IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

Design and Implementation of an OTP-Based Access Control System for Electrical Distribution Panels

Dr. Rahul Agrawal[1], Dr. Sunil Magan More[2], Siddharth Pawar[3], Rahul Chavanke[4], Sakshi Pawar[5] Neha Chaudhari[6]
Head of Department, Electrical Engineering[1]
Assistant Professor, Department of Electrical Engineering[2].
UG Students, Department of Electrical Engineering[3,4,5,6]
Guru Gobind Singh College of Engineering & Research Centre, Nashik, Maharashtra, India

Abstract: *This research presents a One-Time Password (OTP)-based security system designed to improve the safety of linemen working on electrical distribution panels. During maintenance of live power lines, linemen are exposed to significant risks, often due to communication failures between the control room and field personnel, which may lead to the accidental re-energization of circuits. To address this, the proposed system employs a microcontroller integrated with a GSM module to create a secure, OTP-enabled access mechanism. Before initiating repair work, linemen can safely disable the power supply by entering an OTP through a keypad. Additionally, the system supports remote operation via SMS, enabling linemen to control the panel door from a distance—enhancing both safety and convenience. The use of GSM technology ensures reliable communication without the limitations of Bluetooth range or dependence on manual procedures. Unlike conventional password-based systems that are vulnerable to forgotten credentials or fixed passwords, this solution generates a new OTP for each access, providing secure, single-use control. By preventing unauthorized access and accidental power restoration, the system significantly reduces the chances of electrical hazards. This innovation not only enhances linemen's safety but also streamlines maintenance procedures, contributing to a more secure and efficient electrical distribution network.*

Keywords: OTP-Based Microcontroller, GSM Module, Distribution Panel

I. INTRODUCTION

In the field of electrical maintenance, ensuring linemen safety during repair and servicing of live distribution panels is a persistent challenge. Incidents caused by accidental re-energization of power lines due to human error or miscommunication have underscored the need for a more secure and automated access control mechanism. To address this concern, the present research proposes the design and implementation of an OTP-based access control system using a microcontroller and GSM module [4, 5]. This system ensures that only authorized personnel can access and control the distribution panel by requiring a dynamically generated one-time password (OTP) for operation. With integrated SMS-based remote control, the system eliminates the limitations of conventional password systems and Bluetooth-based solutions, significantly improving operational safety, reliability, and convenience for maintenance workers in the electrical domain [1.2.3]

Electricity plays a fundamental role in modern society, powering industries, homes, and essential services. However, maintaining electrical infrastructure presents significant risks, especially for linemen who repair live electrical lines. Electrical accidents during maintenance often stem from miscommunication between maintenance teams and substations, leading to accidental power restoration and electrocution hazards [6].

To mitigate these risks, this research introduces an OTP-based security system for controlling distribution panels. The system ensures that only authorized personnel can access and operate the panel by requiring an OTP for activation and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

deactivation. By integrating a microcontroller with a GSM module, the system allows secure, remote-controlled power line operation, reducing reliance on manual communication and improving overall safety [7].

1.1 Motivation

Linemen face severe risks due to electrical faults, inadequate safety measures, and human error. In many cases, accidental energization of power lines has resulted in fatal injuries. Conventional systems rely on static passwords or Bluetooth-based control, which have several limitations, including limited range and vulnerability to unauthorized access.

The motivation behind this project is to enhance linemen's safety by incorporating modern authentication mechanisms like OTP-based security and remote operation capabilities. By ensuring that only authorized personnel can control power lines, this system reduces the likelihood of accidents, making electrical maintenance safer and more efficient.

1.2 Objectives

The primary objectives of this research are:

- To develop a secure OTP-based system that ensures only authorized personnel can operate distribution panels.
- To integrate a microcontroller for managing OTP operations and controlling the panel's locking and unlocking mechanisms.
- To implement GSM-based remote control, allowing authorized users to activate or deactivate the panel from a remote location.
- To enhance system security through OTP verification and real-time GSM alerts, preventing unauthorized access and accidental power restoration.

II. RESEARCH CONTRIBUTION

This project introduces an OTP-based security system that addresses the identified gaps by:

- Replacing static passwords with dynamically generated OTPs.
- Utilizing GSM technology to provide secure, remote access to the distribution panel.
- Enhancing communication between linemen and control centers through real-time OTP validation.
- Offering a cost-effective and scalable solution that can be adapted to various electrical maintenance scenarios.

