Protection Data-in-Motion Stored in Database System

Laheeb Mohammad Ibrahim **Mohammed Zaki Hasan**
mzhasasn@uomosul.edu.iq
College of Computer Sciences and Mathematics
University of Mosul, Iraq

Received on: 15/05/2004 **Accepted on: 30/05/2005**

ABSTACRT

In this project, a simple model of the client/server relational database has been designed through using the idea of the SQL (Structure Query Language) server, and the single file of the database by the Micro software Access 2000.

We also configure the TCP/IP (Transform Control Protocol/Internet Protocol) to make connection between two computers, on one of these computers, Windows 2000 NT Adv. Sever has been installed, and which is considered to be the server computer, and the other installed by the Windows NT XP Professional as the client computer.

Finally, a normal security environment must be built to protect the information, or data-in-motion between two computers in order to increase the level of security to an acceptable level.

Keyword : TCP/IP, Structure Query Language (SQL)**,** Windows NT XP

حماية البيانات المخزنة في نظام قاعدة البيانات

لهيب محمد ابراهيم **محمد زكي الليلة**

كلية علوم الحاسوب والرياضيات

جامعة الموصل

تاريخ استلام البحث: 2004/05/15 **تاريخ قبول البحث: 2005/05/30**

الملخص

في هذا المشروع تم تصميم نموذج مخدم/مستفيد لقاعدة البيانات العلائقية من خلال استخدام فكرة لغة الاستفسار الهيكلية (SQL) والبرنامج التطبيقي لبناء قاعدة البيانات اكسس الإصدار (2000).

وقد تمت تهيئة الاتفاقيات (TCP/IP) لتحقيق الاتصال بين حاسبتين إحداهما نُصَّبَ عليها نظام ويندوز (2000) مخدم متقدم (Win2000 Adv. Server) واعتبرت بمثابة خادم وأخرى نُصَّبَ عليها نظام ويندوز اكس بي (Widows XP) واعتبرت بمثابة مستفيد.

في النهاية يجب بناء بيئة أمنية لحماية المعلومات المنتقلة من خلال الشبكة ما بين العديد من ألحوا سيب المشتركة فيما بينها وبصدد رفع مستوى الحماية إلى الحد المعقول.

الكلمات المفتاحيه: TCP/IP ، لغة الاستفسار الهيكلية (SQL)، Windows NT XP

1. Introduction:

Sensitive data, or information stored on networked servers is at risk from attackers who only need to find any one way inside, or outside the network to access this secret information. Additionally, perimeter defenses like firewalls cannot protect stored sensitive data from the internal threat, employees, and customers with the means to access and exploit this data.
Encryption can provide strong security for data at rest and motion, but developing a database encryption strategy must take many actors into consideration [Website, krelineccrypt, (1)].

Encryption the sensitive data in the database tables before sending them to the client, or before any accessing from client, through the blowfish algorithm that have varying in the key length, provide the normal strength of the security in the protection of the data-in-motion.

2.Encryption of "Data-at-Motion":

Encryption of “data-in-motion” hides information as it moves across the network from the database server to the client application or from the client to the database sever.

