



E-ISSN: 2707-6628
P-ISSN: 2707-661X
www.computersciencejournals.com/ijcit
IJCIT 2025; 6(1): 125-128
Received: 22-02-2025
Accepted: 25-03-2025

G Sai Ram

Assistant Professor,
Department of ECE,
Siddhartha Institute of
Engineering and Technology,
Ibrahimpatnam, Telangana,
India

P Meghana

Student, Department of ECE,
Siddhartha Institute of
Engineering and Technology,
Ibrahimpatnam, Telangana,
India

P Nandini

Student, Department of ECE,
Siddhartha Institute of
Engineering and Technology,
Ibrahimpatnam, Telangana,
India

V Mahanthi

Student, Department of ECE,
Siddhartha Institute of
Engineering and Technology,
Ibrahimpatnam, Telangana,
India

Corresponding Author:

G Sai Ram

Assistant Professor,
Department of ECE,
Siddhartha Institute of
Engineering and Technology,
Ibrahimpatnam, Telangana,
India

Finger based protection system to avoid exam paper leakage

G Sai Ram, P Meghana, P Nandini and V Mahanthi

DOI: <https://www.doi.org/10.33545/2707661X.2025.v6.i1b.125>

Abstract

The need for robust security mechanisms to prevent exam paper leakage has become paramount due to the increasing incidence of unauthorized access and breaches in educational institutions. Traditional methods, such as physical locks and manual surveillance, have proven inadequate in safeguarding sensitive examination materials. This project proposes a Fingerprint-Based Protection System designed to mitigate these security challenges. The system employs two fingerprint sensors for dual authentication, enhancing security by ensuring only authorized personnel can access exam papers. Additionally, a 3x4 keypad is used for PIN verification, providing an extra layer of security. The Arduino micro controller processes input from the fingerprint sensors and keypad, controlling the physical lock mechanism through a motor driver and DC motor. An LCD display offers real-time status updates, while a GSM module sends OTP to authorized person. By automating security processes, this project aims to reduce human error and provide a reliable, efficient, and secure solution to protect exam papers from leakage.

Keywords: Fingerprint protection system, exam paper security, unauthorized access prevention

Introduction

Internet of Things (IoT) is a combination of digital-machines, computing devices, mechanical machines, objects with UID's and ability to transmit the information over a network without interference of human to human or human to computer interaction [1-2]. There are many other contribution factors which paved the way for this rapid development say embedded systems, control systems, building automation, home automation and wireless sensor networks [3]. There are various layers in IoT. They are Sensing Layer, Network Layer, Data processing layer, Application layer [4]. Radio frequency (RF) refers to the oscillation rate of electromagnetic radio waves between 3 GHz and 300 GHz and alternating radio signaling currents, the frequency band used for communication and broadcasting. It is a process of transmitting a data or power between multiple points that are connected by an electrical device. RFID is the use of radio frequency waves for transmitting data. RFID is a wireless non-contact wave. Tagging items with RFID tags enables users to identify inventory and assets automatically and uniquely RFID is a radio frequency-operated system which is used to auto-identify for the different items. The key components of the RFID system are two. There was an error. Whether the item with the RFID tag is beyond the range of this radio waves, otherwise this RFID reader would be returned with input. There's no control in passive RFID tags and RFID readers/antennas are powered by the RF Frequency Power. The readers and the antenna transmit the signal to control the tag and mirror the reader's energy back. Biography is a means of calculating the physical assets of a individual in order to test their identification. This may involve fingerprints and eyes or behavioural attributes such as a simple method of complementing the protection authentication puzzle. A biometric sensor is a transducer that transforms an individual in an electrical signal into a biometric test. Biometric therapies include primarily biometric fingerprinting, iris, ears, speech and so on. In general, light, temperatures, speed, electrical capacity and other energies are read or measured in the sensor. The biggest concerns for the students involve the loss of question articles, which include the test being postponed or cancelled. We read about the postponement/cancellation of the exam every year in the newspaper or on the television because of papers leaks. Even the institution itself does not realize whether knowledge on question papers is published. So, in less time and with minimum effort, some students get a decent rank and those who really merit the rank do not even get the limit despite hard

working. This will adversely affect students and demoralize society's development. The major crisis goes over the world is exam paper leakage due to manhandle of the question paper. It can leak over any parries or different organization. Existing system are proposed GPS, GSM and wireless sensor based tracking system. In arm-based controller is proposed consisting of electromagnetic lock and also gives a valid OTP to the persons or users. This will monitor the question paper box and alert in stipulated timing. Active RFID tags are used in order to explore the indoor location of an object in. In order to overcome the various flaws, combination of biometric and RFID authentication systems-based storage box is proposed in this paper. Inside this implemented box we are keeping our question paper with a noted way. With a solid fingerprint and respected RFID the box can be open by proposing we can achieve our problem statement positively. In this paper, biometric and RFID based authentication system based on IoT. This system consists the modules are Fingerprint sensor, RFID reader, buzzer, LCD, Piezo electric plate, motor. All of these modules are connected and controlled by Node MCU. The rest of the paper is organized as follows: System implementation is discussed in section 2. In section 3 discussed the results of system. The conclusion is given in the last section.