III. METHODOLOGY

3.1 System Architecture

The proposed system comprises the following components:

- **Microcontroller (Arduino):** Manages OTP authentication and panel operations.
- **GSM Module (SIM800L):** Sends OTP codes and allows remote operation via SMS.
- **Relay Circuit:** Controls the locking and unlocking of the distribution panel.
- **4x4 Keypad:** Used for OTP entry by the lineman.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

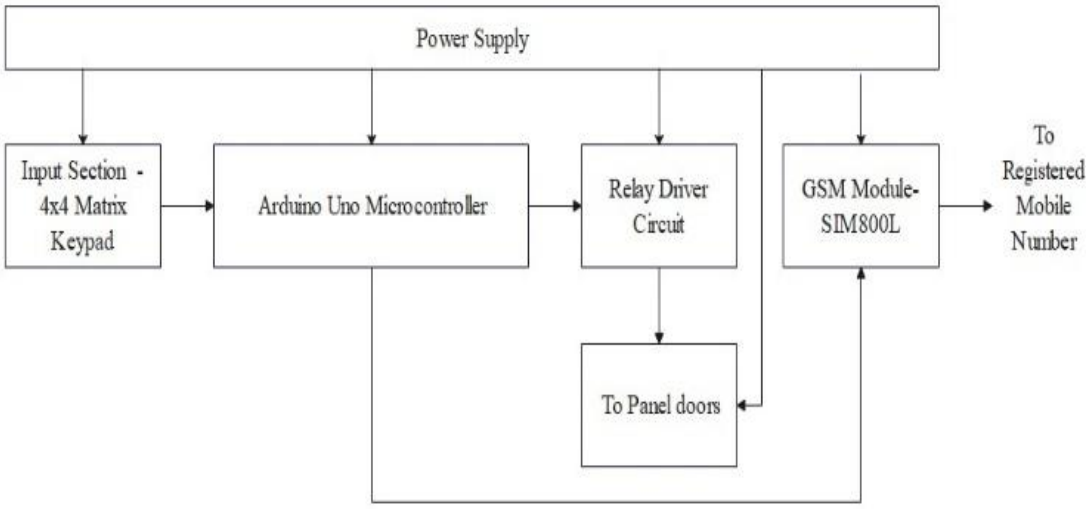


Figure No.1 Block Diagram

The Figure No. 1 shows block diagram of a **GSM-based Security System with Arduino Uno** for controlling and monitoring panel doors. Here's a detailed explanation of each block:

1. Power Supply

- Provides the required electrical power to all components: the keypad, Arduino Uno, relay circuit, and GSM module.
- Ensures stable and regulated voltage supply for reliable operation.

2. Input Section – 4x4 Matrix Keypad

- Acts as a user interface for password entry.
- Sends the entered key data to the Arduino Uno microcontroller.
- Typically used to input a passcode for door access control.

3. Arduino Uno Microcontroller

- Acts as the central control unit of the system.
- Receives input from the keypad.
- Processes the input and compares it with the predefined password.
- Based on the input, it controls the relay driver circuit (to open/close doors) and communicates with the GSM module.

4. Relay Driver Circuit

- Receives control signals from the Arduino.
- Operates the **panel doors** (lock/unlock mechanism) by switching a higher voltage load using relays.
- Essentially acts as an interface between the low-power Arduino and high-power door mechanisms.

5. Panel Doors

- These are the doors of the secured panel or locker.
- Controlled electronically via relays, depending on password verification.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

6. GSM Module – SIM800L

- Communicates wirelessly with a **registered mobile number**.
- Sends SMS alerts (e.g., access granted/denied, tampering detected).
- Receives power from the supply and control signals from Arduino.

7. To Registered Mobile Number

- The GSM module sends notifications to the user's mobile phone.
- Enhances system security by informing the user of system status or intrusion attempts.

3.2 Overall Operation:

User enters a passcode via the 4x4 keypad.
Arduino processes the input.
If correct:
Activates the relay to open the door.
Sends confirmation SMS to the registered number.
If incorrect:
Denies access.
May send alert SMS for unauthorized attempt.