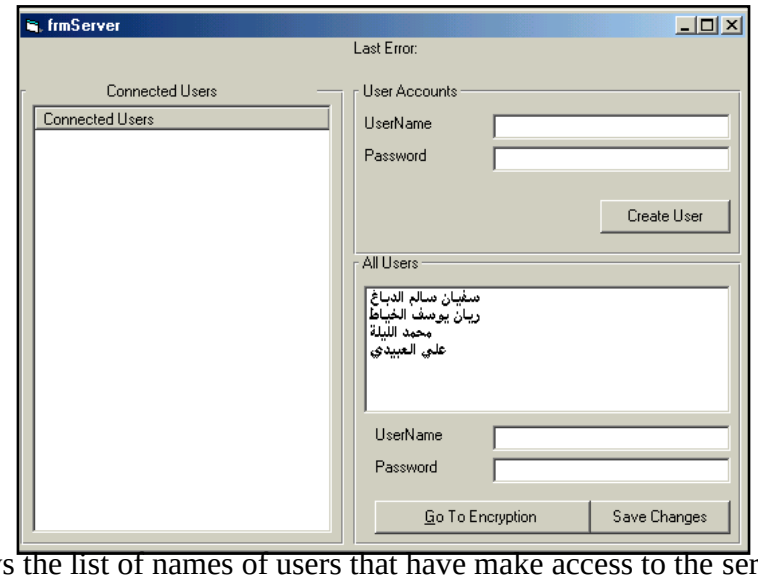
Data-in-motion includes traffic moving over local network, the Internet, or even over a wireless network. The various standards for this type of encryption include SSL (Secure Sockets Layer), TLS (Transport Layer Security) which is developed by Netscape Corporation is widely-used over the internet to give users established digital identities, it is leading security protocol for the internet, and it provides data encryption, data integrity and client/server authentication [An Oracle Company, 1999, (2)], it creates a secure “tunnel” between two points using a combination of data encryption and public/private keys that enable the data to be readable only by the server and the client, and IPSEC (Secure Internet Protocol), which is used in the installing of the protocol security, will be described later. Most database vendors have adopted the SSL standard, and include the ability to send traffic between the client and database vendor over an SSL tunnel using some combination of RSA, RC4 (Random Code), DES, or Diffie-Hellman algorithm [Protegrity, 2001, (3)].

Windows 2000 NT Professional provides two primary methods for securing the “data-in-motion”, which is described during this paper. Finally, there are top five steps to protect data-in-motion [SiGABA, 2002, (4)]:
1. Recognize that security needs.
2. Declare the mobile data a strategic asset.

3. Implement the encryption for both data at rest and motion.
4. Define and enforce content management polices.
5. Educate the users.

3. Customizing the Interface for Server:

In the client/server implementation, onloading database processing to the server, the database server must accept any SQL (Structure Query Language) from the client computer, execute the query and then return the answer to the client computer. The main of the server is described in the following figure, with its accessories, creating a new user, saving any change, and others each time the user has been connected to the database server, displaying its names, with the number that accessed to the server, at connected users list object.



Displays the list of names of users that have make access to the server

Figure 1: The main of the server

Each time the user has been connected to the database server, displaying its names, with the number that accessed to the server, at connected users list object.

If the database administrator want to create a new user, will be given it a name, password and setup his/her privileges.

4. Customizing the Interface for Users:

Because the database's tables contain sensitive data, which need protection from unauthorized access through the network, only a few people can look at all data fields, the program cannot allow every employee, or customer to read the sensitive information such as the social security number, salary, and others.

An application, if it is widely usable, can identify the kinds of access different groups of users require and then customizes itself for each group of users. For example, depending on the company's, policies, secretaries might be allowed to read personal information, such as home phone number and address, but unable to access financial information [Rod, 1997, (5)].

The security of Micro software Access 2000, which is the setting UerLevel Security, is the most flexible and secure method of protecting sensitive data, code, and object design in database application that must be used as developed in access.

Access UserLevel security is similar to the security used in most network environments, such as Microsoft Windows NT Server. When users start access, they enter a name and password in the Logon dialog box [Library of Congress, 1999, (6)].

Access stores information about users and groups in a database is called a workgroup information file. A workgroup information file stores the following:

- The name of each user and group.
- The list of users that makes up each group.
- The encrypted logon password of each user.
- The security identifier (SID) of each user and group.

Permissions that assign to users and groups for the objects in a database are stored in hidden system tables within the database [Library of Congress, 1999, (6)].

Now, the users and group permissions are setup for specific objects likes database, table, query, form, report, and macro, the permissions given to user for a number of operations that described in the table below, including open/run, read design (read data) are modifying design (delete data, insert, update, alter), and administer.

