RFID Security Using miniDES Algorithm in Deployment of Bike Renting System

Kurra Mallaiah
Advanced Numerical Research & Analysis Group(ANURAG),
DRDO, Hyderabad, Andhra Pradesh, india-500058
E-mail: km_mallaiah@yahoo.com

Abstract
Radio frequency identification (RFID) is a generic term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an entity or person wirelessly, using radio waves. Unlike bar-code technology, RFID technology does not require contact or line of sight for communication. RFID data can be read through the human body, clothing and non-metallic materials. RFID Systems technically consist of RFID Tags, Readers, Communication Protocols and Information Systems. These technical parts enable the collection of data on the tagged object or person. In most of today's RFID Systems the data on the tag is accessible by anyone who is able to operate a RFID reader in such cases how much these RFID tags are protected? The tags accessed data should be only readable to authenticated people. The challenge in providing security for low- cost RFID tags is that they are computationally weak systems, unable to perform even basic symmetric-key cryptographic operations et al "ARI JUELS(2004)" . Security for RFID systems has to start at the base of the technology. Information on the tags has to be stored in a secure way by using a lightweight crypto algorithm. The processing capabilities of many RFID based embedded systems are easily besieged by the computational demands of security processing, leading to failures in sustaining required data rates or number of connections et al "SRIVATHS RAVI & ANAND RAGHUNATHAN, PAUL KOCHER, SUNIL HATTANGADY" . In this paper, I explore a concept of miniDES symmetric key algorithm is suitable for RFID tag security deploying in the Bike renting system. I consider the type of security obtainable in RFID based devices with a small amount of rewritable memory, but very limited computing capability. My aim is to show that miniDES algorithm is efficient and sufficient to provide the security for the RFID based systems, there is no need for very complex cryptography algorithms which requires high power of computational power. And the automation of bike renting system definitely enhances the performance of the bike renting process
Keywords: Radio frequency Identification, Bike renting, miniDES, embedded systems, cryptography, smart card systems

1. Introduction

1.1 RFID

RFID is an ADC technology that uses radio-frequency waves to transfer data between a reader and a movable item to identify, categorize and track. A radio-frequency identification (RFID) tag is a small, inexpensive microchip that emits an identifier in response to a query from a nearby reader. The price of these tags promises to drop to the range of $0.05 per unit in the next several years et al "ARI JUELS(2004)" , offering a viable and powerful replacement for barcodes. It's grouped under the broad category of automatic identification technologies. RFID is in use all around us. There are two sorts of RFID tags. One is passive and the other is active. Active RFID tags need a battery built-in it and passive RFID tags not necessary. A RFID system provides diversified frequency bands et al "KUO-SHIEN HUANG, SHUN-MING TANG(2008)" :

Low Frequency: 125-134 KHz
High Frequency: 13.56 MHz
Ultra High Frequency: 902-928 MHz
Microwave Frequency: 2.4 GHz

Components of RFID

A basic RFID system consists of three components as shown in the Figure 1.1 An antenna or coil, a transceiver (with decoder), Transponder (RF tag) electronically programmed with unique information. The antenna emits radio signals to activate the tag and to read and write data to it. The reader emits radio waves in ranges of anywhere from one inch to 100 feet or more, depending upon its power output and the radio frequency used. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit (silicon chip) and the data is passed to the host computer for processing. The purpose of an RFID system is to enable data to be transmitted by a portable device, called a tag, which is read by an RFID reader and processed according to the needs of a particular application. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, date of purchase, etc. RFID technology has been used by thousands of companies for a decade or more. . RFID quickly gained attention because of its ability to track moving objects. As the technology is refined, more pervasive – and invasive - uses for RFID tags are in the works. A typical RFID tag consists of a microchip attached to a radio antenna mounted on a substrate. The chip can store as much as 2 kilobytes of data. To retrieve the data stored on an RFID tag, you need a reader. A typical reader is a device that has one or more antennas that emit radio waves and receive signals back from the tag. The reader then passes the information in digital form to a computer system.

