www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16639-16642

A General Framework for Multi-level security to restrict unauthorized users in Sulaymaniyah E-Court Database

[a]Rzgar Sirwan Raza , [b]Zana Azeez Kakarash

[a,b] Department of IT, College of Science and Technology
University of Human Development
Qaradagh, Sulaymaniyah, Kurdistan Region, Iraq
rzgar.sirwan@uhd.edu.iq , zana.azeez@uhd.edu.iq

Abstract - Data is vulnerable at many points in any computer system, and many security techniques and types of functionality can be applied to protect it. Sulimanyah Court is a big and popular Government sector in Iraq. Many clients accessing E-Court Systems, SES (Sulimanyah E-Court Systems) is using SQL SERVER database to store and accesses court cases with different clients. Most of the security models available for databases today protect them from outside, unauthorized users and cannot be provides internal security in relationship with the user type of access to the database.
This database can access by hundreds of clients. We propose a framework to increase security needs of database systems. Clients in this approach can be analysed to instituting sub channels between specific (groups of) users such that authorized subchannels appropriating from accessing objects that contain some sensitive information and restricting unauthorized users. In this paper we propose a general framework for Multi-Level Security (MLS) in Sulaymaniyah E-Court database.

Keywords: **security techniques, Multi-Level Security (MLS), E-Court Database, authorized subchannels, restricting unauthorized users, internal security, types of access, unauthorized users.**

I. INTRODUCTION

The term e-Court is referred to use new information and communication technologies (ICTs) by courts as applied to the full range of court functions, E-court has received more and more importance and it can provide a non-stop court information services to citizens, enterprises, public officers, Court administrations and agencies over a network [1]. The central challenge of e-Government service is how the new technology can be used not only to increase efficiency for public administration, but also to strengthen confidence in privacy measures by creating mutual transparency between public administration and citizens [2].
Sulimanyah E-Court System, is not only the database to store data but also deal on data. This Court consist of nine courts: cassation court, appeal court, first instance court, personal status courts, Criminal court, felony courts, misdemeanors courts, Juvenile court and investigation court. Then each court is subdivided into many courts. Sulimanyah Court has more than 300 employees and all of them have an account and privileges to access the database objects. Database also hires many online visiting citizens to create new case or deal on cases.
In this research, we focus on the challenges, obstacles, and Multi-Level Security (MLS) in e-Court, we have to consider all of the clients in the e-Court database. According to the involved communities, an explicit classification of e-Court databases is proposed. It provides a way to an understanding of the challenges and Multi-Level Security (MLS) in e-Court. Further detailed classification of e-Court applications is provided in a subsequent section. Then the challenges and obstacles in e-Court are considered from some perspectives. The Multi-Level Security (MLS) of e-Court are described next. Finally, the last section provides conclusions and outlines future research directions.

II. INDI RELATED WORK

The Multi-Level Security-DBMS techniques in this approach we will describe in the following sections have strong anterior in mainstream DBMS technology. Specifically, techniques of query modification, constraints, views and access controls. This section discusses each of these techniques in this application, in order to put their use in later sections into perspective.

Query modification was used in the INGRES relational DBMS [3] to implement integrity constraints,views [4] and discretionary access control [5]. The SQUEL query language is used to specify these integrity constraints, views and access control restrictions. When users entered SQUEL data retrieval or update requests, the DBMS would modify each request, based upon the SQUEL constraints, and then apply the modified request to the database.

Integrity constraints are enforced by modifying every update request into a new update request that is ensured not to violate those integrity constraints. Likewise, all retrieval and update requests against views are modified into new requests against the base relations. Discretionary access control constraints are enforced by modifying all requests into new requests which contain no access violations [6].

Our approach uses integrity constraint, access control and query modification to enforce mandatory access controls, specified by means of constraints, on every client's access request. It also goes beyond simply modifying the query, in that all data returned is checked for access violations, using trusted computer base (TCB) type enforcement [7].