At the beginning, Admin is the default user account, before User Level security is established, all users are automatically logged on using the Admin user account, which owns and has full permissions on all objects

created in the database. When establishing User Level security, it is important to make sure that the Admin user does not own or have any permission on the objects.

The groups created from the User Level security wizard define the users with their names and the password, and at which group working such as (readonly, fullpermissions, and others). There are two types of permissions:

Explicit permissions are permissions granted directly to a user; no other users are affected. Implicit permissions are permissions granted to a group; all users who are members of a group get the permissions assigned to that group [Library of Congress, 1999, (6)]. It is worth noting that a single group has been created, which consists of numbers of users, and the explicit permissions are assigned to them.

Table (1) describes the full permission for the users of the database

Name of User	Password	Permissions			
		Open/run	Read design	Modify design	Administer
Administrator	Mohammad77	√	√	√	√
First-user	Testfirstuser	√	√		
Second-user	Testseconduser	√			

At each accessing to the database from the Micro software Access 2000, the user name of administrator and password must be entered, and this person is the only one having the rights to access the database.

5. The Encryption Algorithm & the User Authentication:

The database administrator wants to encrypt the records, or just one record which that contain the sensitive data; it must Go to Encryption command to work at frmBlowfish form encryption, described in figure 2 below.

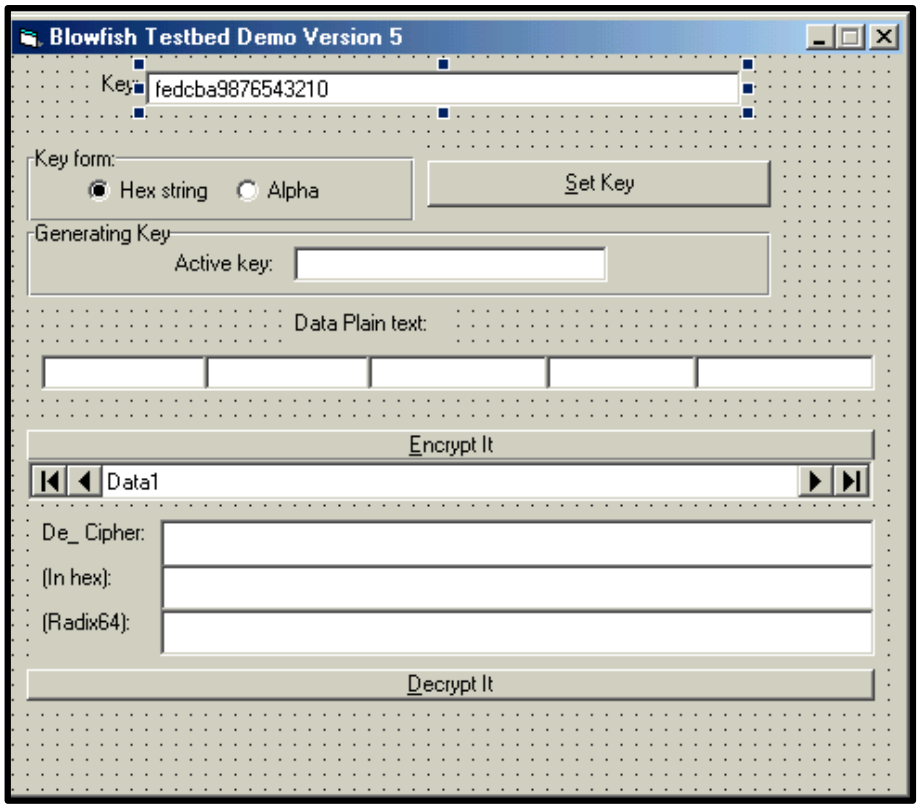


Figure 2: The frm Blowfish form encryption.

Whenever the database administrator begins to encrypt the sensitive data, which is stored in the database, it will be unreadable to client's user that has access to the database server.

