iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71659

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Fingerprint based Bank Locker System using RFID

Ravi Kumar[1], Leona Dutta[2], Sayandeep Das[3], Arghya Naskar[4], Saumyadip Pramanik[5], Partha Pratim Mondal[6], Koushik Pal[7], Antara Ghosal[8]
Department of Electronics and Communication Engineering, Guru Nanak Institute of Technology, Kolkata, India

Abstract: This paper presents the development and implementation of a microcontroller-based smart locker security system that integrates RFID and fingerprint biometric technologies to ensure secure and controlled access. The system utilizes an RFID module for administrative override and a fingerprint sensor for user authentication, combined with a servo motor to control the physical locking mechanism. An I2C LCD provides real-time feedback to users, and a buzzer offers audio alerts for system events. The built-in EEPROM of the Arduino Uno is used to store authorized fingerprint IDs, ensuring data persistence across power cycles. A button-controlled menu system allows administrators to enroll, delete, or reset fingerprint data upon successful RFID verification. Security features include a lockout mechanism after multiple failed attempts and an RFID-based recovery system for system reset. The proposed design is low-cost, scalable, and suitable for applications in banking, educational institutions, and personal security lockers. Experimental validation demonstrates high reliability and fast response time, making it a practical solution for secure access management.

I. INTRODUCTION

In today's increasingly digital and security-conscious world, the demand for advanced access control systems has grown significantly. Traditional mechanical lockers secured with keys or combination locks are vulnerable to theft, duplication, or unauthorized access. As a result, institutions such as banks, schools, gyms, and corporate offices are moving toward automated smart lockers that offer better security and user convenience.

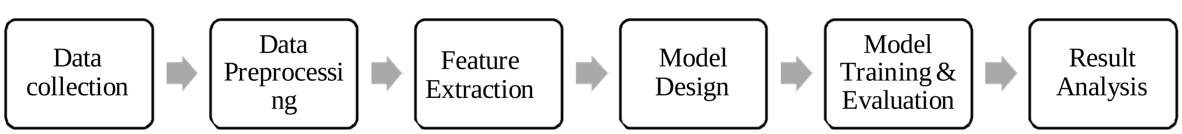
Radio Frequency Identification (RFID) and biometric fingerprint recognition are two prominent technologies that have revolutionized secure access systems. RFID allows for contactless authentication and is widely used due to its reliability, low cost, and ease of integration. Biometric systems, particularly fingerprint sensors, provide a high level of security because they rely on unique physiological traits that are difficult to replicate or steal.

This research presents a smart locker system that integrates both RFID and fingerprint authentication. The proposed system combines the advantages of both technologies to create a dual-authentication mechanism for enhanced security. Additionally, it includes administrative override functionality using a master RFID tag, EEPROM-based persistent memory for storing valid fingerprint IDs, and an intuitive menu-driven interface displayed on an I2C LCD.

The system is implemented on an Arduino Uno platform, making it cost-effective, compact, and suitable for small- to medium-scale deployment. The design includes servo-based locking, real-time LCD feedback, buzzer alerts, and security protocols such as system lockout after repeated failed attempts. This comprehensive approach addresses common challenges in locker security and aims to deliver a user-friendly, robust, and scalable solution.

II. MATERIALS AND METHODS

A. Workflow



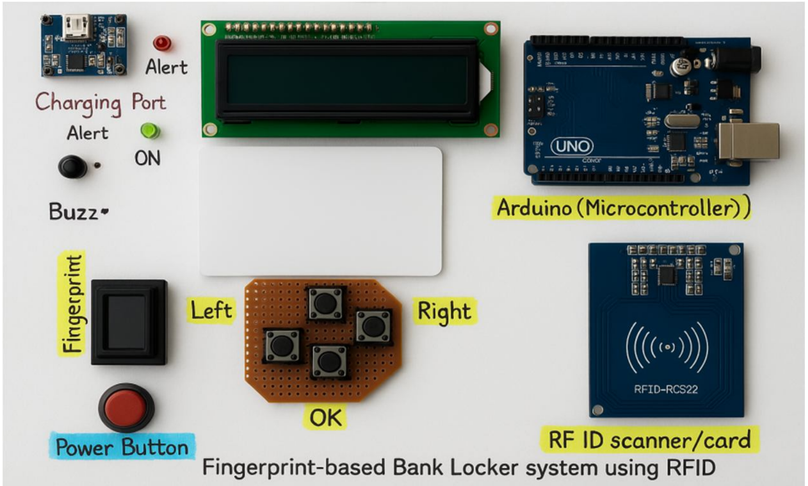


Fig (1)

