# Information Security in Electronic Toll Fare System

Neeta Ranjan, S.D.Joshi and Rajiv Ranjan

***Abstract*-- As road infrastructure financing are turning towards a utilitarian basis, car toll systems are deployed at ever more places. Car tolls have several effects on the aggregated infrastructural use. The toll systems which are currently used are not well developed and there is no record of the vehicles crossing the toll. Moreover the payment systems which are available at toll stations reduce the speed of traffic. The idea is to develop a toll system which will overcome all these difficulties. RFID tags are deployed for this purpose. Widespread deployment of radio frequency identification (RFID) tags may create new threats to user privacy. So the data in the tag which is used for toll system is encrypted using encryption techniques with some modification in the existing technique.**

***Index Terms*-- RFID , tags , reader , security, tracking.**

## I. Introduction

RADIO Frequency Identification (RFID) has received much attention in recent years. It is used to automatically identify the objects using radio waves. The use of an RFID system is appropriate basically everywhere that something has to be automatically labeled, identified, registered, stored, monitored or transported. RFID systems are available in a wide variety. Despite the wide range of RFID solutions, each RFID system is defined by the following three features [1] [6]:

1. Electronic identification: The system makes possible an unambiguous labeling of objects by means of electronically stored data.

2. Contact less data transmission: Data identifying the object can be read wirelessly through a radio frequency channel.

3. Transmit when requested (on call) - A labeled object only transmits data when a matching reader initiates this process[1]

RFID is a type of automatic identification system. 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 specifies about the product tagged such as price, color, date of purchase etc.[6]

In a typical RFID system, individual objects are equipped with a small, inexpensive tag, which contains a transponder with a digital memory chip that gives a unique electronic product code. The interrogator, an antenna packaged with a transceiver and decoder, emits a signal activating the RFID tag so it can read and write data onto it. 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. [6] [7]

### *A. Basic RFID system:*

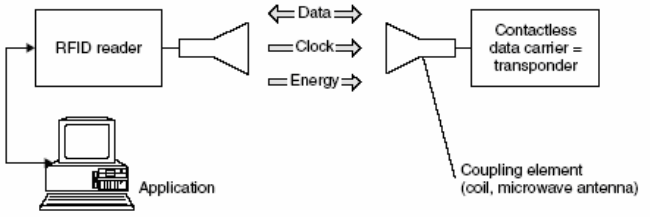



**Figure 1** The reader and transponder are the main components of every RFID system

*(a) Reader:*

The reader communicates with the RFID tag via radio waves and passes the information in digital form to computer system. The underlying principle is inductive coupling. The coiled antenna creates a magnetic field with the coiled antenna of the tag. The tag draws energy from this field and uses it to send back waves to the reader, which is turned into digital information, such as the tags electronic product code.[1] [7]

### *B. Tag:*

The tag consists of a microchip antenna which picks up signal from the reader and sends back signal to the reader. It contains a unique serial number, along with other information, like a customer's personal information. RFID tags can be active tags, passive tags and semi-passive tags. These tags come in variety of shapes and sizes viz. size varying from 2mm to 5cm. [7]

Neeta Ranjan, Lecturer, Vidyavardhini's C.O.E & Tech. Vasai, (e-mail: neetaranjan@rediffmail.com)
S.D.Joshi, Consultant, Crompton Greaves, Mumbai. (e-mail: sj20124@gmail.com)
Rajiv Ranjan, Manager IT operations, Bank of America . (e-mail: rajivranjan78@rediffmail.com)

*C. Antenna:*

Antenna is the conductive element that enables the tag to send and receive data. Passive tags usually have a coiled antenna of the reader to form a magnetic field. The tag draws power from this field [7].

