International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

EMBEDDED BASED DOCUMENT LEAKAGE PROTECTION SYSTEM

Akash[1],Jaibheem[2],Prakash[3]
Student, Dept. of E&CE,
VNEC, Shorapur
Jaibheembg88@gmail.com

Sharangowda S. Patil[4]
Asst.prof Dept,ECE
VNEC Shorapur

***Abstract* – The main document leakage protection system is to design and develop to the stop the corruption by putting a stop to leakage of the documents with the help of technology i.e., Document Leakage Protection System. This document leakage protection mechanism there will be a box which will have a transceiver unit, a locking and unlocing mechanism. The box will be locked administrator, if the box is tampered before the time. It will generate the alaram. A signal will be generate from base station which deactivate the lock.**

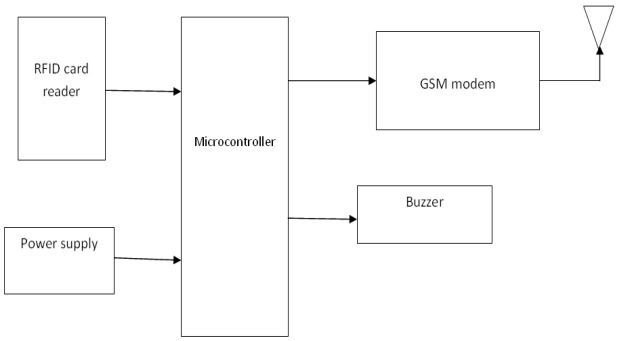
1. INTRODUCTION

The main aim to the document leakage protection system to implement a system which will help to stop the malpractice of leaking the important and confidential documents.

Data leakage protection system requires series of preparation work, including data classification, risk assessment and privacy requirement.

To achieve the document leakage protection system using micro-controller now easily implemented within embedded software of micro-controller and document leakage protection system aims at putting together a robust microcontroller based power supply unit access LCD screen 0.30 output range (upto 80w), computer connectivity and control and over load protection all implemented.

2. BLOCK DIAGRAM & WORKING



GSM modem is connected to the box containing question papers along with the microcontroller. Mobile of Authorized person in University board acts as the Base station. To open the question paper box, RFID is needed to be swiped with a valid RFID tag and then RFID will compare with data such as RFID address. If the comparison is failure , then controller sends ”WRONG ACCESS” message to the Base station through GSM modem and If anybody tries to open the box before the pre-defined time with a valid RFID tag also, then controller sends ”RULES VIOLATED” message to the Base station through GSM modem. The password is sent from the Base station to the college at the time of opening the BOX.

If the person enters the wrong password, then controller sends ”PASSWORD MISMATCH” message to the Base station through GSM modem. If the person enters the correct password, then BOX is opened with the help of the DC motor.

3. IMPLEMENTATION

GSM Modem

GSM stands for Global system for Mobile Communication. This is the structural set developed by the Europian Telecommunication standard institute (ETSI) to describe the technology for second generation. The GSM architecture which involve the (ms) mobile station directly interacts with a base station controller (BSC) BTS and BSC combined together forms the (BSS). More than one BTS are connected with one BSC, the BSC further interacts with mobile station controller (MSC) which is the heart of GSM network (MSC) gives connectivity to the PSTN and other PLMNS and (MSC) also responsible to interact with HLR and VLR.

RFID Reader

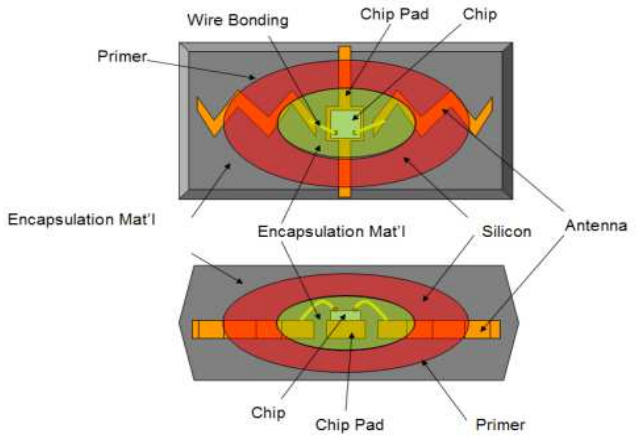
The document leakage protection system based on RFID security system, and its stands for Radio Frequency identification. Generally a RFID System consists of (2) parts A reader and one or more transponders, also known as Tags. RFID System evolved from bar code means automatically identity and track product and people.