Literature Survey

A Finger print Based Protection System to avoid Exam paper Leakage.

Effective ways to use Internet of Things in the field of medical and smart health care

The recent advancements in technology and the availability of the Internet make it possible to connect various devices that can communicate with each other and share data. The Internet of Things (IoT) is a new concept that allows users to connect various sensors and smart devices to collect real-time data from the environment. However, it has been observed that a comprehensive platform is still missing in the e-Health and m-Health architectures to use smartphone sensors to sense and transmit important data related to a patient's health. In this paper, our contribution is twofold. Firstly, we critically evaluate the existing literature, which discusses the effective ways to deploy IoT in the field of medical and smart health care. Secondly, we propose a new semantic model for patients' e-Health. The proposed model named as 'k-Healthcare' makes use of 4 layers; the sensor layer, the network layer, the Internet layer and the services layer. All layers cooperate with each other effectively and efficiently to provide a platform for accessing patients' health data using smart phones.

Test event generation for a fall-detection IoT system

The Internet of Things (IoT) is a popular paradigm which has been applied to different areas, such as smart cities, medicine, or business processes. One of the main drawbacks of an IoT system is the amount of information it has to manage and to monitor. This information arrives as events that need to be processed in real-time in order to make correct decisions. The event processing languages (EPLs) were designed to handle this information by defining event patterns which describe relevant situations to be detected and filter the information. In the majority of the relevant situations to detect, the events have a specific behaviour which must be analysed not only to define the event patterns but also to simulate them to test the IoT system. Moreover, in several situations it is quite difficult to obtain test events

with specific values: adverse environment conditions, rise or fall in blood pressure, heart attack, falls, among others. In this paper, we introduce a complete study of falls as relevant situations; we show an analysis of the fall-involved events of two types of falls based on an IoT prototype, the event patterns to detect the falls and their test using the IoT-test event generator (IoT-TEG) tool. The fall analysis has highlighted the necessity to improve IoT-TEG with a new functionality which allows defining the desired conduct by defining behaviour rules.

IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices

The Internet of Things (IoT) is rapidly spreading, reaching a multitude of different domains, including personal health care, environmental monitoring, home automation, smart mobility, and Industry 4.0. As a consequence, more and more IoT devices are being deployed in a variety of public and private environments, progressively becoming common objects of everyday life. It is hence apparent that, in such a scenario, cybersecurity becomes critical to avoid threats like leakage of sensible information, denial of service (DoS) attacks, unauthorized network access, and so on. Unfortunately, many low-end IoT commercial products do not usually support strong security mechanisms, and can hence be target of-or even means for-a number of security attacks. The aim of this article is to provide a broad overview of the security risks in the IoT sector and to discuss some possible counteractions. To this end, after a general introduction to security in the IoT domain, we discuss the specific security mechanisms adopted by the most popular IoT communication protocols. Then, we report and analyse some of the attacks against real IoT devices reported in the literature, in order to point out the current security weaknesses of commercial IoT solutions and remark the importance of considering security as an integral part in the design of IoT systems. We conclude this article with a reasoned comparison of the considered IoT technologies with respect to a set of qualifying security attributes, namely integrity, anonymity, confidentiality, privacy, access control, authentication, authorization, resilience, self- organization.

FID based security for exam paper leakage using electromagnetic lock system

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/cancelled 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".

Landmarc: Indoor location sensing using active RFID

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".

RFID technology and its applications in Internet of Things (IoT)

Radio frequency identification system (RFID) is an automatic technology and aids machines or computers to identify objects, record metadata or control individual target through radio waves. Connecting RFID reader to the terminal of Internet, the readers can identify, track and monitor the objects attached with tags globally, automatically, and in real time, if needed. This is the so-called Internet of Things (IoT). RFID is often seen as a prerequisite for the IoT. This paper introduces the technologies of RFID and IoT, discusses the applications and challenges of RFID technology used in IoT.

Related Methodologies

This section uses established procedures to conduct a thorough analysis.

Embedded Systems Design Methodology

This methodology involves designing a system that integrates hardware and software to perform dedicated tasks. In the proposed project, an Arduino Uno micro controller acts as the core embedded platform that coordinates the input and output devices such as the Fingerprint Sensor, Keypad, GSM, LCD, and Drive motor. The design ensures the system is allowing only authorized persons to access or print exam paper using Fingerprint authentication.

