6th International Symposium on Advances in Science and Technology
SASTech
Malaysia | Kuala Lumpur
24 - 25 March, 2012
Scope of the Symposium
Organised by:
Khavaran Institute of Higher Education
Hosted by:
Geospatial Association of South East Asia

A Novel IT-based Access Management System and Authentication Method

Farhang Padidaran Moghaddam, Department of Industrial Computing, Faculty of Information Science and Technology, National University of Malaysia
padidaran@ftsm.ukm.my
Riza Sulaiman, Department of Industrial Computing, Faculty of Information Science and Technology, National University of Malaysia
rs@ftsm.ukm.my
Mohamed B. Daud, Faculty of Engineering, University Putra Malaysia
mdaud@eng.upm.edu.my

Paper Reference Number: 6-11-24-188
Name of the Presenter: Farhang Padidaran Moghaddam

Abstract

Focal point of proposed system is improving electronic access control systems. Regarding to suggested system and method, Clients can apply for their desired access code, which is available for a specific duration using an online booking system. The key/ticket can be printed at home without using any special peripheral equipment. The issued key is recognizable by offline and the standalone lock system. Barcode as a code carrier has been chosen, according to its advantages, such as reduced cost of key production, ease of generating, and it's highly resistant. The Verifier Machines can be located at each entry point are standalone devices, and are not connected in any way neither between them nor to any central database, server or portal. The system is generally designed for places where some people make use of it of a particular time and location like remote lodgings/hotels, vacation homes, clubs, some departments of factories, parking entrances and so on. Users can create their own access code from anywhere at any time using the online portal. Thanks to proposed encryption / decryption scheme, the system gives a reliable solution to design a method and system for generating access codes and authenticating the key or ticket/coupon with offering a safe and fast way. A prototyped verifier machine is made to validate generated access code. The major contributions of the study are user convenience in making desired key, cost reduction in producing the barcoded-key as well as to empower remote and disconnected lock systems for using the Internet- made keys.

Key words: Access Code, Encryption, Barcode, Internet, Offline Machine

1. Introduction

The Traditionally, locksmiths and installers have developed their skills around conventional mechanical devices, while access control companies concentrating on electronic or computer controlled systems (Norman, 2007). 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 (Tonbridge, 2006). The advent of electronic lock systems (Hyatt *et al.* , 1998) has revolutionized the hospitality industry and access management systems by offering a safe and efficient way of controlling access to lodging 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. Contemporary electronic lock systems for public or restricted places (Tischendorf, 1999), (Kucharczyk *et al.* , 2000), (Rodriguez *et al*. , 2005), (Cayne *et al.* , 2006) have had some major problems which are listed on below:

- Some lock mechanisms should be connected to a central server, so, when the line or the dispatching source was disconnected, the lock system will be out of order.
- A connected network is needed for performing the authentication, whole of the system will be down if network disconnected, furthermore, installations and upkeep cost must be considered.
- Customers should refer to the front desk or the key supplier center for registering and receiving the code, therefore the system can't provide anonymity for clients. Furthermore, the existence of front desk is not affordable in some remote lodgings.
- Authenticating the key code includes performing a comparison of the key code with information stored in a key code table which includes an entry for the electronic locking device, and wherein the entry includes one or more of a valid secondary key code, activation/expiration information, and wireless communication device identification information. What happened if the key code table was cleaned or copied by an invader?
- The system uses communication network interconnecting a telecommunication system, cost of installation and maintenance for wide coverage ranges network need to be taken into account.

The major intention of our system *i*s covering described problems in electronic lock/key systems. Our proposed framework provides a Web-based solution for issuing the Internet-made key and accessing to disconnected areas, which are disconnected from any server or portal.

2. The System Architecture

There are four major steps involved in conducting our framework:

a) Defining an authentication system for generating the key and identifying the authorized client.
b) The selection of an appropriate code carrier and choose its type, which has been used as a key / ticket.
c) Designing a web-based portal for performing registration, booking and online generating temporary cipher-coded key for a particular place.
d) Prototyping An offline and standalone Verifier Machine for identifying a user requesting access.