1.2 Embedded systems

According to SearchEnterpriseLinux.com "An embedded system is some combination of computer hardware and software, either fixed in capability or programmable that is specifically designed for a particular kind of application device". Embedded systems control many devices in common use today. Embedded systems are controlled by one or more main processing cores that are typically either microcontrollers or digital signal processors (DSP). Physically embedded systems range from portable devices such as digital watches and MP3 players, to large stationary installations like traffic lights, factory controllers, or the systems controlling nuclear power plants. Complexity varies from low, with a single microcontroller chip, to very high with multiple units, peripherals and networks mounted inside a large chassis or enclosure. In general, "embedded system" is not a strictly definable term, as most systems have some element of extensibility or programmability. For example, handheld computers share some elements with embedded systems such as the operating systems and microprocessors which power them, but they allow different applications to be loaded and peripherals to be connected. Moreover, even systems which don't expose programmability as a primary feature generally need to support software updates. On a continuum from "general purpose" to "embedded", large application systems will have subcomponents at most points even if the system as a whole is "designed to perform one or a few dedicated functions", and is thus appropriate to call "embedded". The program instructions written for embedded systems are referred to as firmware, and are stored in read-only memory or Flash memory chips. They run with limited computer hardware resources: little memory, small keyboard and/or screen. or non-existent

1.3 Smart card systems

A smart card, chip card, or integrated circuit(s) card (ICC), is defined as any pocket-sized card with embedded integrated circuits.

Contactless Smart Card

The chip contactless smart card communicates with the card reader through RFID induction technology. In this technology it is not necessary to insert the card into the reader to read the card's content, using air communication the tag's content will be accessed by the reader. This is more vulnerable to security attacks in the contactless smart card systems. This technology is more prone to security attacks like interruption of operation, covert transactions, Denial of services, eavesdropping and many more. Therefore providing a viable security in contact less smartcard systems are mandatory because nowadays these cards are being used in many applications in day to day life.

2.Related work

Automation of bike renting system using RFID tags. According to the need, the renting bike store attaches RFID tag to the bikes et al "KUO-SHIEN HUANG, SHUN-MING TANG(2008)" which contains the unique serial number encrypted by the miniDES algorithm. The RFID tags that are available with a fixed frequency are set with rented bikes and the RFID reader will read the card and the identity number which is uniquely present on the RFID tag. The reading of the Unique Hex code on the card takes place only when RFID card has the same frequency that of the reader frequency. The card data that will be fed to the system using microcontroller with a serial port communication and this will be maintained in database in the system in .NET frame work. Here combining the power of both Microsoft .Net and embedded systems for user convenience. This is actually done because need a large data base to maintain the complete data of bike that are in the hire. The microcontroller receives the RFID card data from RFID reader using serial communication. Microcontroller decrypts the deceived data using MiniDES algorithm and compares with the valid available RFID numbers in the controller which ensures the authentication of the tag and hence the security of the system. In the microcontroller the time is taken from RTC and the time and take of the bike holder will be recorded. The RTC time and status of the bike are fed to the system using the serial communication. Where in .Net OUT time and IN time and status of the bikes are stored in the database, using OUT and IN time rent amount is calculated.

When bike is going from garage on rent the bike's attached tag is read by the RFID reader and communicates to the microcontroller using serial communication where bike's OUT time is recorded in the system. When bike comes for delivery again the bike's attached tag is read now time is recorded as IN time,using OUT and IN time the bikes rent is calculated. The tag assigned to the bike is read twice, one at the time of bike going out garage on rent and second at the time of delivery. The cards that are assigned to the bikes are passive ID cards. This passive card doesn't have any power. This is activated with the help of the frequency that is generated by the reader itself. Figure 2.1 illustrates the complete functional block diagram of the system

2.2 Connectivity among modules of system at operation

Figure 2.2 illustrates the connectivity among modules of system at operation.

2.3 AT89S52 Microcontroller functionalities

AT89S52 is a low-power, high-performance CMOS 8-bit microcontroller with 8K bytes of in-system programmable Flash memory. The device is manufactured using Atmel's high-density nonvolatile memory technology and is compatible with the industry-standard 80C51 instruction set and pinout. The on-chip Flash allows the program memory to be reprogrammed in- system or by a conventional nonvolatile memory programmer. By combining a versatile 8-bit CPU with in-system programmable Flash on a monolithic chip, the Atmel AT89S52 is a powerful microcontroller which provides a highly- flexible and cost-effective solution to many embedded control applications. The AT89S52 provides the following standard features: 8K bytes of Flash, 256 bytes of RAM, 32 I/O lines, Watchdog timer, two data pointers, three 16-bit timer/counters, a six-vector two-level interrupt architecture, a full duplex serial port, on-chip oscillator, and clock circuitry. In addition, the AT89S52 is designed with static logic for operation down to zero frequency and supports two software selectable power saving modes. The Idle Mode stops the CPU while allowing the RAM, timer/counters, serial port, and interrupt system to continue functioning. The Power-down mode saves the RAM con-tents but freezes the oscillator, disabling all other chip functions until the next interrupt. Figure2.3 shows the AT89S52 microcontroller module which receives unique 12 hex characters from RFID reader using serial communication in interrupt mode. Each bike is assigned with a RFID tag these tags data i.e. RFID number is maintained in the microcontroller. It decrypts the received data from reader using MiniDES algorithm and compares with the existing RFID numbers if it matches it is valid one otherwise it is invalid. If number does not match then it will simply ignore that data and will not communicate anything to the system for storing purpose. If the Number matches then it communicates information to the system such as Name of the bike, RFID number, current RTC time and status i.e. OUT or IN. When the first time number matches then it sends status as OUT, in second time it is IN. It reads current date and time from the battery operated RTC and displays this information on the LCD display

