A STUDY OF PROBABILITY TO USE IP ADDRESS NUMBER INSTEAD USING AN EXIST STUDENT ID.

LERPONG CHAIRAT

A THEMATIC PAPER SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(TECHNOLOGY OF INFORMATION SYSTEM MANAGEMENT)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2014

Thematic Paper
entitled

A STUDY OF PROBABILITY TO USE IP ADDRESS NUMBER INSTEAD USING AN EXIST STUDENT ID.

……
Mr. Lerpong Chairat
Candidate

……
Assoc. Prof. Panya Kaimuk, M.D.
Major advisor

……
Asst. Prof. Bovornlak Oonkhanond, Ph.D.
Co-advisor

……
Asst. Prof. Auemphorn Mutchimwong, Ph.D.
Acting Dean
Faculty of Graduate Studies
Mahidol University

……...
Asst. Prof. Supaporn Kiattisin, Ph.D. (Electrical and Computer Engineering)
Program Director
Master of Science Program in Technology of Information System Management
Faculty of Engineering
Mahidol University

Thematic Paper
entitled

A STUDY OF PROBABILITY TO USE IP ADDRESS NUMBER INSTEAD USING AN EXIST STUDENT ID.

was submitted to the Faculty of Graduate Studies, Mahidol University
for the degree of Master of Science
(Technology of Information System Management)
on
July 04, 2014

……
Mr. Lerpong Chairat
Candidate

……
Asst. Prof. Supaporn Kiattisin,
Ph.D.
Chair

……...
Assoc. Prof. Panya Kaimuk, M.D.
Member

……
Asst. Prof. Bovornlak Oonkhanond,
Ph.D.
Member

……....
Lect. Waranyu Wongseree,
Ph.D.
Member

…… ……
Asst. Prof. Auemphorn Mutchimwong,
Ph.D.
Acting Dean
Faculty of Graduate Studies
Mahidol University

……
Lect. Worawit Israngkul,
M.S. (Technical Management)
Dean
Faculty of Engineering
Mahidol University

ACKNOWLEDGMENTS

I wished to express my gratitude to Assoc. Prof. Panya Kaimuk, M.D., my major advisor and Asst. Prof. Bovornlak Oonkhanond, Ph.D., my co-advisor for their valuable advice gridline during organization of this thesis. I would like to thanks to Assoc. Prof. Dr. Supaporn Kiattisin and Lect. Dr. Waranyu Wongseree, for their valuable advices to my success.

This study cannot success without the support from all staffs in the Faculty of Technology Information System Management. I would like to thank all staffs in the Faculty of Technology of Information System Management for useful information support.

And I also thank all friends in class for suggestions in everything for causing to my success

Finally, thank to my parents and family, for their sacrifices, encourage and understanding.

Lerpong Chairat

A STUDY OF PROBABILITY TO USE IP ADDRESS NUMBER INSTEAD USING AN EXIST STUDENT ID.

LERPONG CHAIRAT 5237449 EGTI/M

M.Sc. (TECHNOLOGY OF INFORMATION SYSTEM MANAGEMENT)

THEMATIC PAPER ADVISORY COMMITTEE: PANYA KAIMUK, M.D., BOVORNLAK OONKHANOND, Ph.D.

ABSTRACT

The main aim of this research is to describe advantages in the use of IPV4 adoption for traditional student ID cards and employee ID badges. Presently, the number of students is increasing in all universities and different companies in Thailand need to be categorized to the same standard. IVP4 is one of the solutions to manage all such information.

The possibility of using an IP address number instead of using existing student IDs and employee ID cards, which are completely customised by administrators such as; Insert, Edit, Delete, and view in order that all the information, which is separated into different places, is able to be processed easily.

After the simulation has been completed, the system testing was performed. The result shows that the hypothesis is trustworthy, which is the IP Address can be used in increasing safety, comfort, flexibility and could also be applied to other utilities in information management.

KEY WORDS: RFID / IP ADDRESS / IPV4 / STUDENT ID / SMART CARD

58 pages

การศึกษาความเป็นไปได้ในการใช้หมายเลขไอพีแทนหมายเลขประจำตัวนักศึกษา
A STUDY OF PROBABILITY TO USE IP ADDRESS NUMBER INSTEAD USING AN EXIST STUDENT ID.

เลอพงษ์ ชัยรัตน์ 5237449 EGTI/M

วท.ม. (เทคโนโลยีการจัดการระบบสารสนเทศ)

คณะกรรมการที่ปรึกษาสารนิพนธ์ : ปัญญา ไข่มุก, M.D., บวรลักษณ์ อุนคานนท์ Ph.D.

บทคัดย่อ

งานวิจัยฉบับนี้ ผู้วิจัยขอนำเสนอระบบอำนวยความสะดวกโดยการนำระบบ IPv4 มาแทนหมายเลขประจำตัวนักศึกษาและพนักงาน และใช้เทคโนโลยี RFID สำหรับจัดเก็บข้อมูลเพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ของมหาวิทยาลัย ซึ่งการนำหมายเลข IPv4 มาใช้แทนหมายเลขประจำตัวนักศึกษาและพนักงานในปัจจุบันจะสามารถนำมาระบุตัวตนของผู้ใช้งาน และยังสามารถนำไปใช้เป็นหลักการสร้างหมายเลขประจำตัวนักศึกษาของมหาวิทยาลัย ส่งผลให้ในอนาคตหมายเลขประจำตัวนักศึกษาและพนักงานทั้งหมดจะสามารถระบุให้เป็นมาตรฐานเดียวกันได้ทั่วประเทศ

ดังนั้นในการศึกษาความเป็นไปได้ในการนำ IPv4 มาแทนหมายเลขประจำตัวนักศึกษาและพนักงานบนเทคโนโลยี RFID จะช่วยเอื้อให้มหาวิทยาลัยสามารถจัดเก็บข้อมูล Insert),แก้ไขข้อมูล (Edit),ลบข้อมูล (Delete), แสดงผลข้อมูล (View) วิเคราะห์และประมวลผลข้อมูลการใช้งานคอมพิวเตอร์ของนักศึกษาและพนักงานที่กระจัดกระจายอยู่ตามคณะต่างๆได้อย่างถูกต้อง รวดเร็ว และเป็นระบบมากขึ้น

หลังจากจำลองระบบเสร็จสิ้น ได้มีการทดสอบการทำงานของระบบ ผลการทดสอบที่ได้รับถูกต้องตรงตามสมมติฐานที่วางไว้ กล่าวคือสามารถนำหมายเลข IP Address มาใช้เพื่อเพิ่มความปลอดภัย, เพิ่มความสะดวกสบาย, มีความยืดหยุ่นและสามารถนำไปพัฒนาเพื่อใช้ประโยชน์ในด้านอื่นๆได้เพิ่มเติม

58 หน้า

CONTENTS

CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES (cont.)

CHAPTER I
INTRODUCTION

1.1 Background/ The importance of the problem

Thailand has developed citizen identification pattern in order to store basic information, more convenient to store, portability to anywhere, including the ability to retrieve information of the owner of card for check or use in basic information. Evolutions of the identity card of the Thai citizen have been five generations are as follows.

The first generation: The identification document look like a small brochure has 4 folded 8 pages, started to use from 2486 to the end of 2505

The second generation: The cards are a convenient portable size in the rectangle shape with a 2-sided photo the card is black-white containing the basic information of cardholders with a normal typewriter coated with plastic. This type of card started to use from 2506 to 2536.

The third generation: The cards look like the second generation, but different in color print photo. The basic information of cardholders is printed and coated with special materials to prevent counterfeiting. It began to use 13-digit for identification number of citizen, started to use from 2531 to 2545.

The fourth generation: The cards have a magnetic stripe for record information of cardholders, it looks like a credit card, The new information contain on this card is blood group which will be useful in the archives of the Thai Red Cross Society. This type of the cards started to use from 2539 to 2553.

The fifth generation: A pocket-sized smartcard with embedded integrated circuits contains volatile memory and microprocessor components. The card is made of plastic, generally polyvinyl chloride, but sometimes acrylonitrile butadiene styrene or polycarbonate. Smart cards may also provide strong security authentication for single sign-on, started to use from 2550 to present.

The sixth generation: The cards use of RFID technology, but now RFID technology did not make for citizen ID cards. We can be seen from the passenger train (BTS and MRT), employee ID card or student ID card. The card has an internal architecture look like in the smartcard technology but RFID card can be used without touching.

RFID technology that can store a lot of data and high security data, resulting in RFID technology can play an important role in the daily lives of most people. This technology has been applied in many fields to indicate their intended use of human, animal, and products. Automatic identification technology that is available has been developed to facilitate for business, which will automatically read and record information. The result of the popularization of RFID, the researcher expects that the individual must have many cards in use such as citizen identification card, social security card, student card, credit cards, etc.

Present has developed a new Internet Protocol is IPv6 to improve the structure of the protocol to support numbers of IP address and improve other features such as security as well as efficiency in the processing packet. Therefore, it is the origin of the concept of bringing IPv6 to replace the Citizen ID. Because of the IPv6 can be defined in terms of the number of address up to 128 bits or 3.4×10^{38} numbers. It shows that the address number would be sufficient to needs of people around the world. This means that in the future, number of people on the world will be assigned to standard and the number can also be used as a number that represents the identity of one of the world as well.

Researchers have realized the importance of the IP address was used as a model for student ID number on the RFID cards to a processor and storage data of the students as well as the ability to access the database for transactions of the students.

1.2 Objectives of Study

To study the possibility of replacing student ID to IP address for security, convenience, flexibility, variety to development.

1.3 Scope of the Study

The scope of the research on the feasibility of replacing the IP address on student ID card on the RFID card is as follows:

1) Design and apply RFID card reader.
2) Design to store IP address on RFID card.
3) Study on the control of students' computer use.
4) Study on the control in other functions.

1.4 Definition

Radio-frequency identification (RFID) is the use of a wireless non-contact radio system to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking. Some tags require no battery and are powered by the radio waves used to read them. Others use a local power source. The tag contains electronically stored information which can be read from up to several meters away. Unlike a bar code, the tag does not need to be within line of sight of the reader and may be embedded in the tracked object.

Internet Protocol is the primary network protocol used on the Internet, developed in the 1970s. On the Internet and many other networks, IP is often used together with the Transport Control Protocol (TCP) and referred to interchangeably as TCP/IP. IP supports unique addressing for computers on a network. Most networks use the Internet Protocol version 4 (IPv4) standard that features IP addresses four bytes (32 bits) in length. The newer Internet Protocol version 6 (IPv6) standard features addresses 16 bytes (128 bits) in length.

CHAPTER II
LITERATURE REVIEW

The research on “A study of probability to use IP address number instead of using an exist student ID”. Researchers have studied the development of systems using RFID (radio frequency identification) and the Internet protocol. The researcher has been studying concepts, theories, books, documents and related research. The concept of theory and research on RFID and Internet Protocol technology of this study are shown as follows.

2.1 RFID

2.1.1 The management of student ID with RFID technology

RFID technology is a useful and a variety of applications. The highlight is a small chip that can store an ID. A chip that facilitate the integrated system including a security that can be applied to work on the electronic student card. If the RFID system integration can reduce costs is another great feature of the adoption of RFID applications, which makes it comfortable to use. Especially, when the properties of RFID compared to barcodes system. Inevitably implies a better reliability because the code does not disappear, and a memory chips that can store data for long time.

Current, the applications of RFID technology is used in application such as access control to have various styles. It is applied to Log in to used computer and monitor time to use the computer. Meanwhile, it is an aspect of personal identification. To be linked to the issue of tracking location, bringing the car into the parking and access to a locker. Trend in the future, due to the characteristics of integrated the IP Address into the RFID cards are used on university that to increase the security involved in pushing up the development of serious and continuous. RFID technology can be applied to business e-Purchasing on campus. Moreover, the adoption of RFID

in different frequencies according to the various application, support to use with superior features and replaced from barcodes.

RFID (Radio-frequency identification) is the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking. Some tags require no battery and are powered by the electromagnetic fields used to read them. Others use a local power source and emit radio waves (electromagnetic radiation at radio frequencies). The tag contains electronically stored information which can be read from up to several metres (yards) away. Unlike a bar code, the tag does not need to be within line of sight of the reader and may be embedded in the tracked object.

2.1.2 RFID Systems

RFID may only consist of a tag and a reader but an RFID system comprises many other technologies, such as computer, network, internet, wireless devices, and software, all working with the RFID devices to create a complete solution. A typical RFID system is divided into two layers: the physical layer and Information Technology (IT) layer.

The physical layer consists of the following:

- One or more RF tags
- One or more interrogators (readers)
- One or more reader antennas
- Deployment environment

The IT layer consists of the following:

- One or more host computers connected to readers (directly or through a network)
- Appropriate software (device drivers, filters, middleware, databases, and user applications)

Figure 2.1 provides a bird's-eye view of the RFID system, showing tags, readers, network, computers with software applications, and people all interacting to monitor and control business processes. The bidirectional mode of data movement among various parts of the RFID system is depicted at the bottom of the figure. Data may be read from or written to the tag during a business process. For example, a

number may be read from the tag attached to a case of goods passing through the shipping dock, while data may be written to the tag attached to a part moving from one workstation to the other during the manufacturing process.

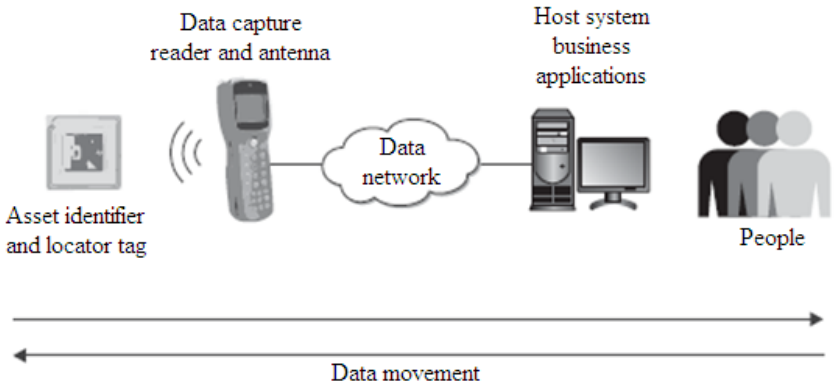


Figure 2.1 Bird's-eye view of an RFID system [4]

2.1.3 Elements of Radio Frequency Communication

Radio frequency communication uses the Electromagnetic (EM) waves with frequencies from a specific part of the EM frequency spectrum. Therefore, the underlying physics behind RF communication is the same as for any communication that uses electromagnetic waves to carry information.

The four major players that make this communication happen are the following:

a) Data signal: This is the wave that actually contains the information that needs to be sent to the receiver.

b) Carrier signal: This is the wave that carries the data signal.

c) Modulation: This is the process that encodes the data signal into the carrier signal and creates the radio wave that is actually transmitted by the antenna to propagate.

d) Antenna: This is a device used to transmit and receive signals such as radio waves.

2.1.4 RFID Tags

A tag, attached to an item that needs to be tracked, contains identification and possibly more information about the item.

The components of a tag are there to support its functionality by:

a) Storing the information about an item.

b) Processing the request for information coming in from a reader.

c) Preparing and sending the response to the request.

To support this functionality, a tag, as shown in Figure 2.2, consists of the following three main components:

1) Chip: The chip is used to generate or process a signal. It's an integrated circuit (IC) made of silicon. The chip consists of the following functional components:

a) Logical unit: Implements the communication protocol used for tag-reader communication.

b) Memory: Used to store data (information).

c) Modulator: Used for modulating the outgoing signals and demodulating the incoming signals.

d) Power controller: Converts the AC power from the incoming signal to DC power and supplies power to the components of the chip.

