Design and Implementation of an Access Control System for a Bank

تصميم وتنفيذ نظام سيطرة على دخول المصارف

Asst. lecturer /Abbas Fadhil Mohammed Ali
Computer Science Department – College of Science Kerbala University
Abbaszain2003@yahoo.com
المدرس المساعد/عباس فاضل محمد علي
قسم علوم الحاسبات- كلية العلوم - جامعة كربلاء
Programmer / Bushra Jabber Mohammed Jawad
Business Management Department – College of Management and Economy – Kerbala University
Bushra_comp@yahoo.com
المبرمج/بشرى جابر محمد جواد
قسم ادارة الاعمال – كلية الادارة والاقتصاد - جامعة كربلاء

Abstract:

The access control system is a system used for protected information in many international companies , there are many ways to protect information , on of then by using the passwords that we use in this research.In this paper , access control system for a bank was presented , the system depended on different password of authorized persons like the manager , the assistant manager and other employees in charge . It consists of two main parts , the first for the customers and the second for the employees . It has many capabilities such as , add , delete , modify , and search for records .Visual Basic 6.0 , Microsoft Access and ADO tool were used to design the system .

الخلاصة:

في بحثنا هذا قدمنا نظام سيطرة على الدخول للمصارف و اعتمدنا في النظام كلمات المرور للاشخاص المخولين للدخول الى النظام كالمدير ومعاون المدير وبقية الموظفين المخولين .يحتوي النظام على جزئين رئيسيين ، الاول خاص بالعملاء (الزبائن) والثاني خاص بموظفي المصرف ز يحتوي النظام أيضاً على العديد من الامكانيات المتاحة للاشخاص المخولين مثل الحذف ، الاضافة ، التعديل ، والبحث عن أي سجل من سجلات الموظفين والعملاء. استخدمنا من اجل تصميم هذا النظام لغة البرمجة Visual Basic 6.0 و Microsoft Access وادوات الربط ADO

1. Introduction

The primary purpose of security mechanisms in asystem is to control access to information.Until the early 1970 , it was not generally realized that two fundamentlly diferent types of access controls exit.Discretionary access control is the most common: users,at their discretion,can specify to the system whocan access their files.Underdisretionary access controls , a user (or any of the users programs or processes) can choose to share files with other users.

Under nondiscretionary or mandatory access control,users and files have fixed security attributes that are usedby the system to determine whether auser can access afile.The mandatory security attributes are assigned administratively(suhe as by aperson called the securityadmInistrator)or automatically by the oprating system,acccording to strict rules.The attributes cannot be modified by users or their programs.if the system determines that ausers mandatory security attributes are inappropriate for access to acertain file,then nobody-not even the owner of the file-will be able to make the file accessible to that user[2].

2. Access control lists

One of the most effective access control schemes, from a user's perspective, is the access control list, or ACL (usually pronounced 'ackle'), the access control list identifies the individual users or groups of users who may access the file. Because all the access control information for a file is stored in one place and is clearly associated with the file, identifying who has access to a file, and adding or deleting names to the list can be done very efficiently. One alleged disadvantage of an access control list scheme is performance: the access control list has to be scanned each time any user accesses(or opens) a file. But with suitable defaults and grouping of users, access control lists rarely require more than a handful of entries. The only performance penalty might be due to there being an extra disk I/O required to fetch the ACL each time a file is opened. This could have a noticeable impact on systems where large numbers of files are opened in a relatively short time. Another disadvantage is storage management: maintaining a variable-length list for each file results in either a complex diroctory structure or wasted space for unused entries. This tends to be a problem only for systems having huge numbers of very small files (typical of the way in which Unix systems are used). Largely because of the complex management required, only a few systems provide the most general form of access control list. If performance is a problem, one approach is to employ a combination of owner/group/other and access control lists. The access control list is only used for files where the granularity of owner/group/other is insufficient to specify the desired set of users [4].

