

Advanced Electronic Protection System to Detect Exam Paper Leakages using Biometric

J.Manga¹, M.Sushmitha², T.Ashwini³ and T.Laharika⁴

¹Assistant Professor/Vignana Bharathi Institute of Technology/Electronics and Communication Engineering, Ghatkesar, Telangana, India

Email: manga.jangidi@vbithyd.ac.in

²⁻⁴ Students/Vignana Bharathi Institute of Technology/ Electronics and Communication Engineering, Ghatkesar, Telangana, India

Email: sushmithamajjiga4005@gmail.com, ashwinithelusuri@gmail.com, laharikatamma1@gmail.com

Abstract— This research study suggests a sophisticated electronic protection solution that uses biometric authentication to reduce the possibility of exam paper leaks. Academic integrity is facing serious issues due to the growing vulnerability of traditional ways of securing examination papers to breaches, which are caused by the expansion of digital technology. Using biometric authentication provides a reliable way to verify the identity of authorized workers and keep private exam materials out of the hands of unauthorized individuals. To provide a multi-layered security strategy, the system incorporates multiple biometric modalities, including fingerprint, iris, and facial recognition. Furthermore, sophisticated encryption techniques are used to protect data storage and transfer. In addition to strengthening exam paper security, the suggested approach expedites administrative procedures, increasing productivity and lowering the possibility of human error. The design, implementation, and evaluation of the suggested system are covered in this work, with an emphasis on how well it detects and stops exam paper leaks while preserving user comfort and system scalability. A buzzer alarm and a message to the university are sent in the event that an unauthorized attempt to access the documents is discovered, alerting the appropriate authorities.

Index Terms— Biometric Authentication, Scalability, Unauthorized, Encryption, Recognition, Integrity

I. INTRODUCTION

The vast availability of digital technology in the current day presents unprecedented difficulties to the integrity of academic assessments. Examinee leaks jeopardize the validity and impartiality of evaluations, making them one of the biggest challenges to academic integrity. More complex protection mechanisms must be developed since conventional exam paper security measures like physical storage and human distribution are becoming more and more vulnerable to security breaches. This study presents a state-of-the-art electronic protection system that uses biometric authentication techniques to detect and stop exam paper leaks. Biometrics provides a very safe way to confirm people's identities by measuring and analyzing distinctive behavioral or physical traits.

Unauthorized access can be successfully controlled and sensitive materials can only be accessed by authorized individuals by integrating biometric authentication into the examination paper distribution procedure. The main goal of this research is to provide a complete solution that improves administrative process efficiency and lowers

the possibility of human error while simultaneously strengthening examination paper security. With the use of cutting-edge digital technologies like biometric authentication and encryption algorithms, the suggested solution seeks to balance user ease and scalability with a strong defense against exam paper leaks. The introductory section of this paper establishes the framework for the subsequent sections, which will examine the current obstacles related to exam paper security, examine pertinent literature on biometric authentication methods, and showcase the architecture, implementation specifics, and security protocols of the suggested system.

II. LITERATURE REVIEW

Exam paper leaks are a serious threat to the validity of academic evaluations, hence strong security measures are required to stop unwanted access and the sharing of private information. We look at current practices and research on exam paper security and biometric authentication methods in this overview of the literature.

Exam Paper Leaks: Unauthorized access to, distribution of, or publication of examination materials prior to, during, or following the examination period is referred to as exam paper leakage. These kinds of things can provide certain people undue advantages, which undermines the validity and impartiality of evaluations. Exam paper distribution via manual processes and physical storage is becoming less and less effective in the face of cyberattacks.

Techniques for Biometric Authentication: By confirming people's identities through distinctive physiological or behavioral traits, biometric authentication is a possible way to improve exam paper security. Biometric modalities that are often used include voice, facial, iris, and fingerprint recognition. These methods offer a high degree of security and precision since biometric characteristics are hard to falsify or duplicate. Integration of Biometric Authentication with Exam Paper Security: The incorporation of biometric authentication with exam paper security systems has been the subject of several investigations. For instance, scientists have created software programs that verify users using fingerprint recognition before allowing them access to test items. Multimodal biometric systems, which combine several biometric modalities for increased security, have been the subject of investigation in several studies.

