International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

SMART DOOR LOCKING SYSTEM USING ARDUINO

[1] Mr. D. Mallesham, [2] N. Veera Swami, [3] B. Veera Kumar, [4] K. Abhinaya Sri, [5] G. Sai Prem, [6] Sunkey Ajay
[1]Assistant Professor, [23456]Students
Department of EEE
Siddhartha Institute of Technology & Sciences, Narapally
dayyalamallesham.eee@siddhartha.co.in, 24tq1a0211@siddhartha.co.in, 24tq1a0203@siddhartha.co.in, 24tq1a0206@siddhartha.co.in, 25tq5a0211@siddhartha.org.in, 24tq1a0214@siddhartha.co.in

ABSTRACT

Doors in homes, laboratories, hostels, and offices are still secured mostly with mechanical locks and keys, which can be lost, copied, or shared without the owner's knowledge, and which give no record of who entered and when. Electronic access control systems solve many of these problems, but commercial units are costly and are often built as closed products that are difficult to repair or adapt. This paper presents a Smart Door Locking System Using Arduino that provides keypad, RFID, and mobile based access to a door through an electrically operated lock, with careful attention to the power supply and drive circuits that make such a lock reliable in daily use.

The system uses an Arduino UNO as the main controller. A 4x4 matrix keypad accepts a personal identification number, an MFRC522 RFID reader identifies authorised cards and tags, and an ESP8266 Wi-Fi module allows the door to be opened from a mobile application and sends entry records to a cloud server. The door is secured with a 12 V solenoid lock driven through a logic-level MOSFET with a flyback diode, and a reed switch confirms whether the door is actually closed. A 16x2 LCD with I2C interface guides the user, and a buzzer gives audible feedback.

Because the lock must work during power cuts, the design includes a 12 V power supply with a small lead-acid or lithium battery backup, a charging circuit, and a buck converter that provides 5 V for the Arduino and modules. The controller monitors the supply voltage and the lock coil current, detects a failed or jammed solenoid, and reports low battery before the backup runs out. The unlock pulse is limited in duration so that the solenoid coil does not overheat, and the lock is designed as fail-secure so that the door stays locked if power is lost.

Security features include lockout after three wrong PIN attempts, an intruder alert when the reed switch shows the door opened without a valid unlock, and an alarm when the door is left open beyond a set time. All events are stored with time stamps from a DS3231 real time clock, kept in local memory when the network is down, and uploaded to the cloud when it returns. The owner can add or remove users and view the access log from the mobile application. Temporary codes that expire after a set time can also be issued to visitors or service staff.

The prototype was tested on a wooden door frame over several hundred lock and unlock cycles. Keypad and RFID access worked reliably, the average time from valid credential to unlock was under one second, the battery backup kept the system operating for more than ten hours, and the coil temperature remained within safe

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

limits. The work shows that a practical and maintainable smart lock can be built from common Arduino components.

I. INTRODUCTION

Security of homes and workplaces depends heavily on the door lock. Mechanical locks remain the most common choice because they are cheap and familiar, but they have well-known weaknesses. Keys can be lost or duplicated, a lock must be replaced when a tenant or employee leaves, and there is no way to know who opened the door or at what time. In shared spaces such as college laboratories, hostels, and small offices, keys are often passed from hand to hand, which makes accountability difficult when equipment goes missing.

Electronic door locks replace or supplement the key with credentials such as a PIN, an RFID card, a fingerprint, or a smartphone. Commercial access control systems offer these features, together with audit logs and remote management, but they are expensive for individual homes and small institutions, and they are often tied to a particular vendor. They also depend on a stable power supply and a correctly designed actuator, and poorly designed low-cost locks frequently fail because of weak power supplies, overheating solenoids, or electrical noise that resets the controller when the lock operates.

The Arduino platform provides an accessible way to build an electronic lock that is inexpensive, open, and easy to modify. The Arduino UNO has enough input and output pins to handle a keypad, an RFID reader, a display, and a lock driver, and it can be connected to a Wi-Fi module for remote access. From an electrical engineering point of view, the interesting part of such a design lies in driving an inductive actuator safely, providing backup power, and monitoring the health of the lock circuit. These aspects decide whether the lock keeps working after months of daily use, and they are often the reason why simple project-level locks fail when moved from the bench to a real door.