3. Capability list

Another type of access control is the capability list or access list. A capability is a key to a specific object, along with a mode of access (read, write, or execute). A subject possessing a capability may access the object in the specified mode. At the highest levels in the system, where we are concerned with users and files, the system maintains a list of capabilities for each user. Users cannot add capabilities to this list except to cover new files they create . Users might, however, be allowed to give access to files by passing copies of their own capabilities to other users, and they might be able to revoke access to their own files by taking away capabilities from others (although revocation can be difficult to implement).This type of access control, while much better than passwords, suffers from a software management problem. The system must maintain a list for each user that may contain hundreds or thousands of entries. When a file is deleted, the system must purge capabilities for the file from every user's list. Answering a simple question such as "who has access to this file?" requires the system to undergo a long search through every user's capability list .

The most successful use of capabilities is at lower levels in the system, where capabilities provide the underlying protection mechanism and not the user-visible access control scheme [3].

4. Access Control Techniques

Access control techniques are sometimes categorized as either discretionary or mandatory.

4.1 Mandatory access control

Mandatory access controls prevent some type of Trojan horse attacks by imposing access restriction that cannot be bypassed, even indirectly. Under mandatory controls, the system assigns both subjects and objects special security attributes that cannot be changed on request as can discretionary access control attributes such as access control lists. The system decides whether a subject can access an object by comparing their security attributes. A program operating on behalf of a user cannot change the security attributes of itself or of any object -including objects that the user owns. A program may therefore be unable to give away a file simply by giving other users access to it. Mandatory controls can also prevent one process from creating a shared file and passing information to another process through that file.

Many different mandatory access control schemes can be defined , but nearly all that have been proposed are variants of the U.S. department t of Defense's multilevel security policy consequently, it is difficult to discuss mandatory controls apart from multilevel security. A few general concepts, however, apply to all mandatory policies [1].

Mandatory controls are used in conjunction with discretionary controls and serve as additional (and stronger) restriction on access. A subject may have access to an object only if the subject passes both discretionary and mandatory checks. Since users can not directly manipulate mandatory access control attributes , users employ discretionary controls for their own protection from other users. Mandatory controls come into play automatically as stronger level of protection that cannot be by passed by users through accidental or intentional misuse of discretionary controls.

(MAC) is an access policy determined by the system, not the owner. MAC is used in multilevel systems that process highly sensitive data, such as classified government and military information .

A multilevel system is a single computer system that handles multiple classification levels between subjects and objects.

- Sensitivity labels: In a MAC-based system, all subjects and objects must have labels assigned to them. A subject's sensitivity label specifies its level of trust. An object's sensitivity label specifies the level of trust required for access. In order to access a given object, the subject must have a sensitivity level equal to or higher than the requested object.
- Data import and export: Controlling the import of information from other systems and export to other systems (including printers) is a critical function of MAC-based systems, which must ensure that sensitivity labels are properly maintained and implemented so that sensitive information is appropriately protected at all times [6].

Two methods are commonly used for applying mandatory access control:

A. Rule-based access controls: This type of control further defines specific conditions for access to a requested object. All MAC-based systems implement a simple form of rule-based access control to determine whether access should be granted or denied by matching:

- An object's sensitivity label
- A subject's sensitivity label

B. Lattice-based access controls: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object [2].

4.2 Discretionary access control

Discretionary access control (DAC) is an access policy determined by the owner of afile (or other resource).The owner decides who is allowed access to the file and what privileges they have.

Two important concepts in DAC are

- File and data ownershipe:Every object in a system must have an owner. The access poliy is determined by the owner of the resource (includin files, directories, data, system resources,and devices). Theoretically,can an object without an owner is left unprotected.Normally,the owner of a resource is the pperson who created the resource (such as a file or directory).
- Access rights and permissions: These are the controls that asn owner can assign to individual users or groups for specific resources [7].

Discretionary access controls can be applied through the following techniques:

- A ccess contorl lists(ACLs) name the specific rights and permission that are assigned to asubject for agiven object. Access control lists provide aflexible methode for applying discretionary access controls.
- Role-based acceess control assigns group membership based on organizational or functional roles. This strategy greatly simplifies the management of access rights and permissions:

Access rights and permission for object are asigned any group or,in addition to individuals.Individuals may belong to one or many groups.Individuals can be designated to acquire

Cumuative permissions(every permission of any group they arein) or disqualified from any permission that isn't part of every group they are in [2].

