Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 3; January-March, 2015 pp. 258-260
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Proposed Methodology for Database Privacy in an Existing System Using Hippocratic Database

Sonali Ganguly[1] and S.P. Singh[2]

[1]Student BIT, Mesra (Noida Center)
[2]BIT, Mesra (Noida Center)
E-mail: [1]sonaliganguly7@gmail.com, [2]spsinghbit@yahoo.co.in

Abstract—*The concept of Hippocratic Databases was first conceptualized in 2002. Since then, several papers have been published where the concept of 'Hippocratic Databases' have been implemented in various domain like e-Learning, web services, virtual community and other platforms where preservation of privacy on a social network is critical. Generally some selected principles of Hippocratic Databases have been modeled based on the type of environment and platform. This paper is an extension of the paper mentioned in references [1]. After study of database level privacy in social network, an attempt is made to implement the principles of Hippocratic databases. This paper presents the method to implement selected principles of Hippocratic databases i.e. purpose, retention and consent on an existing system that captures employee movements through RFID detections rather than building a new system to implement the principles in the database. To implement the above mentioned principles, some changes at schema level were introduced. The paper also highlights the key features of "purpose" principle of Hippocratic Database in the existing system in an elaborative manner.*

1. INTRODUCTION

The concept of Hippocratic Databases evolved from the Hippocratic Oath of medical or law profession. A segment of the oath is given below.

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things to be unutterable." [16]

Based on the Hippocratic Oath, Hippocratic Databases focuses on taking the responsibility for the privacy of data that rests in the database. The ten principles of Hippocratic Databases that supports the Hippocratic Oath are:

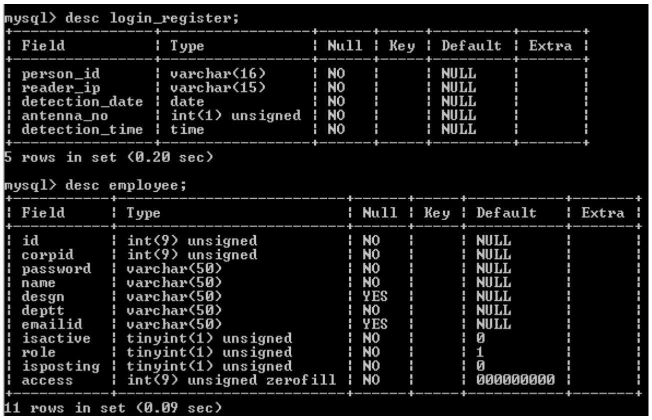
1. Purpose Specification
2. Consent
3. Limited Collection
4. Limited Use
5. Limited Disclosure
6. Limited Retention
7. Accuracy
8. Safety
9. Openness
10. Compliance

The objective is to apply selected principles like purpose, retention and consent of Hippocratic databases to an existing system to improve the understanding of the schema and structure of the database as well as maintain privacy of data.

The paper is divided into 5 sections where section 1 gives a general introduction about Hippocratic Databases and its principles and the objective of the paper. Section 2 describes the existing system and its database schema, screenshots of the tables while section 3 describes the changes proposed in the existing system. Section 4 concludes the paper while section 5 provides the references.

2. INTRODUCTION OF EXISTING SYSTEM

The existing system detects employee movements through RFID detections. The system has two relations; employee and login_register where employee relation stores employee



```
mysql> desc login_register;
+----------------+-----------------+------+-----+---------+-------+
| Field          | Type            | Null | Key | Default | Extra |
+----------------+-----------------+------+-----+---------+-------+
| person_id      | varchar(16)     | NO   |     | NULL    |       |
| reader_ip      | varchar(15)     | NO   |     | NULL    |       |
| detection_date | date            | NO   |     | NULL    |       |
| antenna_no     | int(1) unsigned | NO   |     | NULL    |       |
| detection_time | time            | NO   |     | NULL    |       |
+----------------+-----------------+------+-----+---------+-------+
5 rows in set (0.20 sec)

mysql> desc employee;
+-----------+--------------------------+------+-----+-----------+-------+
| Field     | Type                     | Null | Key | Default   | Extra |
+-----------+--------------------------+------+-----+-----------+-------+
| id        | int(9) unsigned          | NO   |     | NULL      |       |
| corpid    | int(9) unsigned          | NO   |     | NULL      |       |
| password  | varchar(50)              | NO   |     | NULL      |       |
| name      | varchar(50)              | NO   |     | NULL      |       |
| desgn     | varchar(50)              | YES  |     | NULL      |       |
| deptt     | varchar(50)              | NO   |     | NULL      |       |
| emailid   | varchar(50)              | YES  |     | NULL      |       |
| isactive  | tinyint(1) unsigned      | NO   |     | 0         |       |
| role      | tinyint(1) unsigned      | NO   |     | 1         |       |
| isposting | tinyint(1) unsigned      | NO   |     | 0         |       |
| access    | int(9) unsigned zerofill | NO   |     | 000000000 |       |
+-----------+--------------------------+------+-----+-----------+-------+
11 rows in set (0.09 sec)
```