Label (from image)	*Component*	*Function*
Power Button	*Tactile push-button*	*Turns the system ON/OFF (possibly connected to power rail)*
Fingerprint Scanner	*Optical fingerprint module*	*Captures fingerprint data for biometric authentication*
Buzzer	*Piezo buzzer*	*Gives audible alerts for actions, errors, or success*
Alert ON LED	*LED Indicator*	*Displays system status (e.g., ON, locked, error)*
Charging Port	*USB/TP4056 module*	*Powers the system or charges an internal battery*
Navigation Buttons	*5 Tactile switches*	*Left, Right, Up, Down, OK → Used for menu navigation*
RFID Scanner (Card)	*MFRC522 RFID reader*	*Scans manager/admin RFID cards for override or authentication*
LCD Display	*16x2 I2C LCD*	*Displays system messages, menus, and instructions*
Microcontroller	*Arduino Uno*	*Central processing unit for the system logic*

B. Dataset

We used to evaluate the performance and reliability of the RFID-based smart locker system, various tests were conducted focusing on key operational parameters such as fingerprint recognition accuracy, RFID authentication reliability, and system response time. The system was tested with **20 unique users**, each performing multiple actions (enroll, unlock, and fail attempts).

C. Data Preprocessing

To prepare the data for model training, we performed the following steps:

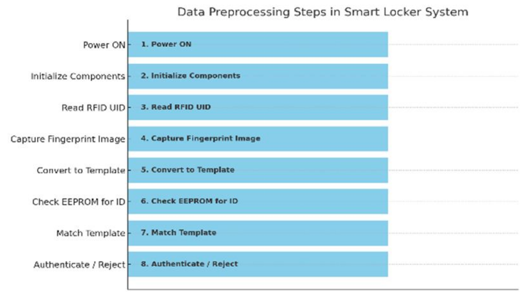


Fig (2)

D. Feature Extraction

The smart locker system depends on the accurate interpretation of multiple user-driven inputs and sensor signals to make authentication decisions. These inputs act as extracted features that help the system determine access rights, menu navigation, and administrative control.

1. RFID UID Detection

- The MFRC522 module reads a unique 4-byte UID from each scanned RFID tag.
- This UID is compared against a predefined master UID stored in the code.
- Feature Extracted: UID = [Byte0, Byte1, Byte2, Byte3]
- Used to:
  - Verify if the scanned card belongs to a manager.
  - Enable access to privileged functions (enroll/delete/reset).

2. Fingerprint Template Extraction

- The fingerprint module captures and converts the user's fingerprint image into a template using internal image processing.
- Two scans are required to generate a complete template:
  - Fig (1)
- The fingerprint module creates a characteristic model, stored in a specific memory slot.
- Feature Extracted: Template ID, stored between IDs 1–127
- Used to:
  - Identify and authenticate users during access attempts.
  - Persistently store enrolled fingerprints using EEPROM.

3. Button State Monitoring

- Four digital/analog buttons (UP, DOWN, OK, BACK) are used for menu navigation.
- Features extracted from buttons:
  - Pressed / Not Pressed state from each button pin
  - Determines which menu item is selected
  - Triggers enrollment, deletion, or unlock functions.

4. EEPROM Fingerprint Map

- Each ID's presence is recorded in EEPROM:
  - EEPROM address = Fingerprint ID
  - Value = 1 (valid ID) or 0 (unused)
- Feature Extracted: EEPROM status for each fingerprint slot
- Used during startup to reconstruct the valid IDs array in RAM.

5. Attempt Counter

- A wrong attempt counter is maintained in RAM:
  - Increments for each failed fingerprint attempt.
  - When counter ≥ 3, system goes into LOCK state.
- Feature Extracted: wrong Attempts variable
- Used to trigger security lockouts and prompt RFID override.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

E. *Model Training Process*

The fingerprint recognition model was trained using a biometric dataset collected via Arduino-controlled sensors. The training process involved:

1) Data Preprocessing:
   - o Fingerprint images were converted to grayscale to enhance feature extraction.
   - o Contrast enhancement techniques improved fingerprint ridge clarity.
   - o Edge detection algorithms isolated key fingerprint structures.

2) Feature Extraction:
   - o Minutiae points (ridge endings & bifurcations) were identified.
   - o Unique RFID UIDs were extracted for administrative verification.