Future Directions: Although there are obstacles to overcome, integrating biometric authentication with security systems for exam papers has enormous potential to improve the accuracy and consistency of academic assessments. The creation of more reliable biometric algorithms, the investigation of novel biometric modalities, and the integration of biometric authentication with other security technologies, such blockchain, are possible future research directions.

EXISTING METHOD	PROPOSED METHOD
Certain electronic peripherals that rely on GSM, UART, RFID, and I2C for operation are incorporated into this framework.	ARDUINO UNO where input, output keypad are connected. Relay and voltage pins where if both are ON motor gets on if not OFF.
Narrowband Time Division Multiple Access (TDMA) is the technology that GSM uses to provide voice and content-based services via cellular networks.	12V adapter connected to 12V adapter to give DC current. 16*2 display used to display messages. Push buttons acting as keypad.
It is more difficult to open a box using an RFID card as a passkey than it is to offer someone else a pin.	DC moto used to open/close the lock so we use Driver board.
With the use of GSM technology, an RFID-based access control system restricts locker access to approved individuals exclusively.	R307 fingerprint module is serial communication device so data get serially passed.
An RFID system basically comprises of a transceiver, a transponder that has been programmed with unique information, and an antenna or coil.	RFID EM-18 Reader reads 12 Digit card with magnetic field and send to controller it checks with code and see valid /not valid.

III. SYSTEM IMPLEMENTATION

A. NODEMCU

A microcontroller may access many networks with the help of an ESP8266. An application from a different application processor can be hosted by this module.



B. RFID READER

Radio waves are used by radio frequency detection (RFID) to track and trace the items that require constant monitoring. RFID operates on the electromagnetic field concept. In addition to producing data, tags also produce radio waves. Therefore, data of some kind are also sent to the RFID reader.



C. FINGERPRINT SENSOR

A fingerprint sensor, sometimes referred to as a fingerprint reader or scanner, is a type of biometric equipment used for identification and authentication that records and examines fingerprint patterns.



D. LCD

An LCD is a type of liquid crystal display module that uses liquid crystal to create sharp images.



E. DC MOTOR

Electric energy is transformed into mechanical energy by a motor. The motor in this system rotates in two directions: one direction is forward, and the other is backward.



F. WIRELESS TRANSCEIVER

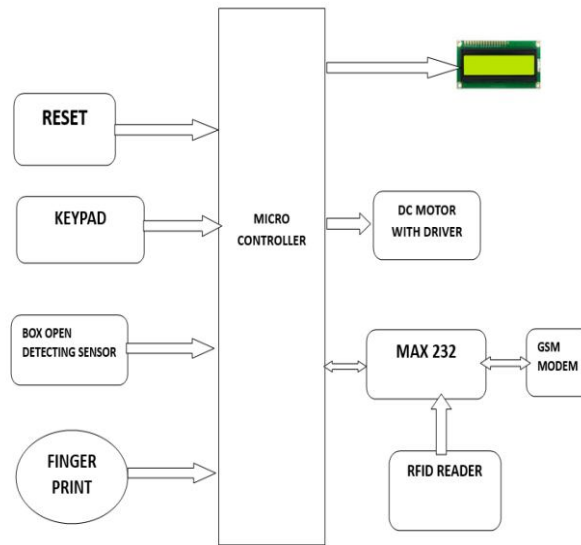
A tiny electrical device called an RF transceiver module is often where radio signals are transmitted between the two devices.

G. GSM MODEM

The GSM (Global System for Mobile Communications) network can communicate with a computer or other electronic device through the use of a GSM modem. By acting as a link between digital gadgets and the cellular network, it enables data transfer using accepted GSM protocols.



