Journal of Software Engineering and Applications, 2014, 7, 461-469
Published Online May 2014 in SciRes. http://www.scirp.org/journal/jsea
http://dx.doi.org/10.4236/jsea.2014.75043

Scientific Research

Using Database Management System to Generate, Manage and Secure Personal Identification Numbers (PIN)

Dipo Theophilus Akomolafe[1], Babajide Olakunle Afeni[2]

[1]Department of Mathematical Sciences, Ondo State University of Science and Technology, Okitipupa, Nigeria
[2]Department of Computer Science, Joseph Ayo Babalola University (JABU), Ikeji Arakeji, Nigeria
Email: dtakomolafe@yahoo.com

Received 15 December 2013; revised 10 January 2014; accepted 17 January 2014

Abstract

A number of problems are associated with the generation, management and security of PINs, a subset of password. The PINs may be recharge card used by GSM operators or for authentication in ATM. The problems associated with the use of these PINs range from scratching off any of the recharge PIN numbers in recharge card to loss of PIN number or entering invalid number in the case of authentication. It usually takes time for the customer service of the service provider or system administrator to provide convincing solution to these problems promptly when it occurred. PINs generation could seem like simply arranging ranges of number and feeding it into the telecommunication systems such as mobile handsets or ATM to grant access but it requires a specialized and secured way to generate, store and manage it in order to achieve prompt access. This paper focused on the development of database concept to provide solution to these problems by desiging a system by which the PINs generated can be effectively stored and managed so that userss can have immediate access to the PINs if they can provide the identification number on the card. Succintly, the paper discusses the design of a system that generates, manages and secures PINs application using Visual Basic Version 6.0 for designing the front and interface and Microsoft Access 2007 as the database. The system was implemented using real data and the result was successful.

Keywords

Database, Password, Passcode, PINs, GSM, Recharge Card, Numeric, ATM

1. Introduction

A password is a secret word which is characters, numbers or combination of both that is used for access approval to gain access to a resource. Passwords are commonly used nowadays by organizations to prevent unauthorized

How to cite this paper: Akomolafe, D.T. and Afeni, B.O. (2014) Using Database Management System to Generate, Manage and Secure Personal Identification Numbers (PIN). *Journal of Software Engineering and Applications*, **7**, 461-469.
http://dx.doi.org/10.4236/jsea.2014.75043

use of their resoueces by their staff and or clients/customers. It is used by people during a log in process that controls access to protected computeroperating systems, mobile phones, decoders, Automated Teller Machines (ATMs), etc. Global System for Mobile Communication (GSM) is a satellite based facility that largely works wirelessly with its base/terminal remotely location in order to allow effective signal transmission to the device known as handsets. It is an open, digital cellular technology used for transmitting mobile voice and data services [1] [2]. The first GSM network was launched in 1991 by Radiolinja in Finland with network infrastructure provided by Telenokia and Siemens Network which later emerged as Nokia Siemens Network [3] [4]. By the end of 1993, over a million subscribers were using GSM phone networks being operated by seventy (70) carriers across forty eight (48) countries [5]. Portio Research estimates that mobile subscribers worldwide will reach 6.5 billion by the end of 2012, 6.9 billion by the end of 2013 and 8 billion by the end of 2016. Ericsson also forecasts that mobile subscriptions will reach 9 billion by 2017.

GSM technology is not free; it goes with tariff which is remotely and effectively managed by the provider in order to give the users satisfaction. This is achieved by generating PINs which are stored and managed remotely by the provider [6] [7]. The recharge card is a paper card that contains the recharge PINs which is in digits that allows the end user to load credit or top up airtime on the mobile phone. Therefore, the PINs allow the users to make use of the operator's resource for the number of time the PIN is scheduled to last. Even some fixed wireless telecom operators also use recharge cards to enable customers load airtime on their box by dialing the activation code and recharge card PINs [8].

2. Objectives

The primary objective of this research is to use database management system to design a fast, reliable, effective and efficient mode of generating, managing and ensuring the security of recharge card PINS to the telecommunication industry which bis also capable to carry out PIN enquiry in case where customer lose any of the PIN numbers in the process of scratching the card. Other objectives are to:

1) Develop a system to generate PINs number;
2) Enable users manage their PIN number.