2) Antenna: In an RFID system, a tag's antenna receives the signal (a request for information) from a reader and transmits a response signal (identification information) back to the reader. It's made of metal or a metal-based material. Both readers and tags have their own antennas.

a) The antennas are usually used by tags (and readers as well) operating at UHF and microwave frequencies.

b) The tags (and readers) operating at low frequency (LF) and high frequency (HF) use inductive coils (as antennas) to send and receive signals in the inductive coupling communication technique.

Both the chip and antenna are housed on a substrate.

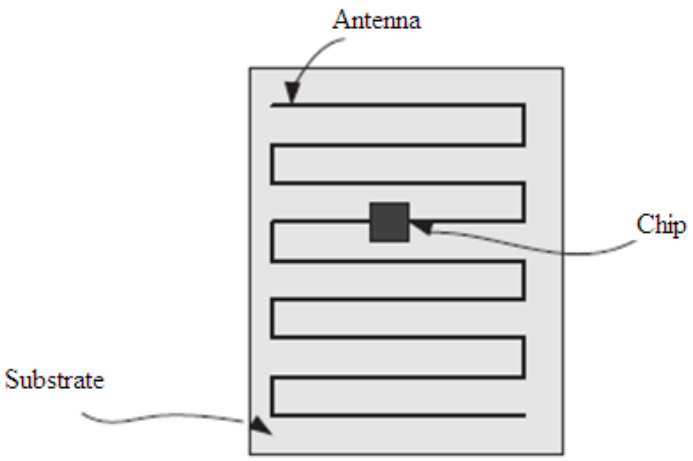


Figure 2.2 Components of a Tag [4]

3) Substrate: This is the layer that houses the chip and the antenna. Substrates can be made of different materials such as plastic, polyethylene terephthalate (PET), paper, and glass epoxy. Substrate material can be rigid or flexible, depending on the usage requirements.

2.1.5 Operating Tag Frequencies.

To respond to readers, tags use radio waves, which are basically the electromagnetic waves covering part of the electromagnetic spectrum of frequencies called radio frequency spectrum. Because the RFID systems generate and radiate the electromagnetic waves that fall in the radio frequency spectrum, they are justifiably classified as radio systems.

Table 2.1 shows the radio frequency ranges that are of interest to RFID systems, along with the ISM frequencies. RFID systems use many different frequencies in the radio frequency spectrum, but there are four most commonly used radio frequency ranges: low frequency (30–300 KHz), high frequency (3–30 MHz), ultrahigh frequency (300 MHz–3 GHz), and microwave frequencies (1 GHz–300 GHz). This table also shows the read ranges for a passive tag (a tag that does not have its own source of power, such as battery) corresponding to each frequency range. An active tag (a tag that has a battery) can have a read range of up to 100 meters.

Table 2.1 Radio Frequency Ranges in Which RFID Systems Can Operate and the Corresponding Read Ranges for Passive Tags [2]

Name	Frequency Range	Wavelength Range	ISM Frequencies	Read Range for Passive Tags
Low frequency (LF)	30-300KHz	10km-1km	<135KHz	<50cm
High frequency (HF)	3-30MHz	100m-10m	6.78MHz, 8.11MHz, 13.56MHz, 27.12MHz	<3m
Ultrahigh frequency (UHF)	300MHz-3GHz	1m-10cm	433MHz, 869MHz, 915MHz	<9m
Microwave frequency	3GHz-300GHz	30cm-1mm	2.11GHz, 5380GHz	>10m

2.1.6 RFID Tag Types

An RFID solution uses a radio frequency (RF) signal to broadcast the data captured and maintained in an RFID chip. An RFID system is composed of three components: a programmable transponder or tag, a reader (with an antenna), and a host. Figure 2.3 shows the basics of how an RFID system works.

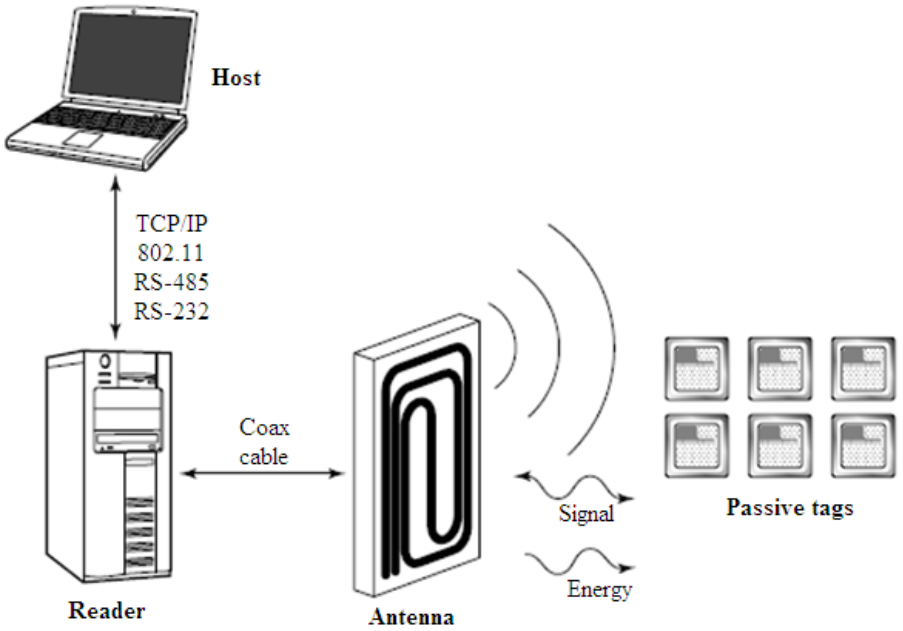


Figure 2.3 An RFID system transmitting data [2]

Much of the criteria for RFID systems depend on the type of tag that you use. Tags can be active, passive, or semi-passive. RFID tags are different types:

a) An active tag has its own battery power to contact the reader. Power from the battery is used to run the microchip's circuitry and to broadcast a signal to a reader. An active tag's onboard power source enables the tag to broadcast a signal out at great range by either constantly beaconing a signal or broadcasting only when the reader talks first. Some of the more powerful active tags can communicate up to 1 kilometer.

b) A passive tag does not require a battery. Rather, a passive tag derives its power from the electromagnetic field created by the signal from the RFID reader to respond to the reader with its information.

c) Semi-passive tags use a battery to run the chip's circuitry but communicate by drawing power from the reader's radio waves (like a passive tag). Because these tags have a battery, they're larger and more expensive than passive tags, but have greater communication ranges. Some active tags can also be made to monitor

sensor inputs, such as the temperature or movement, even without being within an interrogation zone to power up the tag.

The characteristics of passive, semi-passive, and active tags are summed up in Table 2.2.

Table 2.2 Characteristics of Tag Types [2]

Tag Type => Tag Characteristic || V	**Passive**	**Semi-passive**	**Active**
Power source	No power of its own; receives power from the reader's signal	Has its own power source (battery)	Has its own power source (battery)
Communication	Communication must be initiated by the reader	Communication must be initiated by the reader	Can respond to the reader's signal and can also initiate the communication
Size	Small could be as small as (0.15mm × 0.15mm) × 7.5 m	Medium	Largest, typically (1.5×3) × 0.5 $inch^3$
Read range	Short 2mm; few meters depending on the operating frequency	Up to 100 m	Large (up to 1 Km is possible); some limitations apply, resulting from standards and regulations
Memory design	Read only (RO), write once/read many (WORM), or read/write (RW)	Read only (RO), write once/read many (WORM), or read/write (RW)	Read only (RO), write once/read many (WORM), or read/write (RW)

Table 2.2 Characteristics of Tag Types (cont.) [2]

Tag Type => Tag Characteristic || V	**Passive**	**Semi-passive**	**Active**
Memory capacity	Mostly up to 128 bits, but some tags can have memory up to 64 KB	-	Up to 8MB
Cost	Inexpensive	Intermediate	Expensive

2.1.7 RFID Standards and Regulations.

The ISO is an international standards body composed of representatives from national standards bodies, founded on February 23, 1947, this organization sets worldwide industrial and commercial standards, which are popularly called ISO standards.

To be widely accepted, any technology requires some sort of standards and regulations that provide guidelines for designing, manufacturing, and using the technology. Standards are created by industry consortiums such as EPC global or standards-creating organizations such as the International Organization for Standardization (ISO). Standards help provide interoperability among vendors' products, increased demand for products, and reduced costs. Regulations are created by governmental agencies and help improve safety of the technology and create an orderly development and deployment environment in which several similar technologies can operate simultaneously. Two standards developing organizations most instrumental in getting different RFID solutions to work together are EPC global and ISO. EPC global is a non-profit industry organization. The acronym EPC stands for Electronic Product Code.

The ISO has developed RFID standards in Table 2.3.

Table 2.3 Some RFID Standards Developed by the ISO [2]

ISO Standard	Description
ISO/IEC 15961	Information exchange in a radio frequency identification (RFID) system (data protocol for application interface) for item management
ISO/IEC 15962	Data encoding rules and logical memory functions for item management
ISO/IEC 15963	Unique identification for RF tags
ISO/IEC 18000- ii is an integer: 1, 2, 3 …	Parameters for air interface communications for different operating frequencies
ISO/IEC 18047- ii is an integer: 1, 2, 3 …	RFID device tests methods for different operating frequencies
ISO/IEC 19762–3	Automatic identifi cation and data capture (AIDC) techniques: vocabulary
ISO/IEC 24730–1	Real-time locating systems (RTLS): application program interface (API)

2.2 Principles and theories of Internet Protocol.

The Internet Protocol, or IP, is the primary protocol used to provide an end-to-end delivery of packets over a TCP/IP network. Two versions of IP exist: IPv4 and IPv6.

The Internet Protocol is the Network Layer protocol responsible for maintaining the endpoints of an Internet connection. IP defines the addressing scheme used by TCP packets and the encapsulation of the data into the datagram format that is transported over an internetwork. IP is a stateful, but connectionless, protocol. That is, while the endpoints are known and can be either real or virtual, the path between the endpoints is left undefined.

2.2.1 Internet Protocol Version 4.

The first version of the Internet Protocol, version 4 (IPv4), is the dominant standard. It is recognized by the use of a quartet of octet addresses, ###.###.###.###, which is sometimes referred to as the dot decimal notation.

1) Addressing: IPv4's octet addressing scheme defines a 32-bit address space. Each of the four numbers can range from 0 to 255, which defines a limit of 4,294,967,296 unique addresses in the address space. When the designers of IP developed the protocol, they could never have imagined how popular the protocol would become, and so it seemed eminently reasonable that four billion addresses could never be consumed. At the time that IPv4 was specified in 1980, the population of the entire world was estimated to be 4.5 billion people, and so the IPv4 standard allowed for an IP address for every person alive at the time. In an era when refrigerators, toasters, sensors, and almost anything you can think of takes an IP address. This problem has been called IP address exhaustion. By comparison, IPv6 defines a 128-bit address space, which defines 3.4 x 1038 unique numbers.

2) Classes: As more networks were required, the designers of IP realized that while some networks might be large, most networks would be small, with some of intermediate size. The addressing scheme was changed so that the number of octets defining the network ID could vary between one and three octets, while the number of octets assigned to host IDs would vary between three and one octets. A network that required only one octet for the network ID would allow for 224 (16,777,216) hosts; one with two octets for the network ID would allow for 216 (65,536) hosts; and small networks where three octets were used to define the network would allow for only 28 (256) hosts. This is where the notion of network classes comes from. The original assignments for Classes A through E are shown in Figure 2.4 and Table 2.4 lists the different class types, as defined by RFC 791.

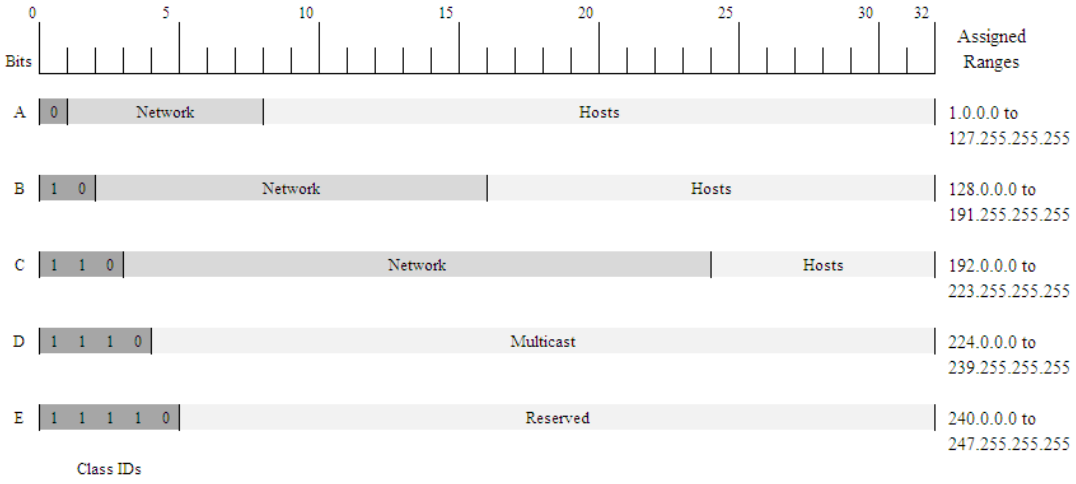


Figure 2.4 IPv4's original network class assignments [13]

Table 2.4 Network Class Types [1]

Class	Leading Bits	Begin	End (Routing block-CIDR)	Default Subnet Mask
Class A	0	0.0.0.0	127.255.255.255 (/8)	255.0.0.0
Class B	10	128.0.0.0	191.255.255.255 (/16)	255.255.0.0
Class C	110	192.0.0.0	223.255.255.255 (/24)	255.255.255.0
Class D (multicast)	1110	224.0.0.0	239.255.255.255 (/4)	N/A
Class E (reserved)	11110	240.0.0.0	255.255.255.255 (/4)	N/A

3) Classless Inter - Domain Routing: Classes became less relevant as the Internet became a public utility and the address space needed to be sliced and diced into millions of pieces. Classes eventually gave way to what is now called Classless Inter-Domain Routing (CIDR), and blocks of addresses are doled out to organizations and ISPs in all kinds of sizes. In the CIDR, IP addresses are assigned in a hierarchical structure that allows the addresses to be routed to the correct network, and if the address is routable, past the network portion to the correct host.

The CIDR scheme breaks the IPv4 address space into blocks that can be doled out, and represents those blocks. Each block is defined by appending a range number to an octet, in the form, ###.###.###.###/N, where N is a number from 0 to 32. (For IPv6, the range number is from 0 to 128.) The range number is in binary, and although it is appended to a dot decimal representation of the IP address, it is necessary to perform a conversion in order to establish the block size. Dot decimal is a 32-bit address space, and the numbers of N represent the excluded portion of the IP range.

The larger the number, the smaller the range of addresses in the block. Table 2.5 lists the conversion of Classes to CIDR block prefixes. So you can see how the VSLM assignment allows for very efficient block assignments of any size.

With the CIDR block assignments, it is no longer necessary to store routes to individual hosts in Internet routers. Instead, using routing prefix aggregation, routes are summarized into the supernets that the blocks represent. If you had four /26 contiguous blocks, that would represent 4 x 232-26, or 256 addresses. The designation of /26 represents a 1/4 C class network. In the routing table, a single entry for the starting IP address in the form ###.###.###.###/24 would be advertised, thus consolidating all of the blocks in the range.

For a larger supernet, consider the address ###.###.0.0/16, which uses a subnet mask of 255.255.0.0. The /16 indicates that this network is equivalent to 256 contiguous C class networks or one B class network, and defines an address space with 65,536 hosts.