IV. BLOCK DIAGRAM



IV. WORKING

1. Connect 12V power supply to the base board.
2. The 16*2 LCD displays a message as "SEND MESSAGE".
3. To register the mobile number enter *UR MOBILE NUMBER
4. Then after registering you get messages to your registered number.
5. Therefore, authorization or appropriate authentication from a sensor is needed in order to add or modify a fingerprint in the sensor .A fresh fingerprint cannot be fused to the database unless top authorities has given their clearance.
6. After registering the mobile number the LCD Display as PUT FINGER.
7. Here is where the user scans in this instance. The user is notified via LCD to disclose their fingerprint. If it matches, the LCD forwards the information to the following iteration and indicates an acknowledgement as "AUTHORISED ID." A beep is followed by the message "UNAUTHORISED ID" when an invalid LCD is detected.
8. A user's fingerprint is asked in this second round of authentication, which follows the processing of an approved ID. The coffer box's motor mechanism can open if this authentication matches as well. If not, the LCD will indicate "UNAUTHORIZED ACCESS," emit a buzzer, and send a message alert to higher officials stating "UNAUTHORIZED ACCESS THE BOX."
9. Then later take the 2 valid cards and scan through it. You get valid if card is matched correctly.
10. After the card is valid the LCD shows ENTER OTP.
11. Put in the legitimate OTP. The lock is released if the OTP is legitimate. The notification "LOCK OPEN" appears.
12. Since every step listed above is being watched over remotely, a data connection interface is required for the live monitoring system.
13. A buzzer sound and the phrase "wrong OTP or wrong user" are heard if the card or fingerprint are incorrect.

V. RESULTS

The 12V is supplied to base board then we get input as 12v . Before regulating voltage it goes to motor and GSM then after regulating it voltage goes to the base board. The cards we use of 12 digit read the RFID by magnetic field and send the data to the controller. The controller will match with the code and checks as valid or invalid. If both (fingerprint and card) gets valid it asks for a OTP to be enter .If the OTP is correct the lock gets open and send the message to the registered mobile number .If any wrong attempt has happened message is send to the registered mobile number and we get a buzzer .



V. CONCLUSIONS

In order to prevent question paper spills, a Node MCU-based prototype in electronic security is accomplished with low design costs, low power consumption, few yard interfaces, and great mobility. As a result, the system response is verified at every point that the system operation specifies. This suggested approach may be used in a variety of industries, including education, where it is considered violent to disclose any kind of data or information. The coffer box or electronic box can be closed after the layout selection design is finished.

REFERENCES

- [1] Nawsheen Promy, Tashfiq Rahman, Sadman Islam, and Saqlain Mahmud Khan, "Automated smart box to alleviate unfair means in public examination"-2020.
- [2] Mamilla Sirisha, Neelam Syamala "RFID Based Security for Exam Paper Leakage System"-2019.
- [3] Kimia Tuz Zaman, Wordh Ul Hasan, Monsur Hillas, Abdullah Al Mahfuj Shaan, Khan Afnan Rahad "IOT based question paper delivery box: A Solution towards preventing question paper leakage "-2020.
- [4] Z. M. Tahmidul Kabir, Md. Jubaer Islam Khan, Al Mamun Mizan, Nirmal Debnath "Smart System Integration of Question Paper Security System "-2019.
- [5] G. Mohammad Abdul Naveed, P.V. Vara Prasad Rao "A Password-authentication system for the Electronic Protection for Exam Paper Leakages" -2019.
- [6] Keerthan K S, Mukesh , Manjunatha G, Karan R Aithal , Dr. K M Sudharshan "Rfid Based Exam Paper Leakage Protection System" -2021.
- [7] IIT Kanpur India (10th ICCCNT 2019) "RFID based Question paper Protection shield".
- [8] Mohd Imran, Azeem Uddin, Farha Rafath, Mohammed Osman, Ayesha Sultana, K. Srikanth "Real Time Application of Advanced Exam Paper Leakage Detection and Alert System with Theft Protection".