RFID & Mobile Fusion for Authenticated ATM Transaction

Kopparapu Srivatsa
ECE/SEEE
SASTRA University

Madamshetti Yashwanth
ECE/SEEE
SASTRA University

A.Parvathy
Assistant Professor / ECE/SEEE
SASTRA University

ABSTRACT

One technical innovation can provide solution to diverse problems. Money has become plastic these days. The introduction of utility cards, mobile banking and internet banking has revolutionized the way we deal with money. The sophistication they bring into one's life is commendable. They make our work convenient. But there lies a potential problem, security. The thrust area is that every transaction of the account should be done with the consent of the customer or account holder. This is possible through the wide spread mobile phone technology. Here mobile phone acts as the interactive medium between account holder and bank. Ones hard earned money should not go into the hands of unworthy persons. This noble theme helped us to think of the innovation **–"RFID & Mobile Fusion for Authenticated ATM Transaction"**. The implementation of this takes the help of RFID card, RFID reader housed in ATM, PC, MICRO CONTROLLER, mobile network and software like AT commands, Keil and matlab.

Categories and Subject Descriptors

D.4.6 Security and Protection

General Terms

Security

Keywords

ATM, PC, µC, Mobile networks, AT commands, Keil and MATLAB.

1. INTRODUCTION

RFID cards have brought a revolution in how industry takes care of large number of products. Either it has products in shopping mall, vehicles in an assembly line of a manufacturing unit or employee attendance etc., RFID card is nothing but a small electronic device either actively or passively functioned. RFID has emerged as a replacement to barcodes which are being used for the object identification so far [13]. Unlike the barcode system, RFID has many different advantages: it can have data memory in addition to identification of data and it can also be recognized out-of-sight even from a relatively long distance. These features can enable various types of application services in addition to simple identification. For example, it can be inventory management, automation of manufacturing process, shipping management, animal tracking, container recognition and ticketing service.

RFID is the core technology for ubiquitous computing environment implementation, together with USN (Ubiquitous Sensor Network). Currently, there is a new stream, called mobile RFID [9]. It has a small binary coded circuit in it which on energizing either changes from 0 to 1 or vice versa. Depending on application they can manufacture the card with capacity to hold more data. The reader is device which emits EM waves continuously and these waves when touches the card reflects and carries the data back to the reader. This is present in the ATM centre.

RFID technology is a bewitch invention which has the ability to deliver embedded information in a tag without any physical contact [13]. On the other hand, that means RFID is vulnerable to security breaches such as cloning and clandestine tracking can even tamper the information in the tag [4]. Problems and solution proposals related to privacy and security of RFID issues are illustrated in the survey paper [2]. To achieve a real RFID credit card holder during trending process, in 2007, [9] proposed mobile phone based RFID architecture for secure electronic payments using RFID credit cards, which are based on the difficulty of factorization [3](public key cryptography, RSA). However there are several vulnerabilities that adversaries can exploit to launch an attack. During the certification process in the RFID system, the tag needs to transmit a fixed data like, ID or other details to the server-side for identification, however, adversaries will also be able to eavesdrop and collect this information even if the data is encrypted. This has raised the cardholder's privacy issues.

The two primary concerns of privacy with RFID tags are clandestine tracking and inventorying [13]. Clandestine tracking deals with the issue of a nearby RFID reader being able to scan any RFID tag, since these tags respond to readers without discretion. Clandestine inventorying, on the other hand, is a method of gathering sensitive information from the tags. Due to the number of logic gates, the current tags are about 2000–10000; they are limited by computing resources and cost, and are mostly used for basic operations. Only around 200-2000 gates are for security design [6]. We propose a mechanism that utilizes mobile communication devices (Mobile Phone or PDAs) and RFID credit cards to establish a trading mechanism in order to improve security and privacy.