Password

A password is a secret word or string of characters that is used for user authentication to prove identity, or for access approval to gain access to a resource. It is necessary to keep password secret from those not allowed access to prevent them from gaining unauthorized access.

The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword, and would only allow a person or group to pass if they knew the password. In modern times, user name and passwords are commonly used by people during a log in process that controls access to protected computer resources, mobile phones, cable TV, decoders, Automated Teller Machines (ATMs), etc. A typical computer user for example has passwords for many purposes such as logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online. Despite the name, there is no need for passwords to be actual words; indeed passwords which are not actual words may be harder to guess, a desirable property. Some passwords are formed from multiple words and may more accurately be called a passphrase. Some passwords may be purely numeric or alphanumeric. The term passcode is sometimes used when the secret information is purely numeric, such as the Personal Identification Number (PIN) commonly used for ATM access and recharge cards. Passwords are generally short enough to be easily remembered and typed.

3. Generation of PIN Number

A **Personal Identification Number (PIN)** is a secret numeric number shared between a user and a system that can be used to authenticate the user to the system. Upon receiving PIN, the system looks up the PIN and compares the locked-up PIN with the received PIN. The user is granted access only when the number entered matches with the number stored in the system. Hence, despite the name, a PIN does not personally identify the user.

The concept of a PIN originates with the inventor of the ATM; John Shepherd-Barron sometime in 1967 as a more efficient way banks could disburse cash to their customers. For authentication Shepherd-Barron at first en-

visioned a six-digit numeric code, given what he could reliably remember. His wife however preferred four digits, which became the most commonly used length in the banking sector. ISO 9564-1, the international standard for PIN management and security, allows for PINs from 4 up to 12 digits, but also notes that "For security reasons, an assigned numeric PIN should exceed six digits in length" [9].

The earliest methods for generating random numbers—dice, coin flipPINg, roulette wheels—are still used today, mainly in games and gambling as they tend to be too slow for most applications in statistics and cryptography [10]. A physical random number generator can be based on an essentially random atomic or subatomic physical phenomenon whose unpredictability can be traced to the laws of quantum mechanics. However, physical phenomena and tools used to measure them generally feature asymmetries and systematic biases that make their outcomes not uniformly random. A randomness extractor, such as a cryptographic hash function, can be used to approach a uniform distribution of bits from a non-uniformly random source, though at a lower bit rate.

In 2010 a team at Bar-Ilan University in Israel was able to create a physical random bit generator at a 300 Gbit/s rate, making it the fastest ever [11]. While people are not considered good randomness generators upon request, they generate random behavior quite well in the context of playing mixed strategy games. Some security-related computer software requires the user to make a lengthy series of mouse movements or keyboard inputs to create sufficient entropy needed to generate random keys or to initialize pseudorandom number generators.

The major flaw of physical method in generating PIN numbers is that considering the huge numbers of recharge card to be generated a day in Nigeria for example, this method is very slow and then this makes it unsuitable. Also organizations with a large number of employees may find this method too slow to handle their employees PIN requirement.

4. 3624 PIN Generation Algorithm

This algorithm generates n-digit PIN based on an account-related data or person-related data, namely the validation data. The assigned PIN length parameter specifies the length of the generated PIN. The algorithm requires the following input parameters:

- A 64-bit validation data;
- A 64-bit decimalization table;
- A 4-bit assigned PIN length;
- A 128-bit PIN-generation key.

The service uses the PIN generation key to encipher the validation data. Each digit of the enciphered validation data is replaced by the digit in the decimalization table whose displacement from the leftmost digit of the table is the same as the value of the digit of the enciphered validation data. The result is an intermediate PIN. The leftmost n digits of the intermediate PIN are the generated PIN, where n is specified by the assigned PIN length.

5. PIN Generation and Verification Techniques

There are a number of techniques for PIN generation and verification depending on the system, purpose and manufacturer. The IBM CCA supports a representative sample, shown in **Figure 1**. The IBM 3624-Offset method in more detail as it is typical of decimalisation table uses [12]. There are several main methods of validating PINs. Some required operations are usually performed within a Hardware Security Module (HSM).