3.3 Circuit Diagram

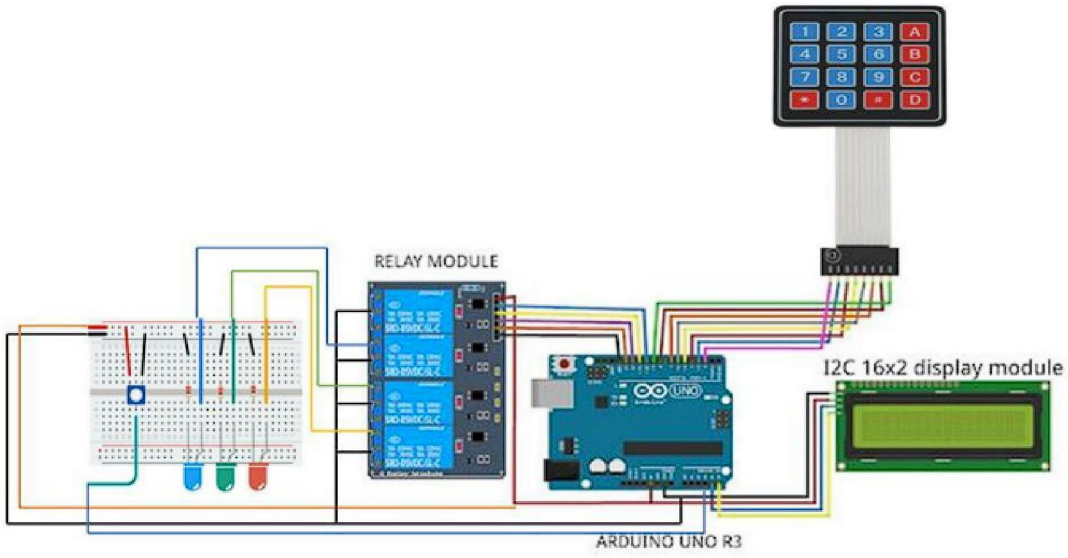


Figure No. 2. Circuit Diagram/ Wiring Diagram

Operation Process

This Figure No. 2 shows circuit diagram illustrates a Keypad-Based Door Lock System using an Arduino Uno microcontroller. The system allows access control through a 4x4 matrix keypad, where users input a password. The Arduino Uno processes the input from the keypad and checks it against a pre-stored password. If the entered password is correct, the Arduino activates a relay module that controls the locking mechanism of a door or panel, effectively unlocking it. Alongside this, a green LED on the breadboard lights up as a visual indicator of successful access.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

To enhance user interaction, an I2C 16x2 LCD display is included in the system. This display provides feedback such as “Enter Password,” “Access Granted,” or “Access Denied,” helping users understand the system's status at each step. The I2C interface simplifies wiring by reducing the number of connections needed for the display.

Multiple LEDs connected via a breadboard are used as status indicators: typically, green for access granted, red for access denied, and possibly blue for system ready. These LEDs are connected to Arduino's digital pins through current-limiting resistors. The relay module, which is powered by the Arduino, acts as a switch to control high-power devices like electronic door locks.

Overall, this system combines user input, display output, and controlled physical access, making it suitable for applications in home automation, secure lockers, office access systems, and more. It is a practical implementation of embedded systems and access control using basic electronic components, as shown in Figure No. 3.

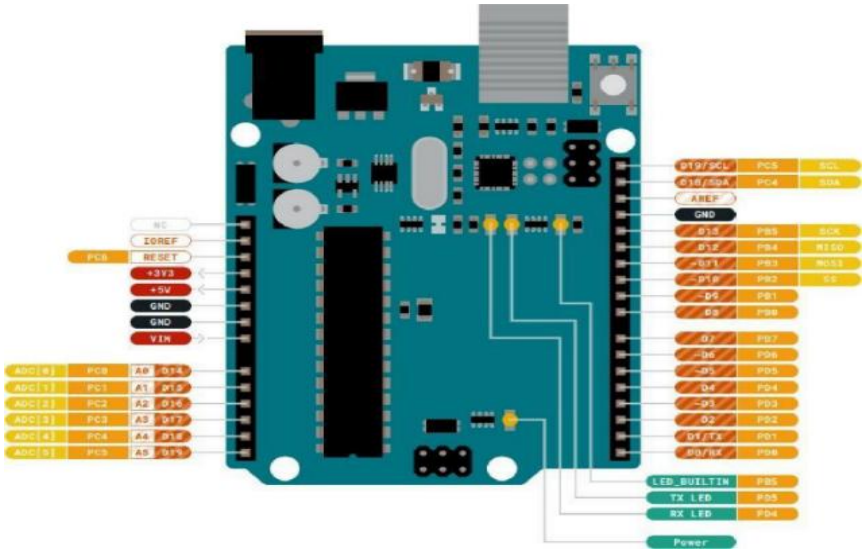


Figure No. 3: Connector Pinout

- **OTP Generation:** When a lineman requests access, an OTP is sent to their registered mobile number.
- **User Authentication:** The lineman enters the OTP on the keypad
- **Verification:** The microcontroller compares the entered OTP with the generated code.
- **Access Control:** If authentication is successful, the relay circuit is activated, allowing safe operation of the distribution panel.
- **Remote Control:** GSM integration enables secure remote activation and deactivation.

