Reliable and Low Cost RFID Based Authentication System for Large Scale Deployment

Muhammad Naveed, Wasim Habib, Usman Masud, Ubaid Ullah, and Gulzar Ahmad
(Corresponding author: Muhammad Naveed)

Department of Electrical Engineering, University of Engineering and Technology
PO Box 814, Peshawar, Pakistan
(Email: {mnaveed,gulzar}@nwfpuet.edu.pk, {uet.wasim, uthmanmasud, ubaid944}@gmail.com)
(Received Oct. 26, 2010; revised and accepted Dec. 26, 2010)

Abstract

Identification is very important nowadays; whether there is need to identify persons, animals or objects, RFIDs provide a very good solution to the problem of identification and authentication. No one can deny the importance of authentication, it is done at the airport, at the railway station, in the library etc, but usually it's done manually. The proposed system is a low cost automatic identification and authentication system which can be deployed at the doors of the building to authenticate authorized people. RFID based system should be very low cost and reliable for large scale deployment, for example RFID deployment in an airport to identify every official and passenger. The proposed system aims to develop a very low cost RFID authentication system based on the low cost components already available in the market. The complete system costs less than $10 USD. This approach not only reduces the cost but also enhances the reliability and ease of maintenance of the RFID based authentication system. The system is also made resistant against any tampering attempt. The proposed system is also accompanied with the PC interfacing and database logging software; which can be used to see the authentication details of the authenticated tags and as well as logs all the authenticated tags with the date and time of authentication to a database. Low cost antenna is also designed to minimize the cost of the system. While keeping the cost low, an impressive range of 10 cm was achieved using passive RFID tags.

Keywords: Authentication, database logging, reliability, RFID, tampering resistant

1 Introduction

No one can deny the importance of identification of persons, animals and objects. Airports, railway stations, cinemas, etc are some places where identification is necessary. Identification can be made automatic using Auto-identification. There are various methods for auto-identification; some of them are bar-code systems, optical character recognition, biometrics, smart cards and RFIDs. This study proposes a general RFID based authentication system which can be used anywhere where authentication of persons or objects is required. The proposed RFID system is also accompanied with PC interfacing and database logging software which is used to display the output of the system and notifies about the validity of the RFID tag and it also logs the authentication details that is RFID tag number along with date and time when the tag was authenticated in a Microsoft Access database. The project aims to develop a very low cost and reliable system, and hence low cost components were used. Low cost RFID module was used which costs only $5 USD. RFID module not only reduces cost as compared to the design of RFID module using discrete components, but it also increases the reliability of the system. Design of the low cost antenna for the proposed system is also part of the study.

For antenna design, concept of magnetic coupling is used; the current flow in the antenna coil induces a magnetic field in the range of communication. In every RFID system, there are two main components; the RFID reader and the RFID tag. The tag is responsible for transmitting and modulating (usually either AM, FM or some variant of the two) the original signal from the reader in a way in which the data is retrievable. The reader's job is to receive and interpret this data. Our RFID system is a passive type, which means that the tag itself does not have its own power source. Because of this, the reader has to perform a second function, which is to send a carrier signal with enough power to power up the tag. The obvious benefit of a system like this is that as long as the reader has the power, tag in close proximity will respond. In modern RFID devices the tag is simply a small integrated circuit with its data encoded on it in some way and a simple LC antenna to receive and retransmit the data. PC interfacing and Database logging software was designed to show the authentication data and also logs it to the database.

The main objectives of this study are:

- To select the appropriate components including RFID reader Module, microcontroller, RFID tag such that the cost should be as low as possible while producing a highly reliable system.

- Design of the low cost antenna to for the RFID reader that meets the specifications to detect the RFID tag at the desired distance.

- Interface RFID Module and microcontroller with each other.

- Software for serial port communication with microcontroller used to capture the authentication data to be displayed and logged to the database.

- The system should be resistant to tampering, in case of tampering the system stops recognizing the RFID tags.

The paper is organized as: Section 1 gives the introduction to the proposed approach, Section 2 presents related work, Section 3 presents the design of the proposed system, Section 4 gives the details of the experiment and shows the results and Section V concludes the paper and give directions for the future work.