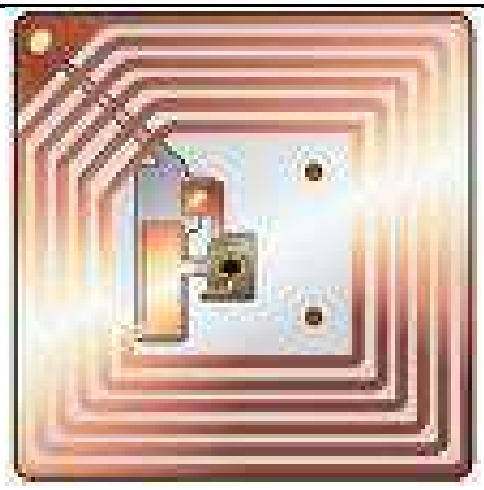
The RFID System can be seen in

1. Access control
2. Control Less payment system
3. Product tracking and inventory control.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

RFID TAG:





An RFID tag is comprised of a microchip containing identifying information and an antenna that transmits this data wirelessly to a reader. At its most basic, the chip will contain a serialized identifier, or license plate number, that uniquely identifies that item, similar to the way many bar codes are used today. A key difference, however is that RFID tags have a higher data capacity than their bar code counterparts. This increases the options for the type of information that can be encoded on the tag, including the manufacturer, batch or lot number, weight, ownership, destination and history (such as the temperature range to which an item has been exposed). In fact, an unlimited list of other types of information can be stored on RFID tags, depending on application needs. An RFID tag can be placed on individual items, cases or pallets for identification purposes, as well as on fixed assets such as trailers, containers, totes, etc.

Tags come in a variety of types, with a variety of capabilities "Read-only" versus "read-write"

There are three options in terms of how data can be encoded on tags: (1) Read-only tags contain data such as a serialized tracking number, which is pre-written onto them by the tag manufacturer or distributor. These are generally the least expensive tags because they cannot have any additional information included as they move throughout the supply chain. Any updates to that information would have to be maintained in the application software that tracks SKU movement and activity. (2) "Write once" tags enable a user to write data to the tag one time in production or distribution processes. Again, this may include a serial number, but perhaps other data such as a lot or batch number. (3) Full "read-write" tags allow new data to be written to the tag as needed—and even written over the original data. Examples for the latter capability might include the time and date of ownership transfer or updating the repair history of a fixed asset. While these are the most costly of the three tag types and are not practical for tracking inexpensive items, future standards for electronic product codes (EPC) appear to be headed in this direction.

The amount of data storage on a tag can vary, ranging from 16 bits on the low end to as much as several thousand bits on the high end. Of course, the greater the storage capacity, the higher the price per tag.

The tag and antenna structure can come in a variety of physical form factors and can either be self-contained or embedded as part of a traditional label structure (i.e., the tag is inside what looks like a regular bar code label—this is termed a 'Smart Label') companies must choose the appropriate form factors for the tag very carefully and should expect to use multiple form factors to suit the tagging needs of different physical products and units of measure. For example, a pallet may have an RFID tag fitted only to an area of protected placement on the pallet itself. On the other hand, cartons on the pallet have RFID tags inside bar code labels that also provide operators human-readable information and a back-up should the tag fail or pass through non RFID-capable supply chain links.