Table No. 1 shows a pinout table for the Arduino Uno R3, detailing the digital and analog input/output (I/O) pins and their functions. Each pin on the Arduino board is assigned a number and a function type—either digital, analog, or power-related. Pins D0 to D9 are general-purpose digital I/O pins (GPIO), which can be configured as either input or output depending on the application. These are used for interfacing with LEDs, sensors, switches, and other digital components.

Pins 11 to 14 serve specific functions related to SPI (Serial Peripheral Interface) communication. Pin 11 (MOSI) is the Master Out Slave In, used to send data to SPI devices. Pin 12 (MISO) is Master In Slave Out, used to receive data from SPI devices. Pin 13 (SCK) is the SPI clock line, and pin 10 (SS) is the chip select pin, which helps select the SPI slave device being communicated with.

Pin 15 (GND) is the ground connection, which is common for the entire circuit. Pin 16 (AREF) is the analog reference pin used to set an external reference voltage for the analog-to-digital conversion.

Pins A4 and A5 (labeled as SD4 and SD5) function as both analog inputs and I²C communication lines. A4 (SDA) is the data line, and A5 (SCL) is the clock line for I²C communication, enabling the Arduino to interface with modules like LCD displays and sensors using just two wires.

DOI: 10.48175/IJARSCT-27709

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

This pinout is essential for understanding how to connect various components to the Arduino Uno for building circuits, writing programs, and enabling communication with external modules and peripherals.

Table No. 1: Connector Design details of right section

Pin	Function	Type	Description
1	D0	Digital/GPIO	Digital pin 0/GPIO
2	D1	Digital/GPIO	Digital pin 1/GPIO
3	D2	Digital/GPIO	Digital pin 2/GPIO
4	D3	Digital/GPIO	Digital pin 3/GPIO
5	D4	Digital/GPIO	Digital pin 4/GPIO
6	D5	Digital/GPIO	Digital pin 5/GPIO
7	D6	Digital/GPIO	Digital pin 6/GPIO
8	D7	Digital/GPIO	Digital pin 7/GPIO
9	D8	Digital/GPIO	Digital pin 8/GPIO
10	D9	Digital/GPIO	Digital pin 9/GPIO
11	SS	Digital	SPI Chip Select
12	MOSI	Digital	SPI1 Main Out Secondary In
13	MISO	Digital	SPI Main In Secondary Out
14	SCK	Digital	SPI serial clock output
15	GND	Power	Ground
16	AREF	Digital	Analog reference voltage
17	A4/SD4	Digital	Analog input 4/I2C Data line (duplicated)
18	A5/SD5	Digital	Analog input 5/I2C Clock line (duplicated)

The Table No.2 shows a pin configuration table for the power and analog section of the Arduino Uno board. These pins are essential for supplying power, grounding the system, and interfacing with analog input devices.

The first pin, NC (Not Connected), is unused. The IOREF pin provides a reference voltage for the microcontroller's logic, typically 5V, ensuring compatibility with other components. The Reset pin is used to restart the Arduino program, manually resetting the board when needed. +3.3V and +5V pins are power output rails that provide regulated voltage for connected components. GND (Ground) pins are essential for completing electrical circuits and are connected to the system's ground. VIN is the input voltage to the Arduino when using an external power source (like a battery or adapter), instead of USB power.

The analog section includes pins A0 to A5, which serve as analog inputs and can also function as general-purpose input/output (GPIO). These pins are used to read analog sensor data, such as from temperature or light sensors. Additionally, A4 (SDA) and A5 (SCL) are used for I2C communication, where A4 acts as the data line and A5 as the clock line, enabling the Arduino to communicate with various I2C-compatible modules like displays, real-time clocks, and EEPROMs.

Together, these pins provide the necessary connectivity for power distribution, analog signal processing, and serial communication, forming the foundation for building diverse Arduino-based projects.