5. Implementation of the system

When the main menu is open , the password (bank) of the system must enter to get in the first window as show in Figure (1) below .

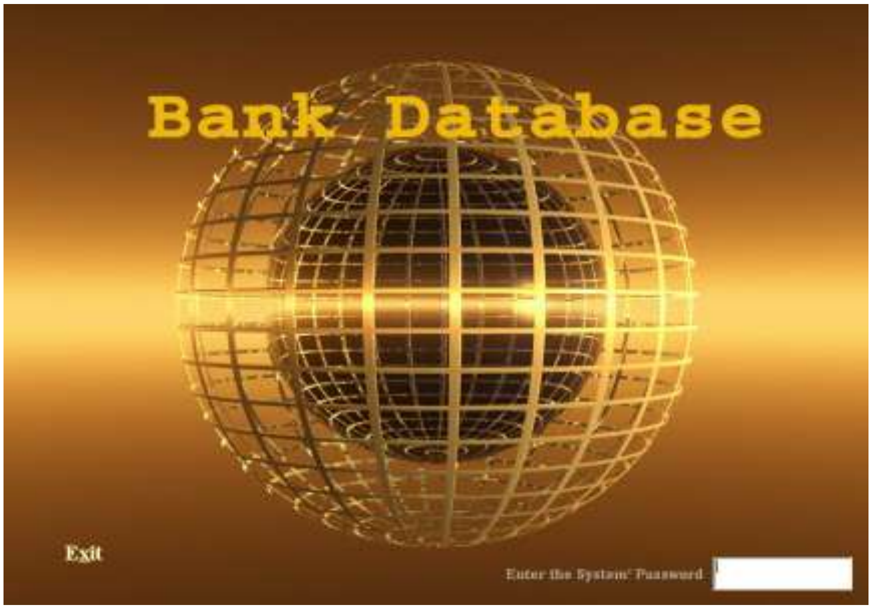


Figure (1): The main password window

Then the window in the Figure (2) below will appear we have four password to enter.

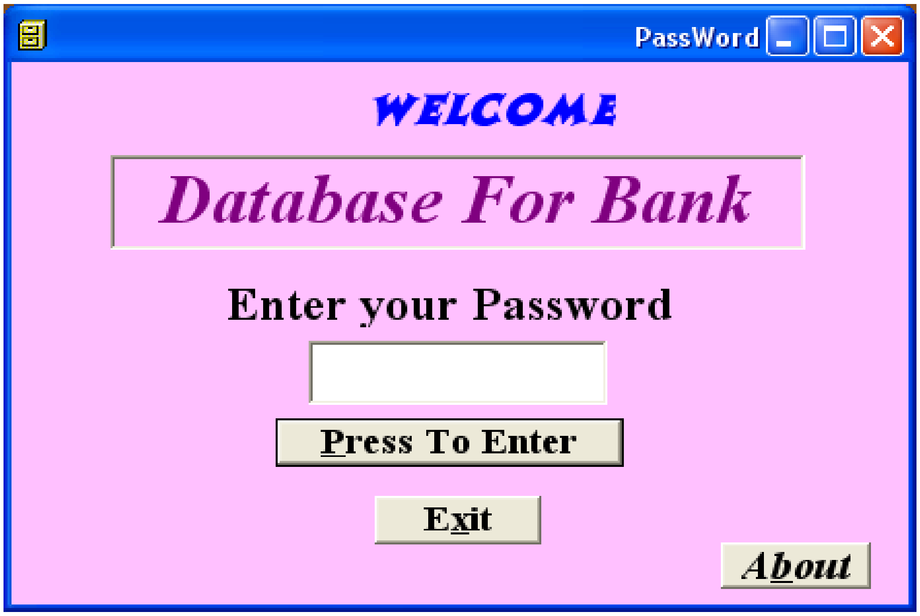


Figure (2) The data base's window

When the Password entered (manager) the window in the figure (2) below will appear .