Like all wireless communications, there are a variety of frequencies or spectra through which RFID tags can communicate with readers. Again, there are trade-offs among cost, performance and application requirements. For instance, low-frequency tags are cheaper than ultra high-frequency (UHF) tags, use less power and are better able to penetrate non-metallic substances. They are ideal for scanning objects with high water content, such as fruit, at close range. UHF frequencies typically offer better range and can transfer data faster. But they use more power and are less likely to pass through some materials. UHF tags are typically best suited for use with or near wood, paper, cardboard or clothing products. Compared to low-frequency tags, UHF tags might be better for scanning boxes of goods as they pass through a bay door into a warehouse. While the tag requirements for compliance mandates may be narrowly defined, it is likely that a variety of tag types will be required to solve specific operational issues. You will want to work with a company that is very knowledgeable in tag and reader technology to appropriately identify the right mix of RFID technology for your environment and applications.

The RF transceiver is the source of the RF energy used to activate and power the passive RFID tags. The RF transceiver

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

may be enclosed in the same cabinet as the reader or it may be a separate piece of equipment. When provided as a separate piece of equipment, the transceiver is commonly referred to as an RF module. The RF transceiver controls and modulates the radio frequencies that the antenna transmits and receives. The transceiver filters and amplifies the backscatter signal from a passive RFID tag.

LCD (Liquid Crystal Display)

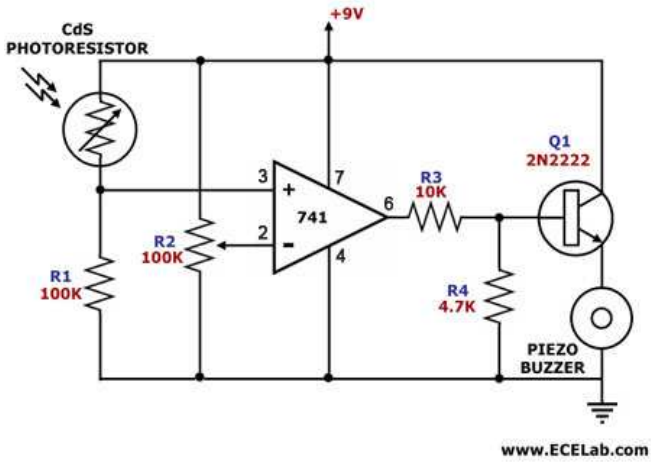
A liquid crystal display (LCD) is a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector. Each pixel consists of a column of liquid crystal molecules suspended between two transparent electrodes, and two polarizing filters, the axes of polarity of which are perpendicular to each other. Without the liquid crystals between them, light passing through one would be blocked by the other. The liquid crystal twists the polarization of light entering one filter to allow it to pass through the other.

Features :

- Interface with either 4-bit or 8-bit microprocessor.
- Display data RAM
- 80x8 bits (80 characters).
- Character generator ROM
- 160 different 5.7 dot-matrix character
- Character generator RAM
- 8 different user programmed 5.7 dot-matrix.
- Numerous instructions: Clear Display, Cursor Home, Display ON/OFF, Blink Character, Cursor Shift, Display Shift.

Shapes and sizes :

Buzzer



A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave oven.

It most commonly consists of a number of switches or sensors connected to a control unit that determines if and which button was pushed or a preset time has lapsed, and usually illuminates a light on the appropriate button or control panel, and sounds a warning in the form of a continuous or intermittent buzzing or beeping sound. Initially this device was based on an electromechanical system which was identical to an electric bell without the metal gong . Often these units were anchored to a wall or ceiling and used the ceiling or wall as a sounding board. Another implementation with some AC-connected devices was to implement a circuit to make the AC current into a noise loud enough to drive a loudspeaker and hook this circuit up to a cheap 8-ohm speaker. Nowadays, it is more popular to use a ceramic-based piezoelectric sounder like a Son alert which makes a high-pitched tone. Usually these were hooked up to "driver" circuits which varied the pitch of the sound or pulsed the sound on and off.

The word "buzzer" comes from the rasping noise that buzzers made when they were electromechanical devices, operated from stepped-down AC line voltage at 50 or 60 cycles. Other sounds commonly used to indicate that a button has been pressed are a ring or a beep.