Table No. 2 Connector Design details of left section

Pin	Function	Type	Description
1	NC	NC	Not connected
2	IOREF	IOREF	Reference for digital logic V - connected to 5V
3	Reset	Reset	Reset
4	+3V3	Power	+3V3 Power Rail
5	+5V	Power	+5V Power Rail
6	GND	Power	Ground
7	GND	Power	Ground
8	VIN	Power	Voltage Input
9	A0	Analog/GPIO	Analog input 0 /GPIO
10	A1	Analog/GPIO	Analog input 1 /GPIO
11	A2	Analog/GPIO	Analog input 2 /GPIO
12	A3	Analog/GPIO	Analog input 3 /GPIO
13	A4/SDA	Analog input/I2C	Analog input 4/I2C Data line
14	A5/SCL	Analog input/I2C	Analog input 5/I2C Clock line

DOI: 10.48175/IJARSCT-27709

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

IV. RESULTS AND DISCUSSION

4.1 Results

The OTP-based distribution panel security system was extensively tested under real-world conditions to assess its efficiency, reliability, and fault tolerance. It consistently generated and validated OTPs for authorized personnel, ensuring secure authentication and seamless access control through microcontroller-based processing. During simulated power failures, the system maintained its encryption protocols and required multi-layer authentication upon restoration, effectively preventing unauthorized activation. Its advanced intrusion detection system successfully blocked unauthorized access attempts by initiating automated security lockdowns and triggering real-time alerts.

To enhance linemen safety during high-voltage maintenance, the system's fail-safe mechanisms were thoroughly validated. It featured an intelligent power isolation function that ensured deactivation unless an authorized OTP was entered, reducing the risk of accidental electrocution. With GSM-based authentication and IoT-enabled remote monitoring, access control was further strengthened, limiting panel operations to registered users. Additionally, a tamper-resistant security feature implemented an adaptive lockout mechanism that temporarily restricted access after multiple failed authentication attempts, while simultaneously sending automated alerts to the control centre for immediate security response. Overall, the system significantly improved cybersecurity, reduced operational hazards, and reinforced the reliability of electrical distribution networks.

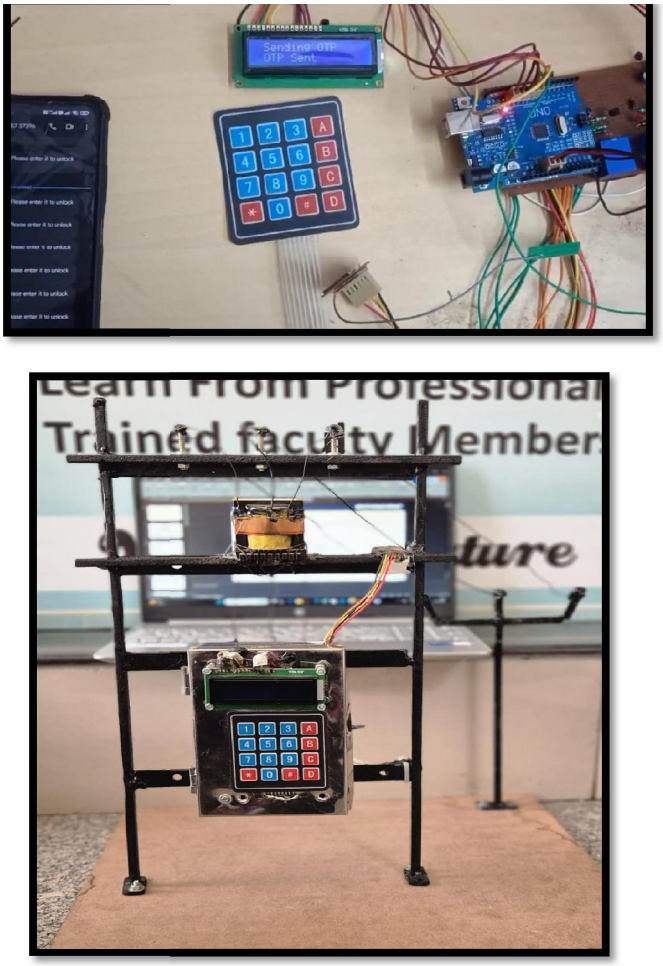


Figure No. 4. Actual Model photo

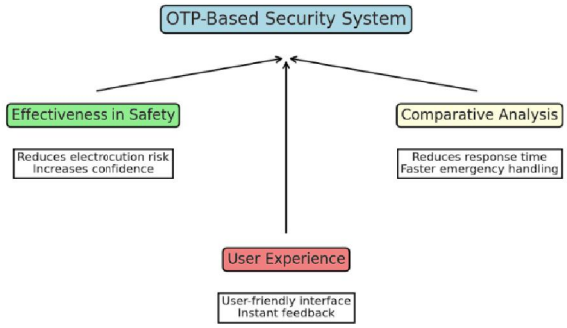
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

