International Journal of Engineering & Technology, 7 (4.36) (2018) 841-844

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

RFID Based Security for Exam Paper Leakage System

Mamilla Sirisha[1*], Neelam Syamala[2]

[1]PG Student, Department of Electronics and Communication Engineering, Marri Laxman Reddy Institute of Technology and Management, Hyderabad, India.
[2]Department of Electronics and Communication Engineering, Marri Laxman Reddy Institute of Technology and Management, Hyderabad, India.
E-mail:syamu35@gmail.com
**Corresponding author E-mail: srireddy1708@gmail.com*

Abstract

The examination may be the heart of the education framework. The principal reason for the examination will be to select the proficient applicants for several positions. Every year we get the news regarding postponed/canceled exam because of paper leakages. So we need come up with manageable and compact result and decided to design and execute an “examination paper leakage security framework “that will be a much-protected framework depend on “ARM processor”. Together with “the GSM modem, keypad, electromagnetic lock, and RFID module “would be utilized in this framework. First, the university will send the exam paper to the college in “an electronic sealed box”that is termed as “Electronic Control Box”. The “Electronic Control Box “will be an embedded framework, which might have been proposed utilizing “ARM processor” that has inbuilt RTC to display “the Electronic Control Box”. Whether anybody tries to open that box previous and afterward the time duration of the RFID swipe, the framework communicates to the university powers by sending “and SMS (Short Message Service)” through the GSM, which several malfunctioning has taken place with “the Electronic Control Box". For instance, whether the secret key doesn’t match then the client who has access to get the message on his telephone. If we enter the invalid secret ID then the ringer will be ON. Therefore we might effectively recognize that the question papers have been leaked.

This paper defines the electronic security for the leakage of question paper that will be an exceptionally protected framework. The examination will be the heart of “the education framework”. We have recommended an electronic framework to identify and avoid the leakage of exam papers. In this proposed system, the exam papers that are in “the electronically locked box” will be sent to the examination centers. The box will be unlocked after a predefined time, date and only by a certified client. Essentially the exam papers will be existing in the sub-boxes. Secret ID secures these boxes; the exam manager will send an SMS with the password to open the specific sub-boxes. The electromagnetic lock is used to unlock the box, when the time, date, and password match. In this framework, we are utilizing a ringer for any unapproved interference.

Key word: Security, Leakage System, RFID

1. Introduction

In society, the education will be the inspiring strength. The calculation of an examination is used to estimate “the knowledge, physical fitness or aptitude, skill, and classification” in numerous subjects. To estimate the set of skills they are conducting an exam may be on paper, in exam centers, on the computers. Also, the principal reason for the examination will be to select the proficient applicants for several positions [1], [2].

Fundamental issues of students are “exam paper leakage”, who endures from the cancellation or postponed of the exam. Every year we gather news something like postponed/ canceled exam because of paper leakages in the daily paper or on TV. Sometimes the university itself does not recognize how there will be spillage of the data related to exam papers. Therefore, some candidates won't get the rank that put maximum efforts and hard work, and some candidates get the good rank in less time and minimum effort. This perspective will make a negative impact on students and discourage the society’s development. Thus we have come up with a convenient and portable result and decided to execute “an examination paper leakage security framework” depend on “ARM processor” [6]. Together with “the ARM processor (LPC2148), keypad, GSM modem, LCD, RFID module, and the electromagnetic lock” would be utilized in this framework [3].

First, the university will send the exam paper to the college in "an electronic sealed box” that will be termed as “Electronic Control Box”. This “electronic control box” is an embedded framework, which might have been proposed utilizing “the ARM processor” that has inherent RTC to observe “the electronic control box”. Whether anybody attempts to unlock the box previous and afterwards the time duration of the RFID swipe [1], [4], the framework communicates to the university powers by sending “a SMS (Short Message Service)” through “Global system for mobile communication (GSM)”, which several malfunctioning has taken place with “the Electronic Control Box".

