CREATING AND ENCRYPTING E-COMMERCE DATABASE FOR SELLING MECHANICAL ELEMENTS

UDC: 004.651
004.738.5:339
Original scientific paper https://doi.org/10.18485/aeletters.2018.3.3.1

Djordje Dihovični[1], Vlado Krunić[2]

[1]Technical College, Bulevar Zorana Djindjica 152a, Belgrade, Serbia
[2]Faculty of Natural Sciences and Mathematics, Mladena Stojanovića 2, Banja Luka, Bosnia and Herzegovina

Abstract:
In this paper it is presented creation and encryption of e-commerce database for selling mechanical elements. It is shown a procedure of creation a database and tables with appropriate data, which is the first step in developing stable e-commerce application. For security reason it is necessary to encrypt the database, and it is described a complete process, and as well it is given part of the code of web application for inserting data into the tables, deleting some data and updating them. In developing e-commerce application for selling mechanical parts, it is applied C# programming language by using ASP.NET, with using HTML language and XML.

ARTICLE HISTORY
Received: 05.02.2018.
Accepted: 21.03.2018.
Available: 30.09.2018.

KEYWORDS
Certificate key, database, data management, data definition, data manipulation, decryption, encryption, structure query language, relational model

1. INTRODUCTION

A relational database is a special type of database in which the data management is based on the relational model. Data in these databases are organized into a set of relations between them which define a specific connection. The relation may optionally also has a foreign key, whereby it has a link to the other routes [1]. Query languages are designed to communicate with a relational database, i.e. to create a relational schema and updating and reading data from a relation. They can be classified in the most general: the languages which derived superstructure from the procedural programming languages, the languages based on the relational domain account or n-topples, languages based on relational algebra and the languages that are based on a combination of relational algebra and relational account [2-3].

The most common query language is SQL (Structured Query Language), developed 80-ies of the last century by the IBM research laboratory in San Jose, California. It is supported by almost all systems to manage relational databases. Despite its high prevalence, great importance is placed on questionable (Query Language), which is also developed in California, at the University of Berkeley [4].

SQL is the last phase of the development of query languages by the IBM research laboratory. The predecessors of SQL are developed by IBM in laboratories with SQUARE query languages and SEQUEL. SQL standard was published in 1989 and immediately was widely accepted in the market. Some of the important features are: a language for defining data (Data Definition Language), a language for data manipulation (Data Manipulation Language), external and internal bonding, cascading update and delete, set operations (union, intersection and difference), and etc [5].

Data definition language is part of the query language, and it is used to create and update objects that make up a relational database, and includes the base relations, relational schema, semantic domains, indexes, and etc.

This part of the query language is used to manipulate data in the database, i.e. for viewing, deleting, inserting and updating data. In this regard,

CONTACT: Djordje Dihovicni, ddihovicni@gmail.com

it consists of four basic commands: SELECT, INSERT, UPDATE, and DELETE [6].

Insurance of database systems is an important task for many organizations. Namely, if organizations are kept private and confidential information, they must apply and meet the many laws and safety standards. Private data is confidential user information, (e.g., credit card number), that may be available to them or to someone else, and before their access, it should be approved by the user [7,8].

The good practise for creating reliable information system is always based on system security and the encryption of the data [9,10].

2. DATABASE CREATION

The database that is created, and subsequently used for the interaction of the web site, has four tables:

1. Mechanical parts: the names of machine parts that are offered, and a description of their country of origin;
2. Warehouse: id item, quantity in stock and the price per share;
3. Customers: customer id, name, address, e-mail and password;
4. Consumer basket: id of the machine parts that are purchased, customer id, id item, order quantity and total price.

The creation of the database will be made by using SQL Server Management Studio.

In Fig.1, it is shown SQL Server Management Studio.