2 Related Work

RFID based systems is an active area of research. Lot of people are working to use RFIDs in different applications. Craig Ross and Ricardo Goto [10] have developed a similar system as ours but there system costs $47 and ours only $10. The range of their card reader is 2.0 inches (5.08 cm) and ours is 10 cm. Li et al. have proposed RFID based information sharing platform to solve the problem of resource sharing. They have [7] integrated number of industries and systems and also presented a user authentication scheme. Syta *et al.* [12] have presented an RFID based authentication middleware that combines point of entry and continuous authentication with transparent on-demand encryption of files. Wu *et al.* [13] have proposed a hash-based authentication protocol suitable for mobile RFID systems. Ahamed *et al.* [1] have presented a secure, mutual offline authentication protocol which is based on Elliptic Curve Cryptography. Florentino *et al.* [5] have proposed hospital automation based on RFIDs. They have proposed a system for automation of a hospital clinical analysis laboratory. Sun *et al.* [11] have proposed a Gen-2 Based RFID authentication protocol to enhance the security and privacy of RFID based system. Chowdhury, B *et al.* [4] have proposed RFID-based real-time smart waste management system using RFID and sensor model. Jeon *et al.* [6] have proposed digital codec design for RFID Tags based upon cryptographic authentication protocol. Cao *et al.* [2] have presented their security analysis of two RFID authentication protocols: LAK and CWH. Zhang *et al.* [14] have described and modelled various security requirements for RFID system. Ideal RFID system proposed by Chen *et al.* [3] complies with EPCglobal Class-1 Generation-2 standards of ownership transfer.

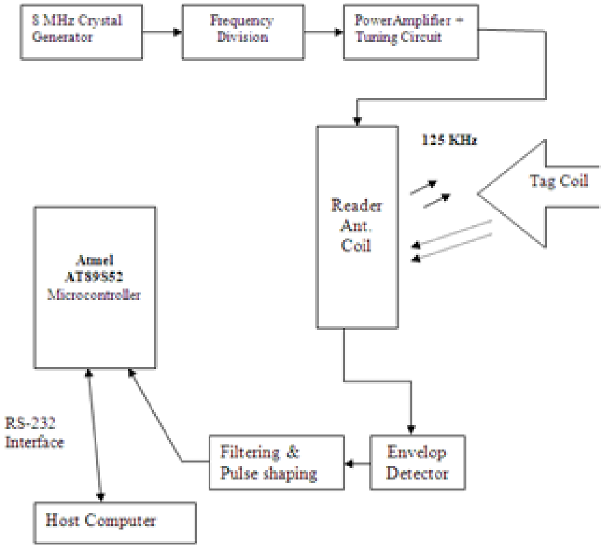


Figure 1: Block diagram of the proposed system

3 Design of Proposed System

As stated before, the two main tasks of our reader circuit, besides the PC interfacing and database logging, is to create a large amplitude carrier signal which will power up the RFID tags present in proximity of the reader and to receive and interpret the modulated response. We have selected appropriate RFID module and microcontroller for accomplishing this task.

The proposed approach has the following design objectives:

- Low cost antenna design.

- Low cost design of the RFID reader.

- Interfacing the RFID reader with PC.

- Design of the database logging and output display software.

- System should be resistant to physical tampering.

Figure 1 shows the block diagram of the complete proposed RFID system. Snapshot of the complete system is shown in Figure 7 at the end of the paper.

3.1 Low Cost Antenna Design

An important hardware element of the proposed system is the antenna coil design. The antenna had to be designed to maximize the induced voltage across coil terminals. For effective radiation of RF signal, the linear dimensions of the antenna should be comparable to the wavelength of the operating frequency. So, a small dipole loop antenna coil, resonating at the desired frequency (i.e., 125 kHz) was used.

Multilayer coils are more efficient to produce large inductance coils in a limited space. Therefore, a typical RFID antenna coil in square shape was formed in a multi-turn structure.