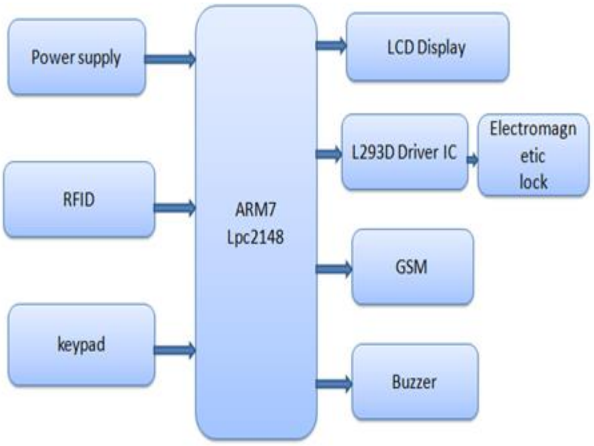


Figure 1: System block diagram

The university management will send a distinctive secret key to the main authority of the college before 10 minutes of the examination. The university provides legal “RFID card with a fake RFID card “to the main authority of the college. The certified person swipes the card [5], if the card is legal, then the framework recognizes for the secret ID. The chief examiner wants to type the secret ID with the use of a keyboard, which is given by the university. Whether secret ID is true, the electromagnetic lock rotates and opens “the Electronic Control Box”. This framework has 2 transceivers, (a) the transceiver 1 is an embedded framework connected to “the electronic control box”. (b) The transceiver 2 will be the mobile with the university powers. The current module deals with the software and hardware.

1.1. Problem definition

In this framework, we would utilize the initial level of security that is an RFID card with a specific or distinctive amount [6], [9], which may be given by the university to each college. “Global system for mobile communication” will be utilized for any unapproved client altering, whether any unapproved clients attempt to unlock the box, then instantly a message will go to the “university management” through the “Global system for mobile communication”. The keypad is the “second level security” in this framework for time, date and secret key matching.

2. Related research

Today the framework that will be in use includes the practice surveyed from many years. This system contains "the sealed boxes “comprising the exam papers that will be dispersed to the examination centers. This framework includes a lot of restrictions that might lead to exam papers leakage at different instances same time the box is moved from “printing area to examination centers”. This happens because of not difficult tampering of sealed boxes and more interference of people.

Another technique that is in use today includes the mailing of the exam papers from the university to particular college’s former to examination. The colleges take the Xerox of the exam paper and then the examination methodology follows. Significantly this specific strategy also includes lots of limitations. The sever interruption might occur, the website might have a chance to be hacked, and more than 100 colleges must take Xerox that includes the threats such as framework failure, energy failure, and the paper leakage.

The knowledge for the suggested framework that includes the electronic security may be determined from current equipment such as “Electronic lockers, automated teller machine (ATM), and other security improved electronic frameworks”. This framework includes the incorporation of specific electronic peripherals that operates on the methodologies depend on GSM, UART, RFID, and I2C [7], [8].

3. System implementation

3.1. RFID reader module

The “Radio-frequency identification (RFID)” utilizes “the electromagnetic fields” to automatically recognize and track tags connected to objects. The “electronically stored data" is held by the use of tags. An “active tags” have a “local power source (like a battery)” and might work hundreds of meters from “the RFID reader”. The “passive tags” gather energy from a close-by “RFID reader's interrogating radio waves”. Dissimilar a barcode, the tag does not need within sight line of the reader. Thus it might be embedded in “the tracked object”. The “Radio-frequency identification (RFID)” [9] is one strategy for“AIDC (Automatic Identification and Data Capture)”. Figure 2 describes the RFID Reader:

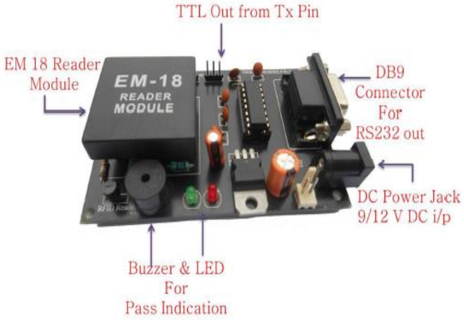


Figure 2: RFID reader

3.2.GSM module

The “European Telecommunications standards institute (ETSI)” is used to develop the “Global system for mobile communication (GSM)” to define the protocols for “second-generation digital cellular networks” is shown in Figure 2.1. 2G networks established for the replacement of "first generation analog cellular networks”, and “the GSM standard” initially portrayed as a digital, “circuit-switched network” improved for “full duplex voice telephony”. This extended time to incorporate information communications initially through “circuit-switched transport”, after that through “packet information transport via GPRS (General Packet Radio Services)” and “EDGE (Enhanced Data Rates for GSM Evolution, or EGPRS)”. Accordingly, the 3GPP recognized as “third-generation (3G) UMTS standards”, followed by “Fourth-generation (4G) LTE advanced standards” that does not portion of “the ETSI-GSM standard”. GSM association is used to possess the trademark of GSM. It might also mention initially to the regular voice codec utilized, “full rate”.

