Resource Availability Of M-Learning Applications Databases

Mihai DOINEA, Department of Economic Informatics, Academy of Economic Studies, Bucharest, Romania, mihai.doinea@ie.ase.ro
Paul POCATILU, Department of Economic Informatics, Academy of Economic Studies, Bucharest, Romania, ppaul@ase.ro
Cristian CIUREA, Department of Economic Informatics, Academy of Economic Studies, Bucharest, Romania, cristian.ciurea@ie.ase.ro

Abstract

The paper analyzes the resource availability of mobile learning applications databases, by identifying database vulnerabilities and determining the databases availability. There are described collaborative integrated systems for resources management inside m-learning applications. Metrics are built for analyzing the security level of m-learning applications.

Keywords: m-learning application, database availability, security, metrics, collaborative

1. Introduction

In the last period, there was a change from using stationary computers for accessing learning resources to using mobile devices that eliminate the space constraint and offer the possibility to access different documents from anywhere (Hoff et al, 2008). As mobile phones continue to develop and acquire new functional characteristics, the applications designed for them will be able to grow with the technology (Finkelstein and Wood, 2009).

In Yuan et al (2010) is considered that mobile learning is a new form of learning, combining mobile devices and networks, expanding digital learning channels, offering educational resources and educational services anytime and anywhere.

In the knowledge-based society, in which organizations carry out their activity, the m-learning process succeeded through the different interaction tools (Mircea and Andreescu, 2011), to offer ample opportunities for learners to collaborate with peers, experts, professionals or with other learners.

The learning process from an organization may be achieved through an m-learning application or an intranet e-learning platform. The intranet-learning platform should focus on how to instruct and stimulate learners to achieve knowledge, and the objective is to visualize traditional classroom education and learning environment in web (Delcea et al, 2010).

Security is an important aspect of how collaboration can be successful for each of the parties involved in the process of education. In the case of mobile learning applications, the implications from a security perspective are much greater than in normal e-learning applications, due to the fact that mobile communication must also be managed by security measures additional to the ones that help and protect the communication between the application components.

The paper is structured as follows:

M-learning system databases section presents the databases characteristics specific to m-learning applications.

M-learning database vulnerabilities metrics section deals with data security issues specific to m-learning applications and presents several metrics developed in order to achieve better results in databases security analysis. Also, a vulnerability minimization process model is proposed.

Databases availability costs analysis is the section where the focus is on the costs related to one of the main characteristic associated to databases security.

The section *Collaborative integrated systems for resources management inside m-learning applications* show how resource management can be improved using collaborative systems.

The paper ends with conclusions and future work.

2. M-learning system databases

M-learning applications could have two types of databases, depending on the architecture: local and remote databases. The paper focuses on remote databases that are stored on a server where the m-learning application connects during the interaction. Figure 1 highlights the databases in an m-learning system.

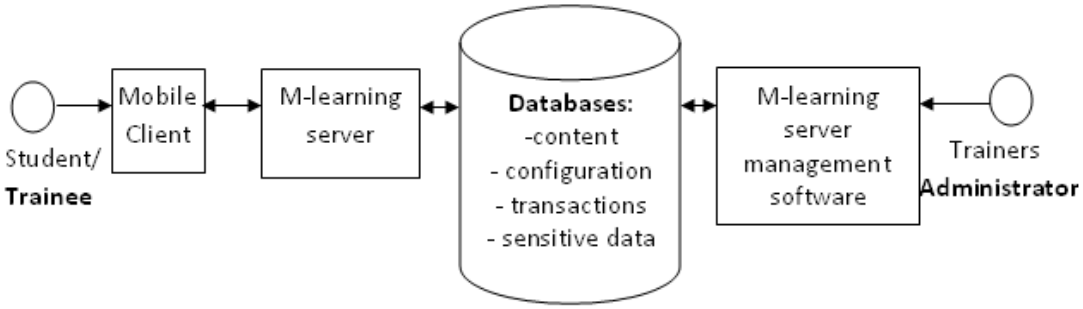

Fig 1. Databases in m-learning systems

Complex m-learning applications databases include different kinds of information:

- Student data
- Teacher data
- Courses and lessons
- Homework
- Users' history
- Test results, mark
- Test responses
- Payment information (for classes, tests etc.)

As can be seen, there is sensitive data that need to be protected. Also, the unavailability of database could lead to high costs and other problems.