Table 2.5 CIDR Block Sizes. [1]

CIDR Block Prefix	Class Equivalency	Unique Nodes
/28	1/16 Class C	16
/27	1/8 Class C	32
/26	1/4 Class C	64
/25	1/2 Class C	128
/24	Class C	256

Table 2.5 CIDR Block Sizes (cont.) [1]

CIDR Block Prefix	Class Equivalency	Unique Nodes
/23	2 Class C	512
/22	4 Class C	1,024
/21	8 Class C	2,048
/20	16 Class C	4,096
/19	32 Class C	8,192
/18	64 Class C	16,384
/17	128 Class C	32,768
/16	256 Class C or 1 Class B	65,536
/15	512 Class C or 2 Class B	131,072
/14	1,024 Class C or 4 Class B	262,144
/13	2,048 Class C or 8 Class B	524,288
/12	4,098 Class C or 16 Class B	1,048,576

4) Subnetting: A subdivided network is called a subnet, which is short for subnetwork, although you almost never hear the latter term in use. Subnets are created by applying a “subnet mask” to the network address space. A subnet mask is a bit mask that hides the network identification portion of a network, along with any range of host values you specify. Most private networks set their systems up with this size of network. In a private network with the range 192.168.1.0 to 192.168.1.255, which is referred to as 192.168.1.0/24 in CIDR, a subnet mask of 255.255.255.0 is applied to hide the network identification. This mask allows any of the 256 values for the host that are possible with the last octet. Suppose that you wanted to create two separate but equal sized subnets from this range.

Subnetting is a lot less mysterious than it might seem at first, if you think in terms of binary addressing. What subnet masking does is take bits that were part of the host’s identification portion of the network block and mask them off so that those bits appear to be part of the network identification portion; as a result, those bits can’t be changed. Figure 2.5 shows how this example looks in binary numbers. Note that the subnet mask suppresses the available range in the last octet.

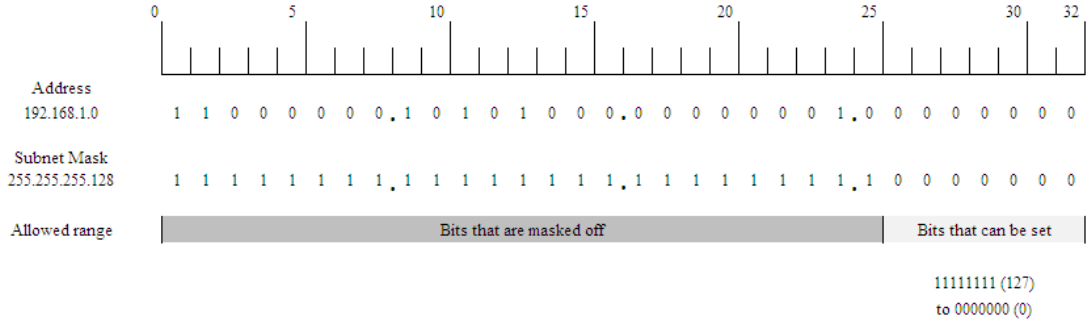


Figure 2.5 Subnetting a /24 network into two identical subnets [13]

Should you want to carve a /24 network into more subnets, you can use the subnet mask values in Table 2.5 to do so. Every bit that is masked beyond the network identification portion of the address is referred to as the subnet identifier. In Figure 2.5, the subnet identifier is 1. Referring to Table 2.6, the network identifier for the subnet mask 255.255.255.240 would be 4.

Table 2.6 Subnetting a /24 Network [1]

Last Octet in Dot Decimal	**Last Octet in Binary**	**Unique Hosts1**	**Number of Possible Subnets**	**Effective CIDR**
255	11111111	NA2	NA2	/32
254	11111110	2 (point to point)	128	/31
252	11111100	2	64	/30
248	11111000	6	32	/29
240	11110000	14	16	/28
224	11100000	30	8	/27
192	11000000	62	4	/26
128	10000000	126	2	/25
0	00000000 (no mask)	256	1 (no subnet)	

2.2.2 Internet Protocol Version 6

The second version of the Internet Protocol, version 6 (IPv6), is the successor to IPv4. IPv6 was designed to provide a significantly larger address space, better granularity (self-auto configuration and improved routing), and improved security.

1) Addressing: IPv6 has a much larger address space; 2^{128} addresses are available. The designers of IPv6 divided the address into several categories. A few leftmost bits, called the type prefix, in each address define its category. The type prefix is variable in length, but it is designed such that no code is identical to the first part of any other code. In this way, there is no ambiguity; when an address is given, the type prefix can easily be determined. Table 2.7 shows the prefix for each type of address. The third column shows the fraction of each type of address relative to the whole address space.

In standard hexadecimal notation, a Global Unicast IPv6 address would be written as eight 4-digit groups, each separated by a colon, as follows:

2001:0db8:3c4d:0015:0000:0000:abcd:ef14

2001:0db8:3c4d: is the global prefix, 0015: is the subnet ID, and 0000:0000:abcd:ef14 is the host identifier (network interface).

There is no need to specify a subnet or the network identification of any routers along the path to that network. The addition of the network identification changes the routing for the entire set of systems on that IPv6 network.

Table 2.7 Type prefixes for IPv6 addresses [13]

Type prefix	Type	Fraction
0000 0000	Reserved	1/256
0000 0001	Unassigned	1/256
0000 001	ISO network addresses	1/128
0000 010	IPX (Novell) network addresses	1/128
0000 011	Unassigned	1/128
0000 1	Unassigned	1/32

Table 2.7 Type prefixes for IPv6 addresses (cont.) [13]

Type prefix	Type	Fraction
0001	Reserved	1/16
001	Reserved	1/8
010	Provider-based unicast addresses	1/8
011	Unassigned	1/8
100	Geographic-based unicast addresses	1/8
101	Unassigned	1/8
110	Unassigned	1/8
1110	Unassigned	1/16
1111 0	Unassigned	1/32
1111 10	Unassigned	1/64
1111 110	Unassigned	1/128
1111 1110 0	Unassigned	1/512
1111 1110 10	Link local addresses	1/1024
1111 1110 11	Site local addresses	1/1024
1111 1111	Multicast addresses	1/256

2) IPv6 datagrams: IPv6 datagrams are both larger and simpler than their IPv4 counterparts. The header portion of the packet is shown in Figure 2.6. That IPv6 doesn't use IP header checksums to verify the validity of a transmitted packet; instead, it relies on other protocols to determine the validity. This has the effect of making IPv6 faster than IPv4.

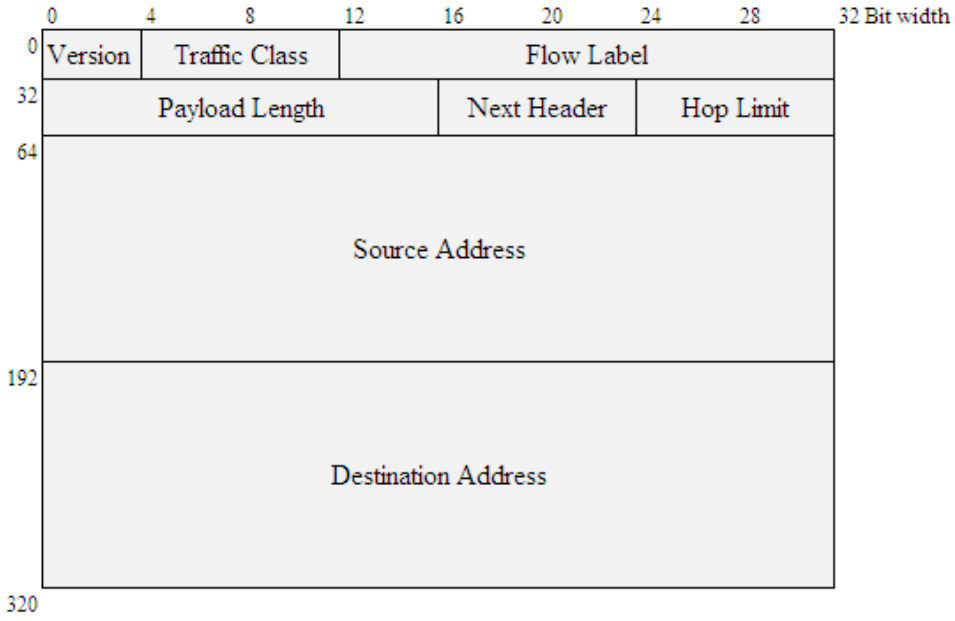


Figure 2.6 IPv6 header structure [13]

The different fields in the IPv6 header have the following purposes:

a) Version: This is indicated by a four-bit representation of the number 6 (0110).

b) Traffic Class: This field provides a packet priority range that is used to control packet traffic based on network conditions. Network messages indicate the amount of congestion on the network that needs to be accommodated.

c) Flow Label: This is a QoS label that is defined for real-time services and is meant to serve the same function as the Service Type field in IPv4. This field is not in current use.

d) Payload Length: This indicates the size of the payload in bytes. A field setting of all zeros indicates that the packet is a “Jumbogram,” which is a packet that can be anywhere from 64KB up to 4GB in size. Jumbo frames require specific network hardware support and a Maximum Transmission Unit (MTU) network protocol that supports their large sizes in order to be used.

e) Next Header: This is equivalent to the Protocol field in the IPv4 header. It can also be used to add an additional header to the packet.

f) Hop Limit: This is the number of network hops that are allowed. This is the current replacement for the Time-To-Live parameter that is used in IPv4.

g) Source Address: This is the IPv6 128-bit address of the source.

h) Destination Address: This is the IPv6 128-bit address of the destination.

2.3 Related Research

The studies related to implementation of a RFID system has found that the neighborhood concept. The publisher has used a project approach in the development of systems for personnel evaluation as follows;

Sandra Dominikus, Manfred Aigner, Stefan Kraxberger (2010) [17] studied on passive RFID technology for the internet of things that show how to modify RFID readers and low-cost tags to make them suitable for a remote two-way communication. They consider the required capabilities of readers and tags and show how communication can be done via mobile IPv6. Security considerations round the description before we can conclude that also passive low-cost RFID tags are able to become part of the future Internet of Things. They provided a concept to integrate passive RFID technology into the Internet of Things. Many new applications will be possible if RFID tags can be accessed via the Internet. They looked at concepts from mobile IPv6 technology and came to the conclusion, that these concepts also work for passive RFID tags.

Dang Nguyen Duc, Hyunrok Lee, Divyan M. Konidala, Kwangjo Kim (2010) [20] studied on open issues in RFID security, they attempt to summarize current research works in the field of RFID security and discuss some of their open issues. Firstly, they outline the security threats to RFID, then we summarize some of the current countermeasures and finally, we draw attention to the open issues and challenges in RIFD security.

CHAPTER III
METHODOLOGY

The research was conducted to analyze the feasibility of using IP addresses instead of the student ID. The purpose of the IP address use of optimization models applied to RFID technology with the IP address to be applied to the student ID or the other side, which can be identified efficiently. The system can be divided into 5 parts as follows:

1) Defining Scope of Research
2) System Design
3) Database Design
4) Screen Design
5) System testing

3.1 Defining Scope of Research

In this research, the researchers have defined the scope of the trial by a single computer by installing the VM Ware. There are making it seem like two computers, main computer for client computer and another is used to server computer. Equipment used in the research can be divided into 2 parts as follows.

3.1.1 Hardware

- Computer
- RFID Reader/Writer
- Low frequency RFID card (1K)

The product data sheet of RFID card and RFID reader as shown in Appendix a.

3.1.2 Software

- VM-Ware
- Microsoft Visual Basic

- Microsoft SQL Server 2005

3.2 System Design

In design of computer systems through RFID card can be divided into 2 parts as follows:

3.2.1 Hardware design

Detailed study of the RFID device model that works and how is connected to the RFID device. Using RFID card and RFID reader are of low frequency that can read data in the near term.

3.2.2 Software design

The program is designed to control access to the computer by using Microsoft Visual Basic, which requires that the program works if the user wants to access the computer, access to the car park, access to the locker and location tracking that can be written to Flowchart as shown in figure 3.1. For access to the computer users will need to tap the RFID card to RFID Reader and then, enter the password. It will provide access to the computer, if pull the card out. It will leave to the main screen users cannot use a computer that can be written to Flowchart as shown in figure 3.2. For access to car park users will need to tap the RFID card to RFID Reader when the vehicle is into parked and then tap again when the vehicle is go out from car park that can be written to Flowchart as shown in figure 3.3. For access to the locker users will need to tap the RFID card to RFID Reader when users need to open the locker that can be written to Flowchart as shown in figure 3.4. For the location tracking when the user is inside the RFID antenna area, the system will detect signal and stamp location to database that can be written to Flowchart as shown in figure 3.5.