This paper describes a Smart Door Locking System Using Arduino that offers keypad, RFID, and mobile access, drives a 12 V solenoid lock through a protected MOSFET stage, operates from a battery-backed supply, monitors lock and battery condition, and records every access event locally and in the cloud. The aim is to provide a secure, reliable, and affordable lock suitable for homes, laboratories, and small offices.

II. LITERATURE SURVEY

Research on electronic door locks has explored a wide range of authentication methods. Keypad based locks using a PIN are the simplest and have been used in many microcontroller projects, although studies note that PINs can be observed by others or shared among users. RFID based systems using passive cards at 13.56 MHz have become common in offices, hotels, and hostels because they are quick to use and each card can be registered to an individual. Biometric locks using fingerprint sensors provide stronger identity binding, and several works report good performance with low-cost optical fingerprint modules, although sensor accuracy falls with dirty or wet fingers. Many authors recommend combining two methods, such as a card and a PIN,

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

for doors that need higher security. Researchers have also examined the weaknesses of common RFID cards, noting that low-cost cards with fixed identifiers can be cloned, and they suggest reading protected memory sectors or pairing the card with a second factor where this is a concern.

Remote and smartphone based access has been a growing theme in recent studies. Bluetooth Low Energy locks allow a user to unlock a door when the phone is nearby, while Wi-Fi and cellular connected locks allow remote unlocking from anywhere and support features such as temporary access codes for visitors. Researchers have used the ESP8266 and ESP32 modules extensively for this purpose because they combine a microcontroller with Wi-Fi at low cost. Cloud platforms and MQTT brokers are used to relay commands and store logs. Security studies point out that remote locks must protect commands against interception and replay, and they recommend encrypted connections, device authentication, and rolling or time-limited tokens rather than fixed passwords sent in plain form. Other studies have highlighted the need for a local fallback, so that the lock remains usable through its keypad or card reader when the internet connection or the cloud service is unavailable.

The electrical design of lock actuators has received less attention in student projects, but it is discussed in work on access control hardware. Solenoid locks and electromagnetic locks are the two main types. Solenoid bolts are fail-secure or fail-safe depending on design, draw a high current for a short time when energised, and can overheat if held on continuously. Electromagnetic locks hold the door with a continuously energised magnet and release it when power is removed, which suits fire exits but requires uninterrupted power. Studies on driver circuits emphasise the use of transistors or MOSFETs rated for the coil current, flyback diodes to absorb the inductive voltage spike at turn-off, and separate supply rails or adequate decoupling so that the switching of the coil does not reset the microcontroller. Measurements reported in such work show that the reverse voltage spike from an unprotected 12 V coil can exceed a hundred volts for a short moment, which is enough to destroy a transistor or couple noise into nearby logic.

Power supply and backup design is closely linked to the reliability of electronic locks. Researchers have examined linear and switched-mode supplies, battery backup using sealed lead-acid and lithium-ion cells, and charge controllers that keep the battery ready without overcharging. Monitoring of battery voltage and warning the user before the backup is exhausted has been recommended in several works, together with low-power sleep modes for the controller to extend backup time. Studies also note that a lock should have a defined behaviour on power failure and that mechanical override through a concealed key is often required by building practice for emergencies. The choice between fail-secure and fail-safe behaviour therefore depends on whether the door protects property or serves as an escape route.

Intrusion detection and event logging complete the functions of a smart lock. Beyond checking credentials, a lock must know whether the door is actually closed and must be able to show later what happened at the door. Door position sensors such as reed switches or magnetic contacts have been used to detect forced opening, doors left ajar, and tailgating. Real time clock modules provide time stamps for each event, and logs are stored on EEPROM, SD cards, or cloud databases. Studies of access control in

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

institutions report that the availability of logs discourages misuse and helps in investigating incidents. The system presented in this paper builds on these works by combining keypad, RFID, and mobile access with a protected solenoid drive, a battery-backed supply, lock and battery health monitoring, and time-stamped logs on an Arduino UNO platform.

