Smart Transport Management System Implemented Using Two-Way Encryption Mechanism in RFID

Parvesh Mor, Himanshu Sharma, and Ankur Sodhi

***Abstract*—This paper presents smart transport management system. radio frequency identification technology (RFID) is used to develop the system. The research was conducted by integrating the RFID technology with the development of software application called Transport management system (TMS) on the host computer. The system is proposed for the state transports in India like Punjab Roadways etc. Many similar applications are there like Toll Plaza fee deduction etc. But smart transport management system (STMS) provides a secure and integrated way to automate the transport functionalities. It uses a two-way encryption mechanism for the information security. A software application is developed in Microsoft Visual Basic.Net for explaining the functionality of transport management system.**

***Index Terms*—RFID, RFID tags, RFID readers, permission, authentication, encryption, cryptography, communication, secure information security.**

I. Introduction

RFID is a rapidly growing technology which is implemented in almost every field. It is popular due to its auto item detection technology [1]. It can detect the items without any type of physical contact. Most of the areas of RFID implementation are related to auto item detection in shopping marts, libraries and contactless payment, etc. There is no need of line of sight. STMS helps in keeping the track of public transport. India is a developing country and due to its large population most of the people prefer to travel through the public transport. So research developed a better solution to automate the transport functionalities with desired security.

RFID system basically consists of three parts: RFID tags, RFID readers and a computer application. Brief description of the parts is as discussed below:

RFID TAG: These are small electronic components having Antenna and Silicon chip further which consists of receiver, transmitter, memory and processor. Generally, RFID tags are attached to the items and scanned using handheld or static RFID reader. Now system can get the information of item without touching it physically. There are three types of tags based on the capability [2]:

1) Passive Tags
2) Active Tags
3) Semi-Passive Tags.

Tags works on radio signals so they have different types of working frequencies. On the basis of these frequencies tags can be classify in three categories [3] shown in Table I:

TABLE I: Types of Tags on the Basis of Working Frequencies

Category	Working Frequency	Distance Coverage
LF	124-135 KHz	30cm
HF	13.56 MHz	1 m
UHF	860-960 MHz	7 m

LF-Low Frequency, HF-High Frequency, UHF-Ultra High Frequency

The aim of the research is develop a transport management system. So tags will be attached to the buses. Due to metallic body of the buses special RFID metal tags are used in the system.

Fig. 1. RFID metal tag.

RFID READER: These are electronic devices which act as a moderator between the tag and the application. These can read and write information to the tag. These are also having an antenna, transmitter and receiver. Reader is connected to the back-end database.

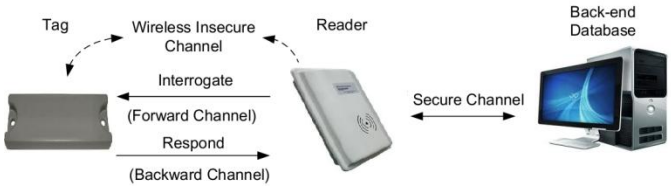

Fig. 2. RFID system.

There are two types of communication between reader and tag: Forward channel and backward channel. While reader communicates to tag it uses forward channel. The signals during this communication are stronger than backward channel because passive tag takes power from these signals only to activate itself. When a tag responds to a reader, it uses backward channel. Generally, there are two types of readers: Handheld and Static.

Here system uses two types of communication, one is between the tag and the reader and another is between the reader and the database. There is a secure channel between reader and database because of the encryption mechanism and wired connection on the other side there is an insecure wireless channel between tag and the reader. Due to the low

Manuscript received February 19, 2013; revised September 20, 2013.
Parvesh Mor is with Lovely Professional University, Phagwara, India (e-mail: parveshmor@gmail.com).

cost and low memory of the tag heavy cryptographic algorithms can't be implemented on the tag.