III. PROPOSED FRAMEWORK

We proposed a framework that contain number of assumptions about the MLS-DBMS environment and operations, these assumptions and their consequences are discussed to confine the scope of the security related design problem.

In present work, each relation (data) is defined as an object and has a security class level (classification), and each user (client) is defined as a subject and has a security class level (clearance) [8]. Every data item in the database has associated with classifications level that may change dynamically [9], also, the multilevel relational database schema contains an additional attribute, called tuple classification (TC) that identifies the security classification of each tuple. Also control of users' access to data must be based upon these classifications; [10] and the classification based access controls cannot be avoided shows in Table (1, 2).

Besides classifying each unit of data, it will be necessary to classify the data depending the content or value, data in multi-level security has four levels of sensitivity, from lowest to highest, are unclassified (U), confidential (C), secret (S), and top secret (TS) [11]. Data in relational multilevel database security are labeled with their own security classification. Clients who need to access data should have the appropriate security classification level as shows in (Fig.1).

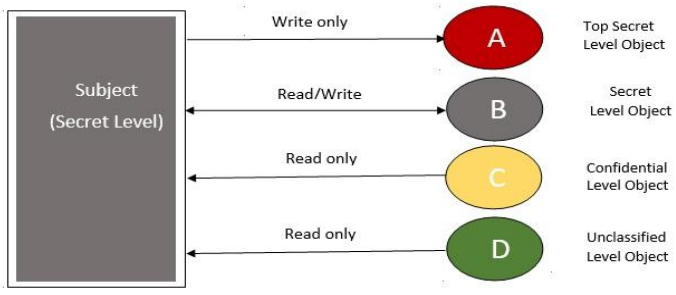

Fig. 1. Available data flow in multilevel secure data model.

IV. E-COURT DATABASE RELATIONAL MODEL

The Multi-Level Security e-Court System database uses the relational data model and a query language based upon the relational algebra [12]. In a relational model, data and relations between them are organized in tables (Fig. 2). The columns of a relation are referred to as attributes. The degree of a relation is the number of attributes defined for that relation. The rows of a particular relation (table) are referred to as tuples. The cardinality of a relation is just the number of tuples it contains.

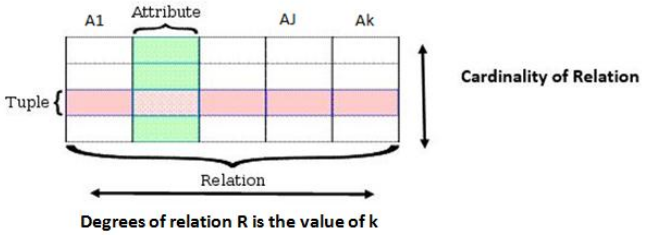

Fig. 2. Relational Database definitions.

V. SECURITY POLICY IN DATABASE MODEL

In relational database model the results of the SQL query is always a relation. Since the data in database is classified at various levels, the result query could contain data items with several different classifications;
In this security approach can be state in terms of difference between the result relations, returned in response to a query, for a secure and non-secure database, in non-secure database returns all tuples satisfying the query, but in multi-level secure DBMS returns only those row which are classified at or below the user's level, hence some tuples are eliminated that contain one or more elements above the querying user's level from the secure result [6] [11].

Our approach can be described the security in terms of classification rules and a classification policy. Classification rules are associate with all data in the database, and the classification policy determines the result of a user's query for a user at a particular security level. Security constraints are the mechanism for defining classification rules, and query modification is the mechanism for implementing the classification policy.

VI. SECURITY CONSTRAINTS

In our framework using security constraint to classified data with different levels, provide powerful classification policy because any subset of data can be specified and assigned a level. Classification of an entire database, as well as classifying by relation or by attribute [13]. Constraints that classify by content provide the mechanism for classification by tuple and by element. Constraints that classify by context are the mechanism for classifying relationships between data. Any subset of the database can be classified based upon content or context. Also the results of applying functions to an attribute or subset of an attribute.
The following examples illustrate classification policies for a relational database and the constraints that must exist to support them.
Define classification levels for the entire database:
l. all data in the entire database is classified T.S.