III. SYSTEM ANALYSIS

The Smart Door Locking System is analysed as four parts: the user interface, the controller, the lock drive and power section, and the network service. The user interface consists of a 4x4 matrix keypad, an MFRC522 RFID reader on the SPI bus, a 16x2 LCD on the I2C bus, and a buzzer. The Arduino UNO checks entered PINs and card identifiers against stored records in its EEPROM and keeps time through a DS3231 real time clock. The lock drive uses an IRLZ44N logic-level MOSFET switching a 12 V solenoid lock, with a 1N4007 flyback diode across the coil and a small shunt resistor that lets the controller measure coil current. A reed switch on the door frame reports whether the door is closed. The power section includes a 12 V adapter, a battery with charge control, and an LM2596 buck converter providing 5 V. An ESP-01 ESP8266 module connected through a level-shifted serial link handles Wi-Fi, receiving unlock commands and sending logs to the cloud.

Existing System

Most homes, hostels, and laboratories still use mechanical locks with physical keys. Keys are easily lost, duplicated at local shops, or shared with people who should not have access, and changing the lock is the only remedy when a key goes missing. There is no record of who opened the door or when, which makes it hard to establish responsibility for lost property. Where electronic locks are used, they are often basic keypad units with a single shared code that is rarely changed and that many people come to know. Many inexpensive electronic locks drive the solenoid directly from a weak adapter without backup, so they stop working during power cuts or leave the door unlocked. Poorly designed drive circuits without flyback protection cause resets and relay failures, and the lock gives no warning when the coil or battery is failing. Commercial access control systems address these issues but are costly and difficult for users to maintain or extend.

Disadvantages of Existing System

- Mechanical keys can be lost, copied, or shared without control.
- No record is kept of who opened the door and at what time.
- Replacing the lock is the only remedy when a key is lost.
- Basic keypad locks use a single shared code that rarely changes.
- Many electronic locks stop working during power cuts.
- Solenoids driven without protection cause controller resets and failures.
- Continuous energising of the solenoid coil leads to overheating.
- Forced opening or a door left open is not detected or reported.
- Low battery or a failing lock gives no warning in advance.
- Commercial access control systems are costly and vendor dependent.

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Proposed System

The proposed system is an Arduino UNO based smart lock that offers three methods of access and a reliable electrical design. Users can unlock the door with a PIN on the keypad, a registered RFID card, or a command from the mobile application sent through the ESP8266 module. When a valid credential is received, the controller turns on the MOSFET for a limited unlock pulse, measures the coil current to confirm that the solenoid has operated, and watches the reed switch to confirm that the door opens and later closes. The flyback diode, separate decoupled supply rails, and a buck converter keep the controller stable while the coil switches. A battery with charge control keeps the lock working during power cuts, and the controller reports low battery and supply failure. Three wrong PIN entries cause a timed lockout, forced opening triggers an alarm and a mobile alert, and a door left open sounds a reminder. All events are time stamped and logged locally and in the cloud, and the owner manages users from the application.

Advantages of Proposed System

- Supports PIN, RFID card, and mobile application access to the door.
- Keeps a time-stamped log of every entry and failed attempt.
- Users can be added or removed without changing the lock.
- Protected MOSFET drive with a flyback diode prevents controller resets.
- Limited unlock pulse keeps the solenoid coil within safe temperature.
- Battery backup keeps the lock working during power cuts.
- Coil current and battery monitoring warn of faults in advance.
- Detects forced opening and doors left open and raises alerts.
- Locks out the keypad after repeated wrong PIN attempts.
- Built from low-cost Arduino components that are easy to repair.

IV. METHODOLOGY

The methodology starts with the selection of a 12 V fail-secure solenoid lock and measurement of its coil resistance and current to size the MOSFET, diode, and power supply. The drive stage is built on a separate board with a gate resistor, a pull-down resistor, a flyback diode, and a 0.5 ohm shunt for current sensing, and decoupling capacitors are added near the controller. The power section is assembled with a 12 V adapter, a battery charge circuit, and an LM2596 buck converter, and the switchover to battery is tested by removing mains supply. Firmware for the Arduino UNO is written as a state machine with idle, verify, unlock, open, and alarm states. PINs are stored as hashes in EEPROM, card identifiers are read from the MFRC522, and the ESP8266 exchanges messages with the cloud using MQTT over a secured connection. The system is tested for access time, false acceptance of unregistered cards, response to wrong PINs, coil temperature after repeated operation, and battery backup duration.