2.4 Evaluation

RFID tags used in deployment of RFID tags in bike renting are 125 KHz and RFID reader is 125 KHz compatible. The reader reads the RFID tag's content wirelessly and decodes and this data will be transferred to the microcontroller using serial communication. Reading of the same tag twice takes place once for at the time of taking bike away on rent and second at the time of delivery. AT89S52microcontroller module receives unique 12 hex characters from RFID reader using serial communication in interrupt mode. Here three bikes are taken as samples and assigned with a RFID tag these tags data i.e. RFID number is maintained in the microcontroller. In microcontroller decrypting the received data using MiniDES algorithm and comparing with the existing RFID numbers if it matches it is a valid one otherwise it is invalid. If number does not match then ignoring that data and will not communicate anything to the system. If the Number matches then communicating information to the system using serial communication such as Name of the bike, ID number ,current RTC time, and status i.e.OUT or IN. When the first time number matches then sending status as OUT, in second time it is IN with each valid tag. Microcontroller reads current date and time from the battery operated RTC as and when receive tag's data from the Reader module and this is being used as OUT and IN time in renting process and displaying this information on the LCD display. At system side using the Microsoft .NET framework receiving the communicated data from microcontroller using serial communication and storing in the SQL database. In .Net using the OUT and IN time the rent amount is calculated for each rented bike when it comes for delivery. Displaying the complete status of the bikes such as OUT time, IN time, amount of rent after each delivery, whether bike is in garage i.e. IN or OUT i.e. on rent on the web portal with search and edit option. Three bikes taken as samples such as HONDA, DISCOVER, and SPLENDOR and assigned with a 125 KHz RFID tags. HONDA's assigned RFID tag number is 0108F6AEBAEB and DISCOVER's tag number is 0108F69498F3 and SPLENDOR ''s tag number is 0108F69499F2 as shown in the Figure 2.4. The output of the bike renting system is shown in the figures Figure 2.4, Figure 2.4.1, Figure 2.4.2 with three sample bikes. It contains RFID number associated with a bike, name of the bike, OUT time of the bike, IN time of the bike and status of the bike and amount. The status OUT indicates the bike is on rent, HONDA's status is OUT as shown in the Figure 2.4 i.e. HONDA bike is on rent. The status IN indicates the bike is inside the Garage, SPLENDER's status is IN as shown in Figure 2.4 i.e. SPLENDER is in the garage. Using OUT and IN time amount of the bike rent is calculated , for SPLENDER rent amount is Rs 2 because OUT and IN time difference is 1 minute only(Rent is fixed Rs 2 for minute for splendor).

Search option

The figure 2.4.2 illustrates the output of the project with a search option with which one can search for all or one specific type of bike status. In above figure 2.4 in search option have All, Honda, Splendor and Discover. If select 'All' as search option gets all bikes status is shown in Figure 2.4, if select Honda as search option get only Honda bikes status as shown in the Figure 2.4.2

Edit option

It has edit option to edit the rent amount and update in the database i.e. one can increase or decrease the rent amount as shown in the Figure 2.4.3

2.5 Microsoft .Net frame work functionalities at system side (PC)

Using Microsoft.Net the following functionalities have been achieved:

Receive data from serial port, segregate the received data, and store the segregated data in the database with options of updating and inserting operations, calculates the bike rent amount using received data, displaying the status of the bikes on the web portal, edit the rent amount Search option for all the bikes status or a specific type of bikes status such HOND, DISCOVERY, SPLENDER The sample output is shown in Figure 2.5 It contains RFID number associated with a particular bike, name of the bike, OUT time of the bike, IN time of the bike and status of the bike and amount. The status OUT indicates the bike is on rent. The status IN indicates the bike is inside the Garage. Using OUT and IN time amount of the bike rent is calculated. It has search option for searching for a specific type of bikes status or all types of bikes status. It has edit option to edit the rent amount and update in the database i.e. one can increase or decrease the rent amount.