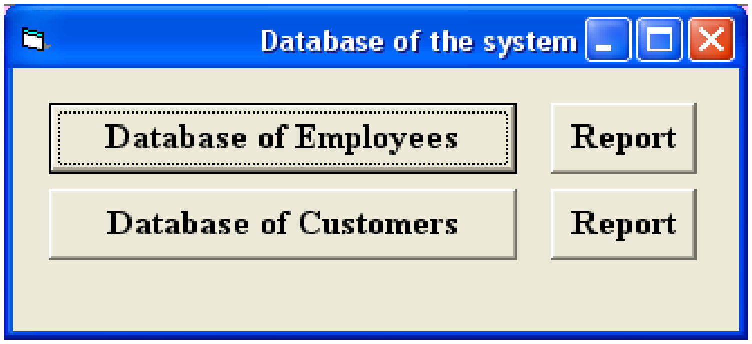
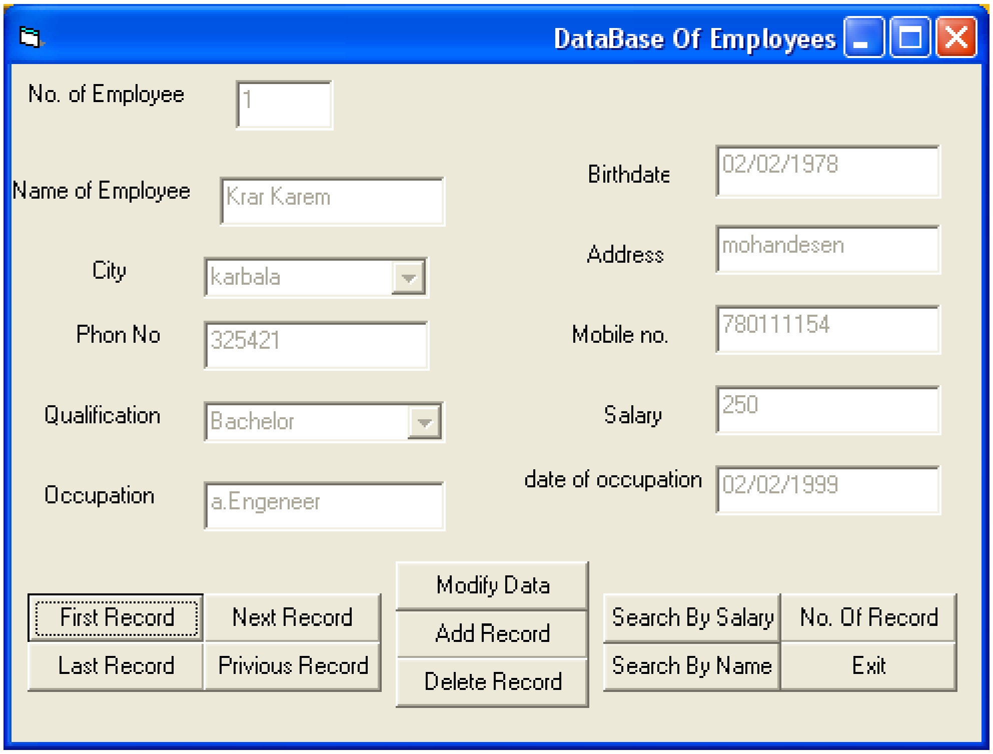


Figure (3) Database of the system windows

This window contains foure choices employees database and customers database and two reports After choosing employees database option the window in the figure (4) below will appears .