Figure 2.1: GSM module

3.3. Electromagnetic lock

An “electromagnetic lock” is a locking gadget (described in Figure 2.2), which comprises of “an armature plate and an electromagnet”. There are 2 primary kinds of “electric locking gadgets”. Locking gadgets might be either "fail-safe" or "fail secure". The fail-safe locking gadgets are opened when de-energized. A “fail-secure locking gadget” is remains locked when the power will be lost. The “typical single door electromagnetic locks” [10] are provided in both “dynamic holding force capacities” such as “600 lbs. (272 kg) and 1200 lbs. (544 kg)". Nowadays, the quality of "magnetic locks" compares greatly with that of “conventional door locks” and the magnetic locks price is less than “conventional light bulbs” to work.

Figure 2.2: Electromagnetic lock

3.4. Working operation

a. The kit is first switched ON by giving the power supply.
b. The LCD gives a welcome message. The kit should be reset for proper functioning.
c. A card is to be shown at the RFID reader which reads the information encoded in the card.
d. The prompt asks to enter a mobile number to which the OTP has to be sent.
e. The prompt asks to show the card. If the card is valid, then it sends an OTP the given mobile number. Otherwise, a message is sent to the number that an unauthorized action has been taken place.
f. The OTP needs to be entered by using the keypad.
g. If the OTP entered is correct, the lock gets opened. Otherwise, a message is sent to the authorities about the unauthorized access.

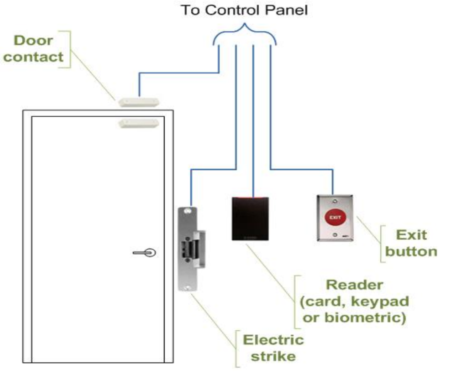


Figure 2.3: Working condition of electronic magnetic lock

3.5. Flow chart

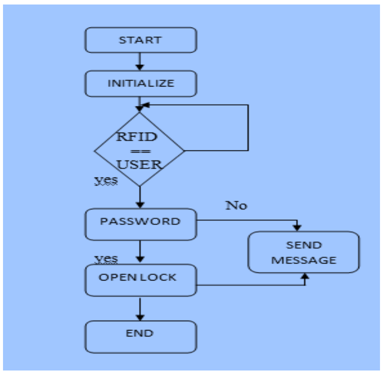


Figure 2.4: Systems design flow chart

4. Hard ware result

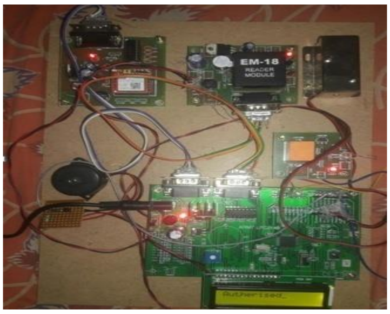
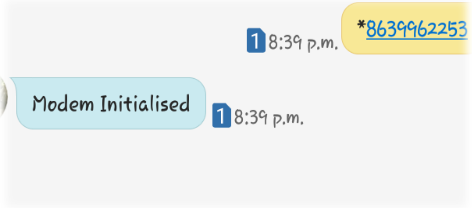


Figure 4: System hardware description

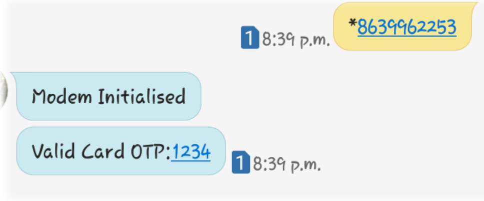
Figure 4 describes "the exam paper leakage security framework”. The “vibration sensor” will be associated to the “microcontroller port pin”. The “GSM module” will be linked to the port pin of transmitter pin of the microcontroller and the “receiver pin” is linked to “the RFID reader module”. The “matrix keyboard” will be linked to complete 8-bit port, when it gets the vibrations before the time, then it is linked to the ground i.e.“active low”. And “the controller programming” is used to examine the information from the inbuilt mobile number and sent the SMS that is at command design.