3. Security concern of Low cost

RFID based systems Any RFID Reader can read the RFID tag when their frequency ranges matches. It is obvious that the owner of the tag is authorized to read and understand the content of tag for business purpose. Here the question is how to provide the security to the tags by which only owner of the tag can understand the tag's content even though unauthorized people have the access to the tag? The challenge in providing security for low-cost RFID based systems is that they are computationally weak devices, unable to perform very complex cryptographic operations. In any business model usage of technology should enable to use the cost effective tags and at the same time they should be secure in temperament. Under these circumstances the security of the tags has to begin from the basis technology. Symmetric key algorithms are assumed to be better security algorithms. The standard available symmetric algorithms require very high computational power and the storage size of the algorithms are very high. The low cost RFID systems require very light weight crypto algorithms and their storage size is very minimal. When we use the 8-bit microcontroller with 8K bytes of in-system programmable Flash memory and the computational power of this controller is minimal and storage size of this controller is 8kb only. Providing the security for deploying RFID technology in the bike renting system with low cost microcontrollers is very challenging. The miniDES algorithm is very much suitable under these circumstances to provide the security for RFID based systems.

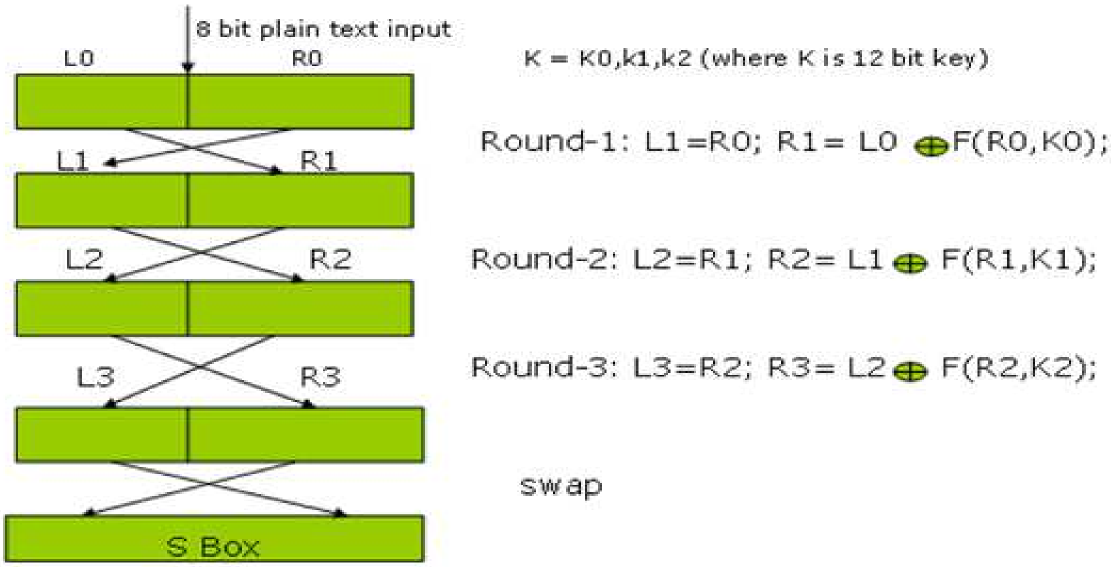
4. MiniDES Algorithm

MiniDES is a symmetric key encryption algorithm. the time complexity of the algorithm is O(n) where n is the size of the input characters. In symmetric key encryption, you and your friend share a "secret" key. Using this key, you can encrypt a message into "cyphertext". Cyphertext looks like a random sequence of characters and is completely meaningless to anyone unless they also have the secret key, in which case they can decrypt the cyphertext back into the original message and read it. Figure 4 shows the symmetric encryption method.Symmetric cryptography also provides a degree of authentication because data encrypted with one symmetric key cannot be decrypted with any other symmetric key. Therefore, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense. MiniDES algorithm takes 8bit plain text as input and this input is divided into two groups each of four bits such as upper four bits into L0 and lower four bits into R0. The algorithm takes three rounds with a swap to encrypt a character.

Encryption

The received 8-bit plain text is sub divided into two groups each of with four bits. Move the upper four bits into L0 and lower four bits into R0. The 12bit key has also be sub divided into three groups such as k0, k1, k2 each of with four bits. Consider the example: k=101010101010 then key sub groups become k0=1010; k1=1010; k2=1010 these sub keys are being used in the encryption of the input 8-bit plain text.