*D. Frequency of operation*

Frequency of interest is in the range of 100 KHz to 5.8GHz. Up to 13.56 MHz inductive coupling transfers information. The frequency used for this application is 13.56 MHz. In the GHz domain however transmission is taking place due to electromagnetic radiation by propagation of radio waves. At these frequencies damping effect is considerable compared to lower bands. They have the ability to penetrate through obstructions along the way of propagation. [3]

## II. RFID IN CAR TOLL SYSTEM

*A. Block diagram of RFID system*

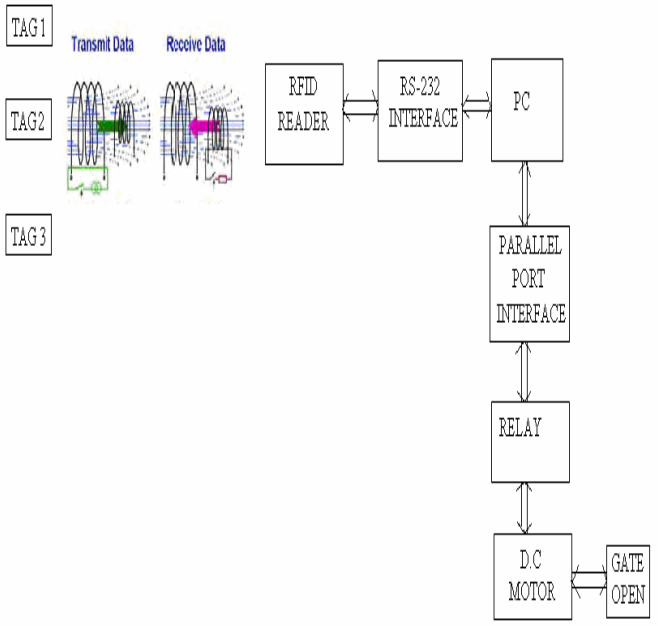



Fig 2 shows the block diagram of an RFID based car toll system

Fig 2 shows the block diagram of an RFID based car toll system. The tag and the reader used here is a product developed by Philips (mifare).Mifare technology uses a contact less interface. A carrier frequency of 13.56 MHz is used for energy transfer and data transfer between the reader and the card. The read/write range is limited to a distance of less than 10 cm.

The contact less principle can be explained in simplified terms using the operating principle of the transformer. The antenna coil of the reader generates an alternating magnetic field at 13.56 MHz. In simplified terms the reader antenna can be regarded as the primary winding of a loosely coupled transformer. The card antenna acts as a secondary winding that picks up the part of the generated magnetic field. This provides the card chip with necessary energy. The magnetic field is amplitude modulated by the reader to transfer data from the reader to the card. Load modulation is used to transfer data in the opposite direction (from the card back to the reader).

Data (including user data) can be transferred after the card has been selected. The following rules apply:[2] [3]

'Reader Talks First': the transceiver always transmits first and the card replies.

The card always replies with an agreed time. And the communication can be established by simple read and write commands.

By using RS-232 interface the reader is connected to the PC. From the parallel port of the PC hardware is designed for opening and closing of the gate.

(a) Overview of car toll system:

1. The car toll system is designed in such a way that only authorized person can access the operating system.
2. Four logins are created for the same viz Administrator, supervisor, users. Administrator is assigned the highest login level=4, Supervisor =3 and users/operators =2.
3. Administrator is having the right to create new account, delete an account on customers request, create new login, delete login, observe all the reports like the daily report, monthly, yearly, new customers report and deleted account report.
4. Supervisor does not have the right to delete account, create new login and delete login.
5. Operator is having the right of only creating and updating a customer's account.
6. Once the account is updated the gate of the toll opens and the customer is allowed to pass through it.

*B. Block diagram of RFID reader:*

RFID reader used is developed by Philips. The MFRC522 is a highly integrated reader/writer for contact less transmission at 13.56MHz. The MFRC522 reader supports ISO 14443A/Mifare mode.