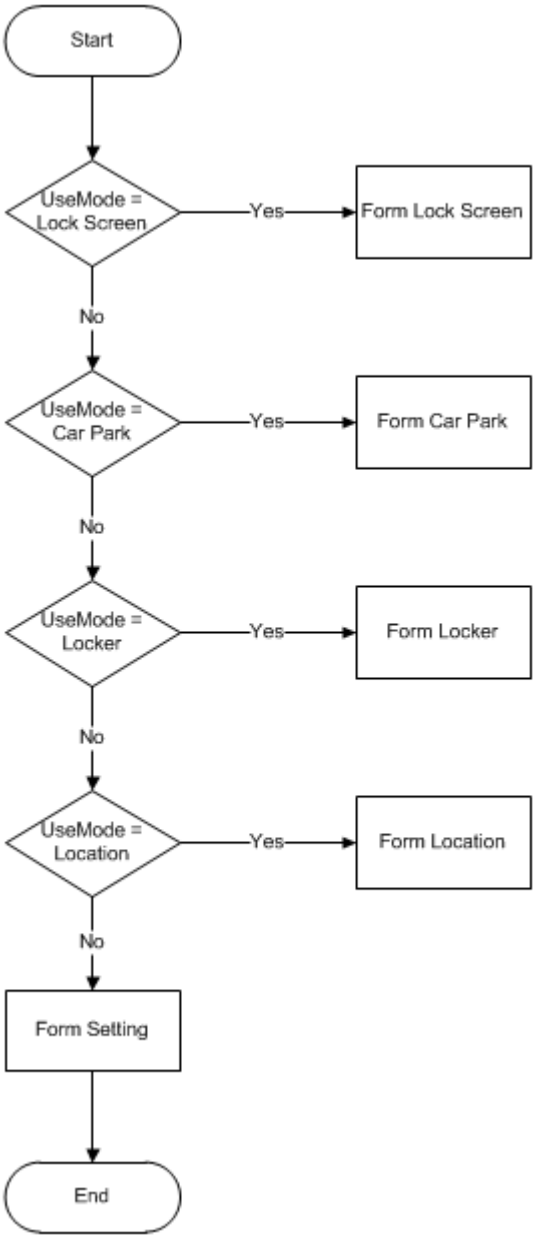


Figure 3.1 System Flowchart

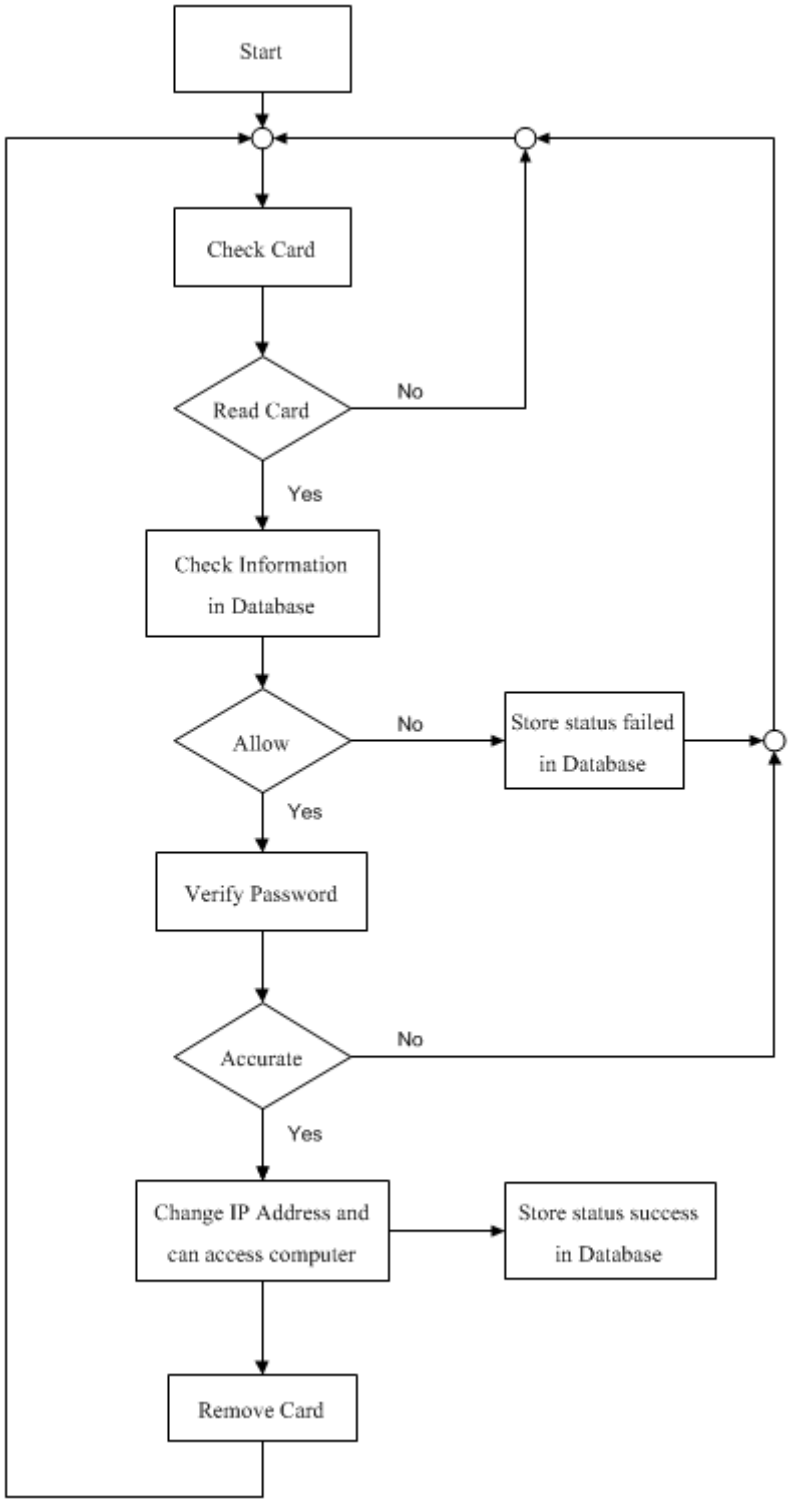


Figure 3.2 Flowchart of system Computer using

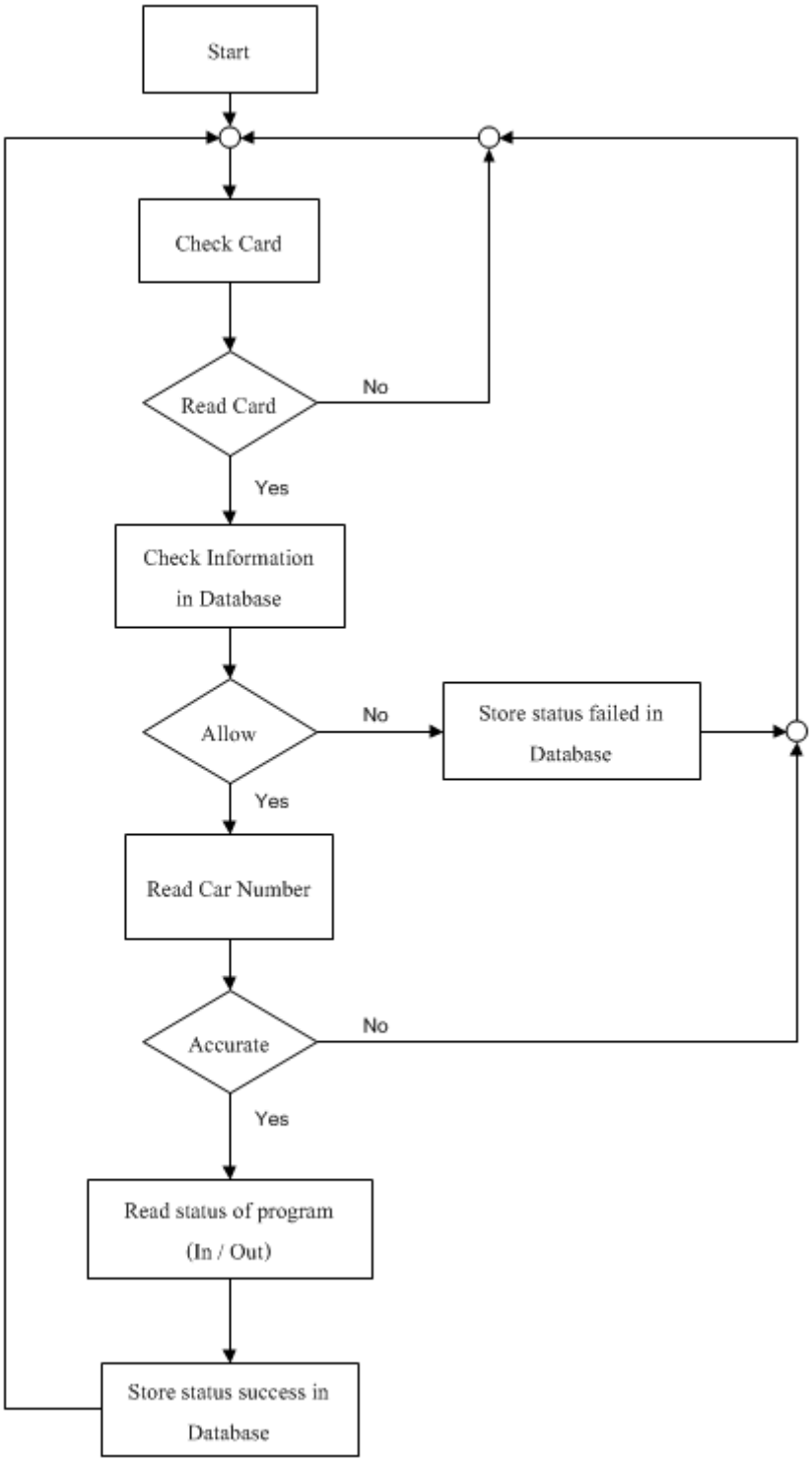


Figure 3.3 Flowchart of Car Park system

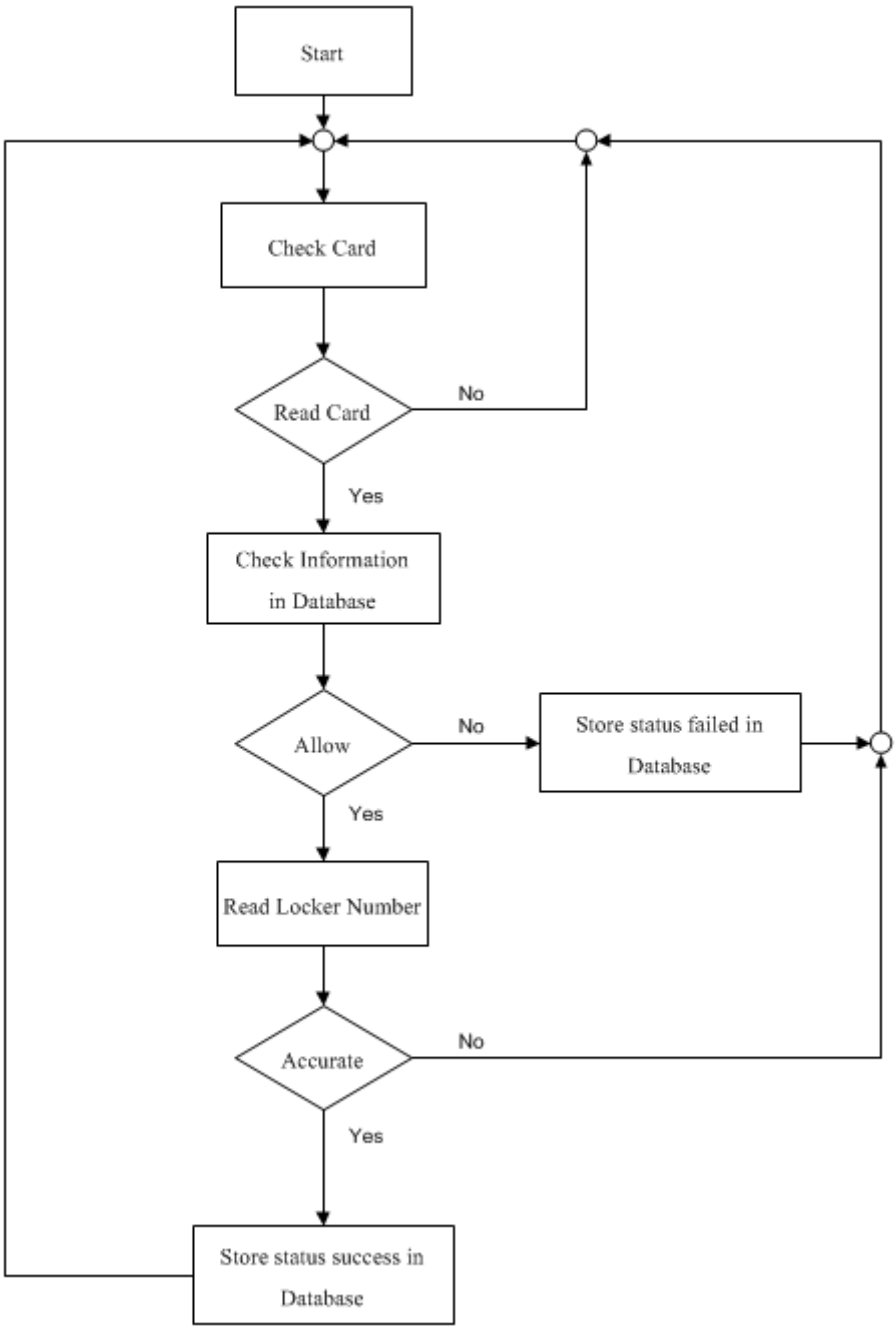


Figure 3.4 Flowchart of Locker system

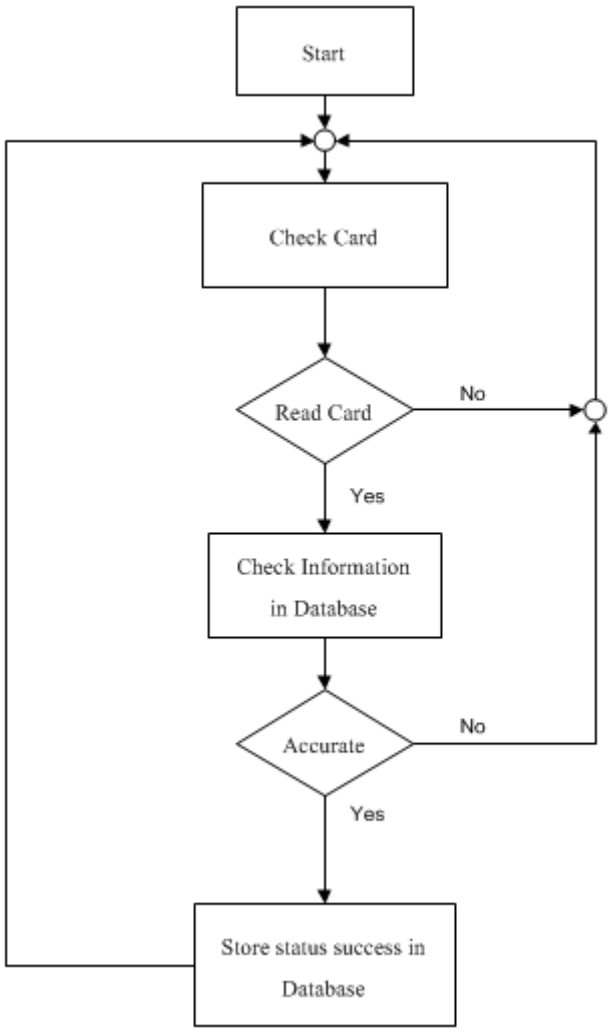


Figure 3.5 Flowchart of Location tracking system

3.3 Database Design

The analysis of designed the system access to use computer through RFID is used to manage Microsoft SQL Server 2005 for database storage system. Data model presents all details related to database design and shows the relation of the various files within the system. This diagram is Entity Relationship Diagram as shown in figure 3.6, and the data dictionary of this system as shown in Appendix b.

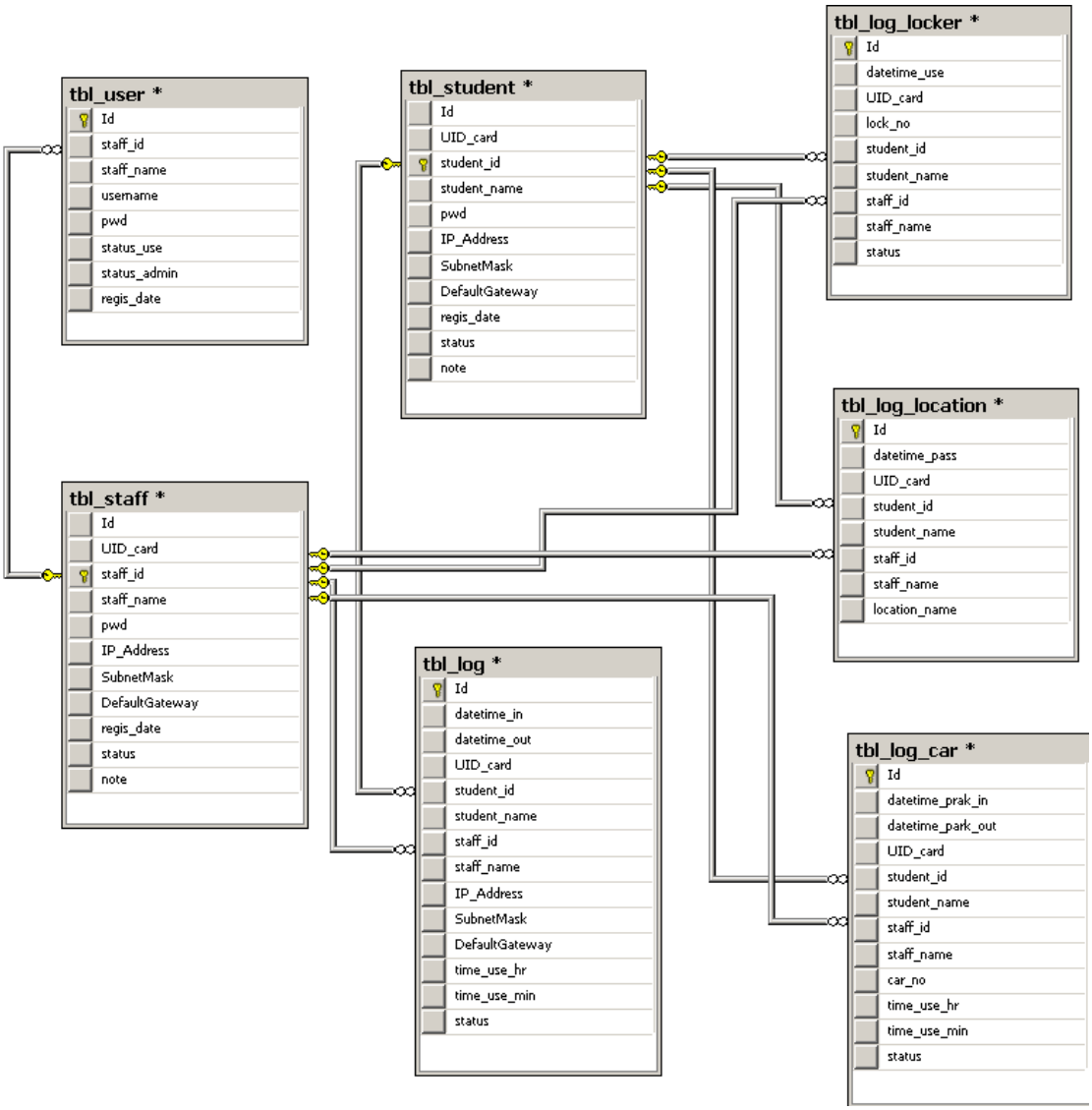


Figure 3.6 Entity Relationship Diagram

3.4 Screen Design

Screen design work will be designed as follows.

- Screen design when open program, it show the logo of the university and message "Please Touch Your Card on Reader"
- Screen design for verify password.
- Screen design for data management of students and administrator, were forced to fill in the name, surname, date, password, access (allowed or not allowed), UID card, IP Address, Subnet Mask, Default Gateway.

3.5 System Testing

In this research the system testing will be connecting to the simulate network to using by VMWare program, connect between Computer Client and Computer Server. It's have to check that to connect by Ping command as shown in figure 3.7. before the assess overall processes by tested from register user, delete name, add name, modify name, set authorization, application test then check IP Address on the computer using the DOS Command: ipconfig see that the IP has been changed or not and check transaction log.

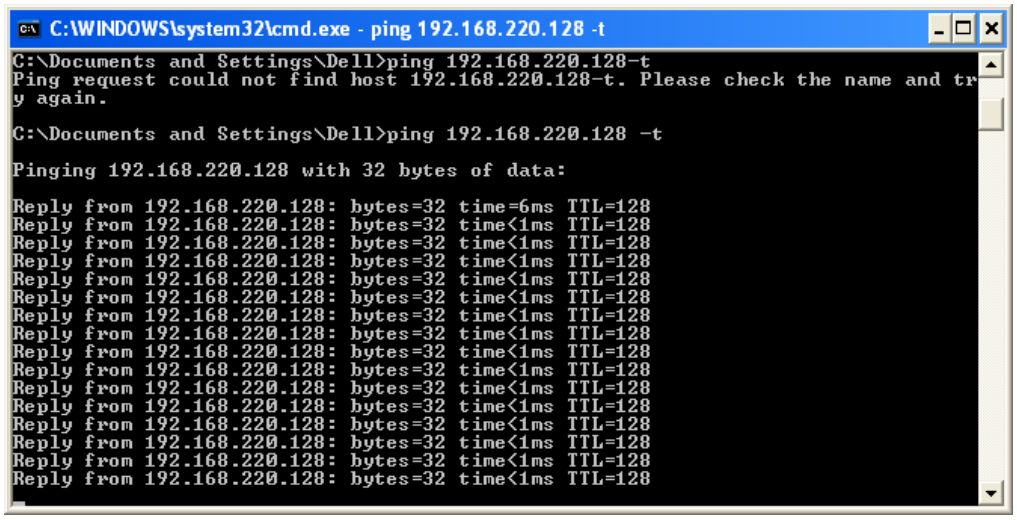


Figure 3.7 Ping Command between Client and Server.

CHAPTER IV
RESULTS AND DISCUSSION

After the design of substitution of Student id card with IP address is completed. In order to apply RF ID technology to be the model for the future development, the researcher would like to present the analysis of the research to fulfill the purpose of the research as follows.

4.1 Perform test by recording and define the right of students and university staffs.

4.2 Perform test of logging in the computer of students and university staffs.

4.3 Report the record of log in/out the computer.

4.4 Additional test to control the car coming to car park by using RFID card.

4.5 Additional test to control locker accessibility by using RFID card.

4.6 Additional test to monitor the student location by the RFID card..

In performing test, one computer server and one client computer is necessary by simulating the virtual program VMware in order to make the main window as the Client computer and Window in VMware as the server which Microsoft SQL server is installed.

4.1 Recording test and students and staffs' right definition.

Perform test by open RFID Authentication System Registration program in order to verify name and password of admin to access the system as in figure 4.1. Then connect RFID reader to sync the data between ID Card and the reader. The finding shows that all fields; Name and Surname, Date, Password and Password confirmation, Status (ok or not ok), UID card (pressing to read UID card is needed prior to filling out UID), IP Address. Subnet Mask and Default gateway are completed

as in the figure 4.2. To recheck by verifying name when log-in found that the students and staffs' right have been recorded completely as in figure 4.3

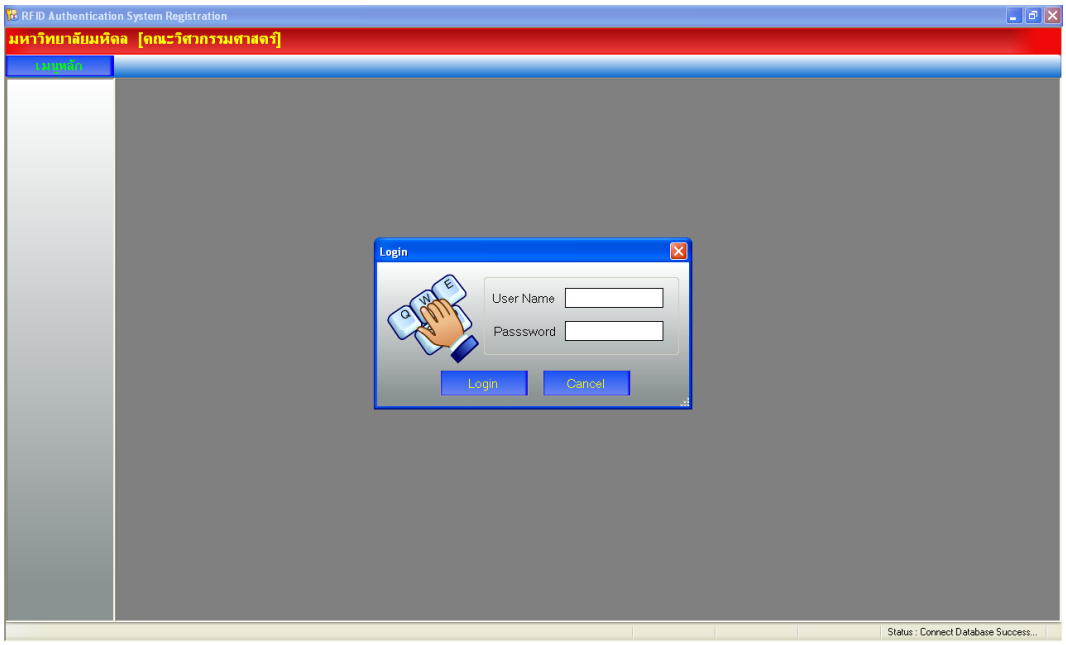


Figure 4.1 Showing the register program.

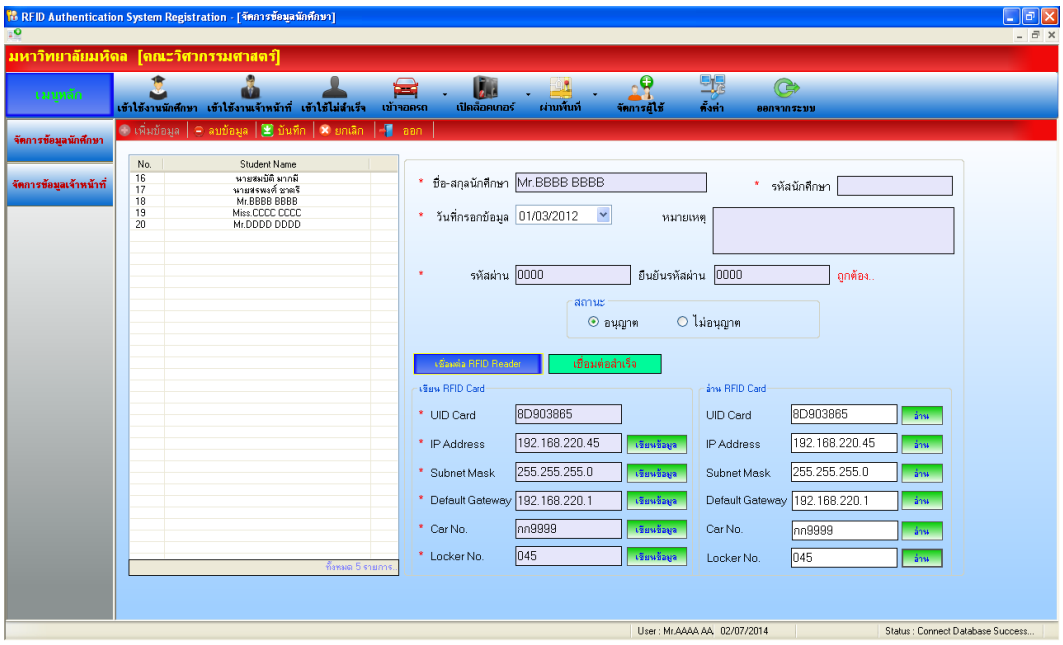


Figure 4.2 Checking data recorded.

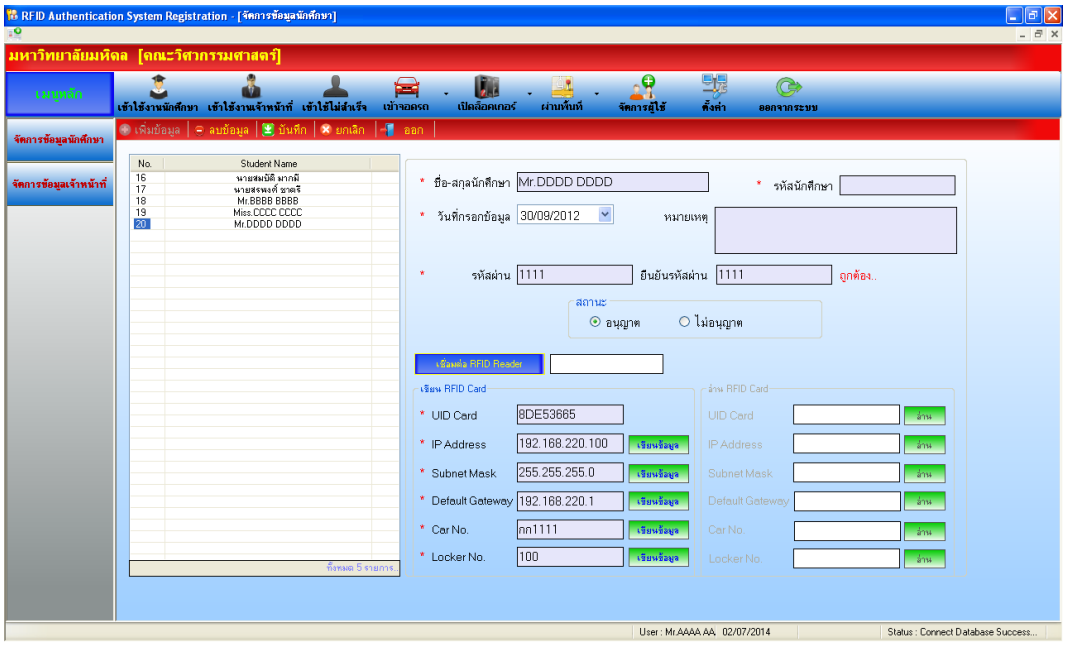


Figure 4.3 Shows the name lists are increasing.

4.2 Perform test students and staffs' accessibility by logging in the computer.

Perform test by opening Pjt AuthIPaddress RFID and participant touch RFID on card reader. The result shows that participant could access to computer to check IP Address by using ipconfig command as in figure found that the data belongs to Mr.BBBB BBBB as in figure 4.5. When move out the RFID from the reader, the system will log-off and the screen turns to home screen automatically.

After the first test completed, the second test is performed again by changing a new RFID. The result shows as same as the first test which participant could log-in to access the computer normally and when check IP Address found that the data belongs to Mr. DDDD DDDD as in figure 4.7

Additional test is performed again using another RFID of Mr. DDDD DDDD used by another reader while the first RFID is using. The result shows that it has been denied due to the same IP Address is detected as the hypothesis. According to the result of the test, it concludes that RFID could be use to verify the personal IP address kept in the database and also protect the duplication of using it unlike log-in by user name and password is available for repeat log-in.

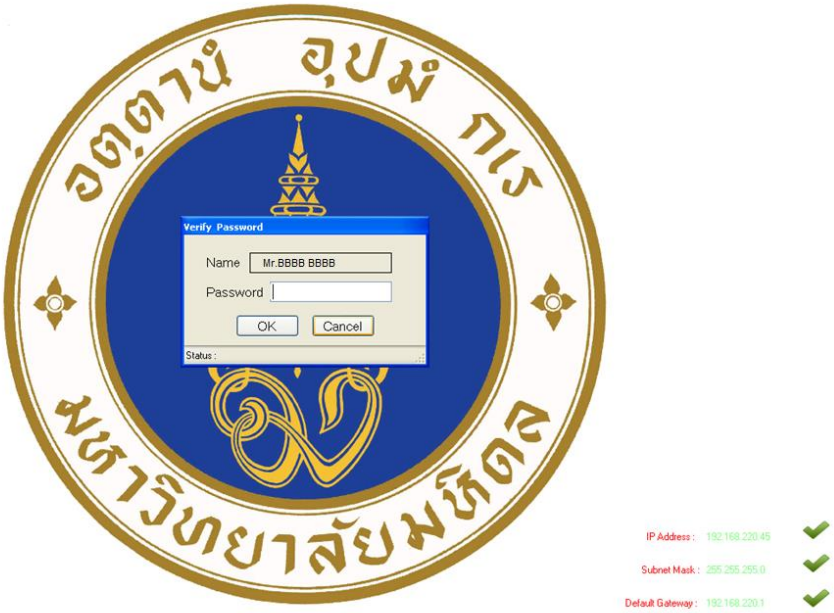


Figure 4.4 Showing the Name, IP Address, Subnet Mask, Default Gateway as access by Mr.BBBB BBBB.

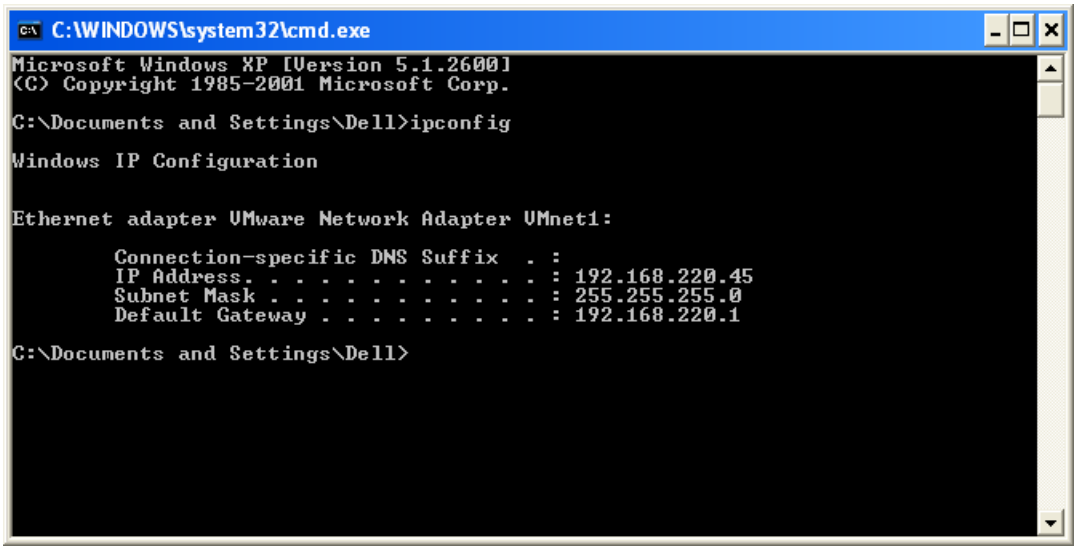


Figure 4.5 Showing the IP Address of Mr. BBBB BBBB.

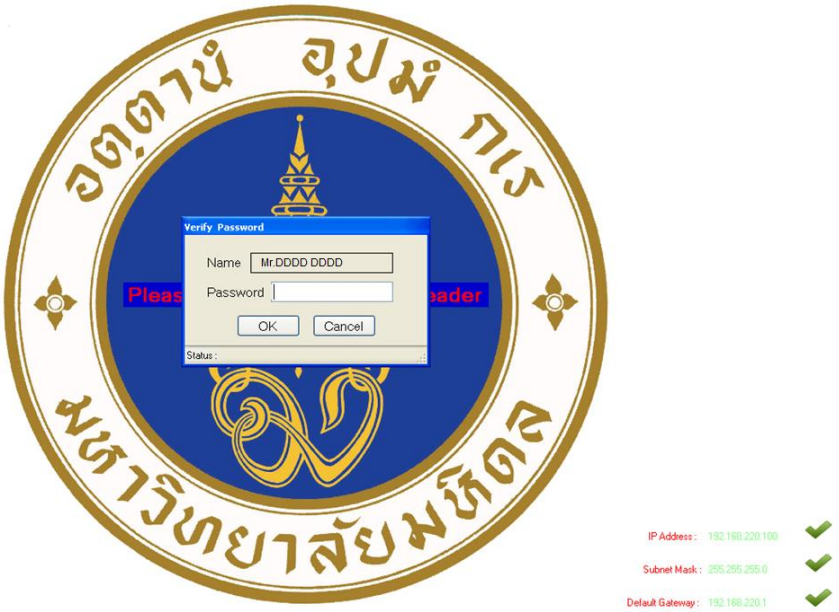


Figure 4.6 Showing the Name, IP Address, Subnet Mask, Default Gateway as access by Mr.DDDD DDDD.

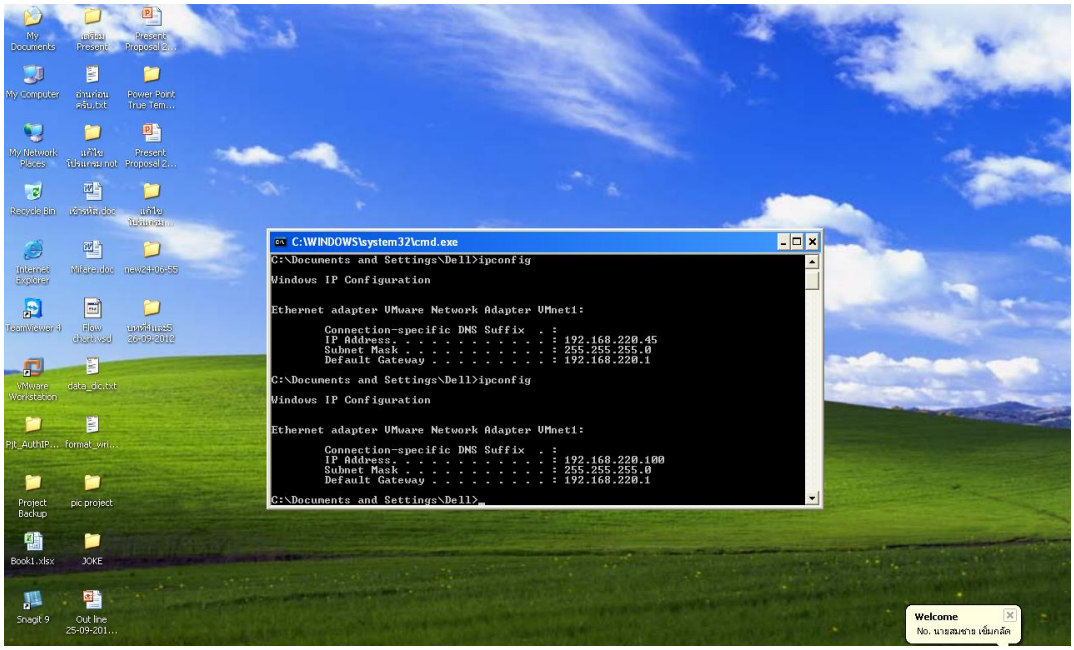


Figure 4.7 Showing the IP Address changes.

4.3 Perform test of report the log of computer access.

During the computer access reporting test, Admin could access by using RFID Authentication System Registration program at the Student access and Staffs access icons. The result shows that the information queried from the program are completely accordance with the record and all errors show correctly.

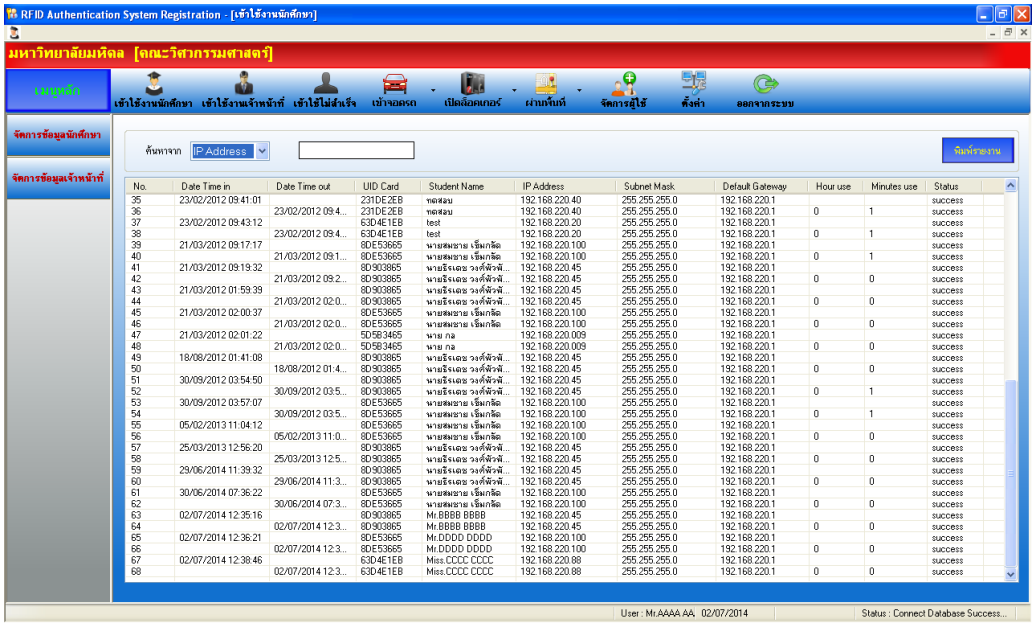


Figure 4.8 Showing the log student access.

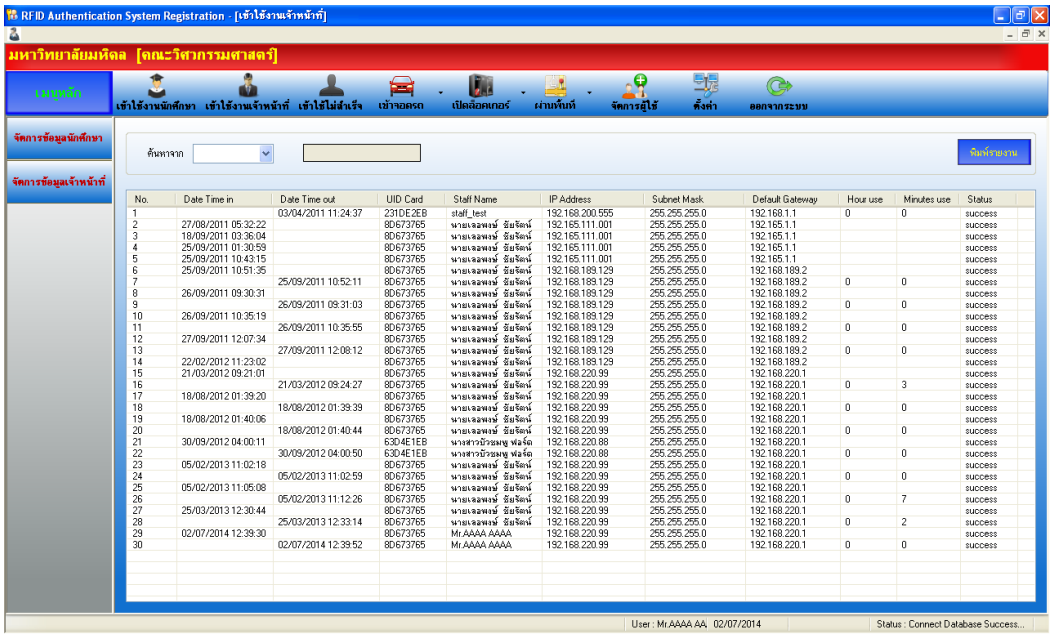


Figure 4.9 Showing the log staff access.

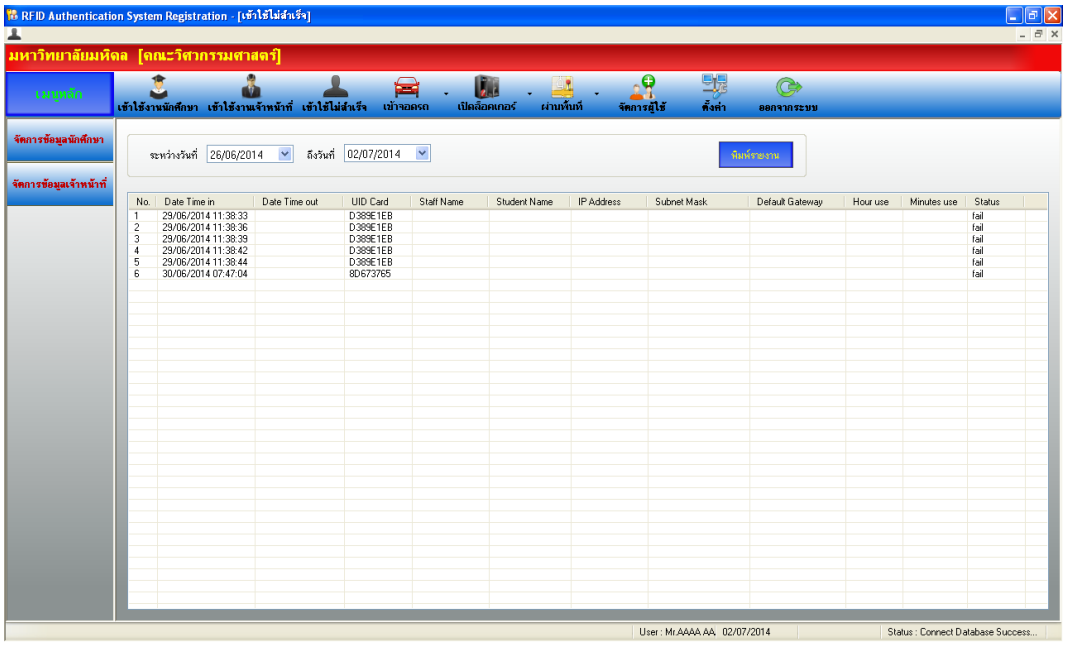
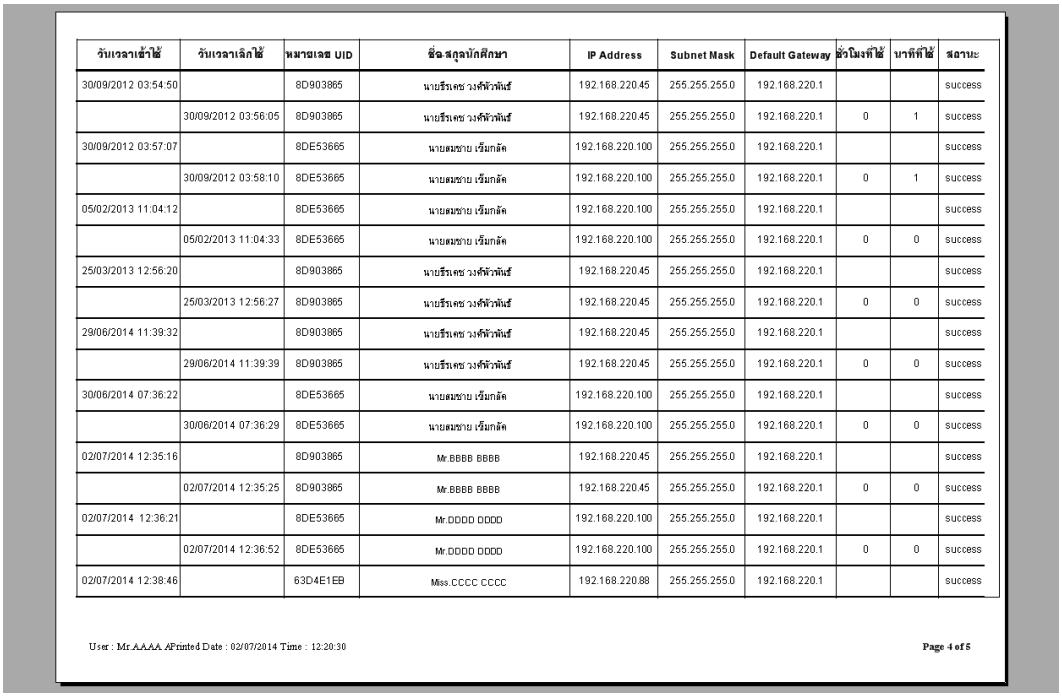


Figure 4.10 Showing the log failed access.



วันเวลาเข้าใช้	วันเวลาเลิกใช้	หมายเลข UID	ชื่อ-สกุลนักศึกษา	IP Address	Subnet Mask	Default Gateway	ชั่วโมงที่ใช้	นาทีที่ใช้	สถานะ
30/09/2012 03:54:50		8D903865	นายรีเดช วงค์พัวพันธ์	192.168.220.45	255.255.255.0	192.168.220.1			success
	30/09/2012 03:56:05	8D903865	นายรีเดช วงค์พัวพันธ์	192.168.220.45	255.255.255.0	192.168.220.1	0	1	success
30/09/2012 03:57:07		8DE53665	นายสมชาย เริ่มกล้า	192.168.220.100	255.255.255.0	192.168.220.1			success
	30/09/2012 03:58:10	8DE53665	นายสมชาย เริ่มกล้า	192.168.220.100	255.255.255.0	192.168.220.1	0	1	success
05/02/2013 11:04:12		8DE53665	นายสมชาย เริ่มกล้า	192.168.220.100	255.255.255.0	192.168.220.1			success
	05/02/2013 11:04:33	8DE53665	นายสมชาย เริ่มกล้า	192.168.220.100	255.255.255.0	192.168.220.1	0	0	success
25/03/2013 12:56:20		8D903865	นายรีเดช วงค์พัวพันธ์	192.168.220.45	255.255.255.0	192.168.220.1			success
	25/03/2013 12:56:27	8D903865	นายรีเดช วงค์พัวพันธ์	192.168.220.45	255.255.255.0	192.168.220.1	0	0	success
29/06/2014 11:39:32		8D903865	นายรีเดช วงค์พัวพันธ์	192.168.220.45	255.255.255.0	192.168.220.1			success
	29/06/2014 11:39:39	8D903865	นายรีเดช วงค์พัวพันธ์	192.168.220.45	255.255.255.0	192.168.220.1	0	0	success
30/06/2014 07:36:22		8DE53665	นายสมชาย เริ่มกล้า	192.168.220.100	255.255.255.0	192.168.220.1			success
	30/06/2014 07:36:29	8DE53665	นายสมชาย เริ่มกล้า	192.168.220.100	255.255.255.0	192.168.220.1	0	0	success
02/07/2014 12:35:16		8D903865	Mr.BBBB BBBB	192.168.220.45	255.255.255.0	192.168.220.1			success
	02/07/2014 12:35:25	8D903865	Mr.BBBB BBBB	192.168.220.45	255.255.255.0	192.168.220.1	0	0	success
02/07/2014 12:36:21		8DE53665	Mr.DDDD DDDD	192.168.220.100	255.255.255.0	192.168.220.1			success
	02/07/2014 12:36:52	8DE53665	Mr.DDDD DDDD	192.168.220.100	255.255.255.0	192.168.220.1	0	0	success
02/07/2014 12:38:46		63D4E1EB	Miss.CCCC CCCC	192.168.220.88	255.255.255.0	192.168.220.1			success

User : Mr.AAAA APrinted Date : 02/07/2014 Time : 12:20:30

Page 4 of 5

Figure 4.11 Showing the report print.