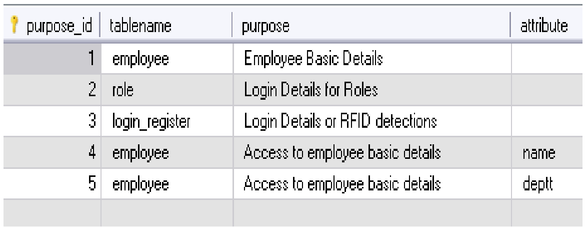
Fig. 1: Description of login_register and employee relation

related information like name, designation, department, etc. while login_register captures the date and time of employee movement from particular locations i.e. where RFID devices are installed. Fig. 1 provides the schematic description of both the relations.

3. CHANGES PROPOSED IN DATABASE

Selected principles of Hippocratic database have been implemented in the proposed methodology.

1. The most critical principle of Hippocratic databases is ‘purpose’. To ensure that the purpose is captured in database level, a purpose relation has been created.



purpose_id	tablename	purpose	attribute
1	employee	Employee Basic Details	
2	role	Login Details for Roles	
3	login_register	Login Details or RFID detections	
4	employee	Access to employee basic details	name
5	employee	Access to employee basic details	deptt

Fig. 2: Tuples in relation purpose

Key features of purpose relation are:

i. Stores the purpose or reason of creating each table in the database. This ensures that the core cause of creating and maintaining a relation is captured during design level. This feature would also aid a new member to understand the reason for the existence of a particular relation in the database since databases generally contain several relations/tables. The corresponding tuples shall be used as informative reference.

ii. This relation will capture the various reasons for accessing a particular attribute of its corresponding relation. Thus access of an attribute shall communicate the purpose of the access.

iii. Purpose relation shall also highlight the unused attributes of a relation. Some attributes of a relation may be obsolete or some new attributes have been introduced but not utilized can be extracted from purpose relation.

In the above table, the tuples with no value in attribute column defines the core cause of creating the relation while the tuples with existing attribute value are used to capture the reason for accessing the particular attribute of a relation. This way purpose definition can be distinguished for a table/relation creation and access of an attribute of a relaation.

The main concept to be implemented is demonstrated in the Fig. below:

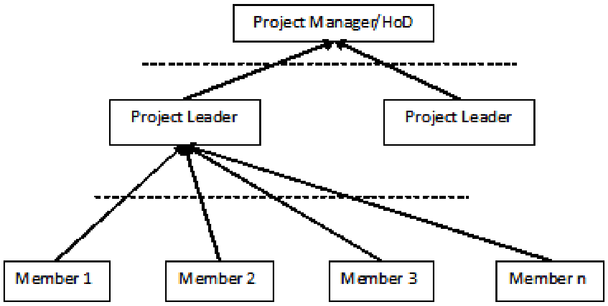
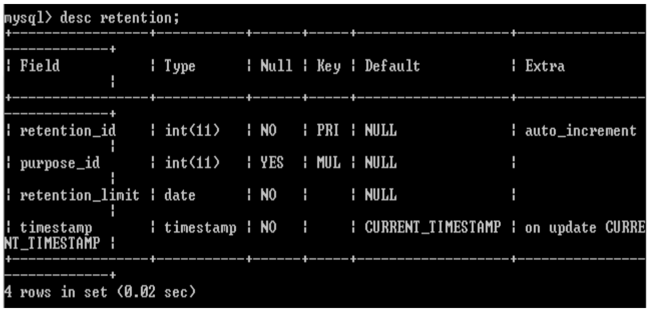


Fig. 3: The level of hierarchy to contemplate the RFID detection

The level of hierarchy is designed in such a manner so that the detections of members can be observed by project leaders while the detections of project leaders can be observed by project manager/HoD.

2. The retention principle is implemented through a retention relation that defines the limit or period for contemplating the RFID detections.



```
mysql> desc retention;
+----------------+-----------+------+-----+-------------------+---------------
-------------+
| Field          | Type      | Null | Key | Default           | Extra
             |
+----------------+-----------+------+-----+-------------------+---------------
-------------+
| retention_id   | int(11)   | NO   | PRI | NULL              | auto_increment
             |
| purpose_id     | int(11)   | YES  | MUL | NULL              |
             |
| retention_limit | date     | NO   |     | NULL              |
             |
| timestamp      | timestamp | NO   |     | CURRENT_TIMESTAMP | on update CURRE
NT_TIMESTAMP |
+----------------+-----------+------+-----+-------------------+---------------
-------------+
4 rows in set (0.02 sec)
```

Fig. 4: Description of retention relation

Retention relation ensures the limit of retention of a particular attribute of a table and its use based on the purpose relation using purpose_id. In this way, the limit of retention for an attribute can be controlled via this table.

