Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Electronic Protection for Exam Paper Leakage

Tai Raskar, Archana Patil, Pooja Bhoir
Department of Electronics & Telecommunication,
Government College of engineering & Research Awasari Kh.
Pune, Maharashtra, India

***Abstract*— Education is simply the soul of a society and examination is the heart of education system. Today, when we come across the news of malpractice in exams, we realize that, knowingly or unknowingly this soul has got irrecoverably corrupted. The main reason for this is exam paper leakage. The serious actions must be taken to prevent this. So we propose an electronic system here to detect and prevent examination paper leakages.**
In this proposed system the question papers will be sent to the examination centres in the electronically locked box, which cannot be opened before the predefined date and time. The box can be opened by authentic user only. The question papers are actually present in sub boxes. These are password protected. The exam controller will send a message containing password to open individual sub box. When the Password, date and timing matches, the box will open through a motorized mechanism. This will help the papers to remain locked and sealed till the time of examination. The light sensors are used to detect any sort of unauthorized tampering.

Keywords-- ARM processor, GSM, LPC2148, RFID, RTC

I. INTRODUCTION

An examination is an assessment intended to measure the knowledge, skills, aptitude, physical fitness or classification in many other topics. A test may be administered orally, on paper, on a computer or in a confined area that requires an examinee to physically perform a set of skills. [1]
The history of examination is very wide. The first a nationwide standardized test was implemented in China, which was called the imperial examination. The main purpose of this examination was to select able candidates for different governmental positions.
The imperial examination was established in 605 AD. And then after different countries adopted the examination systems. England had adopted this examination system in 1806 to select the applicants for positions in Civil Services. This examination system was later applied to education and became a worldwide standard. [1]
Every year news flashes in newspaper and television during the time of examination that the exam is being postponed/cancelled due to the leakage of question papers.
Many times the leakage of question papers will not be known to the universities. In such conditions some students get good ranks by these leaked papers and those students who had worked hard have to compromise with less rank. This factor will have negative effect on the growth of the society .Thus by considering the problems faced by the students and society a system has to be implemented which will help to detect and prevent the leakage of question papers.

II. LITERATURE REVIEW

The question papers are distributed in sealed boxes. This system is being followed since many years. The disadvantages of this system are it may lead to leakage of question papers at various instances in the journey of box from printing location to examination centers. This happens due to easy tampering of sealed boxes and more human interference.
Other method involves the e-copy of the question papers mailed from the university to the colleges prior to examination. The colleges take the printouts of the question paper and then are distributed to the examinees.
This method also has many disadvantages. The website may be hacked, server may also breakdown and number of colleges had to take printouts which involves the threats like power failure, system failure and may lead to leakage or problems in conduction of examination.
The idea for the proposed system which involves the electronic protection is derived from modern day applications like Electronic lockers in bank, Home security systems, office security systems and other security enhanced electronic systems.

III. PROPOSED SYSTEM

A Main box contains the sub boxes in which question papers are proposed to be kept. The RFID tag and GSM modem are connected to the box along with the ARM processor.
GSM modem interfaced to ARM processor always sends the report of activities to university via text messages. The overview of proposed system is shown in figure 1.