No. of Employee 1

Name of Employee Krar Karem

City karbala

Phon No 325421

Qualification Bachelor

Occupation a.Engeneer

Birthdate 02/02/1978

Address mohandesen

Mobile no. 780111154

Salary 250

date of occupation 02/02/1999

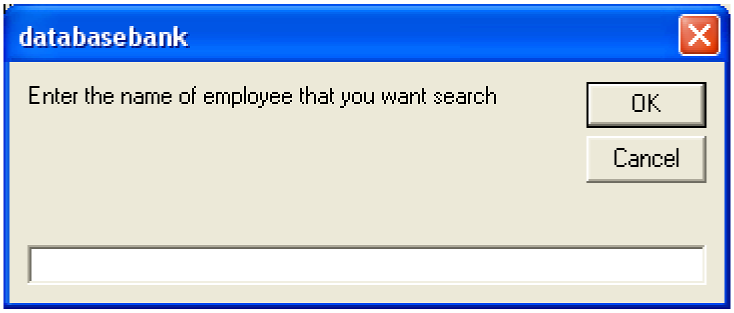
Figure (4) employ's data base of the manager window

The Figure (4) contains the following fields that must fill all :

1- No. of employee
2- Name of employee
3- City
4- Phon no.
5- Qualification
6- Occupation
7- Birthdate
8- Address
9- Mobile no.
10- Salary
11- Date of occupation

The description of the button in the window above are as follows :

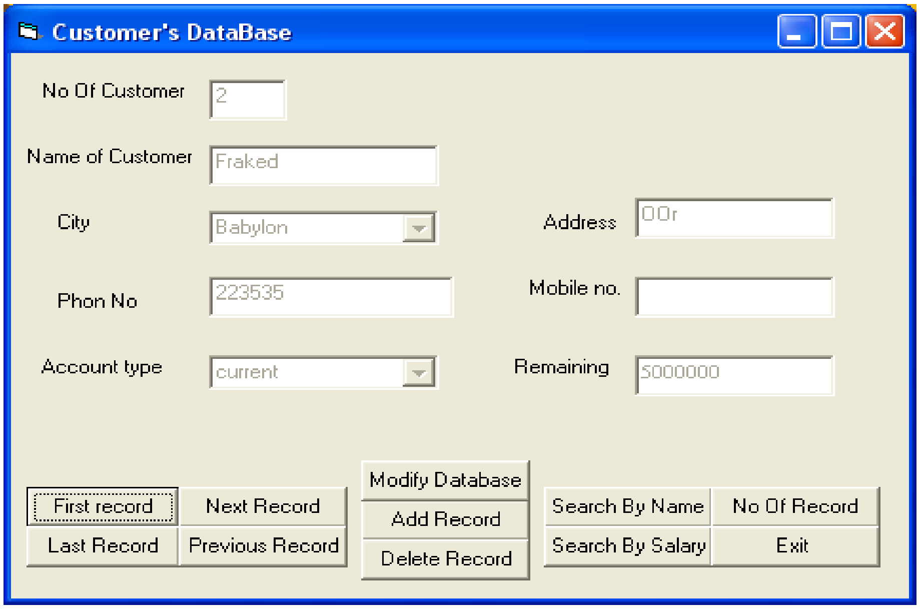
First Record : It displays the database of the first employee and customer .
Last Record : It displays the database of the last employee and customer .
Next Record : It moves to the next record database .
Previouse Record : It moves back to the previous record database .
Search by name : It search for specific name of employee or customer by entering the name in the Dialoge box shown in figure (5) below .



Enter the name of employee that you want search

figure (5) dialoge box for enter the name of employee

Search by salary : It search for the specific employee salary .
Modify: It uses to edit and modify the database by activate all the buttons of the window.
Add : It adds a new database for employee or customer .
Delete : It removes any information from all current record .
No. of records : It displays the number of records of database .
Exit : to exit from the program .
After choosing customers database option the window in the figure(6)below will appears



No Of Customer	2		
Name of Customer	Fraked		
City	Babylon	Address	00r
Phon No	223535	Mobile no.	
Account type	current	Remaining	5000000

