Proceedings of the
International Conference on Mechanical Engineering and Renewable Energy 2013
(ICMERE2013) 1 - 3 May 2014, Chittagong, Bangladesh

ICMERE2013-PI-054

DEVELOPMENT OF AN EMBEDDED ACCESS CONTROL AND SECURITY SYSTEM USING RFID TECHNOLOGY

Md. Ruhul Amin[1,*], Ahamed Nasif Hossain Aoyon [2], Shuva Das[3] and Mujahidul Islam Shakil[4]

[1-4] Department of Mechanical Engineering, CUET, Chittagong 4349, Bangladesh

[1,*]ruhul_cuet08@hotmail.com, [2]aoyon7@gmail.com, [3]shuvome08@gmail.com, [4]mujahidulislam.sh@gmail.com

Abstract- *Radio frequency identification (RFID) is a rapidly growing technology that has the potential to make great economic impacts on many sectors. Deployment of radio frequency identification (RFID) systems is increasing day by day in many industries and applications. This paper is based on automating the access control and security operations involved in an organization or industry. Earlier, access control and security operations are performed by conventional swiping system using bar code readers. Now, it can be carried using non-contact devices, with the help of Radio Frequency Identification (RFID) system. RFID cards are provided to employees, these cards carry their own identification number in a coded format, which can be retrieved by the RFID reader only. By means of this the authentication of the employees can be verified. Then is the access control at various points inside the organization or industry. In order to avoid tress passing and in cases of theft of cards, a keypad system can be added for entering a password. Thereby it achieves a two level security and more reliable system. This RFID technology system finds quite an important application in Pay roll calculation, libraries, defense weapons storage places (where only certain persons are authorized to enter), industrial monitoring and so on. The advancements of this technology have the potential to revolutionize supply-chain management, inventory control, and logistics system.*

Keywords: Radio Frequency Identification (RFID), Bar Code Readers, Radio Frequency, RFID Cards, Identification Number.

1. INTRODUCTION

In a modern world, with little time for bureaucracy, control over property is a major factor of concern to any institution or company. All companies have restricted access areas or places where there must be strict control on the mobilization of material to prevent its disappearance (e.g. libraries, stockrooms, etc.). A solution for easy access by authorized personnel and access to material that saves time that would otherwise be wasted by searching store keys and/or Waiting for the security to arrive should be welcome. Such a solution would also improve ease of return s or request s of equipment. Furthermore, it allows a thorough inventory on all the material, thus, avoiding mysterious disappearances.

In our country we have seen the security personnel checking the employees' identification cards at the entrances to avoid illegal entry. The employees sign a register at the entrance before getting in. This is still being practiced in most of the companies. However, the disadvantages are that, when there is a necessity of providing control at many locations inside the company a person at each point will not be an economical way of implementing it. Then came were the punch cards. Employees possess cards, which are punched when they enter into the building. But it had disadvantages. Workers started to practice buddy punching, for their co-workers.

For punching cards bar code reader are also used in the companies. These are used to check with the employee's identification. The employees swipe the card in the provided slot. Then the access is given after checking the authenticity of the card. This was a substitute to the security and emerged as a new technique in access control. This acted as a starting to the automation of the access control. But, the bar code readers are contact readers where, the cards are required to touch the readers.

With growth of technology and giant leap in the field of Radio frequency transmission, a requirement for the same application using RF is desired. A further improvement is the RF ID card technology, which uses contact less card readers. Bringing the card nearer to the reader suffices for the reader to read the contents of the card. This simplifies the usage for the employees. This technology is crawling into the companies and has the potential to substitute the preceding technologies.

2. OVERVIEW OF RFID TECHNOLOGY

Radio frequency identification (RFID) is used to describe a system that transmits the identity in the form of a unique serial number of an object or person using radio waves. If any conductive materials are put into any electric or magnetic field, it can alter the field's characteristics. That occurs because the conductive material both absorbs and reflects the energy in the field. If the field is a radio frequency, or RF, the conducting material is capable of imparting a reflection of the source field radiation [1]. RFID takes advantages of this characteristic by manipulating sequence and rate at which the reflection occur and it is called modulation. RFID tags are deliberately reflects the source RF in sequence that are interpreted as information in the form of digital data.