Blowfish's form is text cipher that encrypts data in 8-byte blocks which is available in the text object, the form of the Blowfish consists of two parts: the key generation part, which performs in the command bottom (Set, or Generate key). The key generation part converts a variable-length key of at most 56 bytes (448-bits), into several keys arrays totaling 4168 bytes.

All operations are XORs and additions on the 32-bits words. The flow chart in figure 3 describes the structure of the encryption operation.

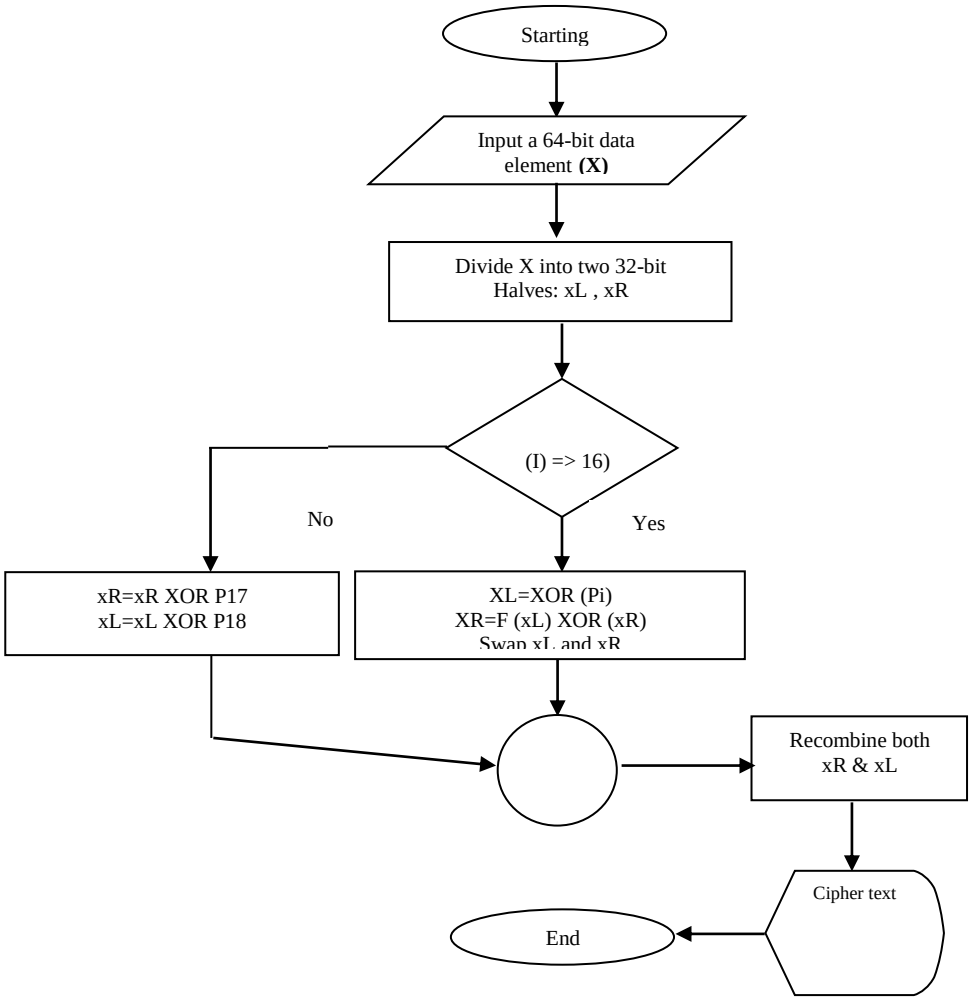


Figure 3: The Flow Chart of Blowfish Algorithm

6. Customizing the Interface for Client:

The secondary form of program is for the client computer, which consists of a number of forms; the graphical interfacing will be described below in the following figures.