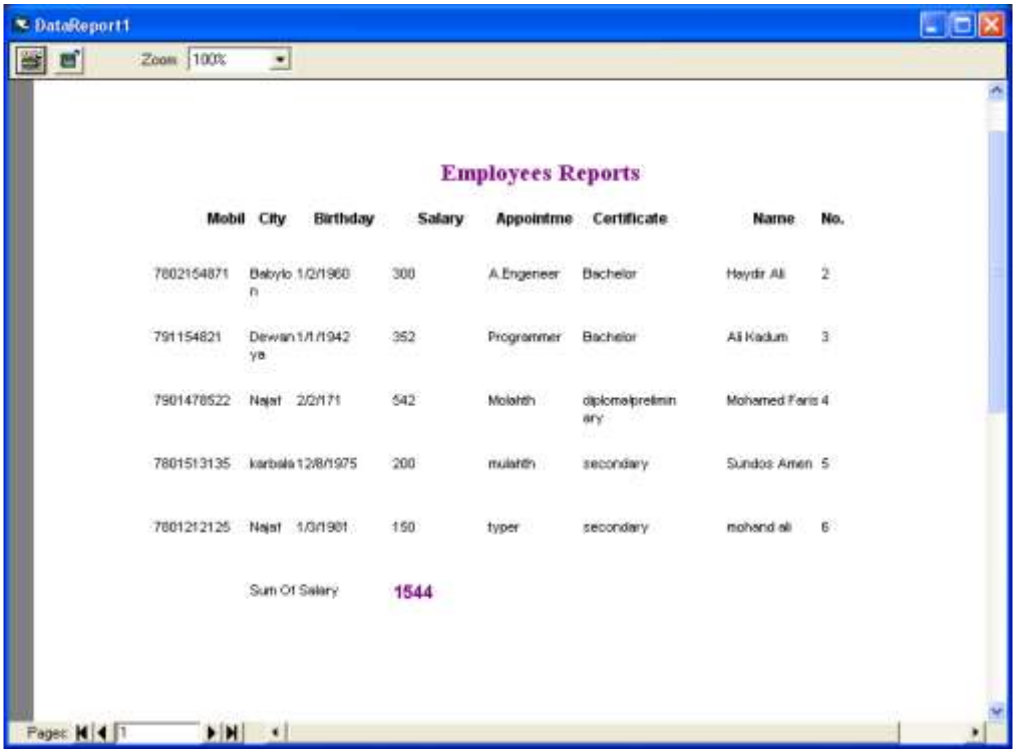
Figure (6) customer's data base of the manager window

The figure (6) contains the following fields that must fill all :
1- No. of customer
2- Name of customer
3- City
4- Address
5- Phon no.
6- Mobile no.

7- Account type
8- Remaning

All procedures done with employees database and windows are similar to the procedures done with customers database .

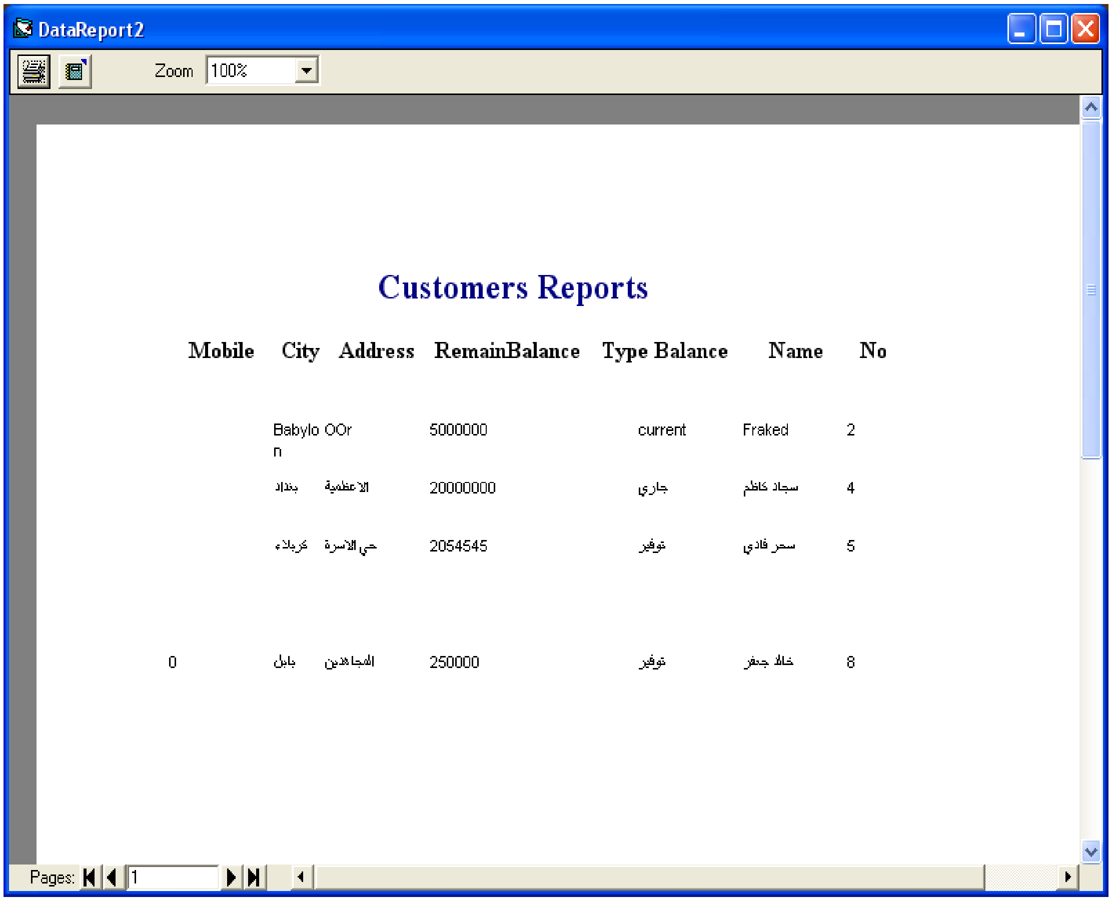
The two report buttons in figure (3) are display all information in the database of the system for employees and customers as shown in figure (7) below, and figure (8) .