2. Review on literature

Most of the previous works assume the communication channel between an RFID reader and its backend server is secure and concentrates only on the security enhancement between the RFID tag and RFID reader [1]. However, once RFID reader modules gets extensively deployed in consumers' handheld devices [1], the privacy violation problems at reader side will become a matter of great concern for individuals and organizations [3]. If the future communication environment for RFID systems is in wireless it increases the insecurity among the three roles. We need to achieve message security, anonymity, availability and protection of information from being stolen or tampered with. Under such infrastructure, handheld device, such as mobile phone, embedded RFID reader modules will be situated everywhere and operated with many RFID tags in various RFID application systems. In the meantime, it is more difficult to secure the privacy of a mobile RFID-enabled device [3]

With the change in consumption habits, trending practices have changed from the traditional to the entity stores patterns. They have gradually transformed into the network of online shopping patterns, and most of online shopping is completed by the transaction through the credit card. However, with the traditional trading protocol, the credit card number and code (three digit code) [9], can be faked by cardholders to carry out all transactions. When the card is lost, the system cannot detect the implementation of the transaction [9], whether it is by the legitimate credit card holder or not. Recently the use of mobile devices [12] has become very common in the world. They have the functionality to read RFID tags and they also have higher computing performance. During transactions process they take less time for encryption, decryption and certification.

RFID based smart stick prototype [8] has been developed to aid and assist the visually challenged (user) in shopping through GORE (Goal oriented Requirements Engineering Methodology). The device developed is based on Radio Frequency Identification(RFID) which operates in the Low Frequency (LF) band. The envisioned device is a combination of a RFID LF reader module and a microcontroller unit to convey all the information pertaining to the product to the user and thereby enhancing their shopping experience.

A secure authentication protocol has been proposed [6] to provide information to an authorized entity, which implements recognition technology in the insecure communication channel even for the communication between the database and the reader.

An evaluation of few protocols related to securely authenticating **RFID** tags and readers are discussed in [3], it also identifies possible vulnerabilities, and provides alternate solutions wherever possible.

An APF (Authentication Processing Framework) proposed in [2] is one of the ways to deter the growing concerns of unauthorized readers from accessing the tag (transponder) which could result into the violations of information stored in the tag.

Furthermore the literature reviews of 85 academic journal papers that were published on the subject between 1995 and 2005 is found in [7]. It organizes RFID studies into four main categories: technological issues, applications areas, policy and **security** issues, and other issues. All the papers in the review are allocated to the main and sub-categories based on their main focus. This article also provides useful insights on the anatomy of the **RFID** literature [12]. Aids the creation and accumulation of knowledge in this domain and discusses the future research in RFID.

3. Methodology

In the electronic payment scheme using normal credit cards, there is no way to automatically identify the owner of the credit card. One of the issues identified with the existing electronic payment scheme is the incapability to recognize the true owner of credit card [6]. A stolen credit card can be used to make online purchases. The main objective of this scheme is to propose the features required for a secure contactless credit card (RFID credit card), and to identify a RFID reader architecture and propose functionalities to enable secure online transactions. Basic block diagram of the proposed methodology has been given in Fig 1. [11].

The working principle is as follows-when the RFID ATM card is brought into the vicinity of the ATM centre, the reader reads the account number and details of card holder. Then this information is sent into the microcontroller which finally reaches the computer.

Here details are checked for genuineness and a message is sent to the card holder whether to proceed the transaction or not. This is done with the help of hyper terminal which is present in windows operating system. In real- time it can also be replaced by either GSM or CDMA technology.

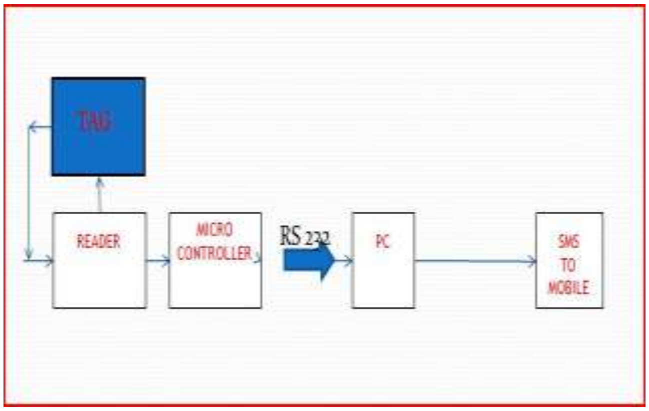


Fig 1. Basic block diagram of the proposed methodology

An RFID system is usually comprised of:

(a) the RFID tag, which contains a digital number associated with the physical object that it is attached
(b) the RFID reader which is connected to a backend database. The reader is also equipped with an antenna, a transceiver and a processor that broadcasts a radio signal in order to query the tag and read its contents.