Accordingly, there are two main components in proposed framework. First, the web-based portal for booking and issuing the key in barcode form and second, verifier machine, which is used in doors or gates as a lock system for verifying access codes and dispatch release signal. Fig. 1 illustrates system components, configuration, and sequences.

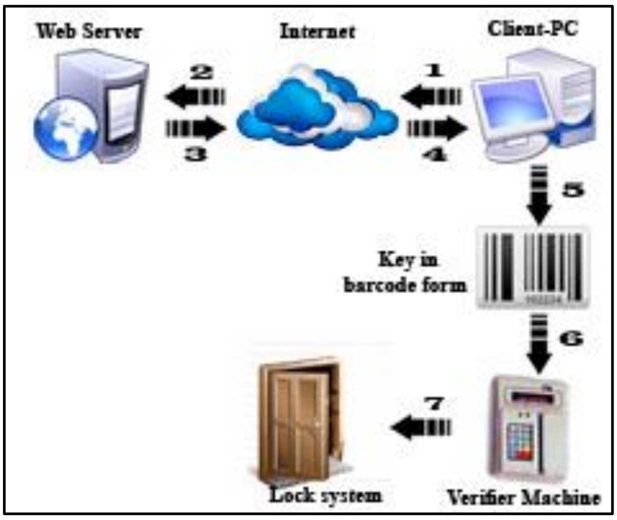


Fig 1: Framework Components and Configuration

3. Coding Methodology

The focal point of this study is how to address new method and system to make an online key which is detectable by offline lock systems. This study is also aimed to formulate a secure access code which is temporary and will be expired on a certain date. In this section, we propose an encryption/decryption scheme to create a safe and immune access code.

A. *Defining an Authentication System*

To create an authentication scheme following steps should be passed:

- Selecting cryptography method for generating ciphered access code
- Categorizing data for making primary code comprising access location information and dated information
- Designing an encryption algorithm for generating the access code in server-side and designing a decryption algorithm for decoding the key in the lock system-side

In what follows, Encryption Algorithms has been surveyed and proper model has been selected.

1) *Encryption/Decryption Model Selection*

A cryptographic mode usually combines the basic cipher, some sort of feedback, and some simple operations. The operations are not complicated because the security is a function of the underlying cipher and not the mode. Efficiency is another consideration. The mode should not be considerably less efficient than the underlying cipher (Schneier, 1996). A third consideration is computational cost. Most public-key algorithms are comparatively computationally costly in comparison with many symmetric key algorithms of apparent equivalent security. This has important implications of their practical use. Most of them are used in hybrid crypto systems for reasons of efficiency; in such a crypto system, a shared secret key ("session key") is generated by one party, and this is a much briefer session key than encrypted by each recipient's public key. Each recipient uses the corresponding private key to decrypt the session key (Milgate, 2006). Symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms. In practice, asymmetric key algorithms are typically hundreds times slower than symmetric key algorithms. So in many applications, a symmetric algorithm is a faster way to encrypt and decrypt messages. As mentioned factors for choosing an encryption algorithm, symmetric key has been chosen and applied.

2) *Data Categorizing*

The system is generally designed for places where some people make use of it of particular time like public events, hotels, clubs, some parts of the factory, parking and so on. Depending on location, we need some data to collect for issuing the access code/ticket. These data must be determined about some kinds of information: About section, department or room and also about the beginning of the validation date and duration of validation. In what follows, we consider specific places and determine which type information needs to generate the code that has been used as a key. For example, in international chain hotels, an international ID-card should be generated for each guest that defines the detail about him/her; Guest's data consist of these sections:

- Location information (country , city , hotel codes)
- Room information
- Dated information

These details are necessary for specifications of guest's location, also time of beginning and ending residence:

Country code; City code; Hotel code; Room code; Arrival Date; Number of nights

Along with, in some parts of factory or office, following data is needed for verification and authentication of an employee for entering into the particular section:

Factory/Office Code, Section Code, Date of Starting work, Validation day numbers

Meanwhile, same categorization can be applied to restricted areas like parks and, temporary ID-card.

3) *Digital Symbolic Coding*

To generate the key and for the beginning of encryption, digits were assigned to each categorized data. Minimum length for each category was assigned, to avoid of primary code length prolongation. Despite, the primary code should be long enough to declare desired info. For example, following code was assigned to guest categorized data. Suggested format for primary code was made for international use and supports a wide range of booking variables (Table 1).

- 3-digit code was assigned to country code that could indicate 999 countries, by default, country telephone codes was selected.
- For city and hotel, a single digit code was assigned; therefore, 9 objects can be addressed to each one.
- Room code was indicated by 4-digit code that comprised of two sections: first 2-digit assigns room's floor and second 2-digit indicates the room number.

- The arrival code is contained 6 digits that marks day, month and, year of arrival.
- 2-digit code was assigned to a number of residence nights that support 99 nights reside duration. A new key should be issued for longer dwell.

Country Code	**City Code**	**Hotel Code**	**Room Code**	**Arrival Date**	**Reside Nights**
XXX	X	X	XXXX	XXXXXX	XX
060	1	4	0514	210911	12

Table 1. Data Categorization for Lodge Rooms

06014051421090812 is a primary code that means room number 14 on the 5th floor of hotel 4 in Kuala Lumpur, Malaysia is reserved since 21 -Sep - 2011 for 12 nights.

Following format was introduced for any department of factory/company or other restricted areas like these locations (Table 2):

Factory/Office Code	**Section Code**	**Date of Starting work**	**Validation day numbers**
XXXXX	XXXX	XXXXXX	XXX

Table 2. Data Categorization for Various Factory/Office Sections

This key should not operate any of the other guests' locked rooms. Similarly, all the guests must have a unique key with them that can operate only in their locked room. This is to ensure that users only can access to the right gate.

4) *Encryption*

Primary code should be encoded to be safe and private. It is necessary that we generate a secure code from the client's data using an encryption model for printing using barcode. Target location's safety and security are depended on the lock system safety and key code robustness. In what follows, generating such access code is described.

a) *Generating Enciphered Access Code*

The working principle of a symmetric encryption system (Biham and Shamir, 1993) is illustrated in Figure 2 On the left side, the sender encrypts the message m with his or her implementation of encryption function E (parameterized with the secret key k). In the resulting, cipher text E_k (m) = c is sent to recipient over a potentially unsecured channel. On the right side, the recipient decrypts c with his or her implementation of decryption function D (again parameterized with the secret key k). In every practically relevant symmetric encryption system (Bellare et al. , 1998):

$$D_k\,(E_k\,(m)) = m \qquad (1)$$

As result, if the decryption is successful, then the recipient is able to recover the plaintext message *m*.

The proposed coding method (Fig. 2) used decimal operations in limited steps. These operations, including simple mathematical operations like add, subtract, multiply and division. The computational cost was reduced, due to this method. According to the suggested algorithm, with limited steps and reduced computational cost, encryption/decryption process is not time-consuming and performed quickly. Some other operations were added to ensure that the generated code is safe and secure. These operations consist of inverting, digit displacement and attaching checksum. Therefore, sequential set of mentioned decimal operations was used to generate the final code; encoded code is 16-digit code, used as a key to access a restricted area.

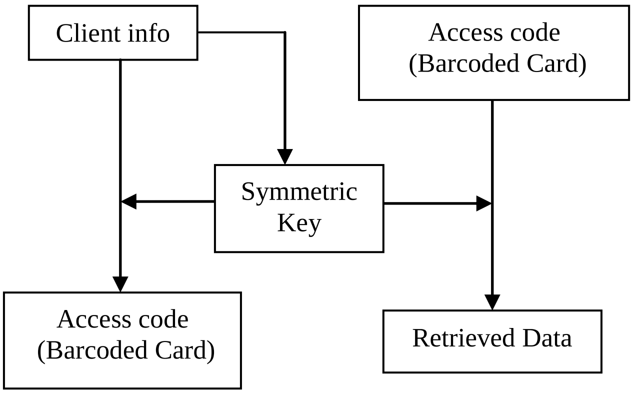


Fig 2. Symmetric-Key cryptosystem that used in proposed en/decryption scheme

5) *Decryption and Verification process*
During the decryption process primary info was retrieved; these retrieved data were used to authenticate and verifying for authorizing users. In fact, verifying consist of comparing decoded data with pre saved one and with particular digits located in the enciphered code. Pre- saved data in the lock system is comprised of location code (country, city and lodging code) and room codes (used for decrypting) for public/remote lodgings, those data are comprised of factory/office code and the section code (used for decrypting) for office/factory. In all mentioned applications, the check digit located in the enciphered code; verifier checks it during the decrypting process. Following steps is considered in the proposed authentication process:

- Enciphered code length checking
- Check digit verifying
- Location checking
- Verifying reside duration

B. *Selection of appropriate code carrier*

An access card must be generated for each client determining details about him/her, her. This card acts as a key, by this card he/she can open/close the door and also able to enable/disable residential equipment. There are some alternatives for choosing as proposed system code carriers like Smart Cards (Hendry, 2001), Contactless Cards (RFID) (Paret, 2005), and Magnetic-stripe Cards. Mentioned cards have some disadvantages (Shapiro, 2008) for home users same as special programmer device requirement, expenses of card/production and the necessity of training. Besides, using the barcode (Sriram and Rao , 1996) as a suitable our system code carrier offers these advantages:

- Lower in Cost: unlike other types that mentioned earlier, a cardboard with a barcode label on it can be used.
- Ease of Generating: desired label can be printed by a normal printer.
- High Resistant: Issued key will be still recognized even when folded, crumpled or wet.

Barcode Access Management (Cheng and Chen, 2002), (Wen, 2008) specifically uses barcode technology to allow the user to enter his control or access number. Many systems are using barcode as code carrier successfully. Barcode as identifying media contains the access or control number. Typically, this media would be an ID tag with a control or access number encoded in a barcode.

1) *Barcode Type selection*

The different bar code symbologies support different types and amounts of data therefore we normally choose a particular symbology based on the type and amount of data that we want to encode in our bar codes. The enciphered code which has been used as key consists of 16 digits. Code-39 (Lifen, 1999) is a suitable selection because it is a numeric code and also could contain 16 digits (Fig. 3). Moreover, barcode reader price is lower than 2D barcodes.

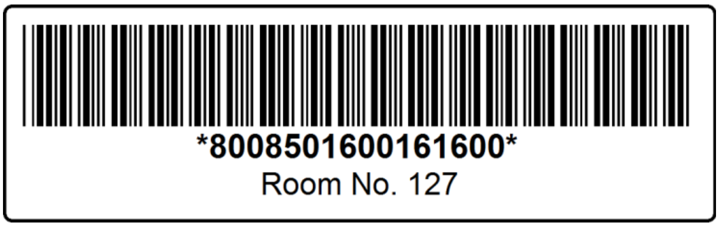
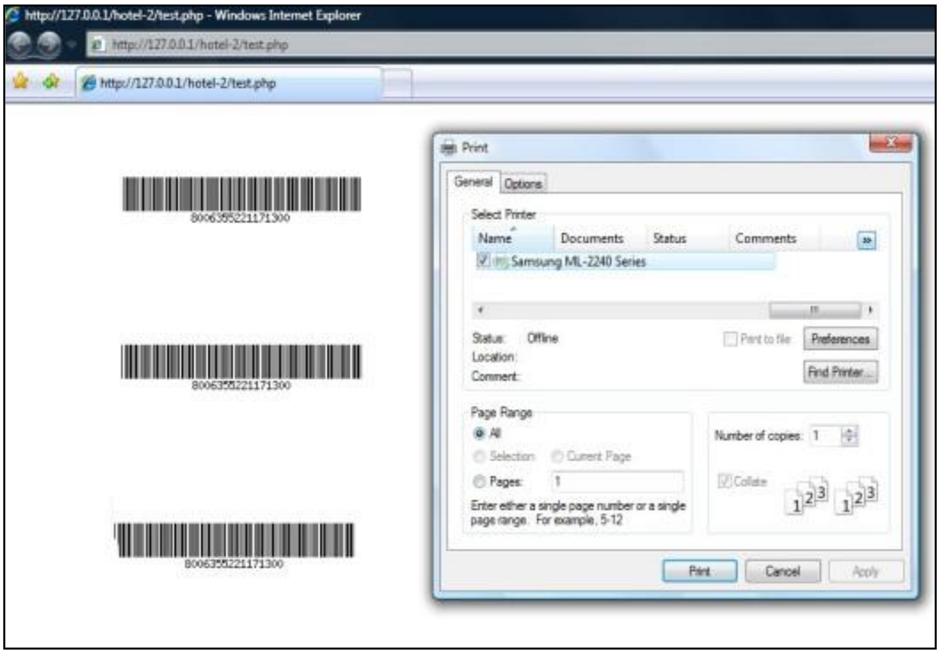


Fig 3. 16-digit Code which Coded using Code-39 form

4. System Implementation

A. *Online Key Issuer System*

A web-based center or portal is required for issuing the key. Generally, this portal should receive primary info and produce the key, with the predefined algorithm. It can show the generated code or provides ready to print barcode key (Fig. 4). Depended on usage, received primary information is different; in the case of lodgings, booking data must be collected and for office/factory sections, department info should be entered. In fact, the code formatting and shape of key are the same for various usages, whereas, initial information is different. Features of the system need to be compatible with usage requirements, meaning that it should include related routines and customer requirements should be covered, also, the system must consider eventual errors. The key issuer system can be used in an offline or online state. The offline application is used for local access only, and remote users cannot use this system for issuing the key. The implemented portal was programmed by Perl Hypertext Preprocessor (PHP) ver. 5.3.10 and its database managed by PHP-MyAdmin (ver. 3.4.9). PHP5 a fully object-oriented language and its platform independence and speed on Linux server helps to build large and complex web applications (Mehmood, 2006). So, in general, PHP is cheap, secure, fast and reliable for developing web applications. The portal is using multi-layer architecture for administrators, managers and clients. Lost Keys and the client password options are placed in the portal to increase client satisfaction and system security.


http://127.0.0.1/hotel-2/test.php - Windows Internet Explorer

http://127.0.0.1/hotel-2/test.php

8006355221171300

8006355221171300

8006355221171300

Print

Select Printer

Name	Documents	Status	Comments
☑ Samsung ML-2240 Series			

Status: Offline

Location:

Comment:

□ Print to file

Page Range

● All

○ Selection ○ Current Page

○ Pages: 1

Enter either a single page number or a single page range. For example, 5-12

Number of copies: 1

☑ Collate

Fig 4. Issued Keys by Portal

1) *Lost Key*

Lose or corrupting the issued keys is inevitable and it must be considered by the system. Proposed system allows users to login to web based-portal and requests for new key in limited times. There are two considered situations:

- The key has been lost before starting validation date; in this state, the new key will be same as lost key and there is no change in the generated code.
- The key has been lost or stolen during the validation days. In this situation, the lost key and its code are not safe. Consequently, the code needs to be regenerated. Date of beginning of validation and the number of valid days are dated information, which is used for making the code, whereas, current date and reminded valid days are used for generating the new code. Verifier machine blocks the lost key and accepts the new key only.

Although, number of key regeneration times is saved and key remaking is allowed in limited times.

2) *The User-defined Password*

It was found that only the barcoded card was not enough secure. Specially, in case of printed barcode card, using on the card was not safe because of ease of duplicating the card. This problem damaged the system security. The recommended solution is using a four-digit password defined by the user. In this system, the password is the guarantor of the authenticity and security of the key. This way, whether the Forger has kept a copy of the barcode key- card, he will not be able to use it since this card will not be valid without knowing the password. The user password is not long, which is easy to memorize, whereas, burst force is prevented, because it is long enough and the attacker should try 9999 numbers to find the right one. The password will be merged with a secret key and the new secret key for encryption/decryption will be generated. The secret key was provided by the system, and the password was received by the customer. Therefore, some steps need to be added to encryption/decryption encryption/ decryption algorithm. Figure 5 depicts modified encryption flowchart.

B. *The Verifier Machine*

An offline and standalone verifier machine has been joined with lock system to identify the security code and able to grant access to authorized clients. The verifier machine is able to:

- Receive the cipher-coded key by barcode scanner or keypad.
- Receive user n-digit password
- Decrypt the security code by using predefined algorithm.
- Verify the validity of security access code by comparing the decrypted codes with stored data.
- Detect the master key and regenerated key.
- Dispatch the open signal to lock system after authenticating authorized user.

The machine comprises a memory that stores predefined data; and a processor operatively coupled to memory, the processor configured to: receive key code from the user and identify the code based on key code.

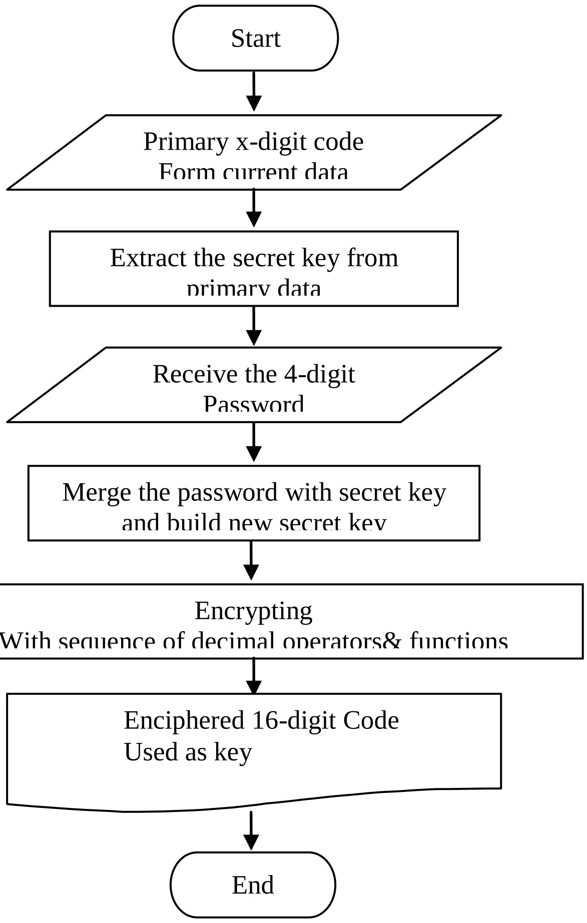


Fig. 5: The Flowchart of Modified Encryption Algorithm

When the key has been stolen or key has been lost, a new key will be issued by the reservation system; however, using the same code for new key is not safe, so new code will be generated for renewed key. The machine should be able to distinguish and accept the renewed code, also, reject the lost key. As a result, there is a located procedure that called Key Accepting Process. Key Accepting Process lets the machine to recognize the renewed key and reject the lost code. Designed verifier machine, which is a standalone device, and is not connected in any way neither among them nor to any central database, server or portal can be located at each door or entry point. Prototype verifier machine (Figure 6) is using Atmel® AVR ATMEGA32 microcontroller as processor. Furthermore, BASCOM® (Compiler version: 1.11.9.0) was used for programming the microcontroller which created by MCS® Electronics. EEPROM memory is saving location code and current date. Number of Microcontroller Program Code lines is 420 lines and verifying time after receiving the codes until sending release signal for master or normal mode is 750□ 20 ms experimentally.