Round 1: Copy the four bit contents 0f R0 into L1 and R1=L0 exclusive or with F(R0,k0), in round 1 the key k0 has to be used.
Round 2: Copy the four bit contents 0f R1 into L2 and R2=L1 exclusive or with F(R1,k1), in round 2 the key k1 has to be used
Round 3: Copy the four bit contents 0f R2 into L3 and R3=L2 exclusive or with F(R2,k2), in round 3 the key k2 has to be used
swap: swap the L3,R3 contents which is the cipher text of 8-bit input



Calculation of F(R0,K0) is as follows:

i) Let us assume that content of R0 four bits are b1b2b3b4 then left shift or right shift the R0 contents i.e. R0=b2b3b4b1(left shift). Now find the Exclusive or of R0,K0 i.e. $W=R0 \oplus K0$

ii) Now let us assume that the four bits of W are 1010 (assume this as ABCD)from the 4x4 two dimensional table select the number corresponding to [AD][BC] i.e. [10][01]. The table contains the 16 hexadecimal numbers in any order starting from 0 to F as shown in table 1. The [10][01] corresponding number in the table 1 is **8.**

iv) Therefore F(R0,K0) is 8

v) Now calculate $R1=L0 \oplus F(R0,K0)$

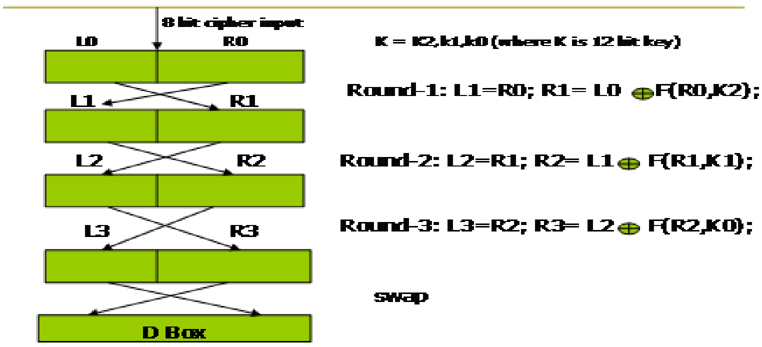
vi) Similarly calculate the R2 & R3 in round 2 and round 3 and swap the L3 and R3 which gives the encrypted cipher text.

Decryption

In the decryption process of miniDES takes an 8 bit cipher text input and does same operations as in encryption process but key value is taken in reverse order. i.e. from k2 to k0.
Round 1: Copy the four bit contents 0f R0 into L1 and R1=L0 exclusive or with F(R0,k2), in round 1 the key k2 has to be used.
Round 2 : Copy the four bit contents 0f R1 into L2 and R2=L1 exclusive or with F(R1,k1), in round 2 the key k1 has to be used.
Round 3:Copy the four bit contents 0f R2 into L3 and R3=L2 exclusive or with F(R2,k0), in round 1 the key k0

has to be used.

swap: swap the L3,R3 contents which is the decrypted input of 8-bits



Calculation of F(R0,K2) is as follows:

i) Let us assume that content of R0 four bits are b1b2b3b4 then left shift or right shift the R0 contents i.e. R0=b2b3b4b1(left shift).

ii) Now find the Exclusive or of R0,K2 i.e. W=R0⊕K2

iii) Now let us assume that the four bits of W are 1100 (assume this as ABCD) from the 4x4 two dimensional table select the number corresponding to [AD][BC] i.e. [10][10]. The table contains the 16 hexadecimal numbers in any order stating from 0 to F as shown in table 1. [10][10] corresponding number in the table 1 is E

iv) Therefore F(R0,K2) is E

v) Now calculate R1=L0⊕F(R0,K2)

vi) Similarly calculate the R2 & R3 in round 2 and round 3 and swap the L3 and R3 which gives the decrypted 8-bits plaintext.