Employees Reports

Mobil	City	Birthday	Salary	Appointme	Certificate	Name	No.
7802154871	Babylon	1/2/1960	300	A.Engeneer	Bachelor	Haydr Ali	2
791154821	Dewanya	1/1/1942	352	Programmer	Bachelor	Ali Kadum	3
7901478522	Najaf	2/2/171	542	Molahth	diplomalpreliminary	Mohamed Faris	4
7801513135	karbala	12/8/1975	200	mulahth	secondary	Sundos Amen	5
7801212125	Najaf	1/3/1981	150	typer	secondary	mohand ali	6
	Sum Of Salary		1544				

Figure (7) Employee report window

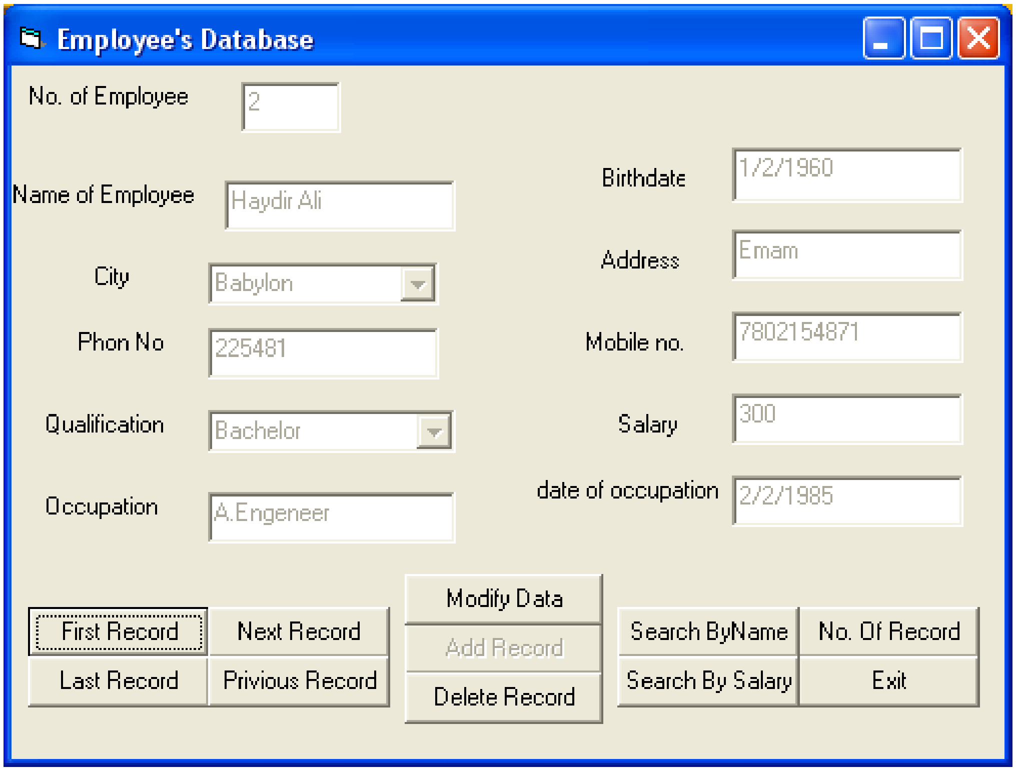


Customers Reports

Mobile	City	Address	RemainBalance	Type Balance	Name	No
	Babylon	OOr	5000000	current	Fraked	2
	بغداد	الاعظمية	20000000	جاري	سجاد كاظم	4
	كربلاء	حي الاسرة	2054545	توفير	سحر فادي	5
0	بابل	المجاهدين	250000	توفير	خالد جعفر	8

Figure (7) Customer report window

In the windows in figure (4) and (6) all the commands are enabled when enter the password of assistant manager (assmanager) then the window in the figure (3) will appear , then when employee's datatbase choosed the window in figure (4) will appear , but the Button Add is unactive that's mean that the assestant's manager can not add new record (or new employee's data) as in window below in figure (8) , and when customer's datatbase choosed the window in figure (6) will appear , but Button Add is unactive that's mean that the assestant's manager can not add new record (or new customer's data)



No. of Employee: 2

Name of Employee: Haydir Ali

City: Babylon

Phon No: 225481

Qualification: Bachelor

Occupation: A.Engeneer

Birthdate: 1/2/1960

Address: Emam

Mobile no.: 7802154871

Salary: 300

date of occupation: 2/2/1985

Figure (8) employ's data base of the assistant manager window

when enter the password of adminstrator (adm) then the window in the figure (3) will appear , then when employee’s datatbase choosed the window in figure (4) will appear , but Buttons Add and Modify are unactive that’s mean that the adminstrator can not add new record and can not modify or edit data in records , and when customer’s datatbase choosed the window in figure (6) will appear , but Buttons Add and Modify are unactive that’s mean that the adminstrator can not add new record and can not modify or edit data in records .