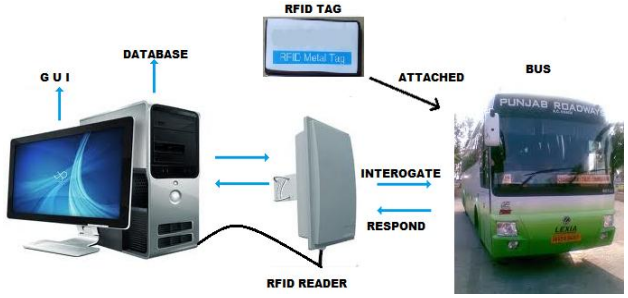

Fig. 3. (a). Conceptual design.

Fig. 3. (b). Proposed implementation view of STMS.

Fig. 3. (a), (b) shows the practical implementation of the Smart Transport Management System. RFID metal tag is attached to the bus. Total four readers are installed at the each bus stand, two at the entry and two at the exit. RFID reader at entry gate will scan each bus when it enters in the bus stand. GUI will show the bus information and store the check in information in database. These buses are already registered with Transport Management System application and their details are in the database. RFID tag attached to bus also store the information like Transponder ID (TID), tag code. Bus record is saved in database corresponding to this tag code number. For private buses there is provision of Bus Stand Entry Fee, so while bus will pass through the Exit gate amount will be deducted from the account of that bus. Thus administration of the bus stand can get all the details of all buses and can easily manage the entry fee service. Smart Transport Management System is going to be an effective application of the RFID technology. It will automate the functionality and reduce the processing time [4].

II. Background of the Research

Most of the areas of RFID implementation are related to auto item detection in marts, libraries and contactless payment, etc. There are many RFID application related to vehicles like automatic toll plaza [5], RFID tracking system for vehicles [6] etc. Various research and studies has been done in this field. For example, Prof. A. A. Pandit *et al.*, (2009) developed RFID based tracking system for vehicles. They discussed three problems related to vehicles such as traffic signal timing, thefts of vehicles and congestions of vehicles on road. The system installed RFID tag on each vehicle and RFID readers on various junctions of city. Traditional traffic signal is static but system provides dynamic traffic signals and it is controlled on the basis of traffic data. For example the speed of vehicles will be more on high congested road to overcome the traffic jam. Vehicles are tracked at various junctions and log record is maintained to prevent the theft of vehicles.

RFID tag that can also be used for automatic fee deduction at car parking or toll plazas was mentioned by Pala *et al.*, (2007). Every vehicle has an associated account. The amount will be deducted from this account only. Customers have to refill their account at the beginning of the month. It is a secure and efficient way for fee collection. Similarly system deducts the toll tax. There is no need to stop the vehicle at barrier. Reader will scan the tag and search for the associated account. If there is enough amounts in the account then vehicle can move uninterrupted through the toll otherwise it will not be allowed through the barrier located a head to toll collection center.

Manfred Aigner *et al.*, (2011) have done a research on new applications of RFID. Research is basically related to use of RFID in open environment. The system is capable to gather the climate change information. Special kinds of UHF RFID tags and readers are used. This project is named as "BRIDGE." It stands for "Building Radio Frequency IDentification Solutions for the Global Environment" [7]. Research explained that use of RFID was limited to organizations only. So the aim of the BRIDGE is global implementation of the RFID. Tags must be able to share information between dynamic coupled organizations. This will reduce the cost of implementation of RFID for the organizations due to shared architecture.

III. Project Plan

The system integrates the RFID hardware and host computer by using an application developed in VB.Net. This application is named as Transport Management System. Application provides an attractive and easy Graphical User Interface (GUI). There are basically two main processes: Check In and Check Out. Check In takes place at entry gates R_1 and R_2 while Check Out takes place at exit gates R_3 and R_4. Ultra High Frequency readers are used.

Check-In Process: When a bus will enter the bus stand then reader will read the tag attached to it. If record of the bus already present in the database then simply makes an entry of bus in Entry table otherwise system will store the bus information in database (see Fig. 4(a)).

Check-Out Process: This process will be done at the exit gate. There are two readers placed at the OUT-Gate. So when a bus exists the bus stand through OUT-Gate its tag will be scanned by the reader. The system will calculate the stay time of bus at bus stand, if it is more than 8 hours then deduct fee for 24 hours otherwise charge for only one trip. There is no need to stop the bus at the barrier if enough amounts is there in the account and if not then bus will not be allowed to go through the barrier until manual payment is made (see Fig. 4(b)).