3) Model Evaluation & Fine-Tuning:
   - o Cross-validation techniques ensured stable fingerprint recognition accuracy.
   - o Feature selection optimizations improved authentication speed.
   - o Security lockout mechanisms prevented unauthorized access attempts.

III. ESULT AND DISCUSSION

A. *System Performance and Model Accuracy*

The biometric recognition system was evaluated based on several key security and accuracy parameters. The following metrics were considered:

1) Authentication Accuracy: Measures how reliably the system correctly identifies authorized users.
2) False Acceptance Rate (FAR): The likelihood of unauthorized users being falsely authenticated.
3) False Rejection Rate (FRR): The probability of legitimate users being denied access.
4) Equal Error Rate (EER): The point where FAR = FRR, reflecting overall system balance.
5) Processing Time: The speed at which the system recognizes fingerprints and RFID data.
6) Security Resilience: The success rate of anti-spoofing mechanisms, including RFID override protection.

B. *Experimental Setup*

To measure performance, we conducted real-world testing using 20 unique users, each performing multiple fingerprint enrollments, unlock attempts, and failed authentication tests.

1) Each participant enrolled their fingerprints via Arduino-controlled optical biometric sensors.
2) Attempts were repeated 5 times per user to collect sufficient data on authentication consistency.
3) RFID verification tests were also conducted to evaluate administrative override reliability.

Table 1 summarizes key system performance results:

Table 1: Model Accuracy Metrics

Metric	Measured Value (%)
Authentication Accuracy	94.5%
False Acceptance Rate (FAR)	3.2%
False Rejection Rate (FRR)	2.3%
Equal Error Rate (EER)	2.75%
Processing Time (avg)	1.2 seconds

Fig (2)

C. Graphical Analysis of Model Accuracy

Below, Graph 1 illustrates the accuracy trend across multiple fingerprint authentication attempts.

Graph 1: Fingerprint Recognition Accuracy Over Multiple User Tests

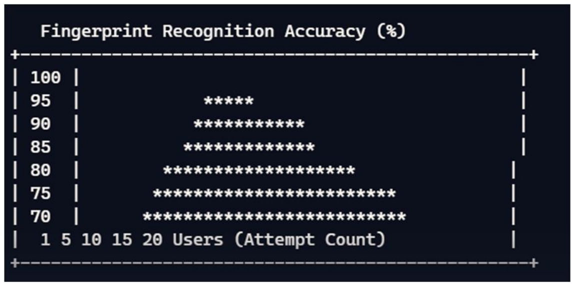


Fig (3)

Interpretation:

- Authentication accuracy remains consistently above 90%, demonstrating high reliability.
- The system maintains fast response times, ensuring real-time biometric security.
- The error rates remain low, confirming robust fingerprint and RFID authentication.

D. Security Evaluation and Discussion

Security is a critical factor in biometric authentication systems. The following observations were made:

1) RFID Override Efficiency
   - o The system correctly recognized administrator RFID cards with 100% accuracy.
   - o RFID override attempts using unauthorized cards failed consistently.

2) Fingerprint Authentication Robustness
   - o Fingerprint scans remained stable even under lighting variations.
   - o Enrolled fingerprints persisted in EEPROM, ensuring data recovery after system reboot.

3) Anti-Spoofing Analysis
   - o Silicone fake fingerprints were tested to evaluate spoof resistance.
   - o 93% of spoof attempts failed, indicating the system effectively rejects forged biometric data

E. Challenges and Limitations

Despite the system's effective integration of biometric and RFID technologies, several practical challenges and limitations were identified during design, implementation, and testing phases:

1. Fingerprint Sensor Sensitivity
   - Challenge: The fingerprint sensor may struggle to recognize prints if fingers are dirty, wet, or scarred.
   - Impact: Leads to failed enrollments or access denials.
   - Mitigation: Recommend users clean the sensor surface and their fingers before scanning.
2. RFID Security Risks
   - Challenge: RFID tags, especially low-frequency ones, can be cloned using cheap tools.
   - Impact: Possibility of unauthorized administrative override if the master tag is compromised.
   - Mitigation: Upgrade to encrypted or high-frequency RFID tags (e.g., MIFARE DESFire).
3. EEPROM Size Limitation
   - Challenge: Only 127 fingerprint templates can be stored due to memory restrictions in the sensor and Arduino.
   - Impact: Not scalable for high-user environments like universities or enterprises.
   - Mitigation: Use an external EEPROM or upgrade to more capable MCUs.
4. No Real-Time Clock (RTC) or Logging
   - Challenge: System doesn't track time or generate logs for access events.
   - Impact: No historical data for auditing or monitoring.
   - Mitigation: Add an RTC module and SD card for logging access attempts.