The algorithm miniDES is simple to implement and it does not required much of computational power, any8-bit Microcontroller with 8K Bytes in-System Programmable Flash like AT89S52 microcontroller is very much sufficient to decrypt the received data from RFID tags. Since RFID tags will have unique sequence of number of 12 hex characters(minimum of 96 bits) in case of passive 125Khz RFID tag therefore it does not look sense if we use very complex crypto algorithms. This miniDES algorithm take only O(12) constant time to decrypt the received 12 hex encrypted characters and the source code size of this algorithm is only 3KB. The processing capabilities of many embedded systems are easily plagued by the computational demands of security processing, leading to failures. Hence usage of this miniDES light weight algorithm will definitely provides the security as well as authentication without demanding the much of computational power unlike other heavy weight crypto algorithms. This MiniDES RFID security mechanism can be deployed in many RFID based applications like Hospital application, Remote application, Army Application, Offices Automation, Industrial application, Renting application, Fashion industry, From manufacturer to store front to VIP management the whole supply chain can be managed, analyzed and optimized Vehicle management, parking, access control, location tracking etc can be realized, Asset tracking, physical assets have tags attached for tracking and audit purposes, attendance register, anti-thief system and many more. This algorithm can be used wherever the RFID tags are being used for identification, tracking and categorization of objects, person.

5.Conclusion and Future scope

The radio frequency identification is a smart identification method. There are three components which are important in the RFID technology; they are RFID tags, RFID reader, and system with appropriate software. The usage of RFID technology in the bike renting process will definitely enhance the performance of system and avoids the manual errors. This Technology provides the business model is more secured and less chance of cheating because the OUT time and IN time of the rented bikes are perfectly maintained using RTC. Providing the authentication using the MiniDES symmetric algorithm and validity of the tag is done in the microcontroller itself. Usage of Microsoft .Net frame work will enable to online the business model and hence have the better availability to the user. The renting data is stored in database which can be used for future reference and to take the necessary actions to enhance the business performance. FID technology is an upcoming technology which is being used in many applications across the world. Security is primary concern in business model because RFID technology is prone to security attacks. Lower complex or light weight cryptography algorithms like miniDES are more suitable for low power RFID based embedded systems.This can be enhanced to maintain a centralized database and update the bike renting information in the central database where multiple bike renting stores are connected across the country using internet.

6. References

ARI JUELS(2004) ,"RSA Laboratories". *Minimalist Cryptography for Low- Cost RFID Tags,* Bedford, MA 01730, USA.

SRIVATHS RAVI & ANAND RAGHUNATHAN, "NEC Laboratories America", PAUL KOCHER, "Cryptography Research", SUNIL HATTANGADY, "Texas Instruments". *Security in Embedded Systems: Design Challenges* .

KUO-SHIEN HUANG, SHUN-MING TANG(2008). *RFID Application Strategy and Deployment in Bike Renting System*, Feb. 17-20, 2008 ICACT 2008.

Figures referred in the text above:

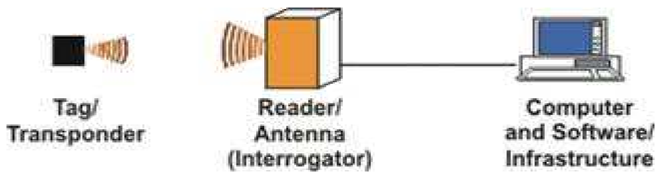


Figure 1.1 RFID components

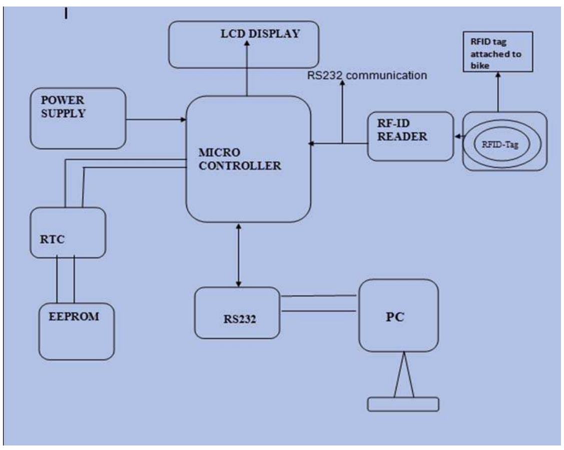


Figure 2.1 Functional block diagram of Bike renting system

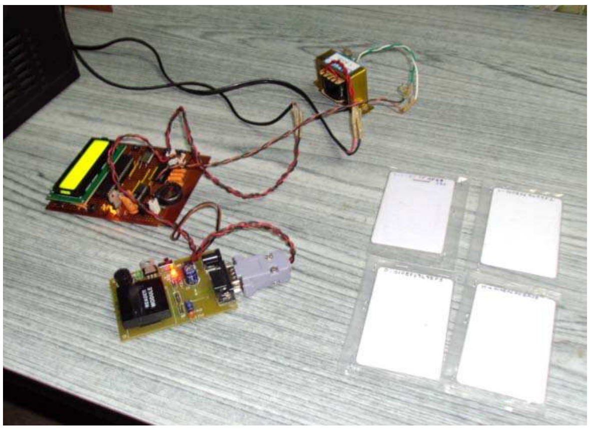


Figure 2.2 connectivity among modules of the system.