4. DC MOTOR

A DC motor is a mechanically commutated electric motor powered from direct current (DC). The stator is stationary in space by definition and therefore its current. The current in the rotor is switched by the comutator to also be stationary in space. This is how the relative angle between the stator and rotor magnetic flux is maintained near 90 degrees, which generates the maximum torque.

DC motors have a rotating armature winding (winding in which a voltage is induced) but non-rotating armature magnetic field and a static field winding (winding that produce the main magnetic flux) or permanent magnet. Different connections of the field and armature winding provide different inherent speed/torque regulation

characteristics. The speed of a DC motor can be controlled by changing the voltage applied to the armature or by changing the field current. The introduction of variable resistance in the armature circuit or field circuit allowed speed control. Modern DC motors are often controlled by power electronics systems called DC drives.

The introduction of DC motors to run machinery eliminated the need for local steam or internal combustion engines, and line shaft drive systems. DC motors can operate directly from rechargeable batteries, providing the motive power for the first electric vehicles. Today DC motors are still found in applications as small as toys and disk drives, or in large sizes to operate steel rolling mills and paper machines.

5. POWER SUPPLY

To achieve document leakage protection system by using power supply. To achieve this, using microcontrollers seems to be the utmost solution. What can be done with discrete electronic circuits inside the devices can now easily be implemented within the embedded software of the µ controller (i.e. a short circuit protection can be implemented with a bulky crowbar circuit or simply with a fast loop in the µC). As a result, this projects aims at putting together a robust microcontroller based power supply unit with easy access LCD screen, 0-30V output range (up to 80W), computer connectivity and control.

6. RESULT

The document leakage protection system to implement with the help of RFID system to stop the malpractice of leaking the important and confidential documents.

7. CONCLUSION

After implementation of embedded based document leakage protection system we conclude that security various important and confidential documents. RFID based document leakage protection system use of various hardware properties like the RFID reader and Tag buzzer. Microcontroller, LCD, GSM and Power Supply. The swapping of tag, validity of the user and the reply of code provide the working of the motor document leakage protection system and display in the LCD.

REFERENCES

[1]. K. Ray and K. M. Bhurchandi, Advanced microprocessors and peripherals: architecture, programming and interfacing. New Delhi: Teta McGraw-Hill Pub.Co, 2000. Call No. TK7895 Mic.Ra

[2]. A. P. Chandrakasan, W. Bowhill and F. Fox, Eds. Design of high-performance microprocessor circuits. New York: IEEE Press, 2001. Call No. TK7895 Mic.Ch

[3]. A. V. Deshmukh, Microcontrollers: theory and applications. New Delhi: Tata McGraw-Hill, 2005. Call No. TJ223 Pro.De

[4]. A. Williams, Microcontroller projects with Basic Stamps. Lawrence, Kan.: R&D, 2000. Call No. TJ223 Pro.Wi

[5]. B. B. Brey, The Intel microprocessors: 8086/8088, 80186/80188, 80286, 80386, 80486, Pentium, Pentium Pro processor, Pentium II, Pentium III, and Pentium 4: architecture, programming, and interfacing, 6th ed., Upper Saddle River, N. J.: Prentice Hall, 2003. Call No. QA76.8 Int.Br

[6]. C. Hellebuyck, Programming PIC microcontrollers using PicBasic. Amsterdam: Newnes, 2003. Call No. TJ223 Pro.He

[7]. C. J. Bergquist, Guide to PICMICRO microcontrollers. Indianapolis, Ind.: Prompt Publications, 2001. Call No. TJ223 Pro.Be

[8]. C. Kuhnel and K. Zahnert, BASIC stamp. Boston: Newnes, 2000. Call No. TJ223 Pro.Ku

[9]. C. Nagy, Embedded systems design using the TI MSP430 series. Amsterdam; Boston: Newnes, 2003. Call No. TK7895 Emb.Na

[10]. D. A. Geller, Programmable controllers using the Allen-Bradley SLC-500 family. Upper Saddle River, N.J.: Prentice Hall, 2000. Call No. TJ223 Pro.Ge