According to their energy resources and computational capabilities RFID tags are distinguished into passive and active. Passive tags, unlike active ones, do not have an internal source of energy and therefore they have smaller size and computational resources. The maximum reading distance of a tag varies from a few centimeters to approximately ten meters. Also, its cost (e.g., for tags like EPCglobal [1] Class-1 Gen-2 passive tags) is about 13 cents per tag [2] and is expected to decrease to 5 cents within the next few years.

A fundamental requirement of pervasive systems in general, is the ability to uniquely identify things and entities [10]. By satisfying this requirement RFID technology brings along with it the benefits of maintaining user’s confidentiality under any circumstances [4]. With their wide deployment, low cost tags have unfortunately been object of various kinds of attacks raising serious concerns.

In [5] the authors classified the threats and possible attacks against RFID systems in 4 different layers. Based on that classification we summarize the possible attacks that can be launched against RFID systems as following:

Physical Layer: in this layer the adversary launches attacks by taking advantage of the fact that he has immediate access to a tag or by exploiting the security holes of the RFID wireless communications. Such category of attacks includes:

(a) Physical removal of the tag from the associated product
(b) Destroying the tag, e.g., by means of exposing it to extreme environmental conditions or static electricity
(c)Using electromagnetic jamming in order to temporarily prevent communication with readers
(d) Taking advantage of the RFID KILL command to make the tag permanently inoperable.

Network - Transport Layer: in this layer the adversary launches attacks on the way RFID systems are communicating and on the packets that are transferred. This sort of attacks include replication of a valid tag, tag spoofing, impersonation of a valid reader, eavesdropping on tag -reader communication and finally attacking systems of the enterprise backbone (database servers, networking devices etc).

Application Layer: in this layer the adversary aims at the exchanged application data. Such attacks include modification of the information contained in the tag's memory, accessing the contents of tag without being authorized, and malicious code injection to the writable memory of a tag in order to harm middleware applications (e.g., by exploiting SQL injection attacks).

Strategic Layer: This layer includes attacks such as social engineering and competitive espionage. More generic attacks that could capitalize on carelessly designed components, practices or policies are also classified in this category.

The RFID works at different frequencies each determining the range of its operation. The card can be of active type, passive type or battery assisted passive (BAP) type. This classification is according to the type of energizing the card employs. Reader on the other hand is classified based on its source of energy either AC or DC. For the implementation transmitter and receiver circuit is used to resemble the operation of the card and reader pair.

3.1 The RFID reader has the following modules:

1. Transmitter module consisting of a transmitting antenna.
2. Receiver module consisting of a receiver antenna. Distance of separation between the transmitting and receiving module depends upon the type of antenna used.
3. Microcontroller to get the count of the RFID tags used.
4. It has a RS232 interface to communicate with external devices

3.2 Power supply

The microcontroller and its auxiliaries need supply for its functioning. This is derived from the power supply unit. There are two power supply terminals. One of them is for the microcontroller unit and the other is for driving the LCD display. The output of this unit is 5v. It has a step down transformer of 230/15 v rating. The 15 v ac supply is connected to a full wave bridge rectifier. The output of the rectifier is pulsating in nature. So to reduce this effect a smoothening capacitor is provided and .the output of this capacitor is connected to two general purpose regulator ic – 7805 .

3.3 AT Commands

AT commands are also known as hayes AT commands. There are different views to understand the meanings of "AT". Some call it "attention telephone", whereas others interpret it as "attention terminal" commands. AT commands allows giving instructions to both mobile devices and ordinary landline telephones. The commands are sent to the phone's modem, which can be a GSM modem or pc modem. AT commands can be used for operations that are usually done from the keypad, for instance calling a number, sending, reading, or deleting an SMS, setting the SMSC number, looking for a GPRS access point, reading and deleting phonebook data, reading the battery status, reading the signal strength, and so on. AT commands allow giving instructions to both mobile devices and ordinary landline telephones. The commands are sent to the phone's modem, which can be a GSM modem or PC modem. When you want to make a pc-based application to interface a mobile phone using USB, IR or Bluetooth, these commands are needed to communicate with mobile phones. Basically such commands are the application layer of mbus or fbus commands AT commands work on devices that have a built-in GSM modem. Connect the mobile phone to your pc in pc suite mode using any available connection (Bluetooth, USB, or IR). Make sure that you have installed the correct GSM modem driver on your pc. You can check it from control panel | system | hardware | device manager

The transmitter section shown in Fig 2 and receiver sections in Fig 3 are paired with encoder and decoder respectively. They are the H12E and H12D. These are useful in converting the RF and IF frequencies of transmitter and receiver to serial data. These have 18 channels each. Fig 4.a and Fig 4.b gives the Initial and final Connection description in HT. Furthermore the AT command window is given in Fig 5.

Then the parallel data sent reaches the microcontroller input and it is checked with the database present in it. The card number and account number read from the card reaches the microcontroller database. It is cross checked and mobile number is sent to the PC for message dispatch [5].

We used Philips 89v51 microcontroller as it has 8k memory and easily writable. The details are sent from microcontroller to the PC using MAX 232 IC, USB and RS 232 cable.