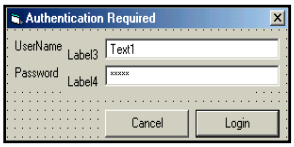


Figure 4.A: Authentication

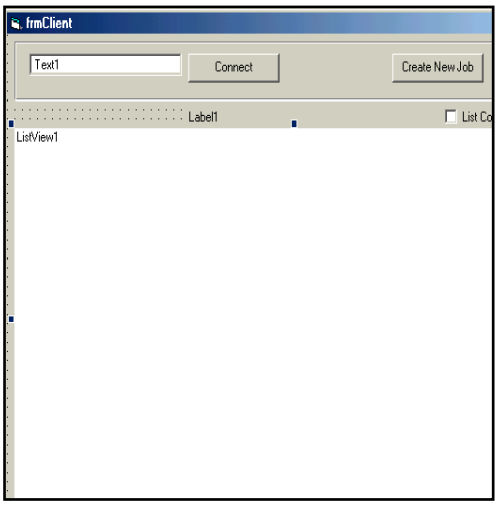


Figure 4.B: Client form

The client/server model implies that there are multiple concurrent user access to the server computer. Each user has a name and a password storing in database table called authentication table, it is necessary to encrypt the whole table with its information, or at least the password field to keep it in safe from the hackers, crackers, or intruders operations, which always drop the table from memory storage.

The work begins from the client computer, user wants to access the server. So, at first the right name of the server or the IP address must be entered, it is (computer1) or (620.20.345.10). Then click the connected command bottom, and wait for minutes to establish the connection between the client and server computers.

At this minute the server, or the claimant ask the user's authentication access methods through displaying the dialog box, about the user name and its password, as shown in figure 4.A above.

At the same time the user enters the name and password, the string's password encrypted by one-way encryption algorithm depending to ACSII

	ID	UserName	Password
	1	سفيان سالم الدباغ	S
	2	يان يوسف الخياط	T
	3	محمد الليلة	M
	4	علي العبيدي	X
▶	(AutoNumber)		

of the characters of password, and then stored inside the database at the authentication table, as shown in figure 5 below.

Figure 5: Authentication Table

When the client has the right access to the database server, each user works with its limited permissions for database table's operations such as creating new person, deleting the full record information of person from the table, modifying, updating, and others, and then sending any changes of information to the database server.

7. Conclusions:

1. Blowfish encryption algorithm can be modified to use for the encryption of the traffic in network.
2. At each time, the length of the key encryption is increased leads to getting more complex security cipher text, with a large number of strings. This may act to the length of field at the database's table, i.e. out of range.
3. By using modern strong authentications methods, such as CRI(Challenge-response identification) more security from the attackers can be obtained.
4. Taking in mind the time optimality for writing the query to obtain a subset of records from one or more tables.

REFERENCES

[1] Web site: Scott A. Banachowski, Zachary N. J. Peterson, Ethan L. Miller & Scott A. Brandt (2002), "**Intra-file Security for Distributed File System**", *Storage System Research Center, University of California, Santa Cruz, CA.*

[2] An Oracle Business White Paper (1999): "**Oracle 8i™ and Internet Security**", *Oracle Company.*

[3] Protegrity (2001): "**The Rule of Database Encryption in Enterprise Security**", *protegrity, Inc., Untied State Of America, Web site: http://www.Protegrity.com/pdf/sd_role_dbenc.pdf.*

[4] SiGABA, Business White Paper (2002): "**Top Five Steps to Protecting Enterprise Data in Motion**", *informational purposes, website: http://www.sigaba.com.*

[5] Rod Stephens (1997): "Advance Visual Basic Techniques", John Wiley & Sons, Inc., Canada.

[6] Library of Congress Cataloging-in-Publication Data (1999): "**Desktop Applications with Microsoft Office Resource Kit**", *Microsoft Corporation, United States of America*.

[7] Thomas Fanghanel (2002): "**Using Encryption for secure data storage in mobile database systems**", *Ph.D. Thesis*, university of Colorado.

[8] Hera (2003): "**Blowfish Algorithm**", *white Paper Web site: http://www.counterpane.com/blowfish.html*