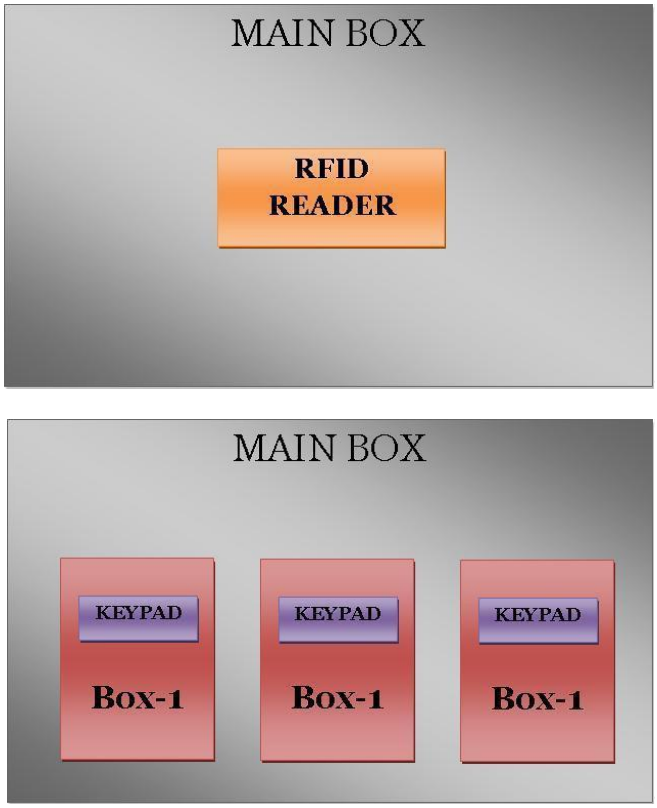

Fig. 1. Overview of proposed system

A. Hardware Design

The proposed hardware design for the system is as shown in figure 2. The heart of the system is LPC2148. Along with it many components are used such as RFID, GSM, key matrix, DC motor and motor drivers, etc are used.

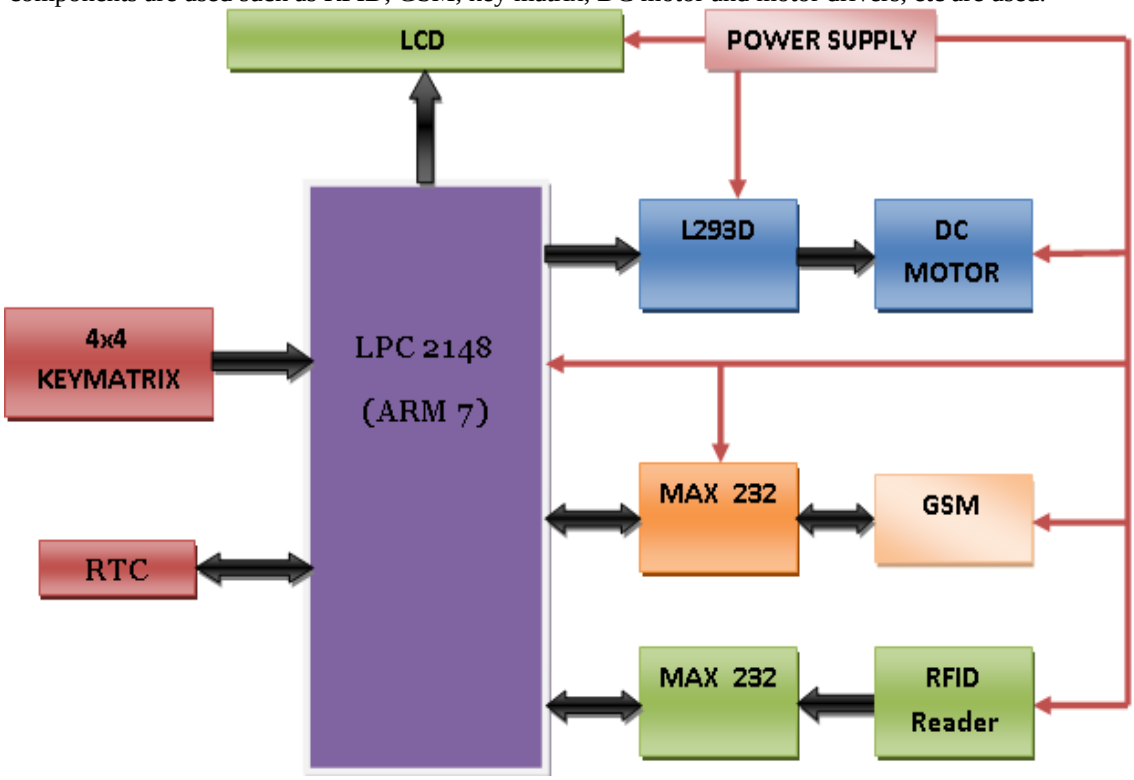

Fig. 2. Block diagram of proposed system

1) ARM7 Processor (LPC2148): It is a 32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package. It has 40 kB of on-chip static RAM and 512 kB of on-chip flash memory. It supports In-System Programming/In- Application Programming (ISP/IAP) via on-chip boot loader software. It has two 10-bit ADCs provide a total of 14 analog inputs. It provides multiple serial interfaces including two UARTs, two Fast I²C-bus (400 kbit/s), SPI and SSP with buffering and variable data length capabilities. [3]

