Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Encryption-based multilevel model for DBMS

*Ahmed I. Sallam, El-Sayed El-Rabaie, Osama S. Faragallah**

Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menouf 32952, Egypt

ARTICLE INFO

Article history:
Received 7 September 2011
Received in revised form
31 December 2011
Accepted 13 February 2012

Keywords:
Database security
Relational database
Multilevel security
SeaView model
Jajodia–Sandhu model
Smith–Winslett model
MLR model
Belief-consistent model
Multilevel database performance

ABSTRACT

In this paper, we propose an encryption-based multilevel model for database management systems. The proposed model is a combination of the Multilevel Relational (MLR) model and an encryption system. This encryption system encrypts each data in the tuple with different field-key according to a security class of the data element. Each field is decrypted individually by the field-key of which security class is higher than or equal to that of the encrypted field-key. The proposed model is characterized by three achievements: (1) utilizing an encryption system as an additional security layer over the multilevel security layer for the database, (2) reducing the multilevel database size, and (3) improving the response time of the data retrieval from the multilevel database. Also this paper summarizes our efforts in implementing a working multilevel secure database prototype. This prototype is used as a research tool for studying principles and mechanisms of the encryption-based multilevel model and multilevel secure database (MLS/DBMS) models (SeaView, Jajodia–Sandhu, Smith–Winslett, MLR, and Belief-Consistent Model). This prototype is implemented to be used to perform a series of experiments to measure the performance cost for applying encryption in multilevel database security.

1. Introduction

In multilevel database systems, data items and subjects have been assigned to classification levels, such as TS (Top Secret), S (Secret), C (classified), U (Unclassified). The classification levels are ordered as TS > S > C > U.

Access by subjects is restricted by mandatory access controls expressed as "no read up, no write down to follow the well-known Bell and LaPadula model. Subject can read the object that has the same classification level or lower and can write on the objects at the same level only" (Bertino and Sandhu, 2005; Imran and Hyder, 2009).

Many models for extending the standard relational model to deal with multilevel relations have been proposed. The SeaView (Pranjic et al., 2002) model was the first formal MLS secure relational database designed to provide mandatory security protection. The SeaView model extended the concept of a database relation to include the security labels. A relation that is extended with security classifications is called a multilevel relation. The Jajodia–Sandhu (Cuppens and Gabillon, 1999) model was derived from the SeaView model. It was shown by Jajodia and Sandhu that the SeaView model can result in the proliferation of tuples on updates and the Jajodia–Sandhu model addresses this shortcoming. The Smith–Winslett (Rjaibi and Bird, 2004) model was the first model to extensively address the semantics of an MLS database. The MLR (Lee et al., 2004; Sandhu and Chen, 1998) model is substantially based on the Jajodia–Sandhu model, and also integrates the belief-based semantics of the Smith–Winslett model. It was shown that all of the aforementioned models can present users with some information that is difficult to interpret. Consequently, the Belief-Consistent MLS (BCMLS) (Pranjic et al., 2003; Jukic et al., 1999; Jukic and Vrbsky, 1997) model addresses these concerns by including the

* *Corresponding author.*
E-mail address: osam_sal@yahoo.com (O.S. Faragallah).
0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2012.02.008

semantics for an unambiguous interpretation of all data presented to the users.

Several commercial database systems like DB2 (IBM) and ORACLE support encryption in their database management systems. In DB2 (IBM), encryption has been added by implementing SQL built-in functions that allow the application to encrypt and decrypt data. When data is inserted into the database it can be encrypted using an encryption password supplied by the user. When the data is retrieved, the same password must be supplied to decrypt the data. In ORACLE, transparent data encryption enables you to encrypt sensitive data, such as credit card numbers, stored in table columns. Encrypted data is transparently decrypted for a database user who has access to the data. Even if the encrypted data is retrieved, it cannot be understood until authorized decryption occurs, which is automatic for users authorized to access the table. When a table contains encrypted columns, a single key is used regardless of the number of encrypted columns. This key is called the column encryption key. The column encryption keys for all tables, containing encrypted columns, are encrypted with the database server master encryption key and stored in a dictionary table in the database.

Our principal objective in this paper is to propose an encryption-based multilevel database model by adding an encryption algorithm to the MLR multilevel model. The encryption system is used as additional security layer over the multilevel security layer for the database which provides high level of security and to solve problems associated with MLR model. Table 1 shows a comparison between the proposed encryption-based multilevel database model and the commercial database systems like DB2 (IBM) and ORACLE that support encryption in their database management systems.

The work presented in this paper offers several major contributions to the field.

1- Adding encryption system as additional security layer over the multilevel security layer for the database which provides high level of security and robustness against database attacks.
2- Reducing the multilevel database size by removing the attributes classification columns and encrypting the attributes by field-key according to its security level.
3- Simplifying the complexity of the multilevel database design by avoiding the creation of the additional columns for attributes classification.
4- Implementing a prototype to be used to perform a series of experiments to measure the performance cost for applying encryption in multilevel database security.

The rest of this paper is organized as follows. Section 2 illustrates the proposed encryption-based multilevel database model. Section 3 shows the implementation of DML (Data Manipulation Language) operations for the proposed model. Section 4 presents the performance study that was instrumented to compare the multilevel secure database (MLS/DBMS) models. Section 5 gives the analysis of the experimental results of the performance study. Section 6 concludes the paper and outlines the future work.

2. The proposed encryption-based multilevel database model

Many multilevel relational models have been proposed and these different models offer different advantages (Rask et al., 2005; Dave, 2008; Garuba, 2003). The MLR model is the most powerful model among the multilevel relational models. So we refine several of the best ideas from MLR model and add new ones to build our proposed Encryption-Based Multilevel Model.

2.1. *MLR model*

Definition 2.1.1. A multilevel relation scheme is denoted by $R(A_1,C_1,A_2,C_2,\ldots,A_n,C_n,TC)$, where R is the multilevel relation, each A_i is a data attribute, each C_i is a classification attribute for A_i, and TC is the tuple-class attribute (Garuba, 2004).

Definition 2.1.2. A relation instance, denoted by $r(A_1,C_1,A_2,C_2,\ldots A_n,C_n,TC)$, is a set of distinct tuples of the form $(a_1,c_1,a_2,c_2,\ldots,a_n,c_n,tc)$.

Definition 2.1.3. A database is a collection of relations. A database state is a collection of all relation instances of a database at a particular time. Table 2 illustrates an example for data stored in multilevel database security in the MLR model format.

Table 1 – Comparison between the proposed encryption-based multilevel database model and the commercial database systems like DB2 (IBM) and ORACLE.

Criteria	Model		
	Encryption-based multilevel database	DB2 encrypted fields	ORACLE transparent data encryption
Encryption in multilevel security	Supported	Not supported	Not supported
Encryption type	Cell-based encryption (one password per cell)	Column-based encryption (one password per column)	Column-based encryption (one password per column)
Encryption key	Key is managed by database engine	Key provided by the user at runtime	Key provided by the user at runtime