SYSTEM ARCHITECTURE

The architecture of the Smart Door Locking System is arranged in layers from the user to the cloud. The User Input Layer consists of the keypad, the RFID reader, and

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

the mobile application. The Authentication Layer on the Arduino UNO compares the credential with stored PIN hashes and card identifiers and applies lockout rules. The Controller Layer manages the lock state machine, the real time clock, and the local display and buzzer. The Lock Drive Layer contains the MOSFET, flyback diode, and solenoid lock, with current sensing for confirmation. The Door Sensing Layer uses the reed switch to detect the actual door position. The Power Supply and Backup Layer provides regulated 12 V and 5 V rails with battery changeover and monitoring. The Connectivity Layer uses the ESP8266 module to send and receive MQTT messages. The Cloud Layer stores logs and user records, and the Application Layer lets the owner unlock remotely, manage users, and receive alerts.

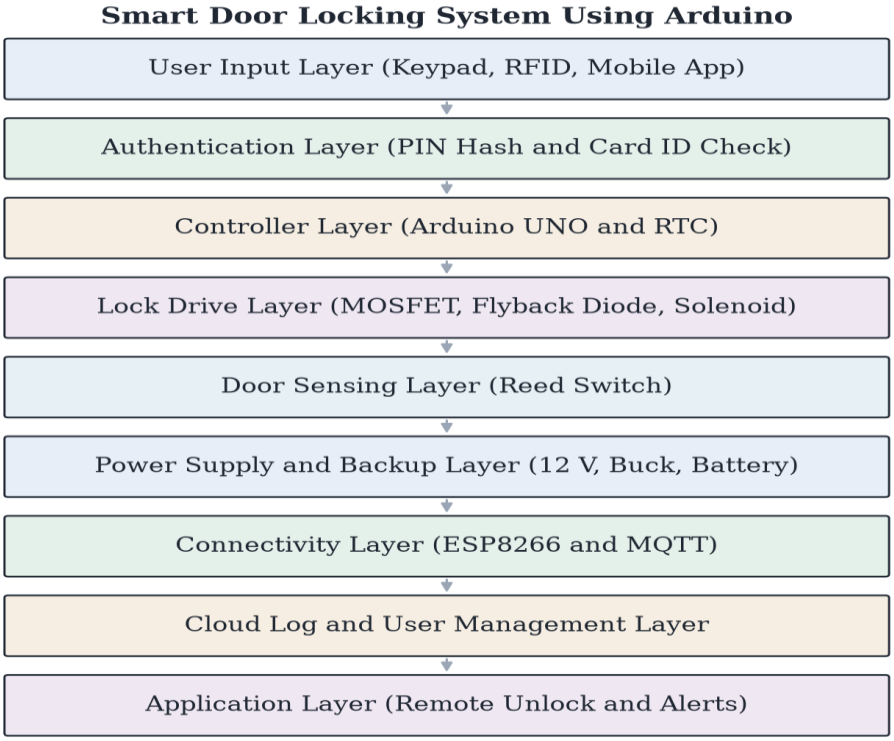
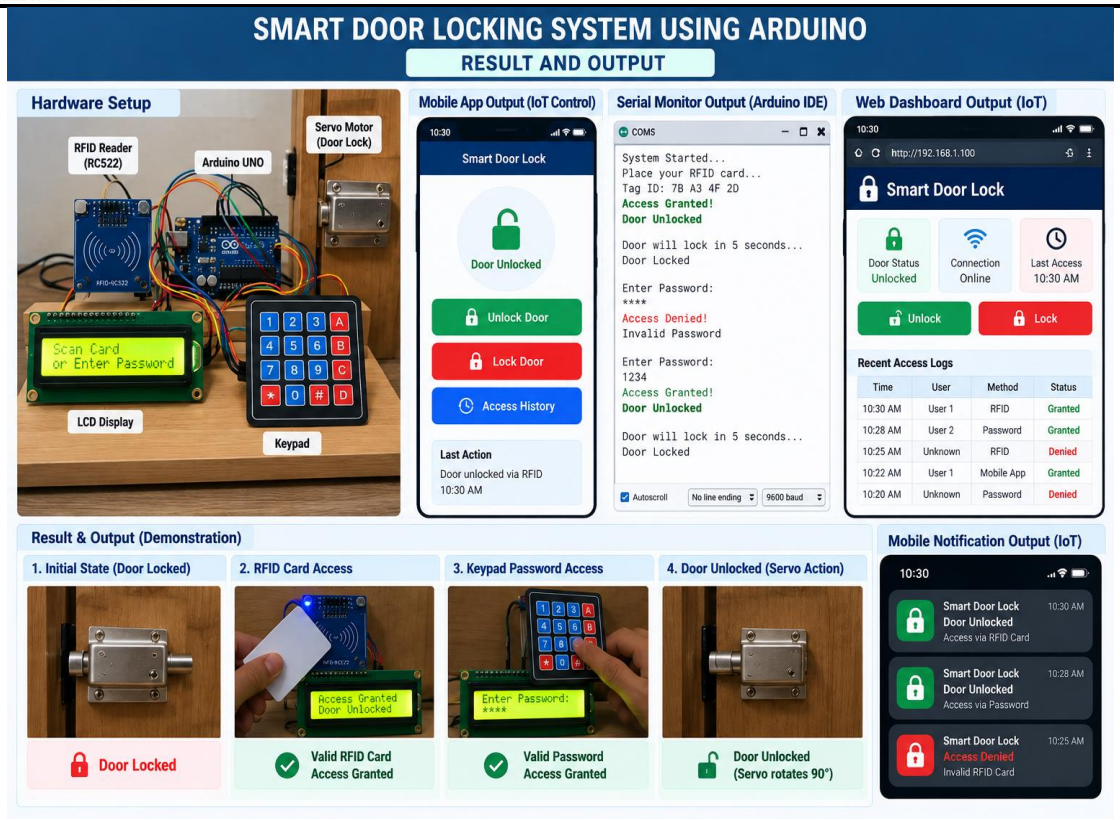