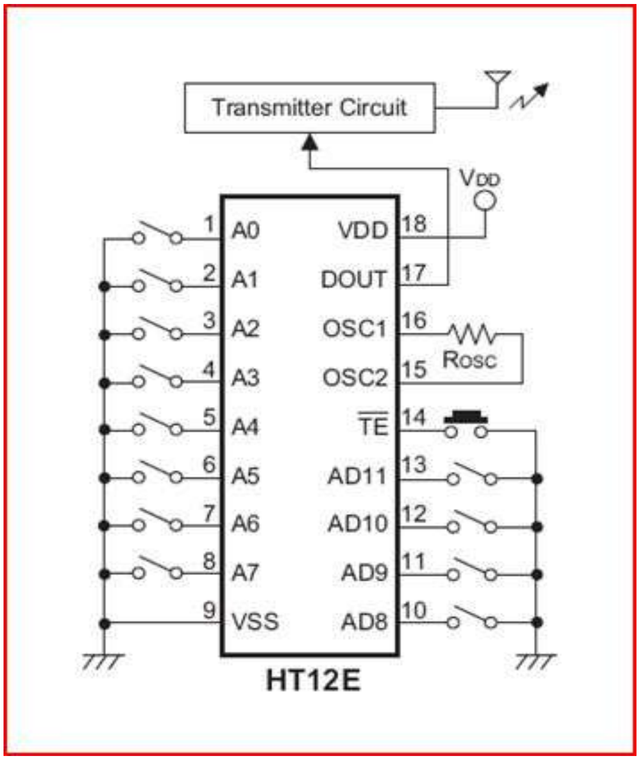


Fig 2. Transmitter section

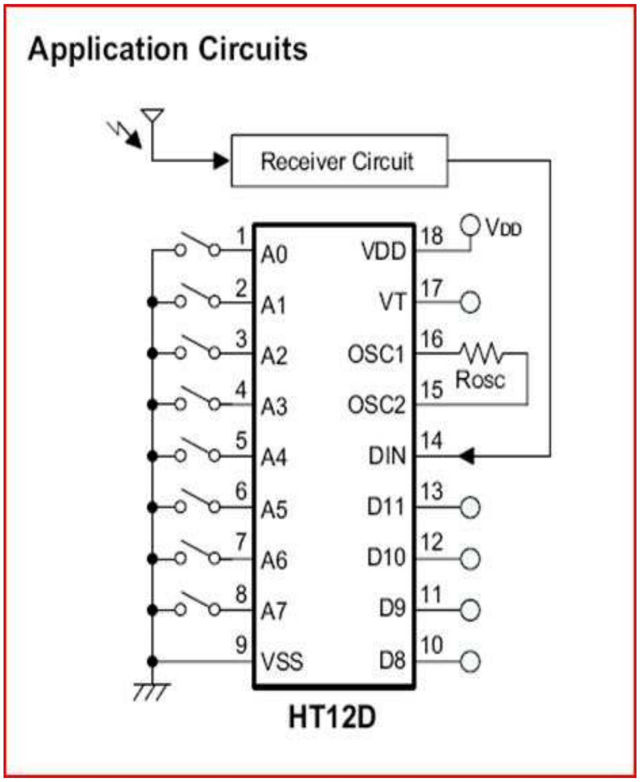
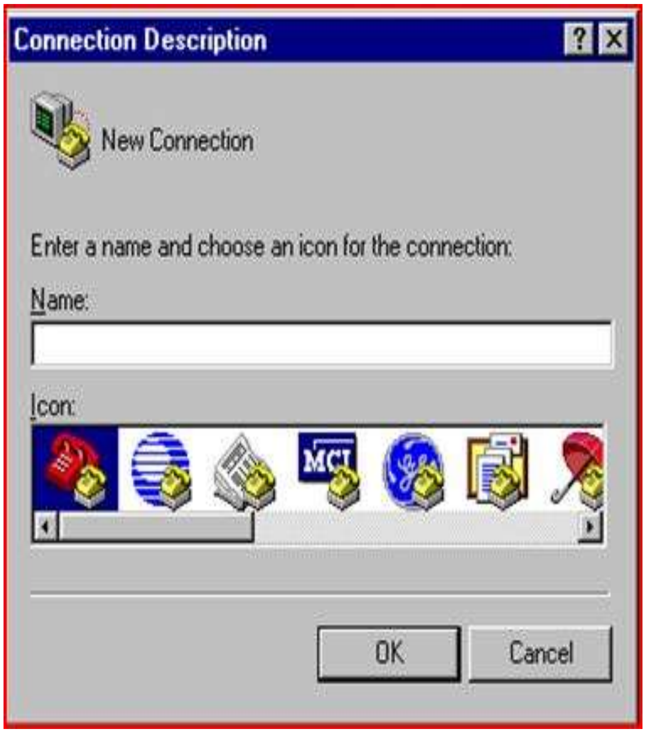


Fig 3. Receiver section


Connection Description

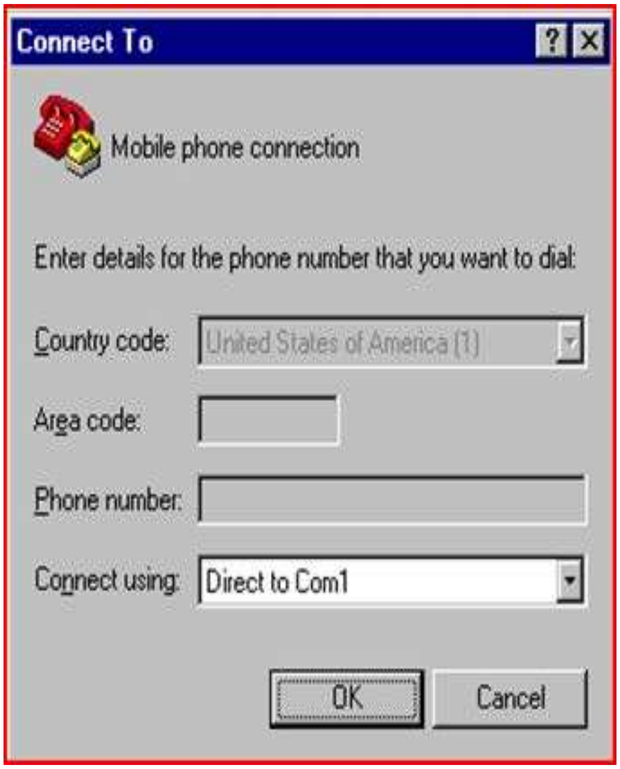
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

Fig 4.a Initial Connection description in HT


Connect To

Mobile phone connection

Enter details for the phone number that you want to dial:

Country code: United States of America (1)

Area code:

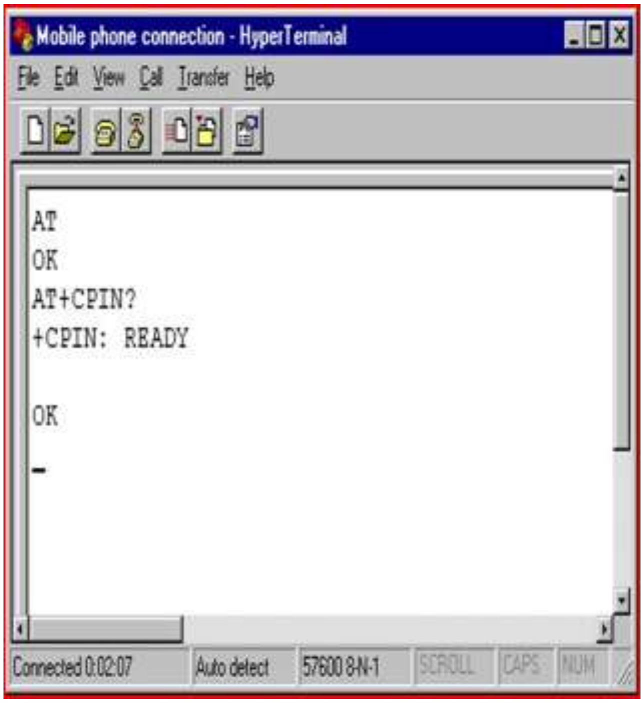
Phone number:

Connect using: Direct to Com1

Fig 4.b Final Connection description in HT

Max 232 is essentially a voltage converter from 5V of microcontroller to 12v of the PC .It connects the USB cable to the PC. The USB cable is a transreceiver for data transfer. RS232 is the serial data traveler which performs the data transfer.

The PC on receiving the data from microcontroller in the hyper terminal sends the data to the message dispensing unit. HT is the communication device in any windows system which enables the PC to send a message to the mobile through wired or wireless connection .These may be Bluetooth, infrared, Wi-Fi, internet or USB. The AT commands provide the necessary instructions to perform the message sending operation.



```
AT
OK
AT+CPIN?
+CPIN: READY

OK
_
```

Mobile phone connection - HyperTerminal
File Edit View Call Transfer Help
Connected 0:02:07
Auto detect
57600 8-N-1
SCROLL
CAPS
NUM

Fig 5. Snapshot of the command window.

Here we use visual basic programming to move the data automatically from the incoming port of HT to message sending device .This can also be done manually by an operator at the bank.

On receiving the message by the card holder, he replies to it. If the reply is ‘YES’ to the question that whether to continue the ongoing transaction attempt, the transaction proceeds or else the message of ‘NOT POSSIBLE’ is displayed on the screen.

The detailed description of the proposed system has been given in Fig 6. A valid user can then enter his secret pin and perform the transaction. Even the mobile banking or the internet banking transactions can also be secured in the way that when we enter the details or try logging in, the control is branched to the authentication part and on completion of the process only the home page is displayed. This process ensures that the transaction is secure.

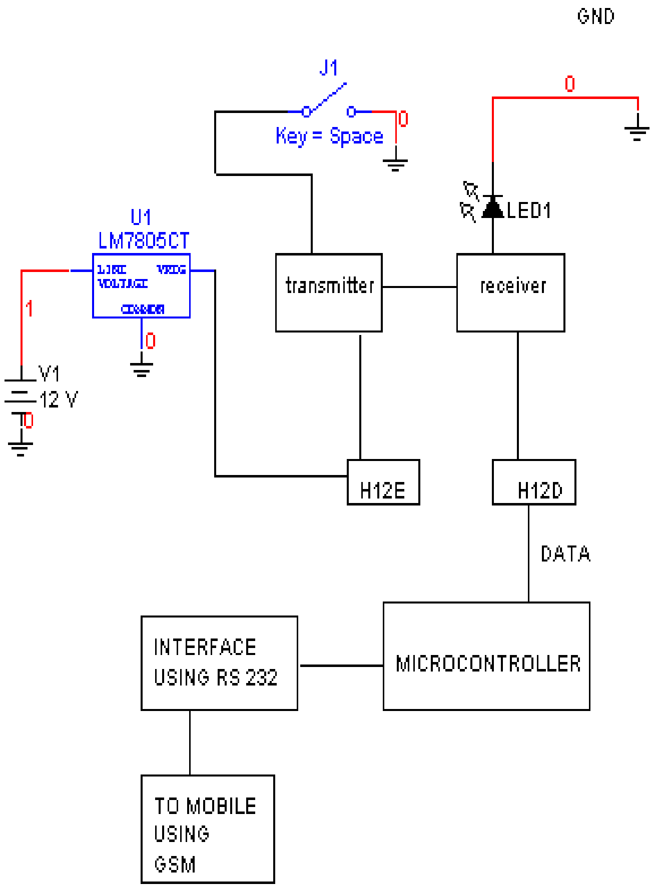


Fig 6. Detailed block diagram of the proposed system.

4. Conclusion

This whole implementation ensures us a secured and authenticated transaction at lowest cost and minimum maintenance. The only thing is that initial cost of RF ID conversion of the entire system is the required one time investment. The value added service that this system provides increases the credibility of the financial institutions, the banks improves the convenience to its customer. Hence as the world progresses through the inevitable and an indomitable quest for knowledge, the aspect of security bound systems are bound to concede with the growing innovations and obviously more vulnerabilities. Hence our application might well solve the aspect of transaction security to a precise and great extent.

5. Acknowledgement

The authors want to heartily thank R.Amirtharajan Project coordinator, Assistant Professor, Dr.R. John Bosco Balaguru, Professor and Dr. K.Thenmozhi Professor ECE School of Electrical and Electronics Engineering, SASTRA University for their critique discussion and valuable suggestion.

References

[1] A. Juels, "RFID Security and Privacy: A Reasearch Survey," RSA Laboratories, 28 September 2005.

[2] John Ayoade, "Security implications in RFID and authentication processing framework" , Computers & Security Volume 25, Issue 3, May 2006, Pages 207-212

[3] A. X. Liu and L. A. Bailey, "PAP: A privacy and authentication protocol for passive RFID tags," Comput. Commun., vol. 32, pp. 1194-1199, 2009.

[4] N. W. Lo and K.H. Yeh, "Novel RFID Authentication Schemes for Security Enhancement and System Efficiency," Lecture Notes in Computer Science, Secure Data Management, vol. 4721/2007, pp. 203-212, 2007

[5] N.W. Lo, Kuo-Hui Yeh, Chan Yeob Yeun, New mutual agreement protocol to secure mobile RFID-enabled devices Information Security Technical Report, Volume 13, Issue 3, August 2008, Pages 151-157S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[6] Mikko Lehtonen, Thorsten Staake, Florian Michahelles, and E. Fleisch, "From Identification to Authentication–A Review of RFID Product Authentication Techniques," Printed handout of Workshop on RFID Security－RFIDSec, Springer, 2006.

[7] E.W.T. Ngai, Karen K.L. Moon, Frederick J. Riggins, Candace Y. Yi " RFID research: An academic literature review (1995–2005) and future research directions" International Journal of Production Economics, Volume 112, Issue 2, April 2008, Pages 510-520

[8] Vinay S, Niha Noor Shaikh and Sridhar Aithal, Design of a Smart Stick Prototype Using Goal Oriented Requirements Engineering Methodology International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 29 Jan 2010

[9]G. Venkataramani and S. Gopalan, "Mobile phone based RFID architecture for secure electronic Payments using RFID credit cards," Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on, pp. 610-620, 10-13 April 2007.

[10] Soo-Young Kang, Deok-Gyu Lee and Im-Yeong Lee, "Secure Multi-Mode Systems and their Applications for Pervasive Computing A study on secure RFID mutual authentication scheme in pervasive computing environment" Computer Communications Vol 31, Issue 18, 18 December 2008, Pages 4248-4254

[11] Selwyn Piramuthu, Protocols for RFID tag/reader authentication
Decision Support Systems, Volume 43, Issue 3, April 2007, Pages 897-914

[12] R. Weinstein, "RFID: a technical overview and its application to the enterprise," IT Professional, vol. 7, pp. 27 - 33, May-June 2005

[13] J. A. Wolff, "RFID tags – an intelligent bar code replacement," IBM Corporation, 2001.