RFID is a flexible technology that is convenient, easy to use, and well suited for automatic operation. It combines advantages not available with other identification technologies. RFID can be supplied as read-only or read / write, does not require contact or line-of-sight to operate, can function under a variety of environmental conditions, and provides a high level of data integrity. In addition, because the technology is difficult to counterfeit, RFID provides a high level of security.

RFID is similar in concept to bar coding. Bar code systems use a reader and coded labels that are attached to an item, whereas RFID uses a reader and special RFID devices that are attached to an item. Bar code uses optical signals to transfer information from the label to the reader; RFID uses RF signals to transfer information from the RFID device to the reader.

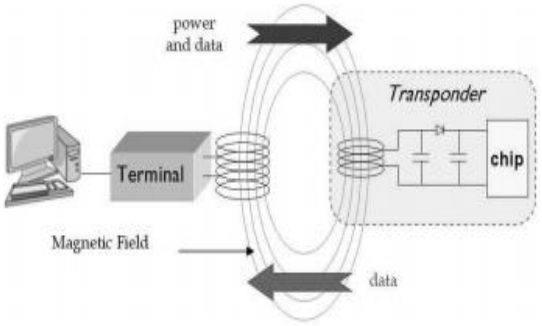
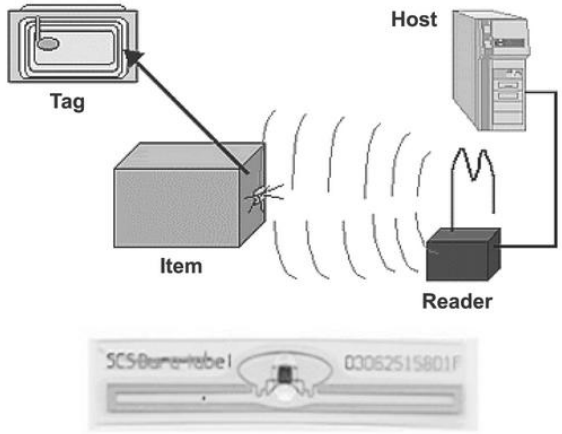


Figure.1: Overview of RFID system.

An RFID system includes three primary components: a transponder (tag), a transceiver (reader) and a data collection device.

RFID tags contain a microchip with some computation and storage capabilities, and a coupling element, such as an antenna coil for communication. There are three types of tags i.e. passive RFID tags, semi-passive RFID tags, and active RFID tags [2]. Passive tags do not have an internal source of power. They harvest their power from the reader that sends out electromagnetic waves. They are restricted in their read/write range as they rely on RF electromagnetic energy from the reader for both power and communication. Semi-passive tags use a battery to run the microchip's circuitry but communicate by harvesting power from the reader signal. Active tags possess a power source that is used to run the microchip's circuitry and to broadcast a signal to the reader.

RFID readers are generally composed of an RF module, a control unit, and a coupling element to interrogate electronic tags via RF communication. RFID reader which reads and writes the data on the tags and finally, a backend database which is used to record the data collected by the tag readers [3]. The authenticated RFID reader performs the following functions such as, authenticates tags that are presented using digital signature verification techniques, programs the chain-of-custody event marker to tags that are presented, creates a digital signature using the reader's private key, Communicates relevant event information, including digital signatures and event markers to the local computer system.



RFID Tag (not to scale)

Figure.2: Components of RFID system.

A data collection device collects the data from the tags and stores. Figure.2 shows the RFID system components.

EPC, the electronic product code, is a major issue when talking about RFID. It is actually a standard proposed by the Auto-ID center with two different types, a 64- and a 96 bit code and 96 bit chip would be the dominant data format for commercial RFID tags. The 96-bit code gives a unique number to 268 million companies, with 16 million different object classes and 68 billion serial numbers in each class [4]. The 64-bit version should be a compromise between the cost of a tag and the number of different codes. This version offers lower cost but fewer serial numbers. The EPC number is made up of a header and three sets of data. The header clarifies the EPC version used, as versions of different length and type might be used in the future. The second part represents the manufacturer's code. The third part identifies the type of product, usually the Stock Keeping Unit (SKU). The big difference to the bar code is the last part of the EPC, the serial number. It refers to one single item of this type of product and makes the EPC a unique code that only exists once, in contrast to the barcode which identifies to the type of

product but not a difference in the single product. EPC was first developed by Auto-ID Center in MIT in 1999. This center developed the initial RFID standard and later transferred to EPC Global for commercialization in late 2003.