User Enrollment

Biometric Data Collection: Authorized personnel (e.g., exam coordinators, invigilators, printers) are enrolled into the system by capturing their fingerprint data.

- **Secure Storage:** Fingerprints are encrypted and stored in a secure, centralized biometric database accessible only to the exam management system.

Biometric Access Control for File Decryption

Exam papers are stored in an encrypted format. Only authorized personnel can decrypt and open the file after fingerprint verification. Used on secure desktops or devices handling sensitive content.

Secure Printing with Biometric Verification

Printers are equipped with fingerprint modules. Print jobs are held in queue until the authorized user scans their fingerprint. Prevents unauthorized printing or theft of printed papers.

Embedded Locker System for Physical Storage

Physical lockers containing printed exam papers are locked electronically. Only accessible via fingerprint

authentication. Ideal for secure storage before exam distribution.

Biometric USB or Drive Access

USB drives containing exam papers are locked with fingerprint authentication. Data becomes accessible only after matching the fingerprint on an integrated sensor. Adds security for paper transport between locations.

Centralized Biometric Server Authentication

Exam centers authenticate personnel remotely using a central biometric server. Access is granted only after biometric approval from a verified database. Suitable for institutions with multiple campuses.

Results and Discussion

This section gives the detailed results analysis of various methods. The simulations of various methodologies are conducted using the same environment. Here, Arduino IDE software tool was used to implement the methodologies.

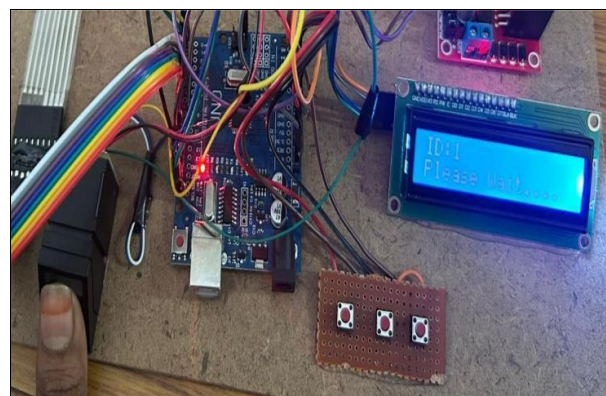


Fig 1: Scanning the Persons Finger Print



Fig 2: Authorised



Fig 3: Accessed the Fingerprint



Fig 4: Finger placed



Fig 4: Enter OTP



Fig 5: OTP Accepted

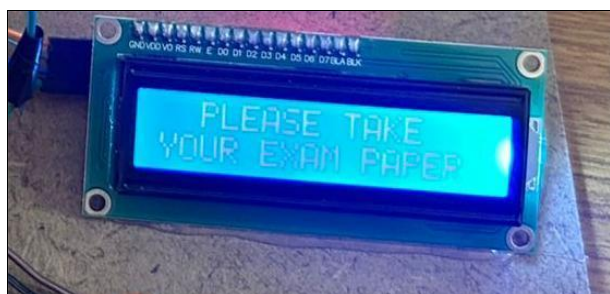


Fig 6: Downloaded the Exam paper

Conclusion

The Fingerprint-Based Protection System for preventing exam paper leakage offers a robust and reliable solution to the security challenges faced by educational institutions. By integrating dual fingerprint sensors and a PIN verification mechanism, the system ensures that only authorized personnel can access sensitive examination materials. The use of an Arduino micro controller to manage the security components, along with an LCD display and GSM module for real-time updates and OTP verification, further enhances the system's effectiveness. By automating the security

processes, this project minimizes human error and provides an efficient, secure method to protect exam papers from unauthorized access and leakage. This innovative approach significantly contributes to maintaining the integrity and confidentiality of examination processes.

References

1. Gaikwad S, Kenjale N, Bagade A, Shiragapur B. Electronic protection for exam paper leakage. UG Scholar.
2. Nagaraja C, Chandra Mouli C, Athavulla S, Bheema Lingaiah T. A microcontroller based programmable power supply. Lab Experiments - A Journal of Laboratory Experiments. 2010 Dec;10(4):249-253.
3. Chandra Mouli C, Ramnath V, Sailaja D, Nagabhushan Raju K. Embedded system based exhaust fan control. Lab Experiments - A Journal of Laboratory Experiments. 2011 Sep;11(3):200-201.
4. Tejaswi Y. RFID based access card for public enrolment and distribution: a research survey. IEEE J Sel Areas Commun. 2013 Sep;2.
5. Garfinkel S, Rosenberg B. RFID: applications, security and privacy. Pearson Education India.