Figure 2.3 Microcontroller module

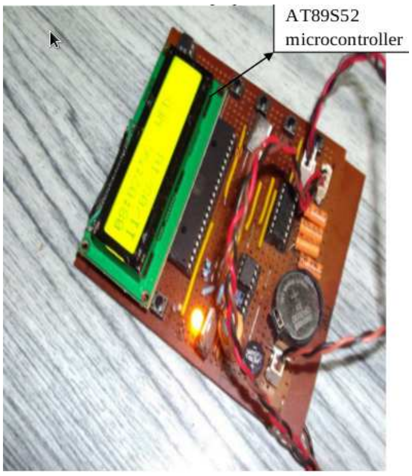
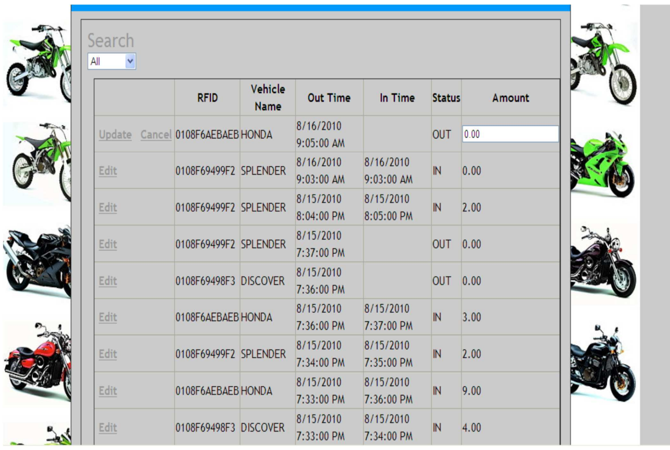


Figure 2.4 Displaying status of the bikes



Search

All

	RFID	Vehicle Name	Out Time	In Time	Status	Amount
Update Cancel	0108F6AEBAEB	HONDA	8/16/2010 9:05:00 AM		OUT	0.00
Edit	0108F69499F2	SPLENDER	8/16/2010 9:03:00 AM	8/16/2010 9:03:00 AM	IN	0.00
Edit	0108F69499F2	SPLENDER	8/15/2010 8:04:00 PM	8/15/2010 8:05:00 PM	IN	2.00
Edit	0108F69499F2	SPLENDER	8/15/2010 7:37:00 PM		OUT	0.00
Edit	0108F69498F3	DISCOVER	8/15/2010 7:36:00 PM		OUT	0.00
Edit	0108F6AEBAEB	HONDA	8/15/2010 7:36:00 PM	8/15/2010 7:37:00 PM	IN	3.00
Edit	0108F69499F2	SPLENDER	8/15/2010 7:34:00 PM	8/15/2010 7:35:00 PM	IN	2.00
Edit	0108F6AEBAEB	HONDA	8/15/2010 7:33:00 PM	8/15/2010 7:36:00 PM	IN	9.00
Edit	0108F69498F3	DISCOVER	8/15/2010 7:33:00 PM	8/15/2010 7:34:00 PM	IN	4.00

Figure 2.4.1 Output with search option

RFID Bike Renting System

Search

All

	RFID	Vehicle Name	Out Time	In Time	Status	Amount
Edit	0108F6AEBAEB	HONDA	8/16/2010 9:05:00 AM		OUT	0.00
Edit	0108F69499F2	SPLENDER	8/16/2010 9:03:00 AM	8/16/2010 9:03:00 AM	IN	0.00
Edit	0108F69499F2	SPLENDER	8/15/2010 8:04:00 PM	8/15/2010 8:05:00 PM	IN	2.00
Edit	0108F69499F2	SPLENDER	8/15/2010 7:37:00 PM		OUT	0.00
Edit	0108F69498F3	DISCOVER	8/15/2010 7:36:00 PM		OUT	0.00
Edit	0108F6AEBAEB	HONDA	8/15/2010 7:36:00 PM	8/15/2010 7:37:00 PM	IN	3.00
Edit	0108F69499F2	SPLENDER	8/15/2010 7:34:00 PM	8/15/2010 7:35:00 PM	IN	2.00
Edit	0108F6AEBAEB	HONDA	8/15/2010 7:33:00 PM	8/15/2010 7:36:00 PM	IN	9.00
Edit	0108F69498F3	DISCOVER	8/15/2010 7:33:00 PM	8/15/2010 7:34:00 PM	IN	4.00