2) Real Time Clock (RTC): LPC2148 includes a low power Real-Time Clock (RTC) with independent power and 32 kHz clock input. It measures the passage of time to maintain a calendar and clock. The main feature of RTC is Ultra Low Power design to support battery powered systems. It provides Seconds, Minutes, Hours, Day of Month, Month, Year, Day of Week, and Day of Year. The architecture of RTC is shown in figure 3. [3]

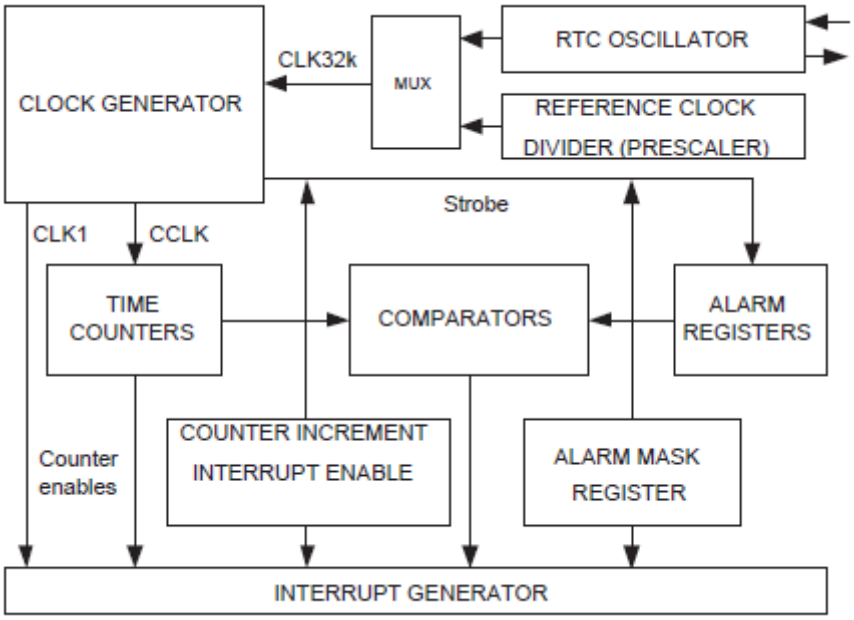

Fig. 3. Architecture of RTC for LPC2148

3) Keypad: Various types of key pads are available in market like push button keypad, membrane switch keypad, capacitive touch keypad, resistive touch keypad, etc. Out of these the push button keypad is to be used due to high rigidity as well as low cost as compare to other keypads. As the password contains only numeric values a 4X4 keypad can be use to load the password into processor. It consists of 16 buttons arranged in the form of an array containing four lines and columns. [5]

4) RFID: The SMB130 is a 28 pin DIP module that includes all necessary components for a 13.56 MHz RFID, aside from a PCB antenna. The module communicates over UART or I2C with simple protocols. It also has 2 general purpose inputs and 2 general purpose outputs for switches, relays, etc. [6]

5) LCD Display: LCD Display generally used to display the messages for local user. It is a 16X2 characters display. [7]

6) DC motor & motor driver: The L293 and L293D are quadruple high-current half-H drivers. The L293 is designed to provide bidirectional drive currents of up to 1 A at voltages from 4.5 V to 36 V. The L293D is designed to provide bidirectional drive currents of up to 600-mA at voltages from 4.5 V to 36 V. Both devices are designed to drive inductive loads such as relays, solenoids, dc and bipolar stepping motors, as well as other high-current/high- voltage loads in positive-supply applications. [8]

7) GSM Modem: The GSM Modem can accept any GSM network operator SIM card and act just like a mobile phone with its own unique phone number. The GSM modem can use its RS232 port to communicate and develop embedded applications. Applications like SMS Control, data transfer, remote control and logging can be developed easily. The modem can either be connected to PC serial port directly or to any microcontroller. It can be used to send and receive SMS or make/receive voice calls. It can also be used in GPRS mode to connect to internet and do many applications for data logging and control. [9]

8)MAX232: MAX232 is from the family of MAX220– MAX249 line drivers/receivers is intended for all EIA/TIA-232E and V.28/V.24 communications interfaces, particularly applications where ±12V is not available. [10]

These parts are especially useful in battery-powered systems, since their low-power shutdown mode reduces power dissipation to less than 5µW. The MAX225, MAX233, MAX235, and MAX245/MAX246/MAX247 use no external components and are recommended for applications where printed circuit board space is critical.

