Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 94 (2016) 453 – 458

Procedia Computer Science

The 2nd International Workshop on Future Information Security, Privacy and Forensics for Complex systems (FISP-2016)

Enhancing Relational Database Security by Metadata Segregation

Devanshu Trivedi, Pavol Zavarsky, Sergey Butakov

Department of Information Systems Security and Assurance Management
Concordia University of Edmonton
Edmonton T5B 4E4, Alberta, Canada
dtrivedi@student.concordia.ab.ca, {pavol.zavarsky, sergey.butakov}@concordia.ab.ca

Abstract

Although many prominent Relational Database Management Systems provides inbuilt security controls and mechanisms, the information resided in the data-store are at great risk. This research aims to reduce the risk of unauthorized data access by providing an extra layer of security. This research proposes a novel method for incorporating information security while designing the relational database by segregating the information on the basis of its sensitivity level and creating referential integrity constraints dynamically at run time. Different techniques to identify and quantify sensitive attributes and restructuring database architecture have been discussed for the proposed approach. The primary keys of the restructured tables and most critical information attributes were secured using Transparent Data Encryption utility provided by Oracle 11g to prohibit illegitimate use of information. The performance of the proposed architecture was evaluated with 1,000,000 records which shows that by increasing the number of records, the response time of Select statement increased dramatically whereas it increased gradually for Insert, Update and Delete operations.

Peer-review under responsibility of the Conference Program Chairs

Keywords: constraint; integrity; Oracle 11g; primary key; procedure; synonym; view; foreign key

1. Introduction

There are mainly three phases where information must be secured. Firstly, in any application where data is being processed. Furthermore, while information travels on network channels. Finally, in data stores where the information reside for future usage. Various database management systems provide different controls for securing the data, once it is stored in database.

* Corresponding author. Tel.: +1-780-604-8258; fax: +1-780-378-8460.
E-mail address: dtrivedi@student.concordia.ab.ca

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.08.070

Oracle 11g provides user access management controls, database redaction policies, data encryption and integrity, wallet manager, auditing [9,10].Whereas Microsoft SQL server relational database is limited in security features with authentication, roles and access management, ownership and user schema management, authorization and permission on objects, encryption[13]. There are many manuals and white papers available from the vendors and third parties on how to secure the data by implementing these controls. But not so many papers provide information on how to integrate security features into relational database at the time of database schema design.

Many ground level concepts of Relational Databases provide low level security to the schema design such as views, synonyms, managing user profiles and access levels. One approach to secure information from unauthorized access is to create views on tables, where user interact with views and if the operation is found legitimate, the changes can be saved in original tables. These views can be created by selecting certain columns and/or rows from a table including permissions which creates restricted access to the information. Also, the Database Administrator can hide schema name or fully qualified object name from database consumers using synonyms.

Another approach is to segregate database columns with respect to their information sensitivity level and creating referential integrity constraints at run time which can make these columns isolated from each other. This mechanism would have one or more attributes/columns in the same table. The isolated tables can be created on different tablespace and placed on different geographical networks/servers. If an attacker gets an access to one table, only partial information will be available which is not sufficient for a successful attack. Such mechanism can decrease the potential risk of unauthorized data access and data-theft.

The information in database can be protected by securing its respective metadata. In a relational database, metadata can be schema name (table, procedure, function, trigger), column name or constraint name, type and definition. The logical alignment of these schemas can also be a metadata. If information from one table is compromised, the other tables which are logically related to that table are more susceptible as an attacker can jump from one table to another using referential integrity constraints. Other tables can be saved from an attacker by protecting such logical relations.

To simulate the above approach, healthcare is an appropriate industry where personal information of people must be protected. The research work was carried by implementation of a system for healthcare in Oracle 11g, where patient's personal data like social insurance number and health insurance number were secured. The system was developed by following object oriented analysis and design principles.

2. Related Works

Although very few papers recommend how to align information security at the time of database schema design, numerous research projects have been done on segregation of datasets. The separation of the data can be achieved in number of ways. One approach is to divide tables into several number of rows or columns. The second approach is to divide data sets based on their usability[4]. Another approach for segregation of data can be based on data ownership[12].

In[1], the concept of dividing the data on the basis of its sensitivity level and creation of logical relationship at run time to secure sensitive information was discussed which has some issues like concurrency, availability, audit and log management. Researchers in[2] have developed a framework to trade and exchange sensitive information on a shared network by calculating risk value for considered information. Risk based calculation for sensitive information was developed to exchange critical information between allies in a war scenario. Authors in[3], developed a method for data leakage prevention for cloud databases where they try to segregate the data over the cloud on the basis of the relationship between attributes. They developed a code scheme algorithm to store each sensitive data into scattered tables with respective code and shared the same code on client site.

In[5], author introduced a method for data recovery, at any point of time for comprehensive versioning systems using indexing called as Hierarchical Spatial-Temporal Indexing Method implemented by dividing the time domain in different partitions and in respect to the frequency of update operation on disk IOs. Whereas, in[8], author introduced a concept called point in time architecture which can be used to recover the data from the database at any given time. Usually, the previous state of data cannot be retrieved, once the operation is performed and new state of the data is committed. According to the concept, one can retrieve the state of the data at any point of time, before or after any operation. This database also can be used for auditing as data is saved at every time stamp.