The frequency used for the communication between reader and tag is one of the leading factors, besides the choice between active and passive tags, affecting the read range for an RFID system [5]. In addition to influencing the read range, the choice of frequency also has an effect on the data transfer rate that can be achieved between tag and reader. Frequency is furthermore influencing the sensitivity to metals and fluids as well as the possible selection of sizes and shapes for the tags. Each of the frequency ranges thus becomes more or less suitable to certain applications.

RFID system utilizes a variety of radio frequencies from 30 KHz to 5.8 GHz. Reading length and writing speed depend on frequency range.

Lower the frequency, lower the read/write speed and lower the cost. Low frequency (LF) (30 KHz-1400 KHz) has small read range and slow data transfer rate. Read range varies from 1 to 200 cm. Low frequency tags can transmit through elements such as water, wood and aluminum. But in the environment with metal like iron, steel the transfer rate decreases.

High frequency (HF) (3MHz-30MHz) has high data transfer rate than low frequency tag. It can penetrate materials and has a read range from 1 to 95 cm. It works well in environments containing fluids. The high frequency tags are less sensitive to metals and sources of electronic noise than ultra high frequency tags.

Ultra high frequency (UHF) (850MHz-960MHz) tag has high data transfer rate, it can store large amount of data and it can read up to 3m. Due to high frequency the transfer rate is also high. A disadvantage of ultra frequency tag is that it is highly sensitive to the presence of water and may not work properly if it is attached to materials with high content of water. Ultra frequency tags are unable to penetrate through wood or water.

In figure 3 the comparison of characteristics among low frequency (LF), High frequency (HF), Ultra high frequency (UHF) is shown. There is another type of frequency which is microwave (2.4GHz-2.5GHz, 5.8GHz) has a read range from 0.3m to 0.9m and these types of tags are small in size

compare to other tags. The characteristics of micro wave frequency are same to ultra wave frequency but the micro wave frequency can read very fast.

3. System Architecture and Components

Managing access to resources is assuming increasing importance for organizations everywhere, from small entrepreneurial companies to large corporate enterprises and government bodies of all sizes. Administering access to resources means controlling both physical access and logical access, either as independent efforts or through an integrated approach. The Physical access control protects both tangible and intellectual assets from theft or compromise. Logical access control enables enterprises and organizations to limit access to data, networks and workstations to those authorized to have such access [6].

The access control system is composed of three elements:

1) A card (an identity credential) that is presented to a door reader.
2) A door reader, which indicates whether the card is valid and entry, is authorized.
3) A door or gate, which is unlocked when entry is authorized.

Behind the scenes is a complex network of computers and software that incorporates robust security functionality.

	LF	HF	UHF	Active
Frequency	125 – 134.2 KHz	13.56 MHz	850 – 960 MHz	100 KHz – 2.45GHz
Range	0.2 – 2m	Up to 1m	Up to 3m	Up to 100m
Cost	Typ. 3 GBP	(Typ. 0.50 GBP)	(Typ. 0.30 GBP)	(Typ. 20 GBP)
Memory	Typ. 64 bits	Typ. 2048 bits	Typ. 96 bits	Typ. 32 bits
Penetration of Materials	V. Good	Good	Poor	V. Good
Data Rate	Slow	Fast	Fast	Fast
Reader Cost	50 – 500 GBP	50 – 3000 GBP	1000- 3000 GBP	200-600 GBP
Read Multiple Tags	Poor	Good	Very Good	Good
Applications	Animal Tags, Vehicle Immobilisers, Industrial Applications	Item Tracking, Access Control, Smart Labels	Box and Pallet tracking Some Item Tracking	Industrial Applications. Asset Tagging Location Systems

Figure.3: RFID frequency range table.

The system is made up of the following components ID credential, Door reader, Door lock, Control panel, Access control server, Software, Database.

When the ID credential is placed before the RFID reader at the door, the reader verifies the ID number from access control software database. If the ID number match with the database then control panel automatically open the door lock to access. The additional control panel is used to check the password verification as a second level security. The whole system's block diagram is shown in figure 4.

4. WORKING PROCESS OF THE SYSTEM

The access control process begins when the user presents the card to the reader, which is usually mounted next to a door or entrance portal. The reader extracts data from the card, processes it and sends it to the control panel. Then the control panel first validates the reader and then accepts the data transmitted by the reader. What happens next depends on whether the system is centralized or distributed.

In a centralized system, the control panel transmits the data to the access control server. The access control server compares the data received from the card with the

information about the user that is stored in a database. Access control software determines the user's access privileges and authorization, the time, date and door entered, and any other information that a company may require to ensure security [7]. When access is authorized, the access control severs sends a signal to the control panel to unlock the door. The control panel then sends out a signal to the appropriate door lock, which unlocks the door.

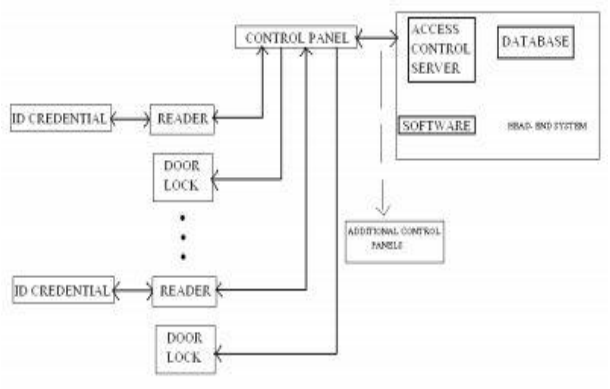


Figure.4: Block diagram of access control system.

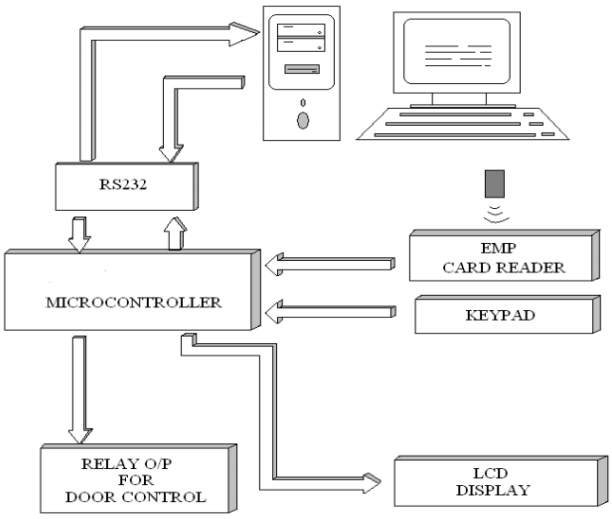


Figure.5: Block diagram of whole system.

In a distributed system, the control panel allows or denies entry. The access control server periodical provides control panels with data that enable the control panel software to determine whether the user is authorized for access. The control panel then performs the access control server functions described above and makes the decision to allow or deny entry. Enabling control panels to perform the decision function has the advantage of requiring less communication between the control panels and a central access control server.

Here we have used centralized system for access control. A block diagram of whole system is given below to understand the working process.

From figure 5 we see that the card reader read the ID number from the ID card and sending the information to microcontroller. The microcontroller then sending this information to software database to verify through RS232 communication system. If ID number matches then the system demand the security password. The user needs to type the password using keypad. If password is correct the microcontroller unlocks the door.

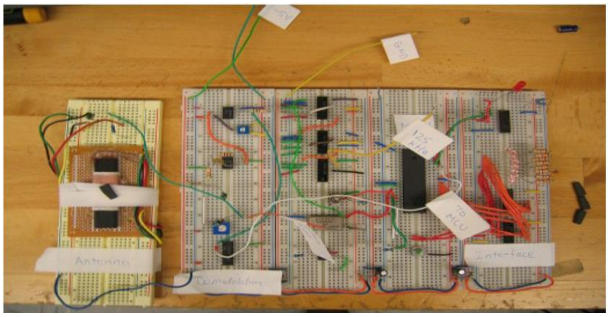


Figure.6: Snap of the circuit setup.

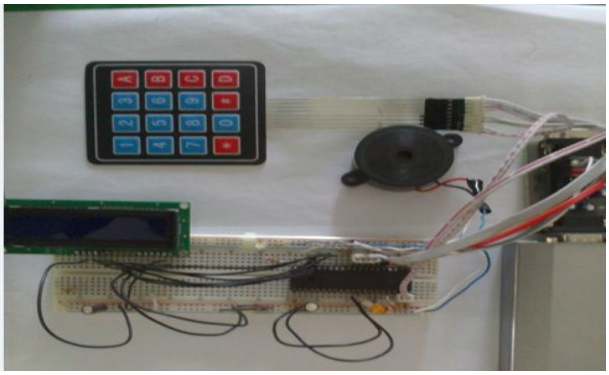


Figure.7: Snap of the circuit setup of password part.

The schematic diagram of whole circuit and RFID reader part are shown below in figure 8.

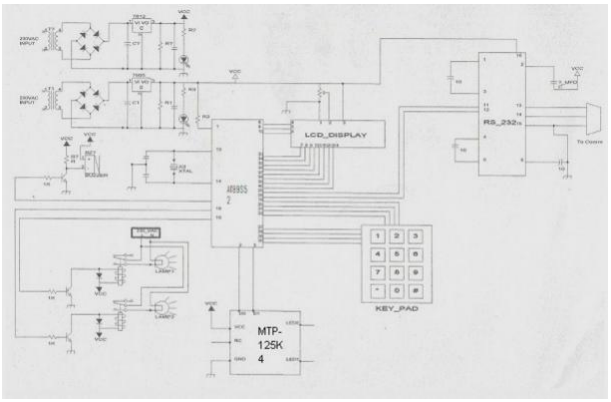


Figure.8: Schematic circuit diagram of whole system.

5. CONCLUSION AND FUTURE WORK

The results show that this system simplifies the bureaucratic methods and successfully automates the access to a restricted area, thus increasing the autonomy of users in the enclosure. The system also provides an

economic and secure solution for access control. The implementation of RFID based system in access control and security operations are bound to increase in the future. The advantages, efficiency and reliability of the system have made it manifest itself over the existing systems. The system achieves a two level security making the incorporating firm more secure.

In the future, this system can be modified for more applications in the field of automation and security. This system can be easily used such as Vehicle Identification, Industrial Monitoring, Animal Identification and many other sectors. Further this system is compatible for the future up gradations like a finger print scanner, retina scanner, monitoring camera, etc. making it more versatile. With the introduction of more smart RFID devices in the near future the system is going to rule the field of access control and security.

6. REFERENCES

[1]. Want, R. In: An Introduction to RFID Technology. Volume5. Pervasive Computing (Jan.2006) 25-33.

[2]. Weinstein, R. In: RFID: A Technical Overview and Its Application to the Enterprise.Volume7.IT Professional (May2005) 27-33.

[3]. G. Avoine. "Cryptography in Radio Frequency Identification and Fair Exchange Protocols", PhD thesis, Ecole Polytechnique F´ed´erale de Lausanne (EPFL), Lausanne, Switzerland, December 2005.

[4]. S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", LNCS 2802, pp. 201-212, 2004.

[5]. Rieback, M., Crispo, B., Tanenbaum, A. In: Is Your Cat Infected with a Computer Virus? Fourth Annual IEEE International Conference on Pervasive Computing and Communications (March2006) 169-179.

[6]. K. Finkenzeller, "RFID Handbook. Fundamentals and Applications and in Contactless Smart Cards and Identification" Second Edition, Chichester: JohnWiley & Sons Ltd. ISBN: 0470844027, 2003.

[7]. Thornton, F., Haines, B., Das, A., Bhargava, H., Campbell, A., Kleinschmidt, J. In: RFID Security. Syngress (2006) 29-54.

[8]. BookTec Information Co.: LibBest – Library RFID Management System. http://www.rd-library.com (2008).