacy threats within a medical organization may come from unauthorized accesses to sensitive data. A basic requirement found in most privacy regulations is that accesses to patient records should only be granted to users with appropriate privileges for intended purposes during given time period [5]. Such a requirement for fine-grained access control (FGAC) can be handled by the application layer or by database systems through view-based security. For example, Oracle's implementation of FGAC, known as Virtual Private Database (VPD), allows policies to be attached to tables and triggered by accesses [6]. Other popular commercial products like Sybase, Microsoft SQL Server, and IBM DB2, all have different degree of support for FGAC. The Platform for Privacy Preferences (P3P) is a standard for encoding a user's privacy preferences and an organization's privacy policies in a machine-readable format, such that a user's browser can interact with the organization's website to determine whether the former's privacy preferences matches the latter's privacy policies [1]. P3P provides a standard language for specifying privacy preferences about disclosing private data, namely, A P3P Preference Exchange Language (APPEL) [7]. Hippocratic Databases (HDB) is designed for preserving privacy in database applications [2].

III. TEN PRINCIPLES

1. Purpose Specification: For personal formation stored in the database, the purpose for which the information has been collected shall be associated with that information.

2. Consent: The purpose associated with personal information shall have consent of the donor of the personal information.

3. Limited Collection: The personal information collected shall be limited to the minimum necessary for accomplishing the specific purposes.

4. Limited Use: The database shall run only those queries that are consistent with the purposes for which the information has been collected.

5. Limited Disclosure: The personal information stored in the database shall not be communicated outside the database for purposes other than those for which there is consent from the donor of the communication.

6. Limited Retention: Personal information shall be retained only as long as necessary for the fulfillment of the purposes for which it has been collected.

7. Accuracy: Personal information stored in the database shall be accurate and up to date.

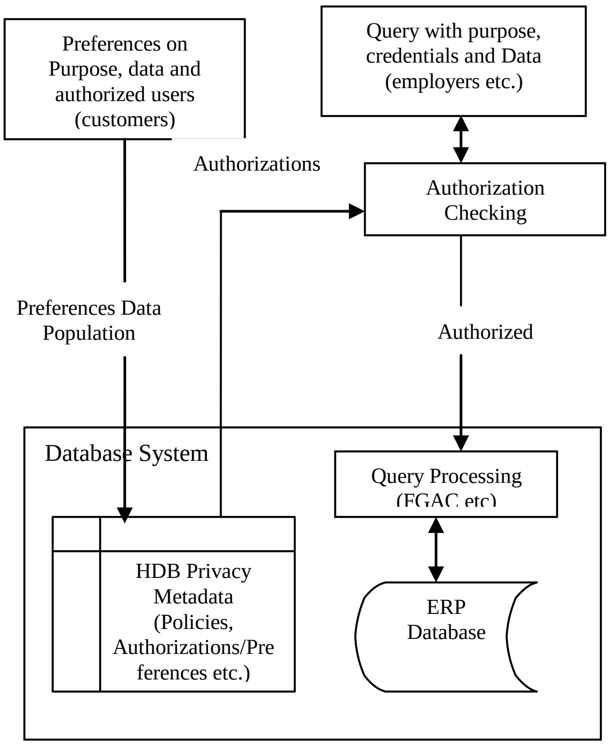
8. Safety: Personal information shall be protected by the security safe guards against theft and other misappropriations.

9. Openness: A donor shall be able to access all information about the donor stored in the database.

10. Compliance: A donor shall be able to verify compliance with the above principals. Similarly, the database shall be able to address a challenge concerning compliance.

IV. ARCHITECTURE

The architecture of the privacy-protection subsystem of an e-Banking system is illustrated in Figure 1. We consider two types of users accessing the e-Banking system. First, customers state their opt-in and opt-out preferences through a web interface. Second, employers need to access the personal information of their customers for treatment purposes. Notice here the employer and customer only refer to their roles in either providing or requesting the private data. Other users of the e-Banking system, such as a worker, may be considered as a customer, a employer, or both depending on their roles with respect to the private data.


Preferences on Purpose, data and authorized users (customers)
Query with purpose, credentials and Data (employers etc.)
Authorizations
Authorization Checking
Preferences Data Population
Authorized
Database System
Query Processing (FGAC etc)
HDB Privacy Metadata (Policies, Authorizations/Preferences etc.)
ERP Database

t**Figure 1. Architecture for preserving privacy**

Customers specify their preferences about disclosing private data in the APPEL language through a web interface. The preferences are checked against the mandatory part of P3P policies for conformance between the client's browser and the web server (this can be implemented in either a client centric or server-centric way [8]). If the preferences match the policies, the preferences are mapped to and stored in the attributes and records of privacy metadata tables in backend HDB for later references. When employers request for accesses to private data, the application will provide authentication credentials and associated purposes together with queries. Based on the purposes and the requested resources, such as records and attributes, the system checks corresponding metadata and determines whether the employer is a legitimate recipient of the requested private data.

V. CONCLUSION

This paper addressed the issue of preserving customers' privacy in e-Banking systems. We proposed to allow customers to specify their privacy preferences in APPEL, which will be recorded as authorization policies in the backend HDB. Employers are then authorized against such policies when their applications request for privacy data. We identified the lack of fine-grained authorizations as a limitation of the original HDB design and provided a solution based on a modified schema. We extended the HDB design to support the multi-dimensional model so it can be used to preserving privacy in analytical data applications. We also showed how hierarchies can be leveraged to simplify the representation of authorizations. Experimental results justified our design. It is our belief that the proposed solution can be integrated into existing e-Banking system to provide customers with better privacy protection.

VI. REFERENCES

[1] World Wide Web Consortium (W3C) "P3P implementation from W3C" http://www.w3.org /P3P/implementations.

[2] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, "Hippocratic Databases," Proc. of the 28th Int'l Conference on Very Large Databases (VLDB), 2002.

[3] *"Health Insurance Portability and Accountability Act,"* United States Public Law 104-191, 1996.

[4] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when disclosing information," Proc. of the 7th ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, 1998.

[5] "Health Insurance Portability and Accountability Act," United States Public Law 104-191, 1996.

[6] T. Kyte, "*Fine-grained access control*," Technical report, Oracle Corporation, 1999.

[7] L. Cranor, M. Langheinrich and M. Marchiori, "A P3P Preference Exchange Language 1.0 (APPEL 1.0)," *W3C Working Draft*, April 2002.

[8] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, "Server-Centric P3P," *Proc. of the W3C Workshop on the Future of P3P*, November 2002.