The next set of constraints define classification levels for a relation:
2. relation R, classified T.S. (all data in the entire relations classified T.S. - equivalent to a T.S. label on each element in relation)
The next set of constraints define classification levels for an attribute:
3.attribute aij classified T.S. (all data in the entire attribute is classified T.S. - equivalent to a T.S. label on each element in attribute)

The next two sets of constraints illustrate classification by context. The first set define classification levels for 2 attributes in the same relation:
4.relationship between attributes in the same relation classified T.S. (they are classified T.S. when read together, but not necessarily when read individually)

The second set define classification levels for 2 attributes in different relations:
5. relationship between attributes in different relations classified T.S.
The next two sets of constraints illustrate classification by content. The first set defines classification levels for all attributes in a relation that satisfies a particular predicate:
6. tuples classified T.S (all data in the tuples is classified T.S.)

The second set define classification levels for a single attribute in a relation that satisfies a particular predicate:
7.elements classified T.S.
The next set of constraints illustrate the classification of a function of an attribute:
8. function of an attribute classified T.S. f = average, count, sum, max, mm

VII. Query Modification

The client's query is modified depend the security constraints so that the response can be assigned a classification which will make it observable to the client [4]. The results of modified query are then executed. Query is modified while client's request this query, modifying the query by applying those selected constraints from set of all constraints, which have classified at least one attribute with a classification level not less than or equal to that of the user, then only the information which is classified at equal or lower level than the user's poses the query is returned as shown in Table (1, 2).

Table 1 Investigate Court Relation in Multilevel Form

CASE NO	CASE TYPE	JUDGE	REGISTERED AT	POLICE STATION	POLICE INVESTIGATOR	DATE OF CRIME	TIME OF CRIME	TC
101 U	Treason U	Majid U	10/01/2015 U	Rzgari U	Ali U	05/01/2015 U	10:20 U	U
102 U	Smuggling U	Majid S	15/06/2015 U	Rzgari C	Kurdo U	10/06/2015 S	21:05 C	S
103 C	Drug trafficking C	Mohamad C	08/01/2016 C	Baxtyari C	Ali C	05/01/2016 C	14:15 C	C
104 TS	Espionage TS	Ahmad TS	15/01/2016 TS	Azadi TS	Ismail TS	09/01/2016 TS	08:25 TS	TS

Table 2 Investigate Court Relation Instance for a C User

CASE NO	CASE TYPE	JUDGE	REGISTERED AT	POLICE STATION	POLICE INVESTIGATOR	DATE OF CRIME	TIME OF CRIME	TC
101 U	Treason U	Majid U	10/01/2015 U	Rzgari U	Ali U	05/01/2015 U	10:20 U	U
103 C	Drug trafficking C	Mohamad C	08/01/2016 C	Baxtyari C	Ali C	05/01/2016 C	14:15 C	C

VIII. Conclusion

We have proposed a framework for an e-Government sector (e-court) in Iraq by defining some levels of classification about sensitive data using classification rules to enforce security policy that the response to a query against a multi-level secure database can be assigned a classification which will make the response observable to the query.