1 8:39 p.m. *8639962253

Modem Initialised 1 8:39 p.m.

Figure 4.1: Device initialize with GSM module

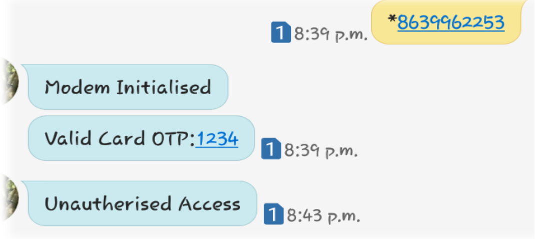


1 8:39 p.m. *8639962253

Modem Initialised

Valid Card OTP:1234 1 8:39 p.m.

Figure 4.2: Authorized person access then OTP Sent to mobile



1 8:39 p.m. *8639962253

Modem Initialised

Valid Card OTP:1234 1 8:39 p.m.

Unautherised Access 1 8:43 p.m.

Figure 4.3: If entered the wrong password it gives unauthorized Access

Applications

i. This project can be extended to protect the answer sheets to send it to the university authorities.
ii. It can also be used in various other applications where protection of documents or any valuables is needed.
iii. Used in banks for security purposes.

5. Conclusion

The Design and its implementation of ARM processor-based electronics protection for the exam paper leakage system were effectively carried out with the advantages of minimum peripheral interfaces, low power consumption, low cost, high portability. The response of the system is successfully tested in all the conditions of the system that is mentioned in the system functionality.

The compact and cost-effective solution for the examination paper leakage system was achieved with the ARM processor controller. This project can be extended to protect the answer sheets to send it to the university authorities. It can also be used in various other applications where protection of documents or any valuables is needed. The embedded system can be programmed to close the Electronic Control Box after the completion of the exam

References

[1] Tejuswi Y, "RFID based access card for public enrollment and distribution: a research survey", *IEEE Journal on selected areas in communication*, Vol.2, No.9, (2013).

[2] Mouli CC, "Embedded System Based Exhaust Fan Control", *Lab Experiments–A Journal of Laboratory Experiments*, Vol.11, No.3, (2011), pp.200-201.

[3] Nalajala P, "Provide Safety in School Children's Vehicle in Urban Environments using Navigation system", *International Journal of Applied Engineering Research*, Vol.12, No.13, (2017), pp.3850-3856.

[4] Nagaraja C, Chandra Mouli C, Athavulla S & Bheemalingaiah T, "A Microcontroller Based Programmable Power Supply, Lab Experiments", *A Journal of Laboratory Experiments*, Vol.10, No.4, (2010), pp.249-253.

[5] Wankhade PP & Dahad SO, "Real time vehicle locking and tracking system using GSM and GPS technology-an anti-theft system", *International Journal of Technology and Engineering System (IJTES)*, Vol.2, No.3. (2011), pp.272-275.

[6] Godavarthi B & Papa RN, "Wireless Sensors Based Data Acquisition System using Smart Mobile Application Internet of things", *International Journal of Advanced Trends in Computer Science and Engineering*, Vol.5, No.1, (2016), pp.25-29.

[7] Godavarthi B, Nalajala P & Ganapuram V, "Design and implementation of vehicle navigation system in urban environments using internet of things (IoT)", *IOP Conference Series: Materials Science and Engineering*, Vol.225, No.1, (2017).

[8] Rao NP, Bhavana G & Teja MLR, "RTOS Based Image Recognition & Location Finder Using GPS, GSM and OpenCV", *International Advanced Research Journal in Science, Engineering and Technology*, Vol.2, No.12, (2015), pp.85-88.

[9] Bhavana G, Mohammad K, Paparao N, "Biomedical sensor based remote monitoring system field of medical and health care", *Journal of Advanced research in dynamical and control systems*, Vol.9, No.4, (2014), pp.210-219.

[10] Paparao N, Ponna M & Bhavana G, "RFID Based Security for Exam Paper Leakage using Electromagnetic Lock System", *International Journal of Pure and Applied Mathematics*, Vol.117, No.20, (2017), pp.845-852.