Using a pre-defined value for the capacitance (2.4nF), we employed equation 1 to determine the value of the inductance of the antenna coil with f0 set to 125 kHz. The inductance was found to be 671 uH.

$$f_o = \frac{1}{2\pi\sqrt{LC}}$$

f_o is the frequancy of carrier signal in hertz.

$$L = \frac{0.0276((x+y+2h)N)^2}{1.908(x+y+2h)+9b+10h}\mu H \qquad (1)$$

where

- x = width of Coil
- y = length of Coil
- b = width of cross - section of the coil
- h = height (coil build up) of cross section

Number of turns (N) for given inductance value was calculated by using Equation (1) (this equation taken from [9]) for rectangular loop antenna. The following formula is also valid for square shaped loop antenna because square is a special case of rectangle. Here we assumed $x = y = 10.16$ cm, $h = 0.35$ cm and estimated $b = 0.2$ cm, which gives $N = 50$ approx.

Snapshot of the designed antenna is shown in Figure 2.

3.2 Design of RFID Reader

Design of the RFID reader is the central part of this study. Reliability and low cost were the main objectives in the design of the RFID reader, so, that it can be deployed on large scale. Low cost RFID module which costs only $5 was used instead of making the RFID module from discrete components. The RFID module not only enhances the reliability but also reduces the cost of the proposed system. Atmel AT89252 was used as processing unit, because it is low cost and low power microcontroller. It costs only $1.

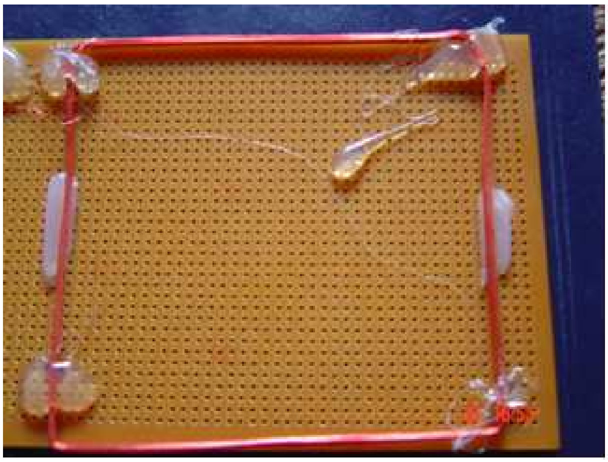


Figure 2: Designed multilayer antenna

3.2.1 RFID Module

The module used in our project is a low cost Chinese equivalent of ATMEL U2270B. The module was used because the fabrication of the module with discrete components is not only costly but it is also not reliable. As compared to ATMEL U2270B having maximum range of 5cm, we have achieved 10 cm range using the Chinese equivalent module, with the same configuration.

It has the following features:

- Antenna driving with carrier frequency of 125 KHz-150 KHz,
- AM demodulation of antenna signal induced by the transponder,
- Suitable for Manchester and Bi-phase Modulation,
- Power supply from car battery or from 5V regulated supply.

The module consists of two IC's i.e., Philips 74HC393D which is a Dual 4-bit binary ripple counter and Philips HEF4069 which contains six hex inverters. T flip-flop divides the input signal frequency by a factor of 2, 74HC393D; a ripple counter containing T-flip flops is used to decrease the frequency from 8 Mhz to 125 Khz. It uses envelope detection using a diode detector to detect incoming signal.

3.2.2 Processing Unit

For processing, Atmel AT89S52 microcontroller was used. It is a low-power, high-performance CMOS 8-bit microcontroller with 8K bytes of in-system programmable Flash memory. The processing unit is responsible for

- Decoding the Manchester encoded data.
- Extracting the data.