6. IBM 3624

The IBM method is used to generate what is termed a natural PIN. The natural PIN is generated by encrypting the Primary Account Number (PAN), using an encryption key generated specifically for the purpose. This key is sometimes referred to as the PIN generation key (PGK).

7. IBM 3624 + Offset

To allow user selectable PINs it is possible to store a PIN offset value. The Offset is found by subtracting natural PIN from the customer selected PIN using modulo 10. For example, if the natural PIN is 1234, and the user

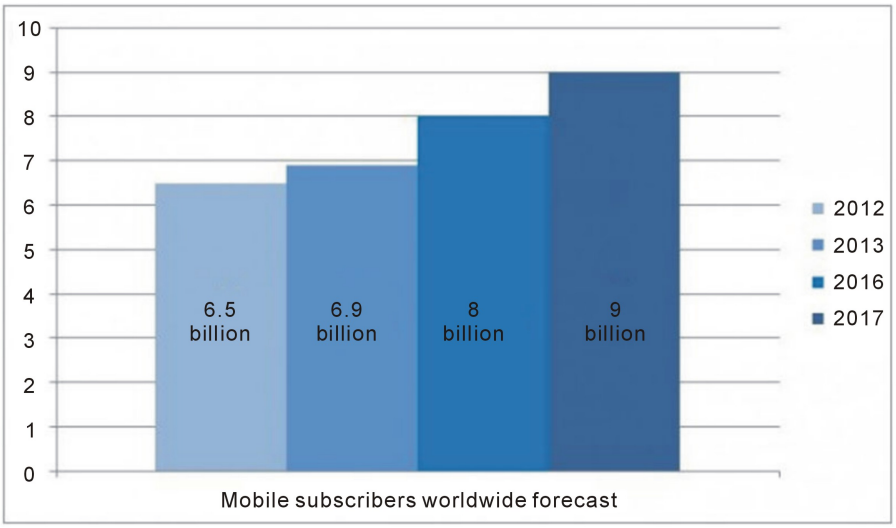

Figure 1. Mobile subscribers worldwide forecast.

wishes to have a PIN of 2345, the offset is 1111. The offset can be stored either on the card track data, or in a database at the card issuer. To validate the PIN, the issuing bank calculates the natural PIN as in the above method then adds the offset and compares this value to the entered PIN.

8. VISA Method

The VISA method is used by many card schemes and is not VISA-specific. The VISA method generates a PIN Verification Value (PVV). Similar to the offset value, it can be stored on the card's track data, or in a database at the card issuer. This is called the reference PVV. The VISA method takes the right most 11 digits of the PAN excluding the checksum value, a PIN validation key index (PVKI) and the required PIN value encrypted with the PIN validation key (PVK) referenced by the PVKI. From this encrypted value, the PVV is found. To validate the PIN, the issuing bank calculates a PVV value from the entered PIN and PAN and compares this value to the reference PVV. If the reference PVV and the calculated PVV match, the correct PIN was entered.

Unlike the IBM method, the VISA method doesn't derive a PIN. The PVV value is used to confirm the PIN entered at the terminal and was also used to generate the reference PVV. The PIN used to generate a PVV can be randomly generated or user selected or even derived using the IBM method.

9. PIN Security

Financial PINs are often 4-digit numbers in the range 0000 - 9999, resulting in 10,000 possible numbers. Switzerland is a notable exception with 6 digit PINs being given by default. However, some banks do not give out numbers where all digits are identical (such as 1111, 2222,...), consecutive (1234, 2345,...), numbers that start with one or more zeroes, or the last 4 digits of your Social Security Number. Many PIN verification systems allow three attempts, thereby giving a card thief a 0.06% probability of guessing the correct PIN before the card is blocked. This holds only if all PINs are equally likely and the attacker has no further information available, which has not been the case with some of the many PIN generation and verification algorithms that banks and ATM manufacturers have used in the past.

Zielinski and Bond (2003) [13] in their PhD research discovered a security flaw in the PIN generation system of the IBM 3624, which was duplicated in later hardware. Known as the decimalization table attack, the flaw would allow someone who has access to a bank's computer system to determine the PIN for an ATM card in an average of 15 guesses [14].