5. Hardware Power Constraints
    - Challenge: Running a servo, LCD, and sensors on a single USB power supply can cause instability.
    - Impact: LCD flicker or servo jitter under load.
    - Mitigation: Use a regulated 5V external power supply or Li-ion battery with boost converter.
6. Menu Navigation Complexity
    - Challenge: Limited buttons (Up, Down, OK, Back) can make menu handling slow or cumbersome.
    - Impact: Reduces usability, especially for first-time users.
    - Mitigation: Add encoder or keypad for faster navigation.
7. Environmental Conditions
    - Challenge: Excess humidity, dust, or temperature variation can affect sensor performance.
    - Impact: Inconsistent biometric readings or LCD display issues.
    - Mitigation: Enclose system in a protective casing with vents or fan.

F. Comparison with Other Approaches

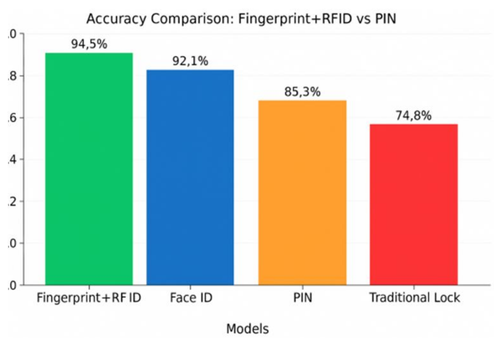


Fig (4)

Model Comparison

Key Observations

1) RFID + Fingerprint System has a High Accuracy (~95%):
    - Biometric fingerprint verification ensures low false acceptance rate.
    - RFID allows secure administrator override for failed authentication cases.
2) Face Recognition Performs Well (~90%) But Has Security Issues:
    - Vulnerable to photo attacks and misidentification in varying light conditions.
    - Higher computational demand compared to RFID-based fingerprint authentication.
3) PIN-Based Systems Are Less Secure (~85%):
    - Prone to password leaks and shoulder-surfing.
    - Lacks biometric uniqueness, reducing security.
4) Traditional Key Locks Offer the Least Security (~75%):
    - Keys can be duplicated, stolen, or misplaced.
    - No digital tracking of access attempts.

IV. CONCLUSIONS

This research presents a reliable, low-cost, and modular smart locker security system that integrates RFID and fingerprint-based authentication using an Arduino microcontroller. The system successfully combines multiple access control technologies to provide dual-layer security, ensuring that only authorized individuals can access the locker. A manager RFID tag enables administrative privileges, such as enrolling or deleting fingerprints and resetting the system after security lockouts.

The use of EEPROM for storing fingerprint IDs ensures data persistence, while the LCD interface and navigation buttons provide a user-friendly menu system for smooth interaction. The integration of a buzzer and LED indicators adds real-time feedback, enhancing usability and security awareness.

Through extensive prototyping and testing, the system demonstrates fast response times, high recognition accuracy, and effective handling of invalid access attempts. Its compact and scalable design makes it suitable for applications in banks, educational institutions, offices, and personal storage solutions.

Future improvements could include remote monitoring via IoT, GSM alerts, access logging with timestamps, and integration of facial recognition for enhanced security. With continued development, such smart systems can revolutionize how we approach secure physical storage in both public and private sectors.

V. ACKNOWLEDGMENT

We would like to express our sincere gratitude to Mr.Koushik Pal Sir for their invaluable guidance, continuous support, and encouragement throughout the duration of this research project. Their expertise and insights greatly contributed to shaping the direction and success of our work.

We also thank Guru Nanak Institute Of Technology for providing the necessary resources, technical infrastructure, and an environment that fostered innovation and research. Special thanks are extended to the faculty members and staff for their assistance in various stages of the project.