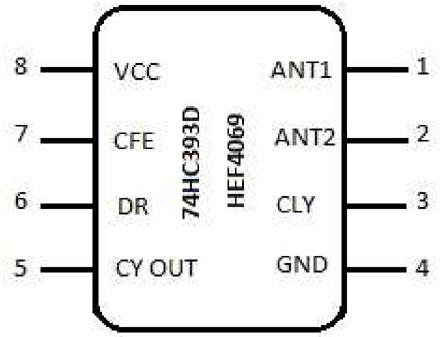


Figure 3: RFID module pin configuration

- Controlling the buzzer that notifies about the validity of the RFID tag.
- Sending the data to serial port to the database logging software.
- Disabling the reader in case of tampering attempt.
- Devices interfaced with microcontroller.
  Following devices were interfaced with microcontroller to design the proposed RFID system:
  - **Buzzer**
    The buzzer is connected with pin P3.4 of microcontroller which is the timer 0 pin. The timer is used to activate the buzzer for a specific time.
  - **RFID Module**
    The carrier Frequency Enable (CFE) pin of the RFID Module is connected with pin P3.6 of the microcontroller. The CYOUT pin of RFID module is connected with pin P3.5.
  - **Body Close Spring (to avoid tampering)**
    The body close spring which is used to activate the buzzer and disable the reading, if someone is tampering with the reader is connected with pin P3.2 which is the pin to generate interrupt 0 of the microcontroller.
- Operation of processing unit.
  Figure 4, shows the complete flowchart for the operation of processing unit. When the microcontroller is powered up it sends a high signal to the buzzer and the red LED showing presence of supply voltage. In order to generate a 125 KHz carrier signal through the antenna coil, the CFE pin of RFID module should be high. At boot up the microcontroller sends a high signal continuously on the pin 3.6.

The tags have a 48 bit number which is unique. The tag is initiated by the transmitted signal through mutual induction.

The same antenna receives the data of the tag. At this time the microcontroller sends a low CFE signal and the antenna no more transmits and receives the data through CYOUT. The CFE is kept low during data transmission because with half duplex communication system, enough energy must be stored by the tag when the RFID reader's activating field is powered up to permit it to transmit its information when the activating field is turned off. This is done to make the receiver simpler as it prevents it from picking the weak signal from the tag in the presence of strong activating field.

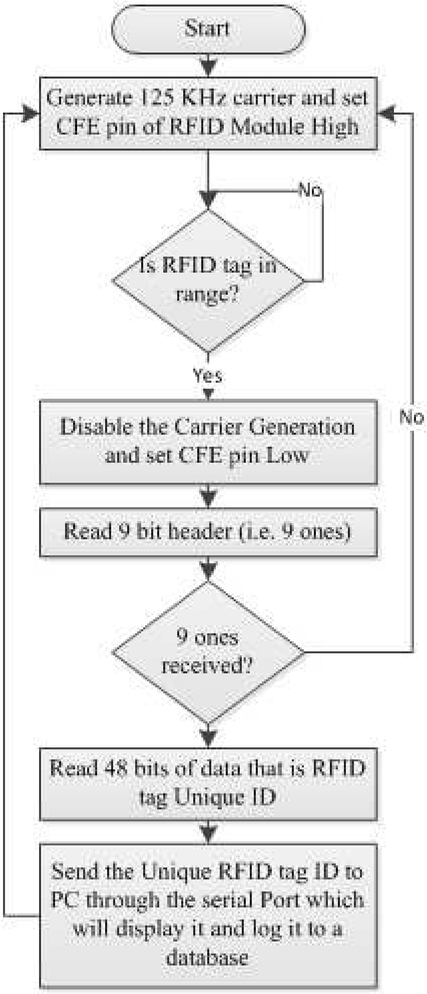

Start
Generate 125 KHz carrier and set CFE pin of RFID Module High
No
Is RFID tag in range?
Yes
Disable the Carrier Generation and set CFE pin Low
No
Read 9 bit header (i.e. 9 ones)
9 ones received?
Read 48 bits of data that is RFID tag Unique ID
Send the Unique RFID tag ID to PC through the serial Port which will display it and log it to a database

Figure 4: Microcontroller's program flowchart

The tag data is brought to microcontroller through CYOUT. The data from the tag is in following form.