10. System Design

This work is carried out to make available a fast, reliable, effective and efficient mode of generating, managing and ensuring the security of recharge card PINS to the telecommunication industry which will be able to carry

out PIN enquiry in the case where customer lose some of the PIN numbers in the process of scratching the card.

Survey of DBMS: Various Database Management Systems (DBMS) are available to handle the task of creating, storing, accessing and maintaining files and database records [15]. Database Management had been simplified in [16]. Available packages of relational systems for mainframes, minicomputers and microcomputers include: INGRES, RAPPORT, R-BASE, PARADOX, MS Access, MS SQL Server, My sql, Oracle. Microsoft Access was chosen for this work because it is accessible in term of distribution with versions of Microsoft Office. MS Access version 2007 is chosen for carrying out this work.

System Modules: All GSM operators do have a billing system adopted to bill customers for the duration of the time used [17]. This software application is designed to generate recharge card PINs of various amount such as N100, N200, N500, and N1000 as the operator desire. Subsequently, on providing the identification number of the recharge card which is also generated with the PINs the authentic PIN can be traced with the appropriate access rights. The system comprises of the following modules:

1) PIN Generation;
2) Card Loading Simulator;
3) PIN Enquiry;
4) View Generated PIN;
5) Add New User;
6) Print Generated Card;
7) Edit User Password.

The operator of this system can generate the recharge card PIN by stating the actual amount and the quantity. The system can be used for monitoring/tracking the PIN generated each day. This information will be useful to determine the authenticity of the generated PIN. The PIN enquiry module can be used to enquiry the actual PIN by providing the identification number of the card. A number of reports can be generated from the system from ready-made reports and impromptu reports. The system also includes an enquiry screen to list users. The add new user and the edit password modules include facility for setting up users and entering system parameters.

This new system design among other things possesses the following characteristics:

1) It meets the ultimate user's need;
2) It is cost effective;
3) The design is highly user's friendly. It is not ambiguous at all;
4) It is flexible such that it can be easily modified to meet future changes/demands;
5) It is maintainable with a comprehensive and precise system documentation/manual.

The Input Design: One of the major components of any system is the input. The input to any system is pivotal to the desired outcome of the system [18]. User's-friendly interfaces were developed in this research to enable user's supply the required inputs and appropriate codes were also written in order to enable the computer carryout processing operations that guarantees the expected result (output). The inputs to this system are to be stored into the database. Appropriate processing operations are applied to these inputs and the results are stored into the database where required reports can be generated.

Database Design: A database is an organized collection of data for one or more purposes, usually in digital form. The data are typically organized to model relevant aspects of reality in a way that supports processes requiring this information.

Below is the description of the tables contained in the Microsoft Access database used for the application.

11. PIN Table

This table (**Table 1**) is used to store the generated PINs.

12. Userstable

This is used to store the authorized Users (**Table 2**).

The Output Design: The expected output of the application is to produce the list of recharge card PINs generated which is carried out by the authorized user(s). This is very vital as it is used to determine the consistency, accuracy, reliability, security and effectiveness of a system. If there is any amendment to be made to the system, the output to a large extent dictates it. The output is simply the desired result expected by the system to generate. The following are some of the expected output to be generated by this system:

Table 1. PIN table.

Field Name	Data Type	Size/width
IdentificationNo	Text	10
PINNumber	Text	12
DateGenerated	Date/Time	
UserID	Text	10
Amount	Text	4
SerialNum	AutoNumber	

Table 2. User table.

Field Name	Data Type	Size/width
UserName	Text	12
Password	Text	12
UserCategory	Text	12

1) Amount of recharge card ranging from N100.00, N200.00, N500.00 and N1,000.00;

2) Details of generated recharge cards such as date, by whom, and serial number which is unique to each generated PIN.

The Softcopy is produced on the Visual Display Unit, and the Hardcopy which is one generated by the Printer is printed out as recharge cards.

13. System Requirements and Installation

The system requirements that will enhance efficient performance is divided into two parts: Hardware Requirements and Software Requirements

Hardware Requirements: The system is made up of the following hardware configurations for effectiveness and best performance.