4.4 Additional test to control the car coming to car park by using RFID card.

For the controlling of car parking management in the university, the researcher would like to present the various uses of IP Address through RFID by adding Field Car no. which is simulated that the students or staffs coming to car park then touch RFID card at the entrance and exit as well in order to avoid the tricky of using it repeatedly. The process of RFID used for this case is the system check when enter the car park if still in the car park the system will not allow when re-enter the car park again.

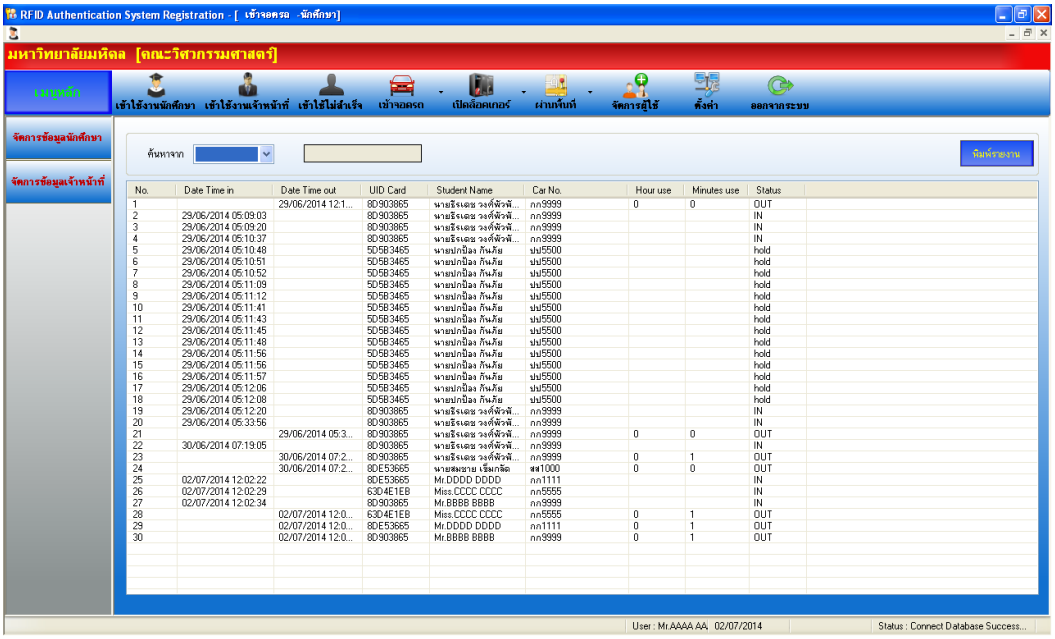


Figure 4.12 Report shows access parking.

4.5 Additional test to control locker accessibility by using RFID card.

For the system controlling the University Locker, researchers adopt the test module by adding Locker no. field which simulated as a tool use for locker management. When the students or staffs want to use Locker service by touching the RFID to the reader. The system checks locker no. which students or staffs have been registered before, such locker open then. The result shows that when RFID was used

with the authorized locker recorded in the reader, the system processes and matches the right locker no. correctly. In addition, the system also send all record such as date and time, UID card, name of student or staffs, IP address, Locker no. and Status to the database as in the figure 4.13

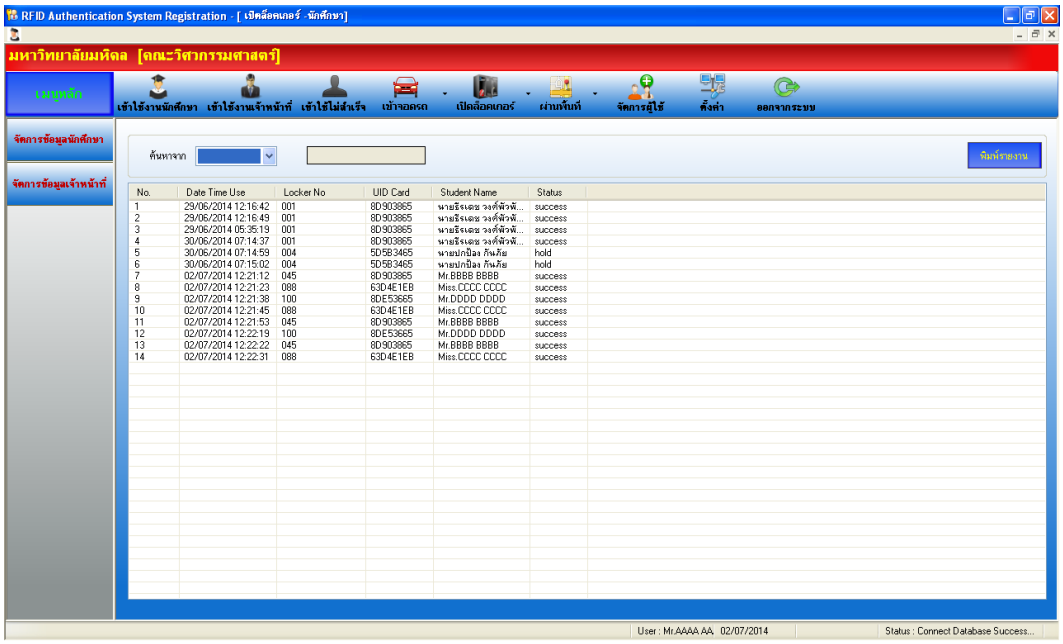


Figure 4.13 Report shows access locker.

4.6 Additional test to record an area or a building access by RFID card.

For this test to control and track students or staffs in a building at the university. The researcher adapted the existing by changing RF Reader becomes RFID Reader Antenna for better transmission.

The test area is divided into 2 zones as in figure 4.14 Which Zone A is corridor and Zone B is classroom. The result shows that when used RFID card into Zone A which the system signal is covered. The system checks who is entering and is the existing person or not. Also send access information to keep in the database such as; Name, IP Address, Building, Floor, zone, access status as in figure 4.15. When get into Zone B out of Zone A coverage, The system check information again from RFID and send to system log accordingly.

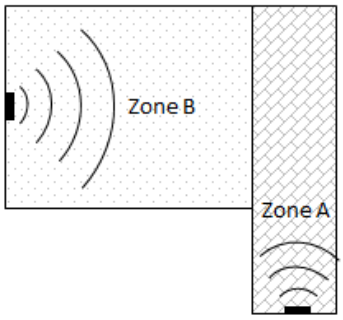


Figure 4.14 Showing the location being tested.

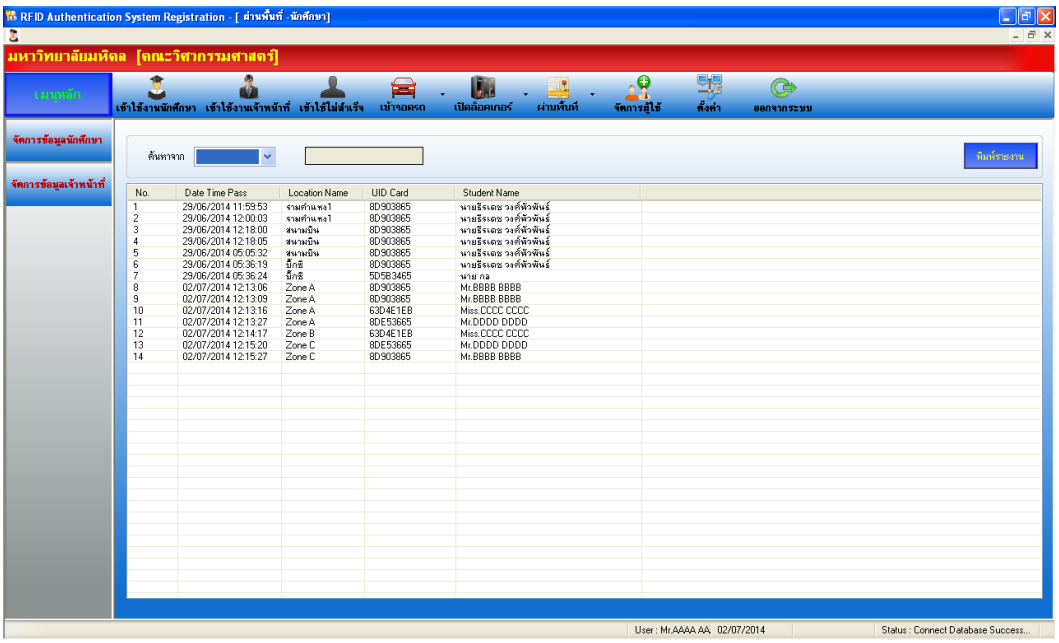


Figure 4.15 Report shows track within designated zones.

4.7 Research discussion.

As per the hypothesis in applying RFID to conduct the cyber crime problem by the use of IP address instead of ID card. The researcher has limit the test by using IP address instead of an existing student ID card .

Researcher approve the hypothesis by taking RFID applied in keeping IP Address which could help the world cyber crime which is tested by installing a simulating software to a computer. The software will connect to RFID Reader and then RFID reader will transmit magnetic wave continuously when the computer is turned on. The system will check RFID when detected in coverage when touch RFID

to The reader. The system will check the information and allow to use computer until taking the RFID of the reader. The computer screen will come to the home screen to be ready for the next user.

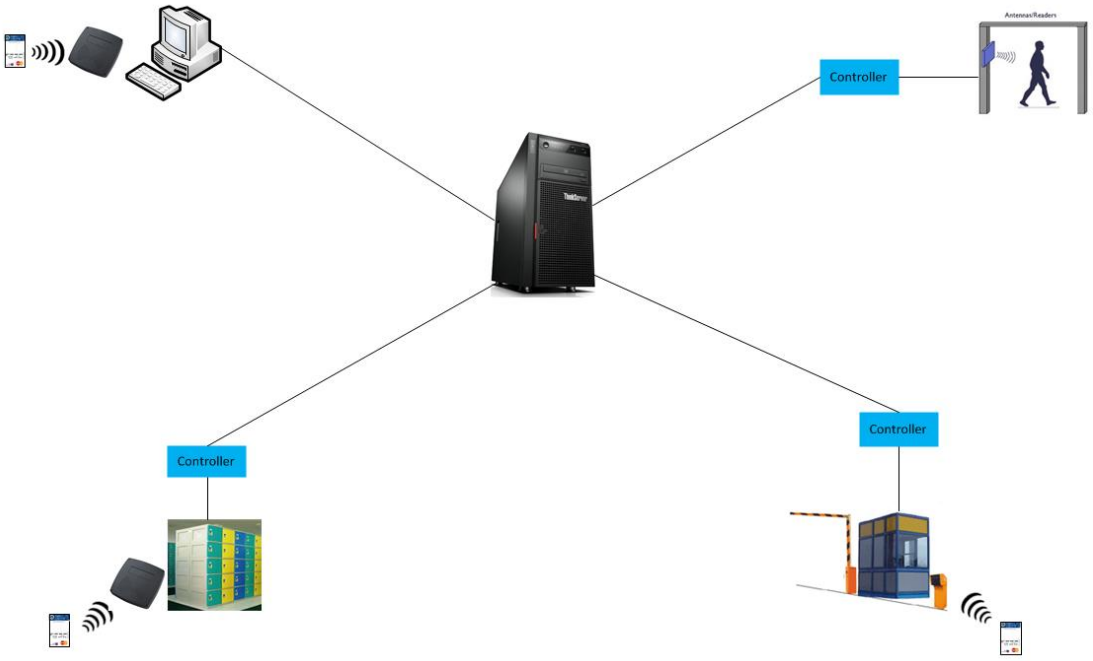


Figure 4.16 Diagram of system.

The results of the additional tests according to the researchers, using essentially the same kit and is more appropriate test equipment. The researchers designed the system to work in harmony with the original test as in figure 4.16. The results showed that the use and processing, as well, which makes use of a visualize of bringing the IP Address instead of a student number in a variety of RFID systems. The results will be seen that using the IP Address instead of a student ID. It can be used in the management of that are complex systems as well, which the different from traditional applications that require access to the User & Password, which can be used in applications that do not check or complexity. Throughout, present the IP Address (IPv6) have a lot, its can replace to student id without duplicates. Moreover, the preparation of the student card and user password which is the original is quite cumbersome for searching and using in complex systems. If IP Address is applied instead of student id, it would create a unity of universities across the country can use

the student id with a data connection through a computer network, which can have all the information online and can also find information quickly as well.

CHAPTER V
CONCLUSION AND RECOMMENDATION

The research was conducted as a model system for the computer, that combination of RFID technology and internet protocol version4 technology with the objective to identify the person using the computer. Using the IP Address instead of the student number, can be summarized that research to advantages, disadvantages and limitations encountered during implementation. The final section will discuss the suggestions to guide for those interested in this research will lead to further development.

5.1 Conclusion

The results obtained from the test divided into sections as follows.

1) Registration

From registration testing of all students and staff can assign different permissions and can modify, add or delete data.

2) Log in

From login testing of all students and staff are touching the card on card reader. As a result, the computer can access and change the IP-Address as the card.

3) Log out

From logout testing of all students and staff pull the card out of card reader. As a result, the computer cannot be used.

4) Switch card

From switch testing both student and staff card. As a result, the computer can be use and IP Address has been change it same the card.

5) Report

The report will be show Date Time in, Date Time out, UID Card, Name, IP Address, Subnet Mask, Default Gateway, Hour use, Minutes use and Status as complete information for that to verify.

From testing to see that the introduction of a number of IP Address instead of the student number. It can actually work, which can be applied to the use of RFID technology with the IP Address to access the computer. It can identify and access the computer and can be used to develop further by expanding the scope of work. Which can summarize advantages - disadvantages are as follows.

Advantages	• Able to track a computer user to quickly. • Can see the behavior of the user. To determine the frequency and duration of use. • The data can be used to analyze the demand and time to prepare to use that computer, to provide adequate equipment to operate within the institution. • Increase the confidence to use anti-theft User & Password to use. • Software development costs are affordable. • RFID technology has been popular and highly Stable & Reliability.
Disadvantages	• Lack of privacy due to watching usage behavior over time. • Increase a hassle to use because it requires student card to use the computer every time.
Limitations	• The experimental results of this research that the Institute has a lot of computer user, it's cannot be tested in the real place.

5.2 Recommendation

From the research of computer access model that using IP Address version4 instead of student ID card, now the IP Address version4 is not enough for using. We have to find a solution to increase the number of IP addresses than IPv4, it is the source of IPv6. IPv6 was developed by the Internet Engineering Task Force (IETF). From the calculation are found the number of IPv6 is enough for using of people around the world, the researcher made a model and have been tested it on a virtual system (VMware).

Suggestion for further, the researcher was suggested as below.

1) In the beginning, use the IP Address with a student id. to verify the information with students who have student id. card number was before. To check the results, and improve to increase the ability for the system to more efficient before modifications are represented by the IP address.

2) Should develop a system to support IPv6 instead of the student number and testing applications with students in the class. It must have equipment.