1010101001011010101010101010101010100110010101010
101100101010110010110010110101001011010101010101010

As we know that the data is in the form of Manchester code (as shown in Figure 5), 1 is represented by a transition from low to high while 0 is represented by a transition from high to low. Hence, each bit is represented by two bits in Manchester code and the decoded response has half the bandwidth compared to that of the transmitted signal and is only 48 bits long.

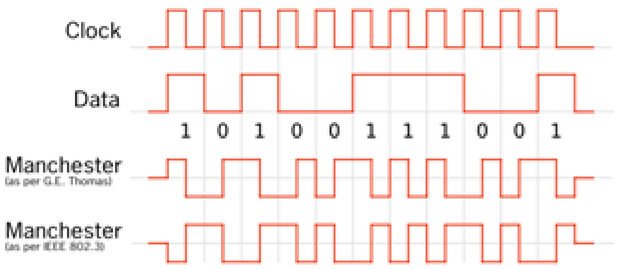


Figure 5: Manchester coding (Figure taken from [8])

The microcontroller uses a delay of 512μs to detect transition, at start the tag transmits a nine bit header of 1's after the header actual serial number is transmitted. The microcontroller stores the data in its internal RAM and forwards it to the serial port for database logging software.

3.3 PC Interfacing and Database Logging

The important feature of this study is that the RFID module is serially interfaced with the PC and special software has been designed for logging the tag ID to the database. Access database was used with the software written in Visual Basic.

For this purpose we used MAX232 IC to serially send the data from microcontroller to the PC. The microcontroller has been programmed to send the tag ID serially to the PC, when the tag is in close proximity with the reader and it is further processed by the software to display it on the screen and log it to the database. Care should be taken to make the communication between reader and PC physically secure; otherwise encryption should be used to avoid the leakage of tag IDs.

3.3.1 Database Logging and Output Display Software

Figure 6 at the end of the paper is a screenshot of the Graphical User Interface of visual basic program used to display the data on the PC which is connected to the RFID reader. The software also stores the tag ID along with date and time at which the tag was read in an Access Database.

As shown in the screenshot the software is waiting for a card to be read by the reader. There are three columns on the left side, the date & time columns show the exact moment at which the card is detected. The card column shows the unique serial number of the proximity card.

The buttons in the control panel provides an interface to the user to control the application. The "Start" button is used to start the reading process from the RFID reader. The "Stop" button is used to terminate the reading process. The "Delete All Records" button is used to wipe out all the previously stored serial numbers. The "About" button gives information about the software.

4 Experiment and Results

The experiment was performed by connecting the RFID reader to the PC, so that it should be connected to the PC interfacing and database logging software. The tags were brought close to the RFID reader at different distances to check the range of the system and as well as the working of PC interfacing and database logging software. The screenshot showing that two tags have been authenticated and the software is waiting for another tag to read is shown in Figure 6 at the end of the paper.

We have achieved an impressive range of 10 cm at 125 kHz using passive RFID tags while keeping the cost of the complete system under $10 USD.

5 Conclusion and Future Work

The system can be improved by increasing the effective range of reader in which the tag can be read. Further improvement can be done by using a method in which the tag encrypts its ID and then sends to the reader, which will eliminate the capturing of the tag IDs and hence cloning the tags.

References

[1] S. I. Ahamed, F. Rahman, and E. Hoque, "ERAP: ECC based RFID authentication protocol," *12th IEEE International Workshop on Future Trends of Distributed Computing Systems*, pp. 219-225, 2008.

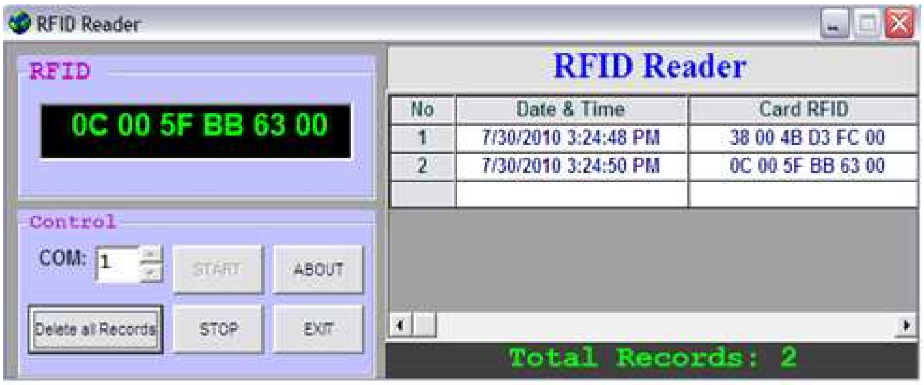
[2] T. Cao and P. Shen, "Cryptanalysis of two RFID authentication protocols," *International Journal of Network Security*, vol. 9, no. 1, pp. 95-100, 2009.