- Pentium IV 1000 MHz Processor, 1G RAM, 120GB HDD, CD ROM;
- SVGA Monitor;
- Uninterruptible Power Supply (UPS);
- Printer.

Software Requirements: The required Operating Systems (OS) is any Window XP or Window 7. They are suitable for installation and will serve as platform on which the new designed application will be installed.

The implementation language is Microsoft Visual Basic 6.0. It is used for the development of the interfaces and their appropriate codes. This programming language is used to provide effective link with Microsoft Access which serves as the database for storing the generated PIN and other details.

System Installation

The basic steps for installing the application are:

- Load the recharge card generation and management application CD into the CD ROM of the computer system;
- Click on run program from the auto run;
- Click next specify the path of installation;
- Follow all the instruction displayed to complete the installation;
- Type in the password as the administrator who manages the application;
- Click on finish and restart the computer;
- After restarting, a short cut icon can be created on the desktop from the start-program menu;
- Load the icon and click on generate recharge card menu to perform the task.

The program design is in modular forms. Modular programming emphasizes the principle as well as the methodology used by programmers by breaking down a large task into small functional parts knows as subprogram. Subprogram is also known as sub system in system analysis. Each of the modules is developed, tested, and completed independently before they are combined with the other ones in the final product. Each unit is designed to perform a particular task or function and can thus become part of a library of modules that can often be

reused in other products that have similar requirements. In this instance, each module performs a unique operation in the whole system.

As greater effort is been required in the overall system design, the same effort is used in the program design. The program design involves the use of Microsoft Visual Basic 6.0 Integrated Development Environment (IDE) for the development of t he interfaces, appropriate VB codes are also written in conjunction with these interfaces for the accomplishment of the tasks to be performed by each of these interfaces. An Interface on its own without appropriate codes cannot guarantee desired/expected result.

14. Description of Interfaces

1) PIN Generator

This interface is used to generate new PIN numbers as desired. **Figure 2** shows the form for designing the PIN generator.

2) PIN Enquiry

This interface shown in **Figure 3** is used to make enquiry about status of the generated PINs and also to search for PIN number using the identification number.

3) Search PIN

This interface is used to display PIN generated with other details. The interface shown in **Figure 4** is also used to search PIN, the date it was generated and the value of the PIN.

4) Add New User

This interface is used to add new user to the system. The interface is as shown in **Figure 5**.

5) Edit User's Password

This interface is used to change user's password. It is impossible to change user's password without using the form shown in **Figure 6**.

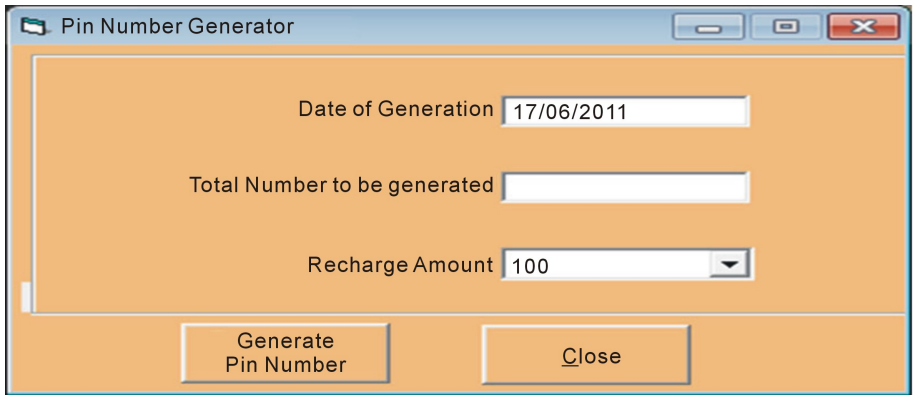

Figure 2. PIN generator.