4.2 DISCUSSION

Figure No. 4 shows the implementation of this system has greatly enhanced safety by significantly lowering the risk of electrocution and other hazards associated with manual line maintenance. Linemen reported greater confidence in performing their tasks, as the system ensured secure power management during maintenance operations.

When compared to conventional methods that rely on manual coordination between linemen and substations, this system proved to be more efficient by reducing the time required to switch power lines on and off. This improvement is especially crucial in emergency scenarios where rapid response is essential.

Furthermore, feedback gathered from linemen through surveys highlighted the system's intuitive user interface and real-time response mechanisms. These features not only streamlined maintenance operations but also alleviated stress, making the process more efficient and user-friendly.



The flowchart visually represents the impact of the OTP-based security system on safety, efficiency, and user experience. At the top, the system is shown as the central element, branching into three key aspects. The first aspect, Effectiveness in Safety, highlights how the system reduces electrocution risks and increases linemen's confidence by ensuring controlled power management. The second aspect, Comparative Analysis, demonstrates that the system improves response time and facilitates faster power switching, making it more effective than traditional manual communication methods, especially in emergencies. The third aspect, User Experience, emphasizes the system's intuitive interface and instant feedback mechanism, which streamline maintenance operations and reduce stress for linemen. Together, these aspects illustrate how the system enhances security, minimizes risks, and improves overall operational efficiency.

V. CONCLUSION

The OTP-based distribution panel has proven to be highly effective in improving the safety and efficiency of electrical line maintenance. By implementing secure authentication, it ensures that only authorized personnel can manage the power supply, significantly minimizing the risk of electrical accidents. Feedback from users and operational data indicate that this system successfully overcomes critical gaps in traditional safety measures, ultimately providing a safer and more reliable working environment for linemen.

ACKNOWLEDGEMENTS

This Paper, **"OTP-Based Protected Security System for the Distribution Panel for Human Safety,"** was made possible through the generous sponsorship and financial support of **Technosys Control Solution, Nashik, Maharashtra, India**. Their contributions provided the necessary resources for the successful execution of this work. We also extend our sincere gratitude to our mentors, faculty members, and peers for their valuable guidance and continuous support throughout the project.

REFERENCES

[1] *Sunil Magan More, A.P.Choudhari, G.K.Mahajan* Protection Technology for Smart Grid Networks, International Conference on Modelling and Simulation an Engineering and Technology Icmset-2014, 15-16 February, 2014

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, June 2025 Impact Factor: 7.67

[2] Phulare, S., Chougule, A., & Nan, N. (2015). Electrical safety sensor for unskilled technicians in India. *IEEE IAS Joint Industrial and Commercial Power Systems / Petroleum and Chemical Industry Conference (ICPSPCIC)*.

[3] Haque, M. I., Kalaskar, S., Raut, M., Walokar, S., Ingole, G., & Sheikh, N. (2020). Electric lineman safety with password-based circuit breaker. *International Journal of Scientific Research and Science Technology (IJSRST), 5*(7), 2395–602X.

[4] Naik, G. S., Kowsalya, S., Meghana, R. N., & Shana, C. M. (2020). OTP-based lineman security system. *International Journal of Engineering Research & Technology (IJERT), 9*(2).

[5] Manikanta, S. P., Srinivasarao, T., & Lovina, P. A. (2020). Password-based circuit breaker. *International Journal of Engineering Research & Technology (IJERT), 9*(2).

[6] Khandelwal, N., Manglani, T., Singh, G., Kumar, A., & Khatr, D. (2015). Automated load distribution with password-protected circuit breakers. *International Journal of Recent Research and Review, 8*(1).

[7] Mohammadinodoushan, M., Cambou, B., Philabaum, C. R., & Duan, N**.** (2021). Resilient password manager using physical unclonable functions. *IEEE Access, 9*, 17060–17070