[3] C. L. Chen, Y. L. Lai, C. C. Chen, Y. Y. Deng, and Y. C. Hwang, "RFID ownership transfer authorization systems conforming epcglobal class-1 generation-2 standards," *International Journal of Network Security*, vol. 13, no. 1, pp. 41-48, 2011.

[4] B. Chowdhury and M. U. Chowdhury, "RFID-based real-time smart waste management system," *Telecommunication Networks and Applications Conference*, pp. 175-180, Australasian, Dec. 2-5, 2007

[5] G. H. P. Florentino, C. A. P. de Araujo, H. U. Bezerra, H. B. de A. Junior, M. A. Xavier, V. S. V. de Souza, R. A. de M. Valentim, A. H. F. Morais, A. M. G. Guerreiro, and G. B. Brandao, "Hospital automation system RFID-based: Technology embedded in smart devices (cards, tags and bracelets)," *30th Annual International IEEE EMBS Conference*, pp. 1455-1458, pp. 20-25, Aug. 2008.

[6] J. Jeo, S. Ryu, T. M. Chang, H. Y. Choi, and M. S. Kang, "Digital codec design for RFID tag based on



RFID Reader

0C 00 5F BB 63 00

No	Date & Time	Card RFID
1	7/30/2010 3:24:48 PM	38 00 4B D3 FC 00
2	7/30/2010 3:24:50 PM	0C 00 5F BB 63 00

Total Records: 2

Figure 6: Snapshot of PC interfacing and database logging software showing the results