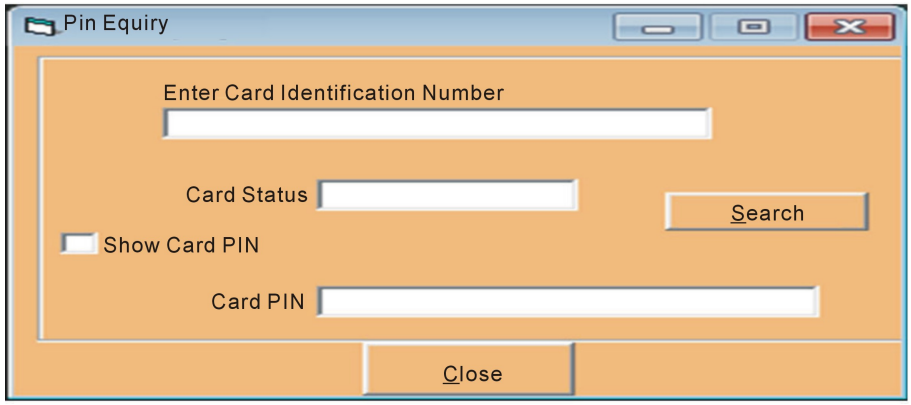

Figure 3. PIN enquiry.

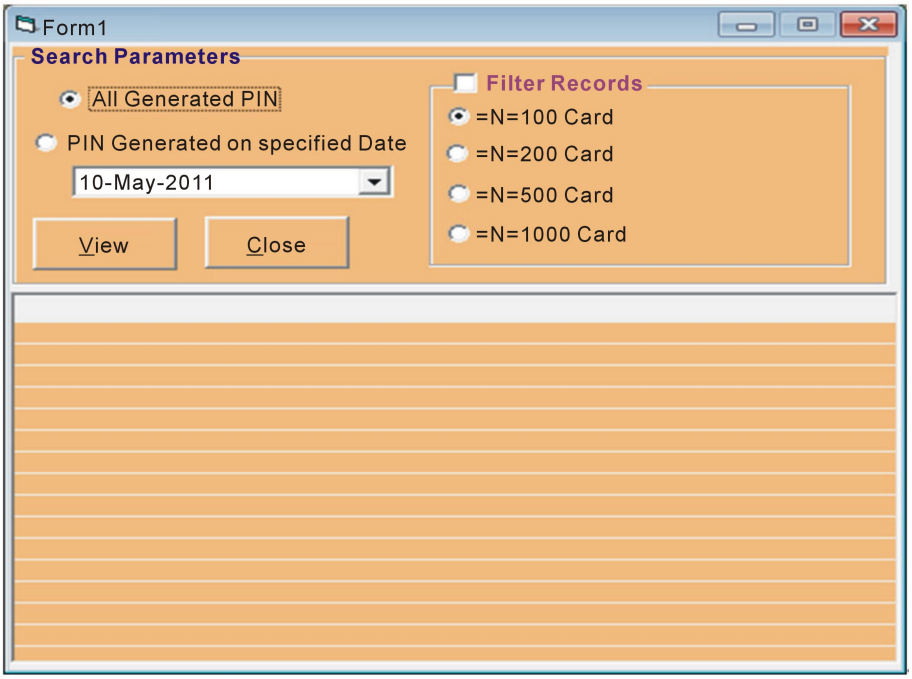

Figure 4. PIN search form.

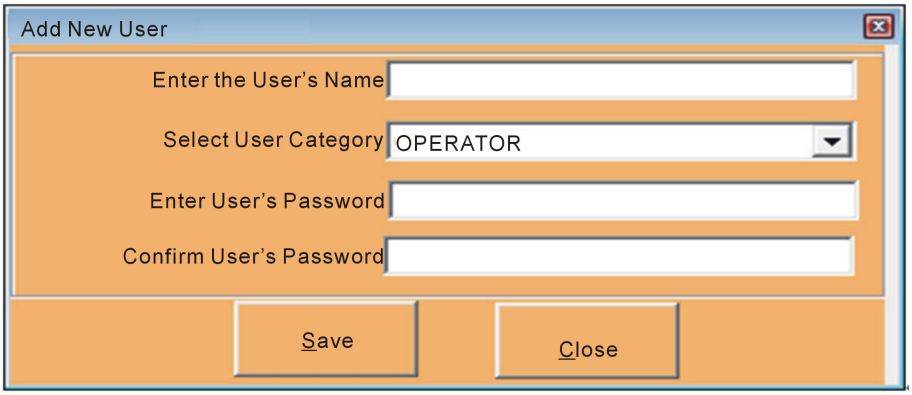

Figure 5. Add new user form.