B. Software Requirements

1. Keil µVision4

The LPC2148 microcontroller is supported by various commercially available IDEs for compiling and debugging of the code. Keil being one of them is the widely used IDE for LPC family of microcontrollers. The µVision4 IDE is Windows-based software development platforms that combines a robust editor, project manager, and make facility. µVision4 integrates all tools including the C compiler, macro assembler, linker/locator, and HEX file generator. [11]

2. Flash magic

The LPC series of microcontrollers are preloaded with the boot loader firmware which allows self programming of microcontrollers using serial port. Flash magic is a utility which provides an interface for reading, writing and verifying the flash memory of the microcontroller. Programming Language used is Embedded C.

C. Technologies Used

1) Radio Frequency Identification (RFID) System: The British pioneered RFID during World War II to identify the own aircraft returning from sorties over occupied Europe. Early radar system could spot an incoming aircraft but not distinguish it. But use of RFID could differentiate it with enemy aircrafts. [12]

In the late 1960s, the U.S. Government starts using RFID to tag and monitor nuclear and other hazardous materials. In 1977 Alamos Scientific Laboratories transferred its technology to the public sector, which encouraged number of companies to explore the new uses of RFID. [12] Although the foundation of the Radio Frequency Identification (RFID) technology was laid by past generations, only recent advances opened an expanding application range to its practical implementation.

RFID is only one of numerous technologies grouped under

the term Automatic Identification (Auto ID), such as bar code, magnetic inks, optical character recognition, voice recognition, touch memory, smart cards, biometrics etc. Auto ID technologies are a new way of controlling information and material flow, especially suitable for large production networks.

The Elements of an RFID System: RFID systems fundamentally consist of four elements: the RFID tags themselves, the RFID readers, the antennas and choice of radio characteristics, and the computer network (if any) that is used to connect the readers. Figure 4 shows the basic RFID system.

Fig. 4.

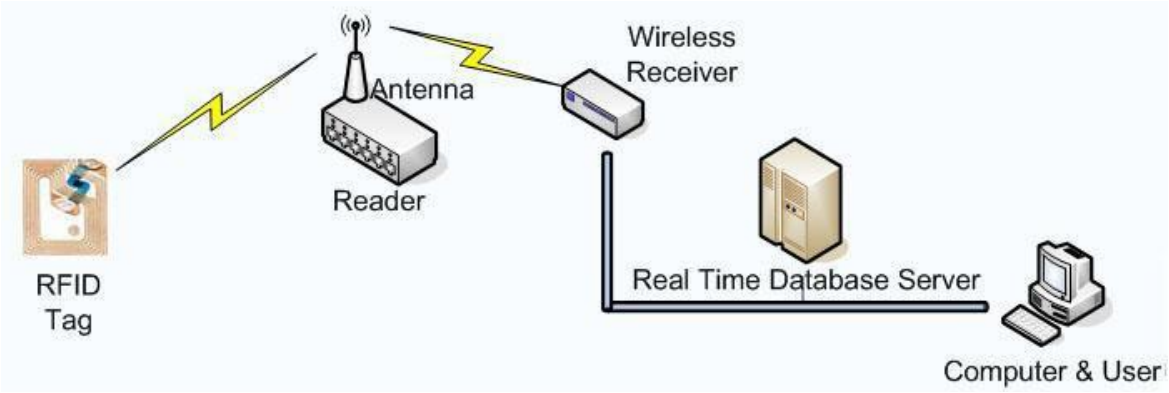

Fig. 4. RFID system

Tag: The tag is the basic building block of RFID. Each tag consists of an antenna and a small silicon chip that contains a radio receiver, a radio modulator for sending a response back to the reader, control logic, some amount of memory, and a power system. The power system can be completely powered by the incoming RF signal, in which case the tag is known as a *passive tag.* Alternatively, the tag's power system can have a battery, in which case the tag is known as an *active tag*. The primary advantages of active tags are their reading range and reliability. With the proper antenna on the reader and the tag, a 915MHz tag can be read from a distance of 100 feet or more.