- Server (storage device)
- Client (refer by the number of student)
- RFID Reader (refer by the number of client)
- RFID Card (refer by the number of student)

3) After the investment has been developing RFID systems, the researcher suggested further by the development of an electronic wallet on the card to be used to pay for products and services of the institution.

4) Should develop a real time notification system or IP address status updates that may be found the problems due to a crime or used misused.

REFERENCES

1 Barrie Sosinsky. (2009). *Networking Bible*, Wiley Publishing Inc., United States of America.

2 Dr. Paul Sanghera and team (2007). *How to Cheat at Deploying and Securing RFID*, Syngress Publishing, Inc., United States of America.

3 Peter H. Cole and Damith C. Ranasinghe (2008) *Networked RFID Systems and Lightweight Cryptography*, Springer-Verlag Berlin Heidelberg, Australia.

4 Mark Brown, Sam Patadia and Sanjiv Dua (2007). *CompTIA RFID + Certification*, The McGraw-Hill Companies, United States of America.

5 Patrick J. Sweeney II, (2005). *RFID For Dummies*, Wiley Publishing, Inc., United States of America.

6 เรืออากาศเอก รุ่งกิจ กมลกลาง (2552). *การประยุกต์ใช้ RFID กับการควบคุมยานพาหนะเข้า - ออก*, วิทยานิพนธ์ สาขาบริหารเทคโนโลยีสารสนเทศ วิทยาศาสตรมหาบัณฑิต สถาบันบัณฑิตพัฒนบริหารศาสตร์

7 ปิยะ โควินท์ทวีวัฒน์ และคณะ (2552). *ระบบบ่งชี้ด้วยคลื่นความถี่วิทยุ Radio Frequency Identification (RFID) System*, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

8 วัชรากร หนูทอง, อนุกูล น้อยไม้ และ ปรินันท์ วรรณสว่าง, *RFID เทคโนโลยีสารพัดประโยชน์*, สาร NECTEC ฉบับที่ กันยายน - ตุลาคม 2547 หน้าที่ 15-22

9 Manutsiri Chansutthirangkool (2005). *Performance Evaluation of Multicast VIDEO Conference Transmission Protocol: A Comparision Between IPv4 and IPv6*, (M.Eng.), Faculty of graduate studies, Mahidol University.

10 Umaphorn Thongrak (2009). *Energy Save Cost Control using RFID Access Card*, (M.Eng), Faculty of graduate study, Sripatum University.

11 โอภาส เอี่ยมสิริวงศ์ (2552). เครือข่ายคอมพิวเตอร์และการสื่อสาร, ซีเอ็ดยูเคชั่น, กรุงเทพฯ

12 ก่อกิจ วีระอาชากุล (2553). Guide & Practice Network Administration, IDC Premier, นนทบุรี

13 Andrew S. Tanenbaum (2010). Computer Networks (5th Edition), Pearson Education Inc., New Jersey, United States of America.

14 สัจจะ จรัสรุ่งรวีวร (2552). เริ่มต้น Visual C# 2008 ฉบับสมบูรณ์, IDC Info Distributor Center, นนทบุรี

15 สุวัฒน์ ปุณณชัยยะ, ต้น ตันฑ์สุทธิวงศ์ และ สุพจน์ ปุณณชัยยะ (2543). เปิกโลกของ TCP/IP และโปรโตคอลของอินเตอร์เน็ต, โปรวิชั่น, กรุงเทพฯ

16 T.S. Lim, S.C. Sim and M.M. Mansor (2009). RFID Based Attendance System, Faculty of Engineering and Technology, Multimedia University, Malaysia

17 Sandra Dominikus, Manfred Aigner and Stefan Kraxberger (2010). Passive RFID Technology for the Internet of Things, Institute for Applied Information Processing and Communications, Graz University of Technology, Austria.

18 Harinda Fernando (2011). Mutual Authentication Protocol for Networked RFID Systems, School of Information Technology Deakin University, Australia

19 Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Eng (2004). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, Massachusetts Institute of Technology, United States of America.

20 Dang Nguyen Duc, Hyunrok Lee, Divyan M. Konidala and Kwangjo Kim (2009). Open issues in RFID security, South Korea

21 Shao Xiwen (2012). Study on Security Issue of Internet of Things Based on RFID, Comput. Inf. Center, Beijing Inst. of Fashion Technol., Beijing, China

APPENDICES

APPENDIX A
PRODUCT DATA SHEET

RFID cards are EEPROM Memory Size 1 Kbyte, divides memory into 16 Sectors (0-15).

The chip consists of a 1 KBytes EEPROM, RF interface and Digital Control Unit. Energy and data are transferred via an antenna consisting of a coil with a small number of turns which is directly connected to the chip. No further external components are necessary.

EEPROM: 1 KBytes is organized in 16 sectors with 4 blocks each. A block contains 16 bytes. The last block of each sector is called “trailer”, which contains two secret keys and programmable access conditions for each block in this sector.

Memory structure of EEPROM 1 K.

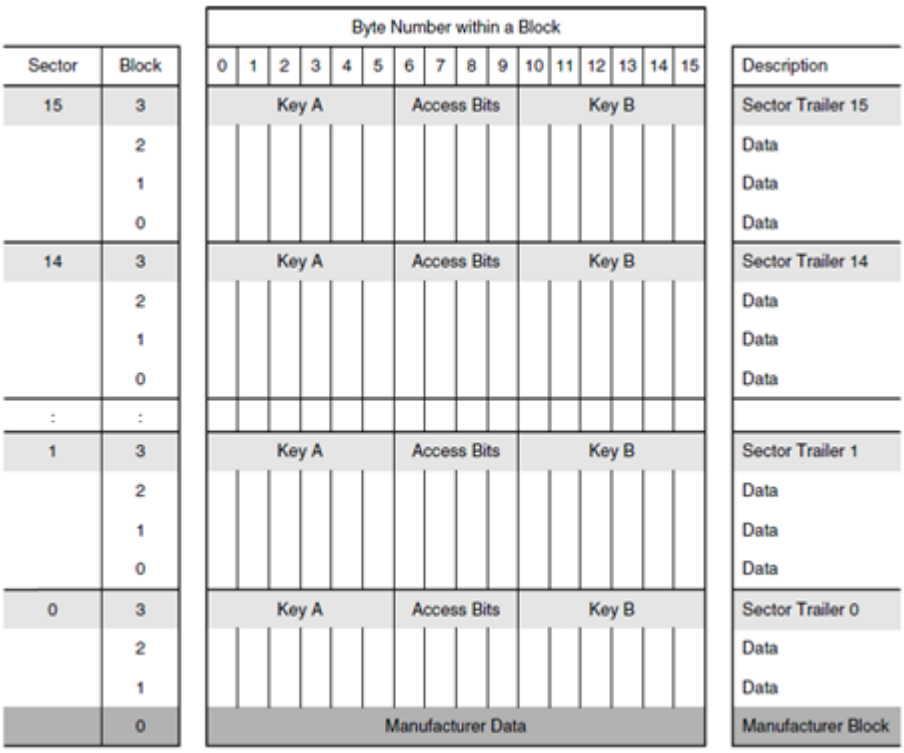


Figure A-1 The Structure of RFID Card.

1) Manufacturer block

This is the first data block (block 0) of the first sector (sector 0). It contains the IC manufacturer data. This block is programmed and write protected in the production test.

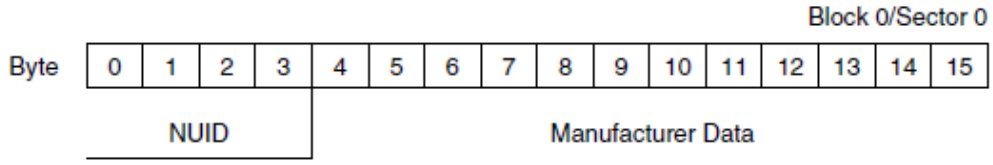


Figure A-2 Manufacturer block

2) Data blocks

All sectors contain 3 blocks of 16 bytes for storing data (Sector 0 contains only two data blocks and the read-only manufacturer block).

3) Sector trailer (block 3)

The sector trailer is the last block (block 3) in one sector. Each sector has a sector trailer containing the key A and key B, used to store key A (right to use) and key B (the right to read / write).

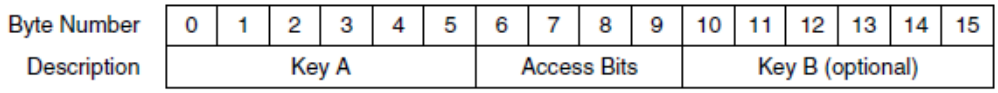


Figure A-3 Manufacturer block

Each sector can not be used block 3, but if memory is not enough, the memory in key B can be used.

The memory can be used as normal is.

Sector 0 = 2 x 16 = 32 Bytes.

Sector 1-15 = 15 x 3 x 16 = 720 Bytes.

Table A-1 RFID Card Reader Specifications.

Host Communication	USB
Communication Speed (RS232)	9600 – 115200 baud rate (default 19200)
Contactless Interface	ISO14443 Type A
Supported card	Mifare® Standard, Mifare® Ultralight, Mifare® 1k/4k
Operation Frequency	13.56MHz
Communication Rate	106Kbit/s
Indicators	2-color LED(Red, Green), one buzzer
Communication Cable on Cable	1.2 meter long USB communication cable
Power Supply	Power supplied from USB (USB Interface)
Current Consumption	< 120 mA
Reading Distance	0 - 5 cm (depending on transponders)
Operating Temperature	0 oC ~ +65 oC
Operating Humidity	0 ~ 95% relative humidity non-condensing
Development Kit	Window-based Reader API and low level communication protocol will be provided by the development kit
Special Feature	Easy update design. The Customized firmware could be implemented to meet the user's special requirement

APPENDIX B
DATA DICTIONARY

Table 1 Data Dictionary of Student

No	Field Name	Key	Description	Length	Type
1	Id		Autorun number	4	int
2	UID_card		Number of UID Card	8	varchar
3	student_id	PK	Student ID.	20	varchar
4	student_name		Student Name	20	varchar
5	pwd		Password to access	20	varchar
6	IP_Address		IP Address is written to the card in sector 01 block 00.	15	varchar
7	Subnetmask		Subnet Mask is written to the card in sector 01 block 01.	15	varchar
8	DefaultGateway		Default Gateway is written to the card in sector 01 block 02.	15	varchar
9	Regis_date		Register Date	8	datetime
10	Status		Permissions - 0 = Not allowed - 1 = Allowed	1	bit
11	Note		Note (optional)	200	varchar

Table 2 Data Dictionary of User

No	Field Name	Key	Description	Length	Type
1	Id	PK	Autorun number	4	int
2	Staff_id	FK	Staff ID.	8	varchar
3	Staff_name		Staff Name	50	varchar
4	Username		User name for register program	20	varchar

Table 2 Data Dictionary of User (cont.)

No	Field Name	Key	Description	Length	Type
5	Pwd		Password to access for register program	20	varchar
6	Status_user		Permissions - 0 = Not allowed - 1 = Allowed	1	bit
7	Status_admin		Permissions for Admin - 0 = Not allowed - 1 = Allowed	1	bit
8	Regis_date		Register Date	8	datetime

Table 3 Data Dictionary of Staff

No	Field Name	Key	Description	Length	Type
1	Id		Autorun number	4	int
2	UID_card		Number of UID Card	8	varchar
3	Staff_id	PK	Staff ID.	20	varchar
4	staff_name		Staff Name	20	varchar
5	pwd		Password to access	20	varchar
6	IP_Address		IP Address is written to the card in sector 01 block 00.	15	varchar
7	Subnetmask		Subnet Mask is written to the card in sector 01 block 01.	15	varchar
8	DefaultGateway		Default Gateway is written to the card in sector 01 block 02.	15	varchar
9	Regis_date		Register Date	8	datetime
10	Status		Permissions - 0 = Not allowed - 1 = Allowed	1	bit
11	Note		Note (optional)	200	varchar

Table 4 Data Dictionary of Computer Using Log

No	Field Name	Key	Description	Length	Type
1	Id	PK	Autorun number	4	int
2	Datetime_in		Login date	8	datetime
3	Datetime_out		Logout date	8	datetime
4	UID_card		Number of UID Card	8	varchar
5	Student_id	FK	Student ID.	20	varchar
6	Student_name		Student Name	100	varchar
7	Staff_id	FK	Staff ID.	20	varchar
8	Staff_name		Staff Name	100	varchar
9	IP_Address		IP Address is written to the card in sector 01 block 00.	15	varchar
10	SubnetMask		Subnet Mask is written to the card in sector 01 block 01.	15	varchar
11	DefaultGateway		Default Gateway is written to the card in sector 01 block 02.	15	varchar
12	Time_use_hr		The number of hours to use.	4	int
13	Time_use_min		The number of minutes to use	4	int
14	Status		Status to access - Success = available. - Fail = no data. - Hold = have data but not allowed to use.	20	varchar

Table 5 Data Dictionary of Parking Log

No	Field Name	Key	Description	Length	Type
1	Id	PK	Autorun number	4	int
2	Datetime_in		Login date	8	datetime
3	Datetime_out		Logout date	8	datetime
4	UID_card		Number of UID Card	8	varchar
5	Student_id	FK	Student ID.	20	varchar
6	Student_name		Student Name	100	varchar

Table 5 Data Dictionary of Parking Log (cont.)

No	Field Name	Key	Description	Length	Type
7	Staff_id	FK	Staff ID.	20	varchar
8	Staff_name		Staff Name	100	varchar
9	Car_no		IP Address is written to the card in sector 02 block 00.	15	varchar
10	Time_use_hr		The number of hours to use.	4	int
11	Time_use_min		The number of minutes to use	4	int
12	Status		Status to access - In - Out - Hold = have data but not allowed to use.	20	varchar

Table 6 Data Dictionary of Location Log

No	Field Name	Key	Description	Length	Type
1	Id	PK	Autorun number	4	int
2	Datetime_pass		Date of detected by the system.	8	datetime
3	UID_card		Number of UID Card	8	varchar
4	Student_id	FK	Student ID.	20	varchar
5	Student_name		Student Name	100	varchar
6	Staff_id	FK	Staff ID.	20	varchar
7	Staff_name		Staff Name	100	varchar
8	Location_name		Name of place	100	varchar

Table 7 Data Dictionary of Locker Log

No	Field Name	Key	Description	Length	Type
1	Id	PK	Autorun number	4	int
2	Datetime_use		Date of using.	8	datetime
3	UID_card		Number of UID Card	8	varchar

Table 7 Data Dictionary of Locker Log (cont.)

No	Field Name	Key	Description	Length	Type
4	Student_id	FK	Student ID.	20	varchar
5	Student_name		Student Name	100	varchar
6	Staff_id	FK	Staff ID.	20	varchar
7	Staff_name		Staff Name	100	varchar
8	Location_name		Name of place	100	varchar
9	Status		Status to access - Success - Hold = have data but not allowed to use.	20	varchar

BIOGRAPHY

NAME	Lerpong Chairat
DATE OF BIRTH	04 June 1977
PLACE OF BIRTH	Yala, Thailand
INSTITUTIONS ATTENDED	South East Asia University, 1997-1999 Bachelor of Industrial Technology (Electronic Engineering) Mahidol University, 2009-2011 Master of Science (Technology of Information System Management)
RESEARCH GRANTS	Mini-Engineering project
HOME ADDRESS	12/16 M.9, Soi Thawi Watthana 51, Thawi Watthana Road, Sala Thammasob, Thawi Watthana, Bangkok, Thailand 10170 Tel. 089-110-4445 E-mail: ninejoker@hotmail.com
EMPLOYMENT ADDRESS	The Siam Commercial Bank Public Company Limited Head Office. 9, Rutchadapisek Road, Jatujak, Jatujak, Bangkok, Thailand 10900 Tel. (02) 544-4391