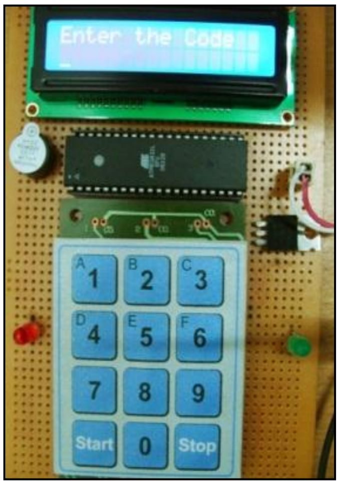


Fig 6. The prototype Verifier Machine

5. Conclusions

An encryption and decryption scheme for remote authentication was designed. Using this method we can generate a specific, temporary and secure the Internet- made code that is understandable by the offline lock system in certain place. This access code can be used in public places as a key that is generated online by the client himself. Presented system, without the need to incorporate specific peripherals in the user computers, allows them to print key-codes at home, guaranteeing authenticity. Public administrations as well as private corporations can benefit from this system having at their disposal a mechanism that is both secure and diverse. Additionally, it gives a more serviceable solution for the users because they don't have to refer to agents or waiting in front-desk queues for booking and key collecting. Following tests were performed successfully, for proving the reliability of the system: paper key stability test, testing the functionality of the simulator application by generating the access code, designed portal could generate the key in the bar coded form, and the prototype verifier machine was tested for decrypting and verifying process. Our system provided an authentication and authorization system which gives both managers and customers added peace of mind and ease, knowing only recognised people can gain access, at the right time and to the right room and location. As a result of the performance of the work was the IT-based keying system, which has the following characteristics was developed:

- Reduced cost of key production; a piece of plain paper or cardboard can be used as key card.
- Application of barcoded cards as the identifier that in turn allows for home-made key/ticket.
- Protection against duplication of a key code by using an individual password chosen by the customer.
- Simplicity of producing and using; the key can be printed by a normal printer.
- Our framework provided a mechanism that facilitates minimization of customer interaction with employees in all service businesses while maintaining a high level of security.
- The offline and standalone lock system can be installed in remote areas without connecting to server, center or portal.

References

Bellare, M., Canetti R, Krawczyk H. (1998). A Modular Approach to the Design and Analysis of Authentication and Key-Exchange Protocols , 30th ACM Symposium on the Theory of Computing, 419–428.

Biham, E. and Shamir, A. (1993). Differential Cryptanalysis of the Full 16- Round DES Proc. Crypto 92, *Advances in Cryptology*, Springer-Verlag, New York.

Cayne, A. J., MacAlpine M., Laidlaw C., and Thomas R. (2006). Intelligent locking system, *US Patent 7113071*, September 26.

Cheng, M.Y. and Chen, J.C. (2002). Integrating barcode and GIS for monitoring construction progress, Automation in Construction 11 (1) , 23–33.

Hendry, M. (2001). "Smart card security and applications. Second edition". ARTECH HOUSE, INC. publication. USA.

Hyatt, Jr.; Richard G.; Trent, D., and Hall, Ch. (1998). Electronic security system, *US Patent 5745044*.

Kucharczyk, D.; Santa F.; Brown S., and Park, M. (2000). Locking Mechanism for use with ONE-TIME Access Code, *US Patent 6300873*.

Lifen H. (1999). Design of Computer Room Management System Based on Binary-Valued Noncontiguous 3 of 9 Barcode , Journal of Hefei University of Technology, Vol. 2, 92-95.

Mehmood N. (2006). Advantages of PHP Development , http://www.articlesbase.com/programming-articles/advantages-of-php-development-71741.html [Online paper].

Milgate A. (2006). Identity and Access Management , http://identityaccessman.blogspot.com [Online paper].

Norman, T. (2007). History of Electronic Security, *Integrated Security Systems Design*, pg. 21.

Paret, D. (2005). *RFID and Contactless smart card applications*. John Wiley& Sons, Ltd. England.

Rodriguez, H., Smith, Jr., James N., and Clifford J. (2005).Electronic key system, apparatus and method, *US Patent 6975202*, December 13.

Schneier B. (1996). *Applied Cryptography* , John Wiley & Sons pub., Second Edition.

Shapiro, J. (2008). *The Disadvantages of RFID Credit Cards*. Retrieved from http://ezinearticles.com/?The-Disadvantages-of-RFID-Credit-Cards&id=163596, July 30.

Sriram T. and Rao V. K. (1996). Application of Barcode Technology in Automated Storage & Retrieval System, Proceedings of Industrial Electronics Conference, 5-10.

Tischendorf, A., Schultz, Kenneth, Lehman, Gary, A. and Demos, G. (1999). Remotely-operated self-contained electronic lock security system assembly, *US Patent 5933086*.

Tonbridge,(2006) . *What's New in Building?*, pg. 24.

Wen-Yuan Chen (2008). Multiple-watermarking scheme of the European Article Number Barcode using similar code division multiple access technique, *Journal of Applied Mathematics and Computation*, Vol.197, Issue 1, 243-261.