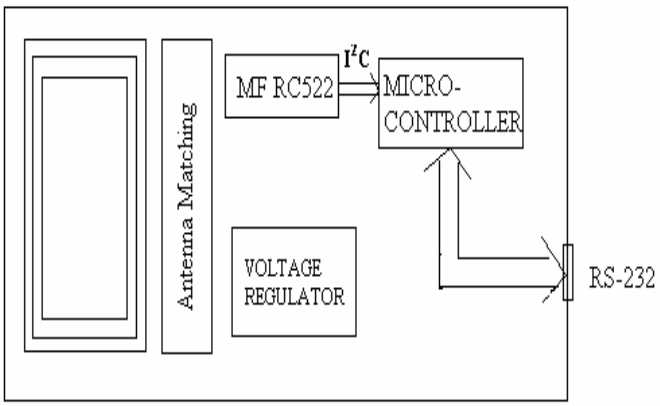



Fig 3 Block diagram of RFID Reader

*C. Block diagram of RFID tag:*

The tag used is MIFARE standard card IC MF1 IC S50. Capacity of the tag is 1KB with a frequency of 13.56 MHz. the block diagram for tag is as shown below

The MF1 IC S50 chip consist of the 1 Kbyte EEPROM, the RF interface and the digital control unit. Energy and data are transferred via an antenna, which consist of a coil with a few turns directly connected to MF1 IC S50.

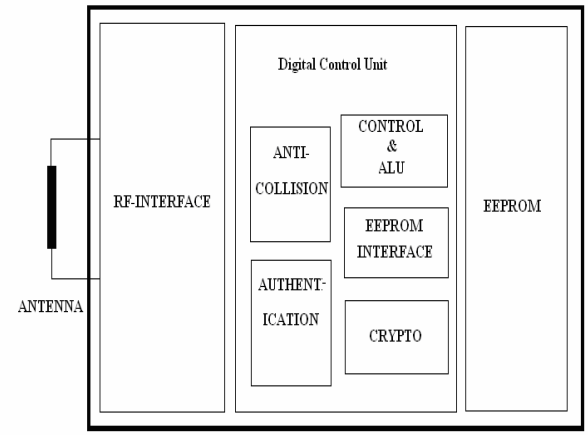



Fig 4 Block Diagram of RFID Tag

**RF- interface:** Modulator/Demodulator, Rectifier, Clock Generator, Power on reset, voltage regulator.

**Anti-collision:** several cards can be selected and operated in a sequence.

**Authentication:** Preceding any memory operation the authentication procedure ensures that access to a block is only possible via the two keys specified for each block.

**Control & Arithmetic Logic unit:** values are stored in a special redundant format and can be incremented and decremented.

**EEPROM Interface:** for interface with EEPROM

**Crypto unit:** this field ensures a secure data exchange.

**EEPROM:** 1 Kbyte are organized in 16 sectors with 4 blocks each. A block contains 16 bytes.

*D. Circuit diagram:*

A dc motor is used as a gate. The specification of the dc motor is 12V, 500mA, 300rpm.So a 12 V supply is required to drive the motor. In this project a 12V power supply is created by using the circuit as shown in fig 5:

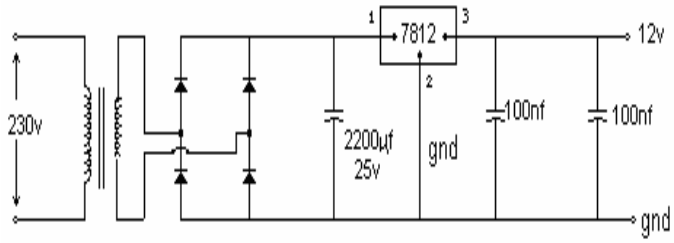



Fig 5 Circuit for generation for +12V supply

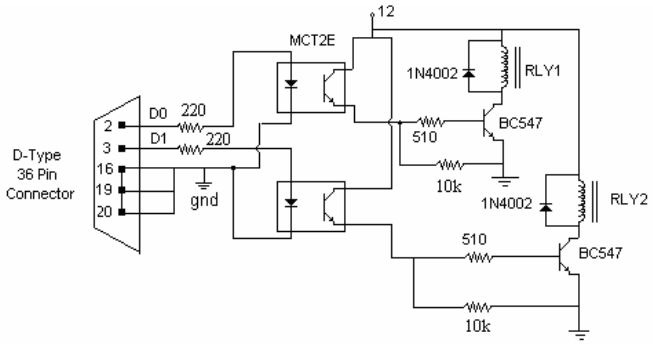



Fig 6 circuit for driving the motor

Fig 6 shows circuit for driving the motor and the relay connections for the motor are as shown in fig 7 . The values from the parallel port of the computer i.e. 00,01 & 10 are given to the two relays RLY1 and RLY2 which decides in which direction the motor will move. 00 means the motor does not move in any direction, 01 means motor will move in forward direction and 10 will move the motor in reverse direction. This motor movement will open and close the gate of the door.

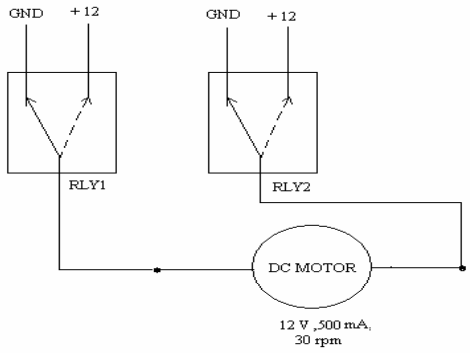



Fig 7 Relay coonnections

*E. Visual Basic-6:*

A visual basic program consists of a visual interface that makes up the windows and controls that the user sees and interacts with. In addition the programming code connects everything together. Each control is both automated and setup to respond to the programming code.

Reading and writing the data into the tag can be achieved by using available protocols of Mifare, and then using the same logic to design the system in visual basic

*F. Security Aspects of Toll Fare System*

1) As computer use grows, the need of security grows with it. The login dialog box is a template added to the system.

2) Encryption & Decryption: - For the security of the data on the tag an encryption technique is used. This is necessary as the data can be read by some unauthorized reader. By encrypting the data it will be very difficult for the attacker to read the data or duplicate the card. The encryption method used is substitution cipher method with some modification.

The encryption method used is as shown in the flowchart. The basic steps used are explained as follows