M-learning database vulnerabilities are viewed with regards to the two main types of database systems, which describe how data is fluctuating over time:

- *static database* is represented by data objects that remain constant over time, or at least over the time period in which the data security is discussed like records id, primary and foreign keys and other unique constraints;

- *dynamic database* is reflected by data objects which are changing in terms of attributes modifications, relationships alteration and also the number of records in the database is in a permanent shifting due to update, insert and delete operations; this includes exam and quizzes answers, history, payments etc.

A database system is vulnerable if, like any other informatics systems, contains some weaknesses, which might be exploited.

For data, security is defined starting from the following three perspectives, (Connolly and Begg, 2004):

- *integrity* features which predict and alert in case of such problems occur due to malicious behavior or a flaw in the database design, like error detection and correction codes which are used for automatically detect and/or correct the compromised data; this is achieved by adding some *redundancy*;

- *availability* features which help the entire system to put at user's disposal data whenever is requested; read access to data is an important and major door to unauthorized takeovers;

- *secrecy* characteristic keeps away any undesired action of viewing the sensitive information; this is done through cryptographic controls, permission policies, roles and privileges.

These perspectives are analyzed in the following sections by a system of metrics and by related costs.

3. M-Learning databases vulnerabilities metrics

In order to analyze the vulnerabilities, several metrics were built and a model for vulnerability analysis is proposed.

The availability, AV, is defined as function is:

$$AV = \frac{AVMT}{AVMT + DMT}$$

where:
AVMT – available mean time described as the time in which the database is functional, capable of processing user's request;
DMT – down mean time as the period in which the database is down due to maintenance procedures, unknown failures, attacks or other inconveniences.

The dimensional analysis of the metric is:

$$[AV] = \frac{[AVMT]}{[AVMT] + [DMT]} = \frac{[sec]}{[sec]} = 1$$

Optimizing resources availability in m-learning databases involves applying a correct treatment for the main vulnerabilities breaches that affects this feature, leading to an improvement of the default security level for the m-learning application.

Database vulnerability supposes the construction of a representative statistic data set with raw data which, after that, must be analyzed for classes and subclasses identification to make a quantitative analysis about the laws that govern this vulnerability characteristic.

For this purpose we need:
- NA – number of distributed applications studied for the vulnerabilities analyses;
- NR_i – number of records concerning the behavior of application *i* database;
- dim – dimension of data set given by the relation:

$$\dim = \sum_{i=1}^{NA} NR_i$$

The data set contains information about the events, effects, time periods for controlling the problems, as well the repairing costs implied by potential accidents. By browsing the entire data set we can observe:

- NTV – number of vulnerability types, obtained as the length of a vulnerability list of codes that were assigned in time as different events were produced;

- f_j – apparition frequency of type j vulnerability, expressed as:

$$f_j = \sum_{i=1}^{NA} g_{ij}$$

where g_{ij} is apparition frequency of type *j* vulnerability on application *i* database.

If we add to the data set new collected information concerning the vulnerability behavior, for example the moments of apparition for the vulnerability associated events, than we can calculate:

- intervals between two random events;
- intervals between two identical events;
- laws of empiric repartition associated to the event apparitions;
- average times of problems solving.

The number of errors on m-learning application size, NED, is defined as follows (Ivan et al, 2010):

$$NED = \frac{NEA}{DAS}$$

where:
NEA – total number of errors identified in the m-learning application;
DAS – the size of m-learning application, measured in number of code lines, *LOC* or *KLOC*.

The number of security vulnerabilities, *NSV*, identified in the m-learning application is defined as follows (Ivan et al, 2010):

$$NVS = \frac{NVDA}{DAS}$$

where:
NVDA – the number of vulnerabilities detected in the m-learning application;
DAS – the size of m-learning application, measured in number of code lines, *LOC* or *KLOC*.

All this information obtained from the data set represent inputs in a vulnerability modeling process for distributed applications.

For the development of database vulnerability minimization of a distributed application a model is designed in which:

- the set of variables is defined: the development cycle length, the resources that are used and the associated costs;
- optimal criteria is presented;
- the data sets for the testing phase is generated;
- measurements are conducted;
- the database behavior is analyzed;

- a refinement process is conducted based on the previous analyze;
- the process of data input is repeated if the resources allow it and the vulnerability is greater than a predefined level.

A diagram is designed, figure 2, based on these steps, putting into the light the finality of vulnerability minimization process.

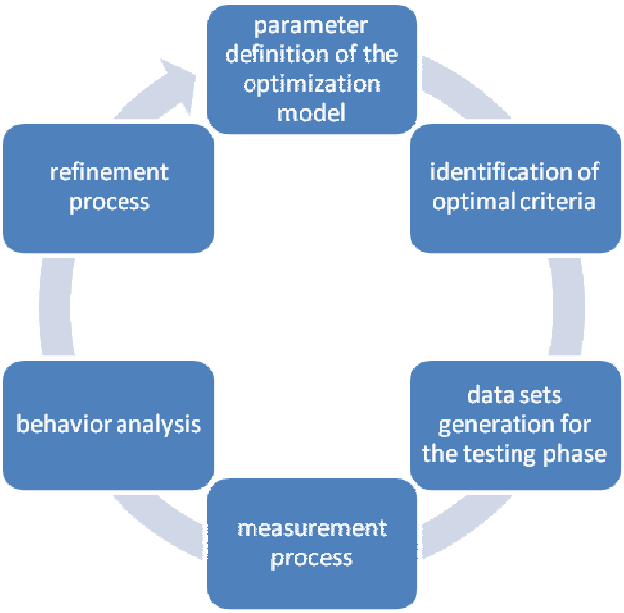

Fig 2. Minimization process of database vulnerability diagram

The more detailed data set is, the coefficients are more stable and the quality of optimization is better.

4. Databases availability cost analysis

Availability is the characteristic that maximizes the profit of a distributed informatics application. At the database level that stores the resources of the application, availability is seen as the average time in which the database is entirely accessed by its users. The lack of availability is due to the following factors:

- deficient design of the database without taking into account the restrictions from the outside;
- the vulnerabilities from the external environment with which the application interacts.

The absence of the availability of a database, called percentage of unavailability, *pd*, is calculated using the formula:

$$pd = (1 - AV)$$

The period of unavailability of a database generates costs, *CID*, calculated based of the formula:

$$CID = pd \cdot CUD$$

where CUD represents the cost for each unit of unavailability calculated as the total number of accesses for total availability, *nra*, multiplied with the cost of each access at the level of resources of the application's database, $cost_{acc}$:

$$CUD = nra \cdot cost_{acc}$$

These costs are supported by the application in the case of the existence of a period of unavailability, when $pd > 0$. Let CAD be the costs of assuring the availability of a database. Table 1 presents two situations in which the availability of a distributed application's database is analyzed.

Table 1: model of availability treatment

Model of availability treatment	Assurance costs, CAD	Unavailability	Unavailability costs
MD_1	0	pd_1	CID_1
MD_2	CAD_2	pd_2	CID_2

The model of availability treatment MD_1 doesn't treat the vulnerabilities that lead to an increase in the availability characteristic, $CAD_1 = 0$. In this case, according to the period of unavailability pd_1 the costs CID_1 are associated.

The model of availability treatment MD_2 analysis the aspects that lead to the diminishing in the level of the availability characteristic having the costs $CAD_2 > 0$. These costs increases the level of AV_2 so that $AV_1 < AV_2 \Rightarrow pd_1 > pd_2$, and the costs supported as a result of the unavailability of the database are lower, $CID_2 < CID_1$.

If, for the MD_1 model, the availability is $AV_1 = 85\%$ and for MD_2, $AV_2 = 90\%$, then, for minimizing the availability costs and reaching its high level, the restriction is given by:

$$CID_1 > CID_2 + CAD_2 \Rightarrow CAD_2 < CID_1 - CID_2 = CUD \cdot (pd_1 - pd_2) \Rightarrow$$
$$\Rightarrow CAD_2 < 0.05 \cdot CUD$$

As the costs associated to the unavailability CUD are fixed, for reaching a high level of this characteristic through justified assurance costs, those last costs are put in correspondence with the effects generated upon the level of availability. In this case, CAD_2 justifies the effect generated at the availability level, having a multiplier of whose value is equal to 0.05 and MD_2 model is accepted to the detriment of MD_1 model.

The average cost of type *j* vulnerability, c_j, is obtained as the sum of the costs for repairing the database by eliminating the events that generated the type *j* vulnerability, divided by the number of events apparitions for the respective vulnerability:

$$c_j = \frac{1}{f_j} \sum_{i=1}^{NA} g_{ij} \cdot cost_{ij}$$

where $cost_{ij}$ represents the repairing cost of the application's *i* database for eliminating the events that characterize the type *j* vulnerability in application *i*.

The dimensional analysis for c_j is:

$$[c_j] = \frac{1}{[vulnerability\ number]} \times [vulnerability\ number] \times [m.u.] = [m.u.]$$

The optimization model takes into consideration this cost analysis, in order to focus on the most important vulnerabilities.

5. Collaborative integrated systems for resources management inside m-learning applications

The collaborative integrated systems have been implemented for the m-learning applications from the educational field to improve the resource management, the document management and process management or the efficiency of collaborative work (Martin et al, 2010).