IX. References

[1] Organisation for Economic Co-operation and Development, Public Management Service, PUMA 16/ANN/Rev1 (2001). "E-Government: analysis framework and methodology". http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=PUMA(2001)16/ANN/REV1&docLanguage=En (Link at 21-October-2012)
[2] United Nations, Department of Economic and Social Affairs (2012). "E-Government Survey 2012. E-Government for the People".ISBN:978-92-1-123190-8. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf (Link at 21-October-2012).
[3] M. Stonebraker, E. Wong, and P. Kreps: The Design and Implementation of INGRES, ACM Transactions on Database Systems, Vol. 1, No. 3. September, 1976, pp.1899222.
[4] M. Stonebraker: Implementation of Integrity Constraints and Views by Query Modification, ACM SIGMOD International Symposium on Management of Data, 1975, pp.65-78.
[5] M. Stonebraker, and E. Wong: Access Control in a Relational Data Base Management System by Query Modification, ACM National Conference Proceedings, 1974, pp.180-186.
[6] Dwyer, D. Jelatis &and M. Thuraising :Multi-level Security in Database Management Systems, Computers and Security, vol 6, no. 3, pp. 252-260, 10.1016/0167-4048(87)90106-4
[7] DOD Computer Security Center: Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD-001-83, August 15, 1983.
[8] D.E. Bell, and L.J. LaPadula: Secure Computer System:Unified Exposition and Multics Interpretation, MITRE Technical Report MTR-2997, July, 1975.
[9] W.E. Boebert, W.D. Young, R.Y. Kain, and S.A. Hansohn: Secure Ada Target: Issues, System Design and Verification, 1985 IEEE Symposium on Security and Privacy, Oakland, CA, April 22-24, 1985, pp. 176-183.
[10] D. Bonyun et al.: A Model of a Protected Data Management System, I.P. Sharp Report ESD-TR-76-289, 1976.
[11]Faragallah, M. El-Rabaie , El-Samie, I. Sallam and S. El-Sayed:"Multilevel Security for Relational Database".ISBN: 9781482205398 - CAT# K21447
[12] J.D. Ullman: Principles of Database Systems, Computer Science Press, 1982.
[13] Dwyer, D. Jelatis &and M. Thuraising :Multi-level Security in Database Management Systems, Computers and Security, vol 6, no. 3, pp. 256, 10.1016/0167-4048(87)90106-4

Authors Profile :

A. Rzgar Sirwan Raza

Education

1. *A Preparatory school from Sep. 2002 to Sep 2003, High school certificate.*
2. *University of Sulaimany, college of science*

department of Computer from 2003 to Sep 2007, and 8th out of 20 students.

3. *I was taking English Course one year in IEC collage from India.*
4. *Now I am finished MSC (Master Computer Science) from University of Hamdard /New Delhi , India.*
5. *Also I have Diploma inGEO_Informatic from PTU(Punjab Technical University) in India.*

Employment history

1) *I participation from two course of CISCO on basic and advance network And window Xp 2003 and another course over MS Visual C# by academyNajah.*
2) *I work on Archiving System from my project to create small System by Oracle 10g and Form Builder for computer science department.*
3) *My MSC project working on Title (Sales Analysis implemented by KDD and Data Mining) .*
4) *For one year working in private sector (Fanoos telecom).*
5) *Now I am Teacher in University of Human Development.*

B. Zana Azeez Kakarash

Zana *is an assistant lecturer (faculty staff member) at Human Development University since 2011. He obtained his M.Sc. in Computer Science from Bharati Vidyapeeth University, Pune -30, India, 2011.*

INTERNATIONAL JOURNAL PUBLICATIONS

1) Zana Azeez Kakarash , Hoger Mahmud Huseen and Mazen Ismaeel Ghareb. **An Investigation into News Webpage interface Design in Kurdistan Region of Iraq.** Second International Scientific Conference held by the University of Human Development 2015.

2) Zana Azeez Kakarash & Raed Ibraheem Hamed. **Evaluate the Asphalt Pavement Performance of Rut Depth Based on Intelligent method**. International Journal of Engineering and Computer science-India 2016.

Academic Appointments:

- ***From 2011*** *- Lecturer at University*
  - *Teaching computer subjects at UHD University in Kurdistan of Iraq. Teaching Java programming, OOP and lab training.*
  - *Head of Information Technology department Member of principals committee till now.*
  - *Teaching computer subjects at Sulaimany University in Kurdistan of Iraq. Teaching Database Management System and lab training.*
  - *Teaching computer subjects at Halabja University in Kurdistan Region Iraq. Teaching Fundamental of computer and lab training.*
- ***2007 – 2008*** *: assistant Teacher and Lab Management, Department of Computer and Statistics, College of Commerce ,University of Sulaimany , Sulaimanyah City, Iraq.*
- ***2006 - 2008 :*** *at Ministry of Peshmarga for about two years like a Database administrator.*