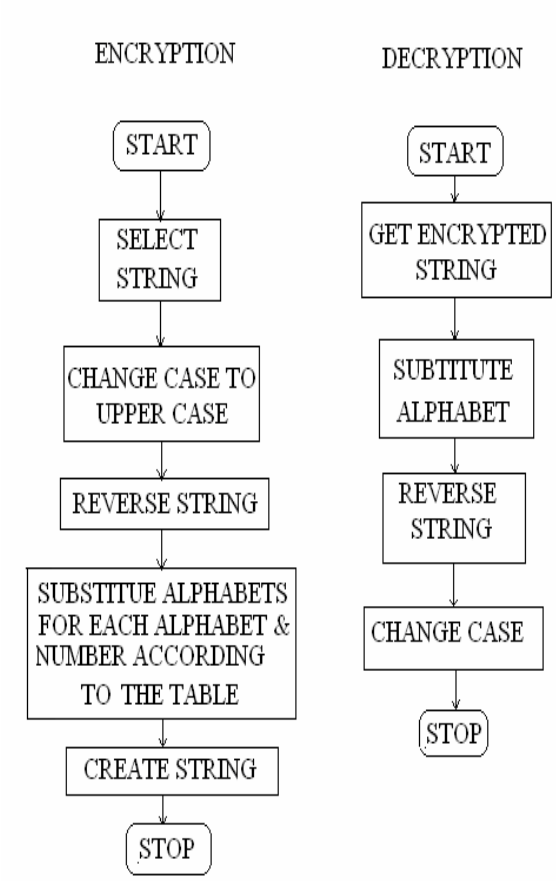
*a. Steps for Encryption:*

**Step 1**: First step is to select the string and then change the case of the string to upper case

**Step 2**: After changing it to upper case reverse the string.

**Step 3**: After reversing the string all the alphabets are substituted by alphabets ranging from A- Z and all the numbers will be substituted by small case alphabets i.e. from a-z. To implement this first a table is created in which a unique alphabet is given for each alphabet as well as number. For example if 'a' is equal to 's' then 's' is not equal to 'a', 's' is equal to some other alphabet(s= p according to the table) unlike the normal encryption technique in which we have fixed substitution i.e. if a = 'n' then n = 'a' or other techniques in which the letters are substituted by a letter some fixed number of positions further down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on.

**Step 4:** Create string and stop




*b. Steps for Decryption:*

Decryption is just the reverse of encryption.
**Step1**: get encrypted string

**Step2**: for decryption substitute alphabet according to the table
**Step3**: reverse the decrypted string and change case to get the final string.

3) The other security feature that is added in the project is that the operator will physically enter the vehicle number by checking the vehicle number on the number plate of the vehicle. This method is a bit time consuming but it adds to the security of the system. First of all a person cannot use other persons RFID card even if the card is robbed. Secondly the same card cannot be used for different vehicles for e.g. a person having card for two wheeler cannot use the same card for car, jeep or any other vehicle. By doing this the toll station can have the exact record as to which vehicle has crossed the toll station and also can avoid the fraudulent use of the card.

4) A unique customer-id is created in this project and then encrypted. This id should match with the id in the database if there is a match then only the system will proceed failing which the system has to reset. This id is created by considering the first three letters of the city followed by the first 3 letters of the state followed by the type of vehicle(for e.g. car is given vehicle type as 3) followed by first 2 letters of the name followed by vehicle number.

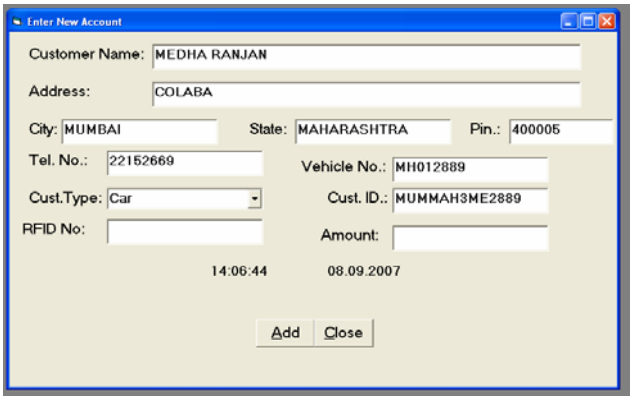
5) Each RFID tag available has its own RFID number. This number is written in the manufacturer's block of the card. Despite of this number present one more random and unique RFID number is given to each and every tag in this project. This number should also match with the number present in the database.

## III. Implementation Results

Some of the implementation results are shown. Result 1 shows that an administrator has logged in. The login name is not case sensitive but the login password is designed to be case sensitive and the password character is '*'. Similarly one can login as a supervisor or user.

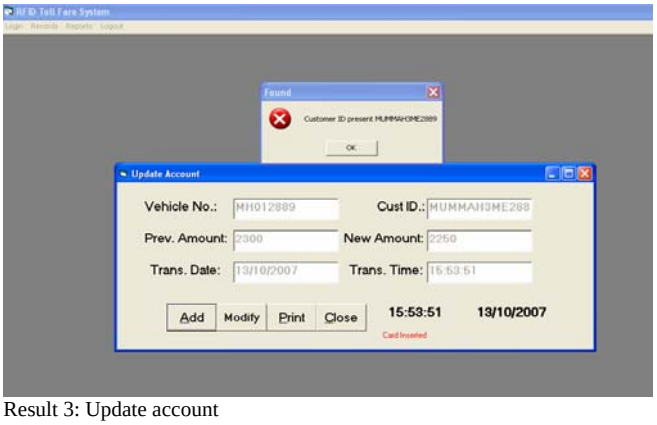

Result 1: Login

Result 2 shows a form for creating new account. After entering certain basic information a unique customer id is automatically created as shown. After this a unique RFID number has to be entered, if the number already exist it will say 'RFID number already exists'



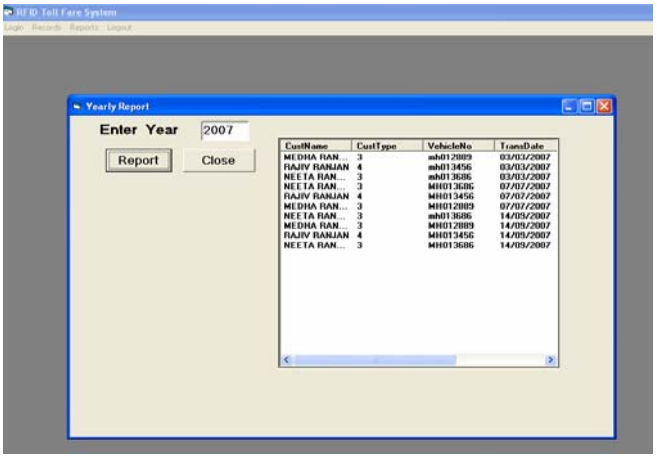

Result 2: Creating new account

Result 3 shows the form for updating an account i.e. next time if the customer comes at the toll station we can update his account by deducting the necessary amount of toll.



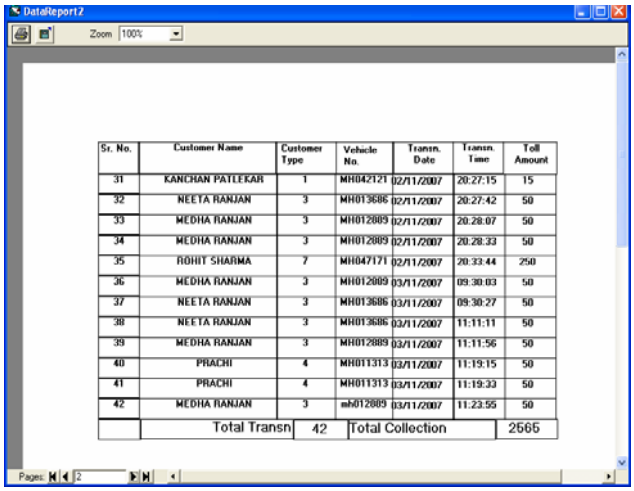

Result 3: Update account

Result 4a shows yearly report, on similar basis we can view daily report, monthly report, new customers report and deleted account customers report.



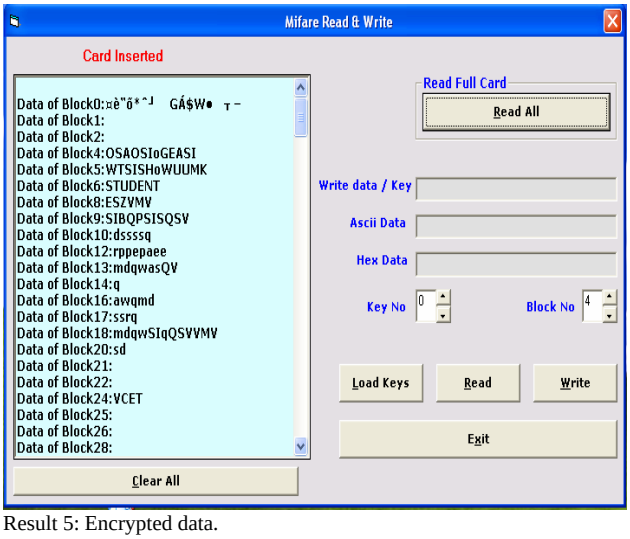

Result 4 a: Yearly report

Result 4b again shows the yearly report with complete information about the customer and also the total toll collected. A printer facility is also provided.