Passive tags, on the other hand, can be much smaller and cheaper than active ones because they don't have batteries. Another advantage is their longer shelf life: Whereas an active tag's batteries may last only a few years, a passive tag could in principle be read many decades after the chip was manufactured.

Between the active and the passive tags are the *semi- passive* tags. These tags have a battery, like active tags, but still use the reader's power to transmit a message back to the RFID reader using a technique known as backscatter. These tags thus have the read reliability of an active tag but the read range of a passive tag. They also have a longer shelf life than a tag that is fully active.

Readers: The RFID reader sends a pulse of radio energy to the tag and listens for the tag's response. The tag detects this energy and sends back a response that contains the tag's serial number and possibly other information as well. In simple RFID systems, the reader's pulse of energy functioned as an on-off switch; in more sophisticated systems, the reader's RF signal can contain commands to the tag, instructions to read or write memory that the tag contains, and even passwords.

Historically, RFID readers were designed to read only a particular kind of tag, but so-called *multimode readers* that can read many different kinds of tags are becoming increasingly popular.

Like the tags themselves, RFID readers come in many sizes. The largest readers might consist of a desktop personal computer with a special card and multiple antennas connected to the card through shielded cable. Such a reader would typically have a network connection as well so that it could report tags that it reads to other computers. The smallest readers are the size of a postage stamp and are designed to be embedded in mobile telephones.

Antennas and Radio: The RFID physical layer consists of the actual radios and antennas used to couple the reader to the tag so that information can be transferred between the two.

Radio energy is measured by two fundamental characteristics: the *frequencies* at which it oscillates and the strength or *power* of those oscillations. Commercial FM broadcast stations in the United States transmit with energy at a frequency between 88MHz and 108MHz, or 1 million isolations per second. The AM spectrum, by contrast, transmits at 500,000 to 1,500,000 oscillations per second, or between 500 kHz and 1500 kHz. Microwave ovens cook with RF energy that vibrates 2.4 billion times each second, which is 2.4GHz.

Most RFID systems use the so-called *unlicensed spectrum*, which is a specific part of the spectrum set aside for use without a radio license. Popular bands are the low- frequency (LF) band at 125–134.2KHz, the high-frequency band at 13.56MHz, the ultrahigh-frequency (UHF) band at 915MHz (in North America; varies in other regions), and the industrial, scientific, and medical (ISM) band at 2.4GHz.

Advantages

Efficiency: RFID tags do not require line-of-sight to be deciphered. They can be read through cardboard, plastic, wood and even the human body. RFID tags can easily track moving objects and send the required information back to the reader. This eliminates human errors, reduces labor and provides quick access to a wealth of information.

Return on Investment (ROI): RFID costs more to implement than a barcode system, but provides a good return on investment in the long run, since RFID is significantly more efficient.

Less Susceptible to Damage: RFID tags are less susceptible to damage. An RFID tag is securely placed within an object or embedded in plastic, enabling the system to be used in a variety of harsh environments, such as areas of high temperature or moisture, or with exposure to chemicals or the outdoors.

D. GSM

The GSM system is a frequency and time division system in which each physical channel is characterized by a carrier frequency and a time slot number. GSM system frequencies include two bands at 900MHz and 1800MHz commonly referred to as GSM-900 DCS-1800 systems. [13]

GSM Architecture: The GSM technical specifications define the different elements within the GSM network architecture. It defines the different elements and the ways in which they interact to enable the overall network operation to be maintained. The architecture of GSM is shown in figure 5.

The GSM network architecture is now well established and with the other later cellular systems now established and other new ones being deployed, the basic GSM network architecture has been updated to interface to the network elements required by these systems. Despite the developments of the newer systems, the basic GSM network architecture has been maintained, and the elements described below perform the same functions as they did when the original GSM system was launched in the early 1990s.