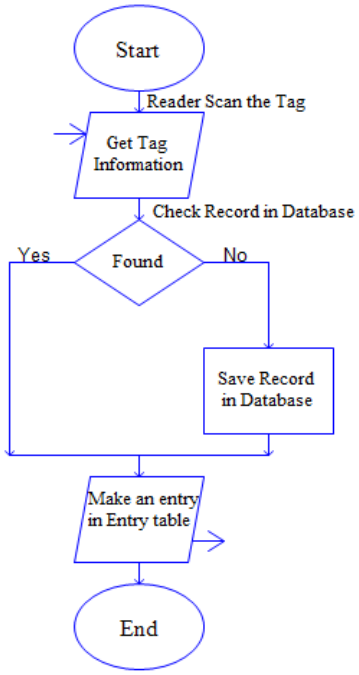

Fig. 4. (a). Flow chart of check-in process.

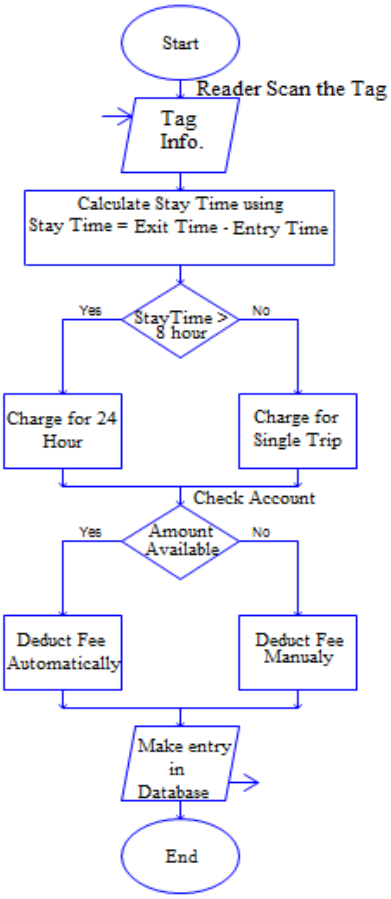

Fig. 4(b). Flow chart of check-out process.

IV. Security Implementation

Every RFID tag consists of two memories Read Only Memory (ROM) and Read Write Memory (RWM). ROM memory consists of TID number which is done by the manufacturer and this cannot be modified. [8] RWM will be used during reader application communication. 32 bits data will be stored on the tag (see Fig. 5).

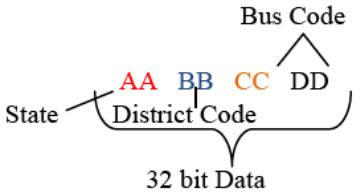

Fig. 5. Data structure.

RFID tag, reader and server communications in the smart Transport management system can be represented as shown in Fig 6. (Abbreviations: D-Decryption, E-Encryption, Info-Information, K_1 and K_2- Private keys)

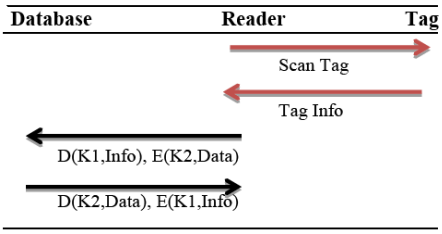

Fig. 6. Tag-reader-server communication processes.

Implementation of complex cryptographic algorithm leads to reduce the performance of the system. STMS is a fast and reliable system for moving buses. Channel between application and database server is wired so it is little secure. A Caesar cipher is enough to provide the best security because key is neither public nor exchanged. So system uses two Caesar cipher algorithms with different keys.