Result 4b: Yearly report with complete information

Result 5 shows the encrypted data on the card.




Result 5: Encrypted data.

## IV. Future Enhancements

Some of the future developments that are possible are as follows:-

1. RFID is used in many different applications. One such application is tracking system. In this project a database containing all the required information for tracking is already created. By interfacing it with a GPS network it is possible to create a global tracking system. [4] [2]

2. Car toll system created in this project is made for only one toll centre. Similarly, we can create the same application for many toll centers and then connect them in one network .Once this is done we can control all the toll centers by a single server.

3. In this project we are using passwords for administrator/supervisor/user, instead of using password we can combine it with some biometric feature like face recognition, vein recognition etc. By doing this we can increase the security of the system.

4. Instead of opening the door of the vehicle by key, we can open the vehicle by RFID tag. Such Tags are available exclusive for opening/closing the door of the vehicle.

## V. Conclusion

RFID payments are a growing industry in many ways reforming the way we make transactions. Radio communication provides efficiency, unmet by any legacy payment system, such as cash and credit cards. This scheme enables a fast and convenient way of collecting car toll requiring no interaction between the toll and the car owner, speed of the traffic also increases. Meanwhile, an anonymous payment solution is provided.

The operator system has been designed in such a way that only authorized person can access the system. Administrator is having all the rights whereas some of the access rights are denied for supervisor and user.

Additional properties that are implemented are the protection for the tag carrier by encrypting the data so that it cannot be read by an unauthorized reader. A unique customer-ID and RFID number is created for preventing the duplicity of the card. Other than this an operator will physically enter the vehicle number by checking the vehicle number on the number plate of the vehicle. By doing this a person cannot use other persons RFID card even if the card is robbed. Secondly the same card cannot be used for different vehicles for e.g. a person having card for two wheeler cannot use the same card for car, jeep or any other vehicle.

Implementation of this system can reduce the crime to a large extent as the toll station will have the exact record as to which vehicle has crossed the toll station and also can avoid the fraudulent use of the card.

The reports of the transaction created based on daily, monthly and yearly basis will help the toll stations to know about their income. These records will also be helpful for the toll stations owners, to present it during the budget meetings. Additional reports that are created are the new customer's report and deleted account customer report. This will enable them to know about who are their new customers and also who all have closed the account with them.

If a customer needs a receipt of the transaction he can get it, also if the toll station owners need the printout of their reports it will be available to them as additional printer facility is also added in the system.

The database which is created is having all that information which can be used for tracking system; one can design a tracking system in future so that it will help the owner of the vehicle to know where his vehicle is.

The hardware implementation like the automatic opening and closing of the toll gates will help to reduce the manpower.

## VI. References

[1] RFID Handbook, http://www.rfid-handbook.com/
[2] Ari Jules,"RFID Security and Privacy: A Research Survey Review", IEEE Trans. Selected Area in Communication, pp. 381-394, February 2006.
[3] Stefan Dahl, "Anonymous Car Toll Payments using RFID Tags", available online, Master of Science Thesis Stockholm, Sweden 2006
[4] De, P.; Basu, K.; Das, S.K., "An ubiquitous architectural framework and protocol for object tracking using RFID tags," *Mobile and Ubiquitous Systems: Networking and Services, 2004. Mobiquitous 2004. The First Annual International Conference on*, vol., no.pp. 174- 182, 22-26 Aug. 2004
[5] Raza, N.; Bradshaw, V.; Hague, M.; "Applications of RFID technology**"**RFID technology(Ref No. 1999/123 IEE colloquium on 25th Oct 1999.
[6] White paper, "Introduction to Radio Frequency Identification". [online]http://www.abetech.com.
[7] Patrick J. Sweeney II, Reference Book on "RFID For Dummies"