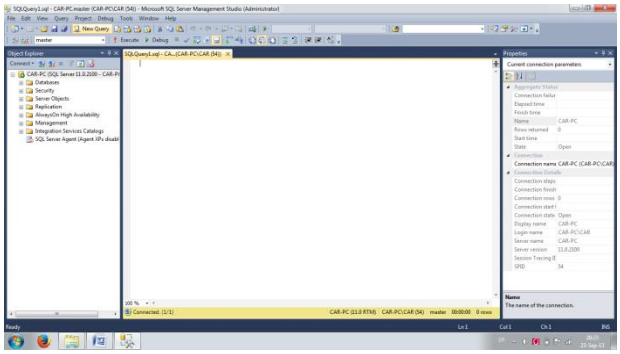

Fig. 1. Creating database in SQL Server Management Studio

The code for creating the database and four tables is presented down below:

```
CREATE DATABASE onlineSellingElements;
GO

USE onlineSellingParts;
GO

CREATE TABLE MechanicalElements

(
idMec  int  NOT NULL PRIMARY KEY,

title varchar(255),
description varchar(255),
countryOrigin varchar(255)
);

CREATE TABLE Warehouse

(
idArticle int NOT NULL PRIMARY KEY,
quantity int,
pricePerShare money
);

CREATE TABLE Customers

(
idCustomer int NOT NULL PRIMARY KEY,
name varchar(255),
lastName varchar(255),
address varchar(255),
mail varchar(255),
password varchar(255)
);

CREATE TABLE ConsumerBasket

(
idMec int NOT NULL PRIMARY KEY,
idCustomer varchar(255),
idArticle varchar(255),
orderQuantity varchar(255),
totalPrice money
);
```

A next step involves entering data into the tables, as it is shown with the code:

```
INSERT INTO MechanicalElements (idMec, title, description, countryOrigin)

VALUES (1, 'gear', 'for servo mover  MKG22', 'Serbia');

INSERT INTO MechanicalElements (idMec, title, description, countryOrigin)

VALUES (2, 'axle', '50x8 mm', 'Serbia');

INSERT INTO MechanicalElements (idMec, title, description, countryOrigin)

VALUES (3, 'bearing', 'ball', 'Serbia');

INSERT INTO ConsumerBasket (idMec, idCustomer, idArticle, orderQuantity, totalPrice)

VALUES (1,'1','1','20','20000');
```

```
INSERT INTO Customers (idCustomer, name, lastName, address, mail, password)

VALUES
(1,'Milos','Milosevic','Srumatovacka','dmc977','dr Wull23');

INSERT INTO Warehouse (idArticle, quantity, pricePerShare)

VALUES (1,'200','1000');

INSERT INTO Warehouse (idArticle, quantity, pricePerShare)

VALUES (2,'200','1000');

INSERT INTO Warehouse (idArticle, quantity, pricePerShare)

VALUES (3,'200','1000');.
```

3. ENCRYPTION OF THE DATABASE

Encryption of database refers to the use of techniques of data encryption, and encryption of databases, that make it data unreadable to those who do not have the key [11].

Encryption is a process in which data are taken with plain text and converted into a form that cannot be decrypted. The result of the encrypted data, is known as cipher text. Once the data is encrypted, they usually have to decrypt. Decryption (decryption rank) returns data encoded text in its original plain text form. The study of these two processes is called cryptography [12].

A process of encryption the data, requires two things: encryption algorithm and encryption key. Description of high level of encrypting data is quite simple: plain text data is inserted into the encryption algorithm. It is also provided the encryption key. Together, the algorithm uses a key and very sophisticated logic to encrypt data. Decryption process is analogous. It also requires a key and algorithm [13,14].

With encryption comes the responsibility to manage encryption keys. If it fails to properly manage keys, it can be disastrous for both accounts. First, the keys are compromised, the data will be decrypted and thus invalidate the entire process [15,16]. Second, if the keys are lost, the data will never be able to decrypt.

The Dana Transparent Encryption (TDE), uses a Database Encryption Key (DEK) which is secured certificate and is kept in the master database [17]. The Database Encryption Key is either protected by certificate or asymmetric key secured by a driver Extensible Key Management (EKM), [18] using the Microsoft Cryptographic API (MSCAPI). The TDE data are encrypted using the algorithms for encrypting, the Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES).

First it is necessary to create a Master Key with a strong password in the database that has been created, as shown below:

```
USE master;

GO

CREATE  MASTER KEY ENCRYPTION BY
PASSWORD=`F87zis$7&iuRiU`;

GO.
```

After creating master key, next step involves creation of the certificate, with the name onlineSellingParts_Certificate, as it is presented down below:

```
CREATE CERTIFICATE onlineSellingParts_Certificate

WITH SUBJECT=`On line selling parts certificate`;

GO
```

then it is necessary to create key for encrypting database *onlineSellingElements* (DEK), with AES_128 algorithm and with appropriate certificate:

```
USE onlineSellingElements;

GO

CREATE DATABASE ENCRYPTION KEY

WITH ALGORITHM=AES_128

ENCRYPTION BY SERVER CERTFICATE
onlineSellingElements_Certificate;

GO
```

It is very important to make security copy of the certificate and the private key, otherwise it is not possible to backup the database:

```
USE master;

GO

BACKUP CERTIFICATE
onlineSellingElements_Certificate

TO
FILE='C: :\Backup\onlineSellingElements_Cert.cer' ;

WITH PRIVATE KEY (FILE = 'C:\Backup\ onlineSellingElements.pvk',
ENCRYPTION BY PASSWORD = 'F87zis$7&iuRiU';

GO
```

Enabling the encryption can be achieved with the following code:

```
ALTER DATABASE onlineSellingElements
SET ENCRYPTION ON;
GO
```

Additional certificate checking, and getting data about encrypting key is given by the following code:

```
USE master;
GO
SELECT * FROM sys.certficates WHERE
pvt_key_encryption_type<>'NA';
GO.
```

4. DEVELOPMENT OF THE WEB APPLICATION

Inserting data into tables of the database is achieved through the following steps [19]:

A) creation of the connection object;
B) creation of the command object;
C) determination of the connection string;
D) determination of the connection used by connection object;
E) determination of the Insert statement for the command text of command object;
F) adding values to the command parameter;
G) open the connection;
H) execute the command;
I) close the connection.

The code for entering new mechanical element into table of the database is presented by the following code, [20]:

```
SqlConnection connection = new SqlConnection();
SqlCommand command = new SqlCommand();
SqlDataAdapter adapter = new SqlDataAdapter();
SqlCommandBuilder builder = new
SqlCommandBuilder(adapter);
DataSet dataset = new DataSet();
connection.ConnectionString = "Integrated
Security=true;Initial
Catalog=onlineSellingElements;" "Data
Source=lara-and-nicki";
command.Connection = connection;
command.CommandText = "SELECT * FROM
MechanicalElements";
adapter.SelectCommand = command;
adapter.Fill(dataset, "MechanicalElements");
DataRow row =
dataset.Tables["MechanicalElements"].NewRow();
row["Title"] = txtTitle.Text;
row["Description"] = txtDescription.Text;
row["Country"] = txtCountry.Text;

dataset.Tables["MechanicalElements"].Rows.Add(r
ow);
```

The erasing of the mechanical element from the table in the database can be achieved by the code, which is shown down below:

```
command.CommandText = "DELETE FROM
MechanicalElementsWHERE idMech=@idMech";
command.Parameters.AddWithValue("@idMech",
txtDelete.Text);
try
{
connection.Open();
int result = command.ExecuteNonQuery();
if (result > 0)
MessageBox.Show("Mechanical element is
erased!");
else
MessageBox.Show("Mechanical element is not
found");
}
```

The data from the tables in the database can be also updated by using similar code.

5. CONCLUSIONS

The first and most important step in starting online selling of the product to potential buyers, is the Web site presentation. The complex process of designing and creating a website consists of three phases. The interface creating includes the first phase of designing of website and it is basically, designing of the page appearance.

The next phase is inevitable part of any of this kind of websites, and it consists of creating a database using relational database. In this paper it is presented a database of online selling mechanical elements, which consists of four tables. The database is encrypted, and data in tables are protected.

The third and the most difficult phase in a process of creating of website is making a link between interface, creating dynamic web applications based on data and interaction with users. It is applied C# programming language by using ASP.NET, with using HTML language and XML.

The stable and protected database which is created, is essential for developing useful e-commerce application for selling mechanical elements.

REFERENCES

[1] D. Sussman, A. Homer, Wrox's ASP.NET 2.0 Visual Web Developer Express Edition Starter Kit. *Wiley Publishing, Inc.*, Indianapolis, 2006.

[2] K. Czarnecki, M. Antkiewicz, Mapping Features to Models: A Template Approach Based on Superimposed Variants. *International Conference on Generative Programming and Component Engineering*, Springer-Verlag Berlin Heidelberg, Vol.3676, 2005, pp.422-437.

[3] Dj. Dihovicni, Pole Assignment for Glass Capilary Tube Drawing Process by using Matlab and Maple Language. *Applied Engineering Letters*, 1 (3), 2016: 67-71.

[4] Dj. Dihovicni, Contructing knowledge database in stability of pneumatic pipelines. *Technical Diagnostics*, 14 (1), 2015: 7-14.

[5] P. Le Blanc, Microsoft SQL Server 2012. O'Reilly Media Inc., C45, California, 2013.

[6] H. Monga, S. Baghla, Approach to security in wireless sensors networks. *Applied Engineering Letters*, 1, (3), 2016: 80-84.

[7] P. Nielsen, Microsoft SQL Server 2008 Bible. *Wiley Publishing, Inc.,* Indianapolis, 2008.

[8] Dj. Dihovicni, M. Medenica, Database linear of scalability and high availability while maintaining a system performance. *10th International Scientific Conference "Science and Higher Education in Function of Sustainable Development"*, Section 2, Uzice, Serbia, 2017, pp.45-53.

[9] Dj. Dihovicni, M. Medenica, Fuzzy support model for long pipelines by using DB2 approach. *Applied Engineering Letters*, 2 (2), 2017: 76-83.

[10] Raman, S. Baghla, H. Monga, Method & Implementation of Data Flow. *Applied Engineering Letters*, 1 (4), 2016: 105-110.

[11] K. Kevin, Cryptography in the Database: Last Line of Defense. *Addison-Wesley*, 2005.

[12] D. Pleskonjić, N. Maček, B. Đorđević M. Carić, Sigurnost računarskih sistema i mreža. *Mikro knjiga*, Beograd, 2007. (In Serbian)

[13] A. Veljović, N. Gojgić, Projektovanje baza podataka, Visoka škola tehničkih strukovnih studija, Čačak, 2006.

[14] L. Ramkilde Knudsen, New Potentially 'Weak' Keys for DES and LOK, Advances in Cryptology - EUROCRYPT' 94, *Proceedings Workshop on the Theory and Application of Cryptographic Techniques*, Springer Nature Switzerland AG, Vol.950, 9-12 May, 1994, Perugia, Italy, pp.419-424.

[15] Kenan, K., *Cryptography in the Database,* Symantec Press, 2006.

[16] N. Galbreath, Cryptography for Internet and Database Applications. *Wiley Publishing, Inc*., Indianapolis, 2002.

[17] Noel Yuhanna, The Forrester Wave: Database Encryption Solutions, Q3 2005. *Forrester Research, Inc.*, Cambridge, 2005.

[18] J. Black, P. Rogaway, Ciphers with Arbitrary Finite Domains, RS Data Security Conference, Cryptographer's Track, Lecture Notes in Computer Science, Springer, 2002.

[19] M. Medenica, Dj. Dihovicni, Security Point of View of ASP.NET Application. *13th International Conference on Advanced Technologies Systems and Services in Telecommunications TELSIKS 2017* - IEEE Conference, 2017, Nis, Serbia, pp.403-406.

[20] Dj. Dihovicni, M. Medenica, Development of software package named "Step method" for robust time delay systems. *International Journal of Latest Research in Engineering and Technology*, 3 (8), 2017: 36-43.