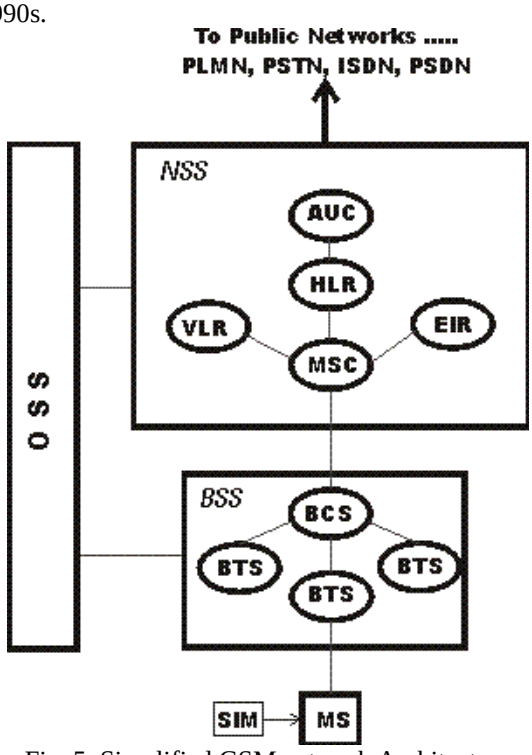

Fig. 5. Simplified GSM network Architecture

GSM network architecture elements: The GSM network architecture as defined in the GSM specifications can be grouped into four main areas, Mobile station (MS), Base-station subsystem (BSS), Network and Switching Subsystem (NSS), Operation and Support Subsystem (OSS)

Mobile station: Mobile stations (MS), mobile equipment (ME) or as they are most widely known, cell or mobile phones are the section of a GSM cellular network that the user sees and operates. In recent years their size has fallen dramatically while the level of functionality has greatly increased. A further advantage is that the time between charges has significantly increased. There are a number of elements to the cell phone, although the two main elements are the main hardware and the SIM.

The hardware itself contains the main elements of the mobile phone including the display, case, battery, and the electronics used to generate the signal, and process the data receiver and to be transmitted. It also contains a number known as the International Mobile Equipment Identity (IMEI). This is installed in the phone at manufacture and "cannot" be changed. It is accessed by the network during registration to check whether the equipment has been reported as stolen.

The SIM or Subscriber Identity Module contains the information that provides the identity of the user to the network. It contains are variety of information including a number known as the International Mobile Subscriber Identity (IMSI).

Base Station Subsystem (BSS): The Base Station Subsystem (BSS) section of the GSM network architecture that is fundamentally associated with communicating with the mobiles on the network. It consists of two elements.

Transceiver Station (BTS): The BTS used in a GSM network comprises the radio transmitter receivers, and their associated antennas that transmit and receive to directly communicate with the mobiles. The BTS is the defining element for each cell. The BTS communicates with the mobiles and the interface between the two is known as the Um interface with its associated protocols.

Base Station Controller (BSC): The BSC forms the nect stage back to the GSM network. It controls a group of BTSs, and is often co-located with one of the BTSs in its group. It manages the radio resources and controls items such as handover within the group of BTSs and allocates channels.

Network Switching Subsystem (NSS): The GSM network subsystem contains a variety of different elements, and is often termed the core network. It provides the main control and interfacing for the whole mobile network. The major elements within the core network include:

Mobile Switching services Centre (MSC): The MSC acts like a normal switching node within a PSTN or ISDN, but also provides additional functionality to enable the requirements of a mobile user to be supported.

Home Location Register (HLR): This database contains all the administrative information about each subscriber along with their last known location.

Visitor Location Register (VLR): This contains selected information from the HLR that enables the selected services for the individual subscriber to be provided. The VLR can be implemented as a separate entity, but it is commonly realized as an integral part of the MSC, rather than a separate entity.

Equipment Identity Register (EIR): The EIR is the entity that decides whether given mobile equipment may be allowed onto the network. Each mobile equipment has a unique number known as the International Mobile Equipment Identity. This number, as mentioned above, is installed in the equipment and is checked by the network during registration.

Authentication Centre (AuC): The AuC is a protected
database that contains the secret key also contained in the user's SIM card. It is used for authentication and for ciphering on the radio channel.

Gateway Mobile Switching Centre (GMSC): The GMSC is the point to which a ME terminating call is initially routed, without any knowledge of the MS's location.

SMS Gateway (SMS-G): The SMS-G or SMS gateway is the term that is used to collectively describe the two Short Message Services Gateways defined in the GSM standards. The two gateways handle messages directed in different directions. The SMS-GMSC (Short Message Service Gateway Mobile Switching Centre) is for short messages being sent to an ME.