Fig. 1 System Architecture

V. RESULT AND OUTPUT

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper



VI. CONCLUSION

This paper presented a Smart Door Locking System Using Arduino that provides keypad, RFID, and mobile access to a door through a 12 V solenoid lock. The Arduino UNO verifies credentials, drives the lock, watches the door position, and keeps a time-stamped record of every event, while an ESP8266 module connects the lock to a cloud service and a mobile application for remote control and user management.

A central part of the work was the electrical design of the lock drive and power supply. The MOSFET stage with a flyback diode and decoupled supply rails prevented the resets and noise problems that are common in simple solenoid circuits, the limited unlock pulse kept the coil temperature within safe limits during repeated use, and coil current sensing confirmed that the lock had actually operated. The battery-backed supply kept the lock in service during power cuts, and the fail-secure behaviour ensured that the door stayed locked if all power was lost.

Testing on the prototype showed reliable access through all three methods, an average unlock time below one second, correct rejection of unregistered cards and wrong PINs, and prompt alerts for forced opening and doors left open. The access log gave the owner a clear view of who used the door and when, which is useful in shared spaces such as laboratories and hostels where accountability is important. The coil current record also proved useful during testing, because a slow rise in pull-in time and a change in current shape gave early notice of a misaligned strike plate before the lock actually jammed.

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Future work will add a fingerprint sensor for two-factor access in sensitive rooms, replace the ESP-01 with an ESP32 to support encrypted connections and Bluetooth unlocking, and reduce standby power so that the lock can operate for longer on battery. Integration with building fire alarm systems for automatic release of exit doors, and trials in a college laboratory over a full semester, are also planned to evaluate long-term reliability.

REFERENCES

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.
[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.
[3] Sv satyakrishna, shirisha rangu, bhargavi nalacheruve. (2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm
[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.
[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, "Real-Time Object Detection in Drone Surveillance Using YOLOv5," in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.
[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, "Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks," in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.
[7] R. D. Kumar, V. N. S. Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.
[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.
[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.
[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.
[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.