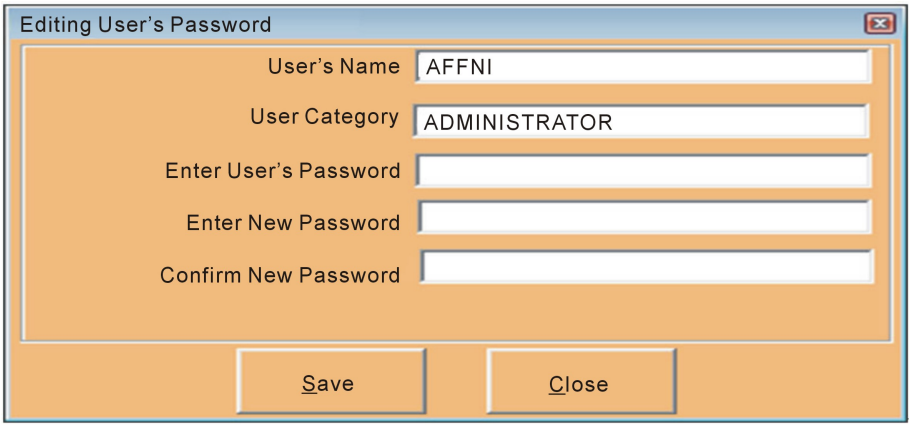

Figure 6. Password edit form.

15. Conclusion

Within the context of utilisation this application system can be of tremendous help in solving some of the identified problems in generating and managing recharge card PINs and PIN enquiries by the telecommunication companies. The developed system can be packaged and improved upon to become a standard one that can be deployed for commercial use. To realise this however, there is a need to carry out activities such as Data test, User acceptance testing, System Review and Deployment. The documented processes in this paper are also good source of information for further database system development and data analysis. The foremost focus of this project is the generation and appropriate management of recharge card. Having identified that simple but effective and secured database will improve the challenge of invalid recharging which occasionally comes up during loading, a database using the method of concatenation and randomization of 12 digits has improved and enhanced smooth performance.

References

[1] Williams, K.B. and Sawyer, S.C. (1999) Using Information Technology, a Practical Introduction to Computers and Communications. 3rd Edition, McGraw Hill, New York.

[2] Sopan, T. (2004) Evolution of the Mobile Technology. Instant Book, New Delhi.

[3] Wikipedia Encyclopedia (2007) Billing in Mobile Communication. www.wikipedia.org

[4] Encyclopaedia Britannica (2007) Student and Home Edition.

[5] Hatem, M. (2006) Introduction to Billing Systems. Design and Strategy Articles, USA.

[6] Stephen, R.S. (1996) Classical and Object-Oriented Software Engineering. McGraw-Hill, New York.

[7] Pressman, R.S. (2005) Software Engineering A Practitioner's Approach. 6th Edition, McGraw-Hill, New York.

[8] Georgia, A.T. (2010) Applications of PIN Numbers. Prisma Book. Pub. Ltd., Marlborough, 12-14.

[9] Lawrence, H. (2006) Introduction to Mobile Telephone Systems. 2nd Edition, Instant Book, New Delhi.

[10] Walker, J. (2009) Generation of Genuine Random Numbers. 4th Edition, Landmark Publication, Cedarburg.

[11] Mathwork, T. (2009) Common Generation Methods. Jasper Publisher Ltd., London.

[12] Anderson, R. (2008) PIN Generation and Verification Techniques. Jaype Publishers Ltd., New Delhi.

[13] Zieliński, P. and Bond, M. (2003) Decimalisation Table Attacks for PIN Cracking. University of Cambridge Computer Laboratory, Hill, UK.

[14] Brown, J.S. (2010). Issues of PIN Security. Cephas Publishing and Co., UK.

[15] David, M.K. (2000) Database Processing. 7th Edition, Macedonia and Evans, London.

[16] Microsoft Encarta (2010) Definition of Terms; Database Management.

[17] Sasha, V.R. (2009) Technology of Subscriber Identity Module (SIM) Card. Berlin.

[18] Perly, G. (1998) Visual Basic Programming Language. 4th Edition, Wesley Publishing, Tokyo.