In the academic field, the electronic integration technology of educational resources supports integration processes that comprise two or more m-learning applications (Evans, 2008). When there is a collaborative system for electronic integration, all electronic resources posted on the university website automatically switches to document management system, without requiring that a person to upload documents in the system. Likewise, a request on the availability of resources on the university website generates a message that is sent in real time to the internal system, so that the user of m-learning application to obtain timely and accurate information.

In the private sector, companies expand the electronic integration beyond the limits of their own organizations to automate the training of employees. As departments of companies become more integrated and the employees becomes users of m-learning applications, traditional security mechanisms are replaces with authorization programs and modern security systems that manage and store the users' data in an intelligent way and correlates them with the rules access of the organization. The rules define the authorizations according to the role that each person has in different educational processes, providing to the company the necessary means to identify users and to provide them, in a secure manner, the data and resources they need, taking into account the needs and access policies.

The integration capacity of resources in the m-learning applications, *ICRMA*, is given by the relationship:

$$ICRMA = \frac{CIR}{VIR},$$

where:
CIR – costs incurred to integrate resources in the m-learning applications
VIR – value of integrated resources.

From dimensional analysis of the indicator, the measure units of *CIR* and *VIR* variables are monetary units, resulting the dimensionless character of the *ICRMA* indicator.

If the value of *ICRMA* indicator is closer to 1, then the resources are more difficult to integrate. The reduced costs compared with the value of resources, made for their integration, show a good capacity to integrate resources in m-learning applications.

6. Conclusions and future work

When analyzing the resource availability of m-learning applications databases, a specific attention should be given to the variables that are influencing it. From this category, the variables that underline the level of resource management represent an important category.
In order to increase the security level of an m-learning application, specialized metrics to measure the quality characteristics levels are used. Collaborative learning processes influence the work with large data sets inside m-learning applications and their security by streamlining operations conducted and increasing the security degree at the database level that stores these data sets.Future work includes the same analysis for mobile databases used by m-learning applications.

Acknowledgement

This work was supported by CNCSIS –UEFISCSU, project number PNII – IDEI 2637/2008, project title: Project management methodologies for the development of mobile applications in the educational system.

References

Connolly, T. and Begg, C. (2004), Database Systems: A Practical Approach to Design, Implementation and Management (4th Edition), Pearson Publisher.

Delcea, C., Ciurea, C. and Bobe, C. (2010), 'Un Modele pour l'Amelioration de la Performance de L'entreprise base sur E-learning Collaboratif' Proceedings of 14th IBIMA Conference, IBIMA 2010, ISBN 978-0-9821489-3-8, 23-24 June, 2010, Istanbul, Turkey.

Evans, C. (2008), 'The effectiveness of m-learning in the form of podcast revision lectures in higher education,' *Computers & Education*, 50(2), 491-498.

Finkelstein, J. and Wood, J. (2009), 'Mobile eLearning Platform for Interactive Patient Education' International Conference on Mobile, Hybrid, and On-line Learning, 2009, ELML '09, ISBN 978-1-4244-3361-2, 1-7 February 2009, 23-27.

Hoff, C., Wehling, U. and Rothkugel, S. (2008), 'ArCoMo-An Artefact-based Collaborative Mobile Learning Environment' Sixth Annual IEEE International Conference on Pervasive Computing and Communications, 2008, PerCom 2008, ISBN 978-0-7695-3113-7, 17-21 March 2008, 383-388.

Ivan, I., Ciurea, C., Pavel, S. and Doinea, M. (2010), 'Security of Collaborative Processes in Large Data Sets Applications,' The 5th International Conference on Applied Statistics, ISSN 2069-2498, November 19-20, 2010, NIS Publishing House, Bucharest, Romania.

Martin, S., Boticki, I., Jacobs, G., Castro, M. and Peire, J. (2010), 'Support for mobile Collaborative Learning applications' Frontiers in Education Conference (FIE), 2010 IEEE, ISSN 0190-5848, October 2010, Washington, DC, USA.

Mircea, M. and Andreescu, A. (2011), 'Using Cloud Computing in Higher Education: A Strategy to Improve Agility in the Current Financial Crisis,' *Communications of the IBIMA*, 2011, 1-15.

Yuan, J., Xing, R. and Wang, J. (2010), 'Applying Research of Mobile Learning Mode in Teaching,' 2010 International Forum on Information Technology and Applications (IFITA), vol. 3, ISBN 978-1-4244-7621-3, 16-18 July 2010, 417-420.