A. For forWard Channel (Fig. 7(a))

Original Tag Data = Decryption (Key1, Tag Info) and Database Data = Encryption (Key 2, TMS Data)

B. For Backward Channel (Fig. 7(b))

TMS Data = Decryption (Key 2, Database Data) and Tag Data = Encryption (Key 1, TMS Data)

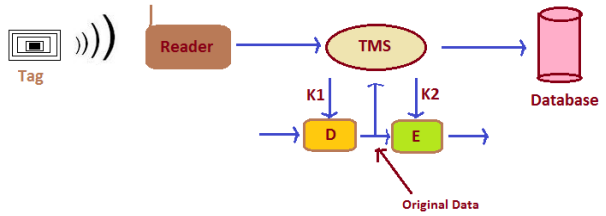

Fig. 7. (a). Forward channel communication.

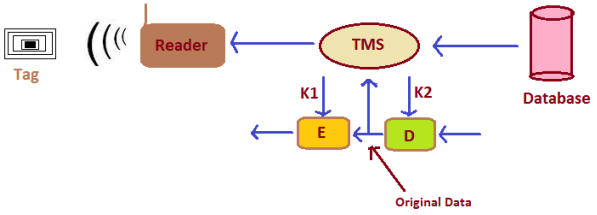

Fig. 7. (b). Backward channel communication.

When a tag comes in the range of the reader, it will be activated and reader will read the tag information this is called Forward Channel Communication. This is also shown in the Fig. 6. The information read by the reader is in encrypted form. Now in order to make this information

original, it will be decrypted with the help of key k1, and the original information will be shown in the application. Change can be made in the information only here. Data will be again encrypted with key k2 and then stored in database. This is known as Backward Channel and is shown in Fig. 7(a).

Database contains an Entry table which will store the check in and check out details of the buses. During forward and backward channel the system uses an encryption mechanism to secure the communication.

Fig. 8(a). Main GUI.

Fig. 8. (b). Add Bus GUI.

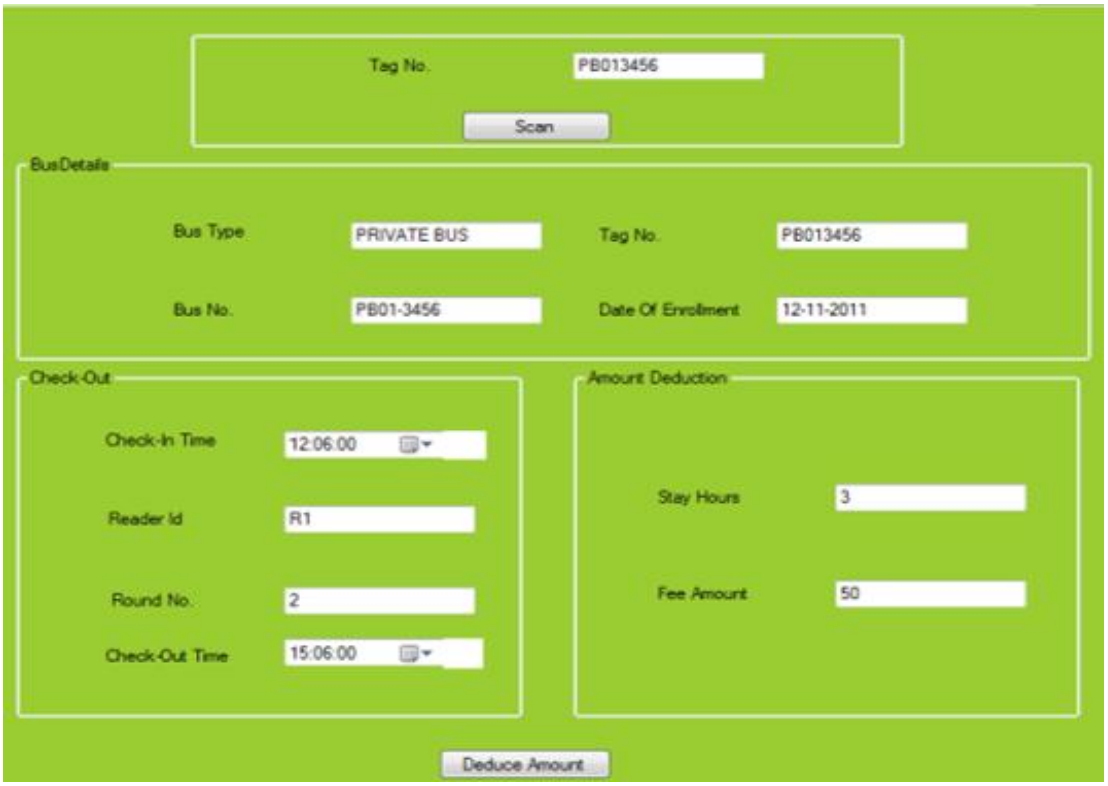

Fig. 8(c). Check-out GUI.

V. Result and Discussion

A. Processing Information

The add bus record GUI was developed to save the data of the bus. The GUI is divided into four sections: Bus Details, Route Details, Time Details, and Tag Details (see Fig. 8).

A unique bus number is provided to every bus on the basis of that system will generate a unique tag number for each bus. This tag number will be saved in encrypted form on the tag. So that if some attacker or intruder read the tag information even then he is not able to do any harm to the system (see Fig. 9).

Bus_Type	Bus_Number	Arrival_Time	Taq_Type	Taq_Number
PRIVATE BUS	PB057882	00:24:00	EPC	PB057882
PRIVATE BUS	PB068273	09:06:00	EPC	PB068273
PRIVATE BUS	PB109703	05:06:00	EPC	PB109703
PRIVATE BUS	PB013456	21:06:00	EPC	PB013456

Fig. 9. Database (decrypted form)

VI. Conclusion

All the objectives have been successfully achieved by the system. The bus information were successfully scanned and saved in the tag and database. Further study can be done to enhance the performance and security of the system.

References

[1] K. Xiaohong, W. Jun, L. Lei, X. Bing, and X. Huazhi, "Applications of intelligent information techn-ology in food logistics," *Computer and Communication Technologies in Agriculture Engineering (CCTAE)*, 2010, pp. 344-348.

[2] M. Rieback, B. Crispo, and A. Tanenbaum, "RFID guardian: A battery-powered mobile device for RFID privacy management," in *Proc. Australasian Conference on Information Security and Privacy (ACISP)*, 2005, pp. 184–194.

[3] M. Rieback, B. Crispo, and A. Tanenbaum, "The evolution of RFID security," *IEEE Pervasive Computing*, 2006, pp. 62–69.

[4] P. Keskilammi and S. Kivikoski, "Radio frequency technology for automated manufacturing and logistics control," *International Journal of Advanced Manufacturing Technology*, 2006, pp. 116-124.

[5] P. Inanc, "Smart parking applications using RFID technology," *RFID Eurasia*, 2007, pp. 1-3.

[6] A. A. Pandit, J. Talreja, and A. K. Mundra: "RFID tracking system for vehicles (RTSV)," in *Proc. International conference on computational intelligence, Communication Systems and Networks*, IEEE, 2009. pp. 160-165.

[7] M. Aigner, T. Burbridge, A. Ilic, D. Lyon, A. Soppera, and M. Lehtonen, "RFID security and privacy-bridge project," White Paper, 2011, pp. 13-20.

[8] M. Lehtonen, A. Ruhaneny, F. Michahelles, and E. leisch, "Serialized TID numbers –a headache or a blessing for RFID crackers?" in *Proc. IEEE International Conference on RFID*, 2009, pp. 233-240.

Parvesh Mor is an assistant professor in computer science at the Department of Networks in Lovely Professional University. He was born in Shimla on 15th August in 1988. He received his B.Tech (Hons) and M.Tech. in computer science from Lovely Professional University, Phagwara, Punjab, India in 2012. In research he is Focusing on Sensor, Network Security and Digital Forensics Analysis.

Himanshu Sharma is an assistant professor in computer science at the Department of Electronics in Lovely Professional University. She was born in Ludhiana, Punjab. She received her B.Tech (Hons) and M.Tech. in computer science from Lovely Professional University, Phagwara, Punjab, India in 2012. She is focusing on Network Security and RFID.

Ankur Sodhi is an assistant professor in computer science at the department of Networks in Lovely Professional University. He is having five year experience in teaching. He is pursuing his Ph.D from Punjab Technical University, Jalandhar.