Operation and Support Subsystem (OSS): The OSS or operation support subsystem is an element within the overall GSM network architecture that is connected to components of the NSS and the BSC. It is used to control and monitor the overall GSM network and it is also used to control the traffic load of the BSS. It must be noted that as the number of BS increases with the scaling of the subscriber population some of the maintenance tasks are transferred to the BTS, allowing savings in the cost of ownership of the system.

IV. WORKING OF PROPOSED SYSTEM

To open the box, RFID is needed to be swiped with a valid RFID tag at predefined date and time only. The RFID module will compare with EEPROM data such as RFID address, RTC date and time.

If the RFID address is wrong, then processor sends “ANAUTHENTIC USER” message to the university through a GSM modem and if anybody tries to open the box before the pre-defined date and time with a valid RFID tag also, then processor sends “OVERRULED” message to the university through GSM modem.

The box will be open only when swiped with a valid RFID tag at predefined date and time and processor sends “MAIN BOX OPENED” message to the university.

Then a password is sent from the university to the college to open the particular sub box which contains the question papers. If the person enters the wrong password, then processor sends “WRONG PASSWORD ENTERED” message to the university through GSM modem. If the person enters the correct password, then sub box is opened with the help of the motorized mechanism.

Both the sub box and box will then automatically closed after a delay of 10 minutes and 11 minutes respectively and processor sends “BOX CLOSED” message to the university through GSM modem.

After completion of the exam, the university sends “NEW PASSWORD” to exam centre. If the BOX is not closed along with answer papers within the specified time given by the university, then processor sends “OVERRULED” message to the university through GSM modem.

Light sensors are mounted inside a box which detects unauthorized tampering.

V. APPLICATIONS

This project is implemented to detect and prevent the leakage of question papers in various university and civil service exams.

It can be modified to protect some secret and confidential information papers related to our country.

VI. CONCLUSION

A cost effective system is proposed here which uses RFID, GSM and Real Time Synchronized clock. Examination section of university can deliver the question papers to the examination centers by password protected electronic security system. All these question papers will have next level security using RFID. Using GSM each activity involving opening and closing the box can be monitored in real time by university examination centre.

ACKNOWLEDGEMENT

We express our sincere gratitude towards the faculty member who have made this project a successful. We also thankful to our Principal Prof. S. V. Joshi for all support and guidance.

Special thanks to our Head of department, Prof. G. R. Phulay and our project guide Prof. A. S. Mane for his kind official support and encouragement, technical guidance throughout the project phase-1. We are also thankful to Prof. A. P. Gargade For his Valuable Guidance.

We would like to express our thanks to Prof. N. P. Futane, for his whole hearted co-operation and valuable suggestions.

Finally, we would like to thank all our staff members of Electronics and Telecommunication Department who helped us directly or indirectly to complete this work successfully.

It is our pleasure to acknowledge sense of gratitude to our group members for their support and encouragement in project work.

REFERENCES

[1] http://en.wikipedia.org/wiki/Test_(assessment)
[2] Arm System-On-Chip Architecture, 2/E by Ferber, Pearson Education India, 01-Sep-2001
[3] ARM System Developer's Guide: Designing and Optimizing System, by Andrew Sloss, Dominic Symes, Chris Wright,Morgan Kaufmann, 10-May-2004
[4] http://www.mikroe.com/downloads/get/1215/
[5] http://www.inmotion.pt/store/rfid-module-sm130-mifare-(13.56-mhz)
[6] www.vishay
[7] http://users.ece.utexas.edu/~valvano/Datasheets/L293d.pdf
[8] http://www.positronindia.in/datasheet/DS_PT0006.pdf
[9] http://www.maximintegrated.com/products/interface/transceivers/rs-232
[10] http://www.keil.com/
[11] Rfid: Applications, Security and Privacy, by Simon Garfinkel, Beth Rosenberg, Pearson Education India, 01-Sep-2006
[12] Principles and applications of GSM by Vijay Kumar Garg, Joseph E. Wilkes, Prentice Hall PTR, 1999
[13] http://www.ti.com/lit/ds/symlink/uln2003a.pdf