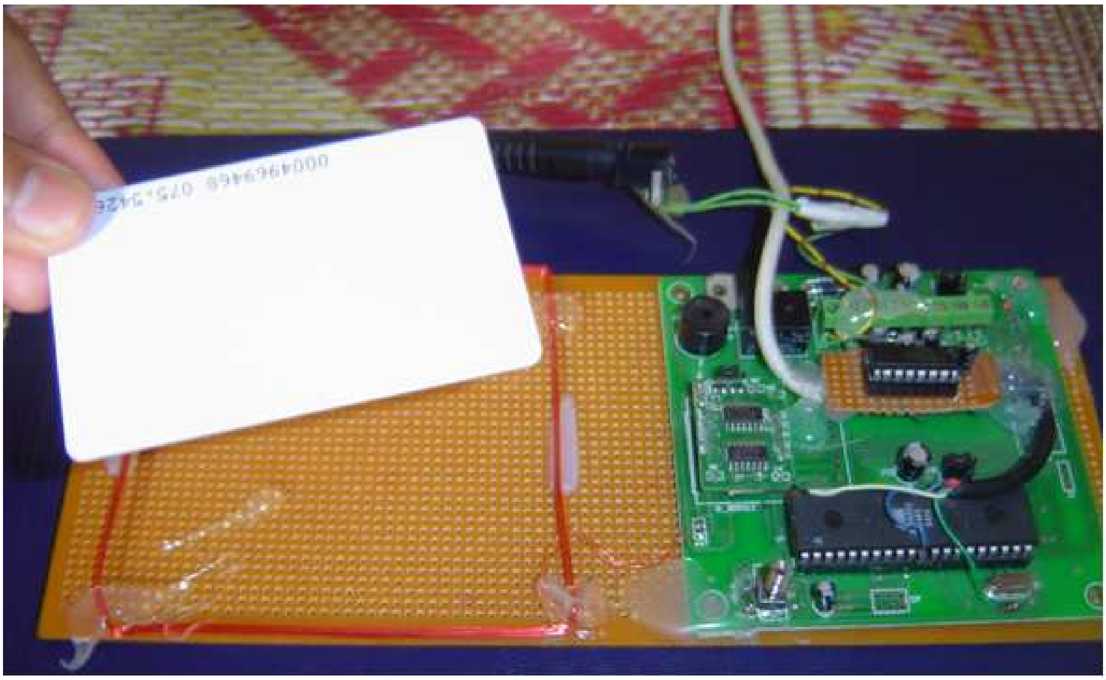


Figure 7: Snapshot of the proposed system

cryptographic authentication protocol," *Future Generation Communication and Networking*, pp. 119-124, 2007.

[7] N. Li, Z. L. Deng, F. Wan, S. Zhu, and X. Liu, "RFID-based information sharing platform," *IEEE International Conference on Communications Technology and Applications*, pp. 1-4, pp. 16-18, Oct. 2009.

[8] *Manchester Code*, Wikipedia, The Free Encyclopedia. (http://en.wikipedia.org/wiki/Manchester _code)

[9] Microchip, *MicroID 125 kHz RFID System Design Guide*, 2003. (http://ww1.microchip.com/downloads /en/devicedoc/51115f.pdf)

[10] C. Ross and R. Goto, *Proximity Security System,* Cornell University Electrical Engineering Final Projects, 2006.

[11] H. M. Sun and W. C. Ting, "A gen2-based RFID authentication protocol for security and privacy," *IEEE Transactions on Mobile Computing*, vol. 8, no. 8, pp. 1052-1062, Aug. 2009.

[12] E. Syta, S. Kurkovsky, and B. Casano, "RFID-based authentication middleware for mobile devices," *Hawaii International Conference on System Sciences*, pp. 1-10, 2010.

[13] K. Wu, E. Bai, and W. Zhang, "A hash-based authentication protocol for secure mobile RFID systems," *First International Conference on Information Science and Engineering*, pp. 2440-2443, 2009.

[14] X. Zhang and B. King, "Security requirements for RFID computing systems," *International Journal of Network Security*, vol. 6, no. 2, pp. 214-226, 2008.

Muhammad Naveed was born in Kohat, Pakistan in 1988. He has received his BSc degree in Electrical Engineering from University of Engineering and Technology, Peshawar in October 2010. He is an active researcher in the area of cryptography and information security and has authored seven research papers. His short book on video compression has been published by Lambert Academic Publishing, Germany. He is currently serving as a Lecturer in the Department of Electrical Engineering of University of Engineering and Technology, Peshawar, Pakistan.

Wasim Habib was born in Armidale, Australia in 1987. He has completed his BSc degree in Electrical Engineering (with majors in communication) from University of Engineering and Technology Peshawar, Pakistan. He has worked as a research internee for more than a year on a project funded by Daimler Chrysler, USA. He has "Juniper Networks" associate and specialist certifications: JNCIA-ER, JNCIS-ER, JNCIA-EX, and JNCIS-SEC. His research interests include computer networks, information security, auto-identification systems and Electronic Fuel injection systems.

Ubaid Ullah was born in Peshawar Pakistan in 1989. He has completed his BSc in Electrical engineering (with majors in communication) from University of engineering and technology Peshawar, Pakistan. His field of interest is communication and computer networks.

Usman Masud was born in Peshawar Pakistan, in 1987. He has completed his BSc degree in Electrical Engineering (Communications) from University of Engineering and Technology Peshawar, Pakistan. He has "Juniper Networks" Associate and Specialist certifications: JNCIS-ER, JNCIA-ER, JNCIS-SEC and JNCIA-EX. His research interests include RF communication, Signal Processing and Computer Networks.

Gulzar Ahmad received his BSc and MSc degree in Electrical Power Engineering from University of Engineering and Technology, Peshawar. He has also received an MS degree in Communication Engineering from George Washington University, USA. He is currently working as an Assistant Professor in the Department of Electrical Engineering of University of Engineering and Technology, Peshawar.