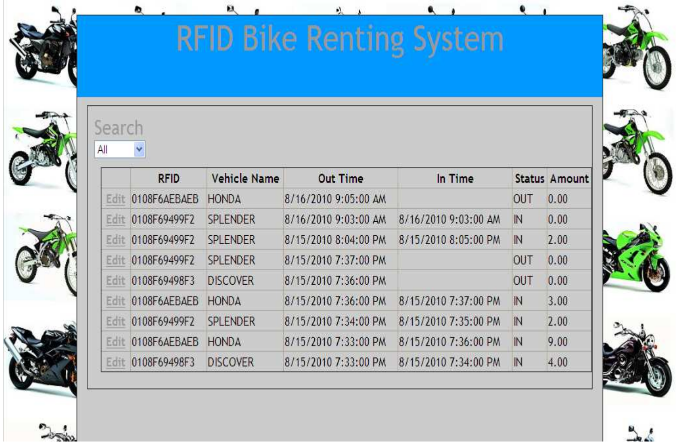


Figure 2.4.2 Search option with Honda

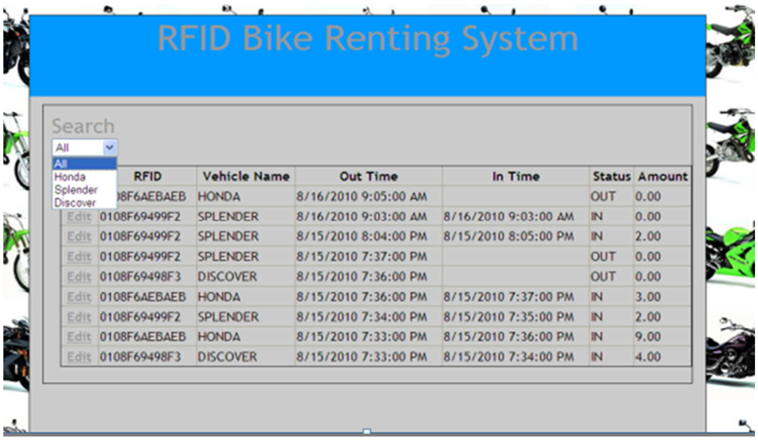


Figure 2.4.3 Output with update option

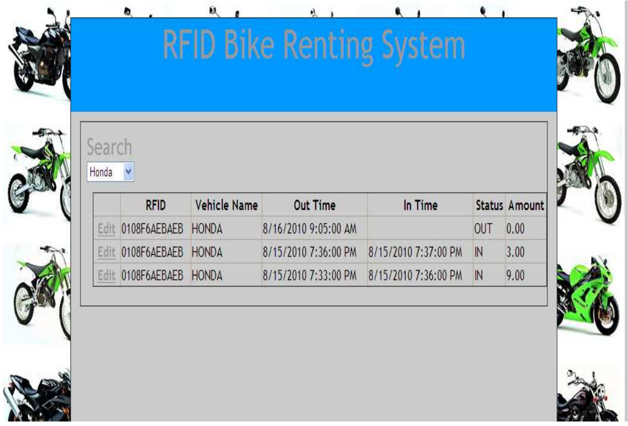


Figure 2.5

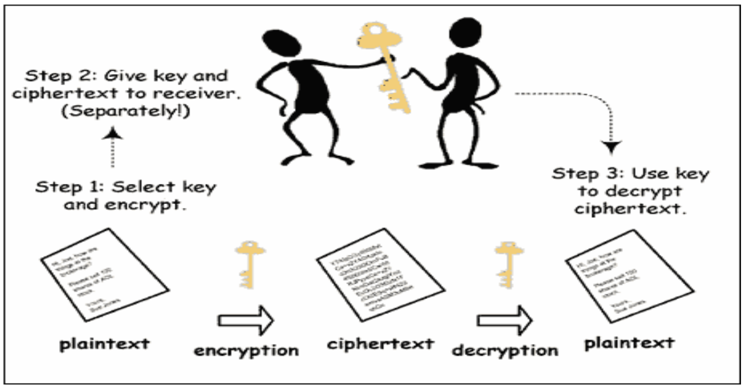


Figure 4

Table 1: 4x4 two diamentional Matrix contains 16 hex numbers starting from O to F in random fashion

	00	01	11	10
00	0	1	3	4
01	7	9	B	D
11	5	A	C	6
10	2	8	F	E

4 x 4 two dimensional table