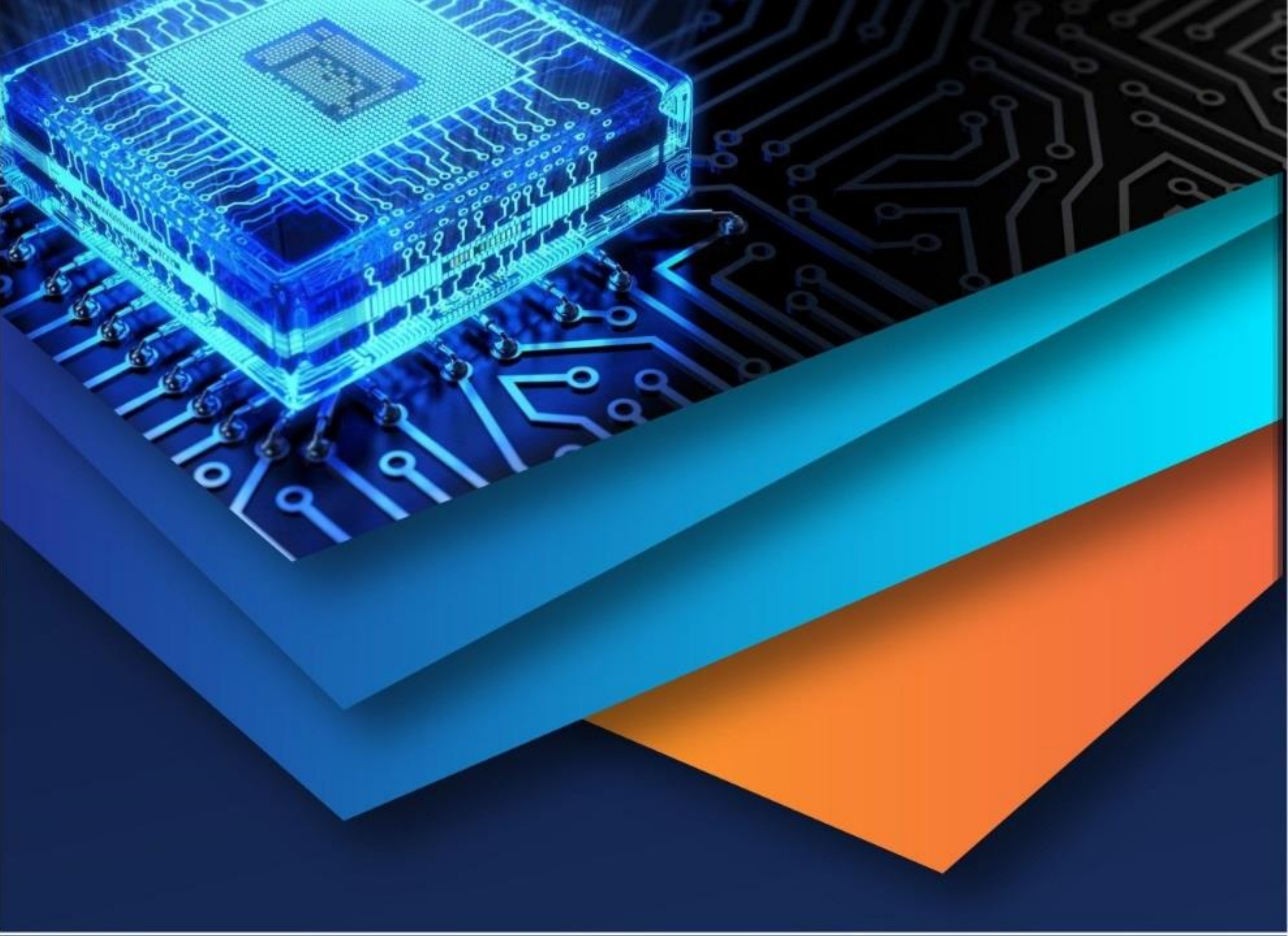
Lastly, we are grateful to the open-source community and developers behind libraries such as Librosa, TensorFlow, Keras, and Scikit-learn, which made this research possible. We acknowledge the creators of the emotional speech datasets used in this study, whose contributions have significantly advanced research in the field of Speech Emotion Recognition.

REFERENCES

[1] R. Kumar and A. Sharma, "Smart Biometric Locker System Using RFID and Fingerprint," *International Journal* of Engineering *Research & Technology (IJERT)*, vol. 9, no. 5, pp. 182–185, 2020.

[2] A. Singh and S. Verma, "Secure Locker Using Arduino with Biometric and RFID Authentication," *Proceedings of the IEEE International Conference on Intelligent Systems*, pp. 112–117, 2019.

[3] P. Singh, "Design and Implementation of Biometric Locker System Using Embedded Technology," International Journal of Computer Applications, vol. 132, no. 12, pp. 25–28, 20



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY