UNIVERSITI PUTRA MALAYSIA

DEVELOPMENT OF A BARCODE-BASED KEY SYSTEM

FARHANG PADIDARAN MOGHADDAM

FK 2009 13

DEVELOPMENT OF A BARCODE-BASED KEY SYSTEM

By

FARHANG PADIDARAN MOGHADDAM

**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia,
in Fulfilment of the Requirements for the Degree of
Master of Science**

July 2009

To my beloved parents and my brother, without whose blessing I would never have reached this position in life.

Abstract of thesis presented to the senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

DEVELOPMENT OF A BARCODE-BASED KEY SYSTEM

By

FARHANG PADIDARAN MOGHADDAM

July 2009

Chairman: Prof. Mohamed B. Daud, PhD

Faculty: Engineering

This study provides a Web-based solution for issuing online key and accessing to disconnected areas which are disconnected from any server or portal. In some locations there is no facility for connecting to server, because of inaccessibility or cost of network connection. Beside, the key must be generated in the easiest way for customer's convenience. Online users can book and reserve their desired room or can purchase their coveted event's ticket by the internet easily. The thesis gives reliable solution to design a method and system for generating access code and issuing the key or ticket with offering a safe and reduced cost way. The issued key is perceptible for offline and standalone lock system. Barcode has been chosen, according to its advantages, such as cheapness, simple product and ease of use. The Verifier Machine can be located at each venue entry point are standalone devices, and are not connected in any way neither among them nor to any central database, server or portal. Functionality of simulator application in generating the access code, ability of portal in issuing barcode form key, stability of printed key and capability of demonstrated standalone machine in decrypting and verifying was tested successfully. The achieved system presents a simple, low cost, and flexible method for authorization and authentication in accessing doors at remote areas.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

PEMBANGUNAN SISTEM KUNCI BERASASKAN KOD BAR

Oleh

FARHANG PADIDARAN MOGHADDAM

July 2009

Pengerusi: Prof. Ir. Mohamed B. Daud, PhD

Fakulti: Kejuruteraan

Kajian ini memberi penyelesaian berteraskan Internet bagi menjana kekunci '*online'* dan akses pada kawasan-kawasan luar liputan yang tidak terhubung dengan mana-mana '*server'* mahupun portal. Sesetengah lokasi tiada kemudahan untuk berhubung dengan '*server'* kerana tiada akses atau kos kepada koneksi jaringan. Lagipun, kekunci mestilah dijana dengan cara yang paling mudah demi keselesaan pelanggan. Dengan ini, pengguna '*online'* boleh menempah penginapan mereka atau membeli tiket melalui Internet dengan mudah. Thesis ini menyediakan penyelesaian yang bernas bagi mencipta satu kaedah dan sistem yang boleh mewujudkan kod akses dan kekunci atau tiket dengan cara yang selamat dan murah. Kekunci yang diutarakan boleh digunapakai untuk sistem kuncian *'offline'* dan *'standalone'*. Penggunaan *'barcode'* telah dipilih berdasarkan beberapa keistimewaannya, seperti kos yang rendah, dan kemudahan penggunaannya. Mesin Verifikasi yang boleh diletakkan pada tiap lokasi adalah alat ‘*standalone*’ dan tidak terhubung sama ada antara satu sama lain ataupun dengan ‘*database*’, ‘*server,* mahupun portal induk. Praktikaliti aplikasi simulator dalam menjana kod akses, kebolehan portal dalam memberi kekunci borang kod bar, kestabilan kekunci yang dicetak dan kebolehan mesin ‘*standalone*’ yang didemonstrasikan dalam membezakan dan mengesahkan isyarat telah diuji dengan jayanya. Sistem yang dicipta ini memberikan kaedah yang mudah, murah dan fleksibel untuk kebenaran dan pengesahan dalam memberikan akses pada kawasan terpencil.

ACKNOWLEDGEMENTS

The author would like to express his thank and gratitude to the members neither of his supervisory committee, Prof. Dr. Mohamed B. Daud, Assoc. Prof. Dr. Abdul Rahman B. Ramli, and Assoc. Prof. Dr. Abdul Azim B. Abd Ghani, for their advice, guidance, support, and encouragement throughout this study. They have also offered their valuable comments and suggestions, which played vital roles in completing the thesis successfully.

Many people contributed to this work by providing their advice, support, and encouragement. The author would like to thank his father, mother, brother, students, and all his friends.

I certify that an Examination Committee has met on 26/07/2009 to conduct the final examination of Farhang Padidaran Moghaddam on his Master of Science thesis entitled "DEVELOPMENT OF A BARCODE-BASED KEY SYSTEM" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulation 1981. The committee recommends that the student be awarded the relevant degree.

Members of the Examination Committee were as follows:

Adznan b. Jantan, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Salasiah bt. Hitam, PhD
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

M. Iqbal b. Saripan, PhD
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

H.M Suzuri, PhD
Faculty of Engineering
Universiti College of Science and Technology, Malaysia
(External Examiner)

HASANAH MOHD.GHAZALI, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of Supervisory Committee were as follows:

Mohamed B. Daud, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Abdul Rahman B Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Abdul Azim B Abd Ghani, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

HASANAH MOHD.GHAZALI, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 10 December 2009

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

FARHANG PADIDARAN MOGHADDAM

Date:

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure **Page**

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
ASP	Active Server Page
BASIC	Beginner's All purpose Symbolic Instruction Code
BIN	Bank Identification Number
C	high-level programming language
CAN	Controller Area Network
CMOS	Complementary Metal-Oxide Semiconductor
CSS	Customer Service Station
DC	Direct Current
DES	Data Encryption Standard, a cryptographic block cipher
DSS	Digital Signature System
EDL	Electronic Door Lock
EDLP	Electronic Door Lock Programmer
EEPROM	Electrically Erasable Programmable Read Only Memory
FTP	File Transfer Protocol
HHC	Hand Held Controller
HTML	Hypertext Markup Language
ID-card	Identification card
IIS	Internet Information Server
ISO	International Organization for Standardization
IT	Information Technology
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LPT	Line Printer, Printer Port

MAC	Message Authentication Code
MHz	Mega Hertz
MIPS	Million Instructions per Second
MPC	Multiparty Computation
MSAC	Monitoring System and Access Control
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy, a computer program for the encryption
PHP	Perl Hypertext Preprocessor
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRBG	PseudoRandom Bit Generating
QB	Quick Basic
RAD	Rapid Application Development
RAM	Random Access Memory
RFC	Request for Comments
RFID	Radio Frequency Identification Device
RISC	Reduced Instruction Set Computer
RSA	initials of these surnames : Rivest, Shamir, Adleman
SDLP	Distributed Lock Protocol
SSC	Spread Spectrum Communication
UART	Universal Asynchronous Receiver/Transmitter
UIP	Universal Interface Programmer
UPC	Universal Product Code
UTP	Unshielded Twisted Pair
VB	Microsoft Visual Basic

CHAPTER 1

INTRODUCTION

1.1 Preface to lock systems

Traditionally, locksmiths and installers have developed their skills around conventional mechanical devices, while access control companies concentrating on electronic or computer controlled systems. Electric lock technology falls between these two areas of expertise and as a result installers and specifiers at both ends of the scale have generally found it a struggle to specify electric locks correctly (Norman, 2007). This need no longer is the case as the new generation of electric locks provides specifiers, installers and end users alike with a wide range of desirable features and functions. For example, not only does this technology improve levels of security, but it is easy to install and offers the opportunity to comply with the latest legislation governing disabled access to buildings. Electric locks are versatile and suitable for use in a wide variety of applications. They provide physical strength that keeps out unauthorized persons, while offering convenience for legitimate users and safety for those who may need to escape from a building in the case of an emergency (Tonbridge, 2006).

Due to the increasing popularity of the Internet (Li and Law, 2007), more and more travelers have moved their information search and travel arrangements activities online. Despite hotels' initial hesitancy toward adopting new information technologies (Law and Jogaratnam, 2005), in recent years, they have been making great efforts to enhance their electronic distribution. This strategy allowed hotels to take advantage of two main directions: first, the Internet has offered an opportunity for hotels to sell and advertise online and use a cheaper distribution system (O'Connor and Frew, 2004) and second, the Internet has created an opportunity for hotels to reduce their mass advertising and allowed them to concentrate on customized marketing messages (Lau *et al*., 2001).

Using the Internet as a reservation method can benefit the hospitality firms and also the customers by reducing costs and providing real-time information to both parties. According to (Cobanoglu, 2001), business travelers still use travel agents as their favorite hotel reservation resource followed by toll free reservation numbers, and then calling the hotel directly. Use of online hotel reservation system follows the previous three media in terms of favor. However, experts in IT predict that within several years the Internet will be one of the most important sources for hotel reservations and services (Cline and Warner, 2001). The number of online hotel reservations in 2001 accounted for 4.9% of total reservations made, and this percentage is expected to more than triple over the next 3 years. While the proportion of online reservations is increasing, only 64% of hospitality firms currently handle such transactions (Cline and Warner, 2001). Because an explosive increase in the number of online hotel reservations is expected, hotel marketers need to understand the determinants of customers' online hotel reservation intentions.

1.1.1 Hotel Lock System

The advent of electronic lock systems (Hyatt *et al.,* 1998) has revolutionized the hotel industry by offering a safe and efficient way of controlling access to hotel rooms. Typical electronic lock systems function with electronic key cards and are controlled by computer systems. Upon checking in at the front desk of the hotel and being assigned a room, a customer is given an electronic key corresponding to the electronic lock securing access to the room. Electronic key cards have attached magnetic strips that are coded by the computers at the hotel check-in desk. The encoding on each key is such that the key functions only on a specific hotel room door. New keys with new codes are created for each room after the departure of each guest. The code from the previous use is erased by the computer, a new pattern is magnetically encoded on the key and the door lock is programmed to recognize the new code. While prior art electronic lock systems (Leon *et al*., 2000) offer many advantages over traditional key systems, they still suffer from significant drawbacks both for the hotels and for their guests (Khanna and WestJet, 2005). Customers arriving at a hotel are still required to check in at the front desk in order to be assigned a room and given the key. Many times, they are faced with long line-ups or staff unavailability, which decrease their satisfaction and minimize the chances of repeat business. For the hotel, adequate checks in service and staff availability are very costly (Shane, 1997).

Therefore a need for a system and a method that would allow guests to arrive at a hotel and go straight to their room without having to use the services and the keys provided at the front desk. Furthermore, the security issue arises for certain customers using the electronic keys provided by the hotel. The electronic key is impersonal and does not contain information that would make it work only for a unique authorized user. In the case in which a key is lost, the customer can provide another one upon by him/herself, which makes the system prone to fraud and abuse. Customers therefore do not feel that they themselves or their belongings are safe at all times (Gon Kim *et al.,* 2006). Hotels are forced to increase security measures in other ways, for example by using video cameras for lobby surveillance and by stiffening identification requirements for obtaining keys. Therefore a need for a system and a method allowing user specific information to be used for providing access to a hotel room.

1.1.2 Access Control

Saying about modem systems and facilities of an accident prevention of objects, it is necessary to mention the monitoring system and access control (MSAC) (Grotesque, 2002). The given class became practically same widespread, as burglar-fire alarm and system of tele-supervision. Any object may not claim to protect ability without equipment MSAC. Considering systems of safety of "intellectual building" there is a question of the necessary minimum of equipment for object, for example, of an apartment house.

The problem of access restriction is not new. With development of progress there were more and more sophisticated identifiers and more and more skillfully their thought up imitations (counterfeit documents or the peeped passwords and codes). The most prevalent way of protection of object from illegal access now – installation