3. Consent principle is implemented through ‘access’ attribute in employee relation. Subsequently, no new relation has been defined. ‘access’ attribute contains the employee id of the superior or the person to whom consent to access detections is permitted.

In this way, only the immediate superior shall have access to detections of movements of employees assigned under him. In case higher level management needs to access the detections of a particular employee then the access permissions shall be provided through consent table.

4. CONCLUSION

After Hippocratic Database emerged in 2002 to protect the privacy of data that rests in database, the principles of Hippocratic Database have been implemented in various different platforms and data sets. Since data is a very critical asset for any organization, these principles can lock the personal information of users at database level. The proposed methodology implements limited principles of Hippocratic databases to an existing system that detects employee movements through RFID to ensure restricted access and privacy of information. To implement the proposed methodology, changes were executed at schema level to ensure restricted access.

In future, statistical analysis shall be done to determine the effect of these changes on the database and the level of privacy and access restriction achieved.

REFERENCES

[1] Sonali Ganguly, S. P. Singh, "A Literature Review on Database Privacy in Social Networks using Hippocratic Database", 5th International Conference on ACSEICT 2014

[2] Oberholzer Hendrik JG, Ojo Sunday O and Olugbara Oludayo O, "A PET evaluation framework for relational databases" SocialCom, IEEE 2013

[3] Rajneesh Kaur Bedi, V.M. Wadhai and Nitinkumar Rajendra Gove, "Hippocratic Social Network", Fifth International Conference on Computational Aspects of Social Networks, 2013

[4] Mohammad Reza Khayyambashi, Fatemeh Salehi Rizi, "An approach for detecting profile cloning in online social networks", 7th International Conference, Kish Island, Iran, IEEE, 2013

[5] Rajneesh Kaur Bedi, V.M. Wadhai and Nitinkumar Rajendra Gove, "Application of Hippocratic Principles for Privacy Preservation in Social Networks", World Congress on Information and Communication Technologies, IEEE, 2012

[6] Jasmin Azemović, "Privacy Aware eLearning Environments Based on Hippocratic Database Principles", BCI, Nova Sad, Serbia, 2012

[7] Maryam Majedi, Kambiz Ghazinour, Amir H. Chinaei and Ken Barker, "SQL Privacy Model for Social Networks", Advances in Social Network Analysis and Mining, IEEE 2009

[8] Norjihan Abdul Ghani and Zailani Mohamed Sidek, "Owner-Controlled Towards Personal Information Stored in Hippocratic Database", International Conference on Computer Technology and Development, 2009

[9] Vanja Bevanda, Jasmin Azemović and Denis Mušić, "Privacy preserving in eLearning environment (Case of modeling Hippocratic database structure)", Fourth Balkan Conference in Informatics, 2009

[10] Norjihan Abdul Ghani, Zailani Mohamed Sidek, "Privacy-Preserving in Web Services using Hippocratic Database" IEEE, 2008

[11] [http://www.theguardian.com/news/datablog/2014/feb/04/facebook-in-numbers-statistics

[12] Andrew Rutherford, Reinhardt Botha and Martin Olivier, "Towards a Hippocratic Log File Architecture", Proceedings of SAICSIT, 2004

[13] G Skinner, E Chang, M McMahon, J Aisbett and M Miller, "Shield Privacy Hippocratic Security Method for Virtual Community", The 30th Annual Conference of the IEEE Industrial Electronics Society, Busan,Korea, 2004

[14] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant and Yirong Xu, "Hippocratic Databases", Proceedings of 28th VLDB conference, Hong Kong, China, 2002

[15] Dianne M. Timm, Carolyn J. Duven, "Privacy and Social Networking Sites", Published online in Wiley InterScience, 2008

[16] Rakesh Agrawal, Paul Bird, Tyrone Grandison, Jerry Kiernan, Scott Logan, Walid Rjaibi, "Extending Relational Database Systems to Automatically Enforce Privacy Policies", Proceedings of the 21st International Conference on Data Engineering (ICDE 2005) IEEE

Ms. Sonali Ganguly is working as a Project Engineer (IT) – I in CDAC, Noida. She received her MCA degree from Guru Gobind Singh Indraprastha University and presently pursuing MTech (CS) part time from Birla Institute of Technology, Mesra (Noida campus). She has three years of work experience in Java, Databases and Quality Assurance. She has published 3 research papers in national/international conferences and journal.

Dr. S. P. Singh is working as an Associate Professor in Birla Institute of Technology, Mesra (Noida Centre). He has received his MSc, MTech and Doctorate degree and has a total 13 years of experience. His subject specialization includes DBMS, Parallel & Distributed Computing, Management Information System and System Analysis and Design. He has contributed in more than 15 papers published in various national/ international conferences and journals.