when enter the password of employee (employee) then the window in the figure (3) will appear , then when employee’s datatbase choosed the window in figure (4) will appea , but Buttons Add and modify and delete are unactive that’s mean that the employee can not add new record and can not modify or edit data in records and can not delet records from database , and when customer’s datatbase choosed the window in figure (6) will appear , but Buttons Add and modify and delete are unactive that’s mean that the employee can not add new record and can not modify or edit data in records and can not delet records from database .

6. Conclusions and Suggestions

1- The security system designed for bank to protect the information from any changes that happen by attackers.
2- The system protected by making special password for each person working in the bank .
3- Design the system using another security method different from password .
4- Apply the access control system on another organization .
5- Increasing the size of data base .
6- Add other options to the system depending on the bank needs.
7- Updating information capability is availalble .

References

1- Blotcky , S. Lynch, K.';and Lipner ; S. "SE/VMS: Implementation mandatory security in VAX/VMS . "In proceedings of the 9th National computer security conference, 2000 .

2- Lipner , S. B. "Non-discretionary controls for Commercial Application . "In proceeding of the 1982 symosium on security and privacy ,2001 .

3- Saltzer, J. H. ; and Schroeder; M. D. " The protection of Information in computer system." , 2004 .

4- U.S. federal standard 1037C , 2001 .

5- U. S. National Information System Security Glossary , 2006

6- Darcy, K. , " How to Deploy an Advanced Building Access System " , 2007.

7- Campbell, J. P. , " Door – Access – Control System Based on finger – vein Authentication " , 2006