IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Anti Sleep Alarm With Driver Safety Using Arduino Uno

[1]Naman Sharma, [2]Niyati Jain, [3]Rishita Rajput, [4]Sujoy Das, [5]Prof.Monika Kapoor

[1234] B.Tech Scholar & [5]Prof. Monika Kapoor

Department of Electronics and Communication,

[1]Lakshmi Narain College of Technology, Bhopal, India

I. Abstract

Driver fatigue is a major cause of road accidents worldwide. Studies suggest that drowsy driving contributes to nearly 20% of serious road crashes. This project proposes a preventive approach: an Anti-Sleep Safety Alarm using Arduino Uno. The device monitors eye movements using an infrared (IR) sensor and activates an alarm when signs of drowsiness are detected. With increased urbanization, long working hours, and vehicular congestion, it becomes imperative to provide technological assistance to drivers to avoid fatigue-related mishaps. The primary motivation behind this system is affordability, ease of use, and effectiveness. As compared to high-end systems based on EEG, camera-based image processing, or AI-based facial analysis, our solution leverages basic electronic components to deliver a robust mechanism. This research details the system design, implementation, testing, and potential for real-world deployment.

II. INTRODUCTION

Drowsy driving remains a major concern in road safety, often leading to serious accidents, injuries, and loss of life. Falling asleep at the wheel can have devastating consequences, making it essential to develop proactive safety measures. This project presents a practical and innovative approach: the design and implementation of an Anti-Sleep Alarm system using Arduino Uno technology, aimed at improving driver alertness and reducing the risk of accidents. The main goal of this system is to effectively monitor signs of fatigue in drivers and provide timely alerts to keep them attentive. Utilizing the Arduino Uno microcontroller in conjunction with key components—including an eyeblink sensor, relay module, buzzer, BO motor with wheels, and a powerful 1-watt red LED—the system is engineered to promote safer driving conditions. This introduction outlines the inspiration behind the project, its core aims, and the hardware used in its construction. By focusing on the urgent need to combat driver fatigue, the proposed solution holds promise in making roads safer and preventing incidents caused by drowsiness behind the wheel.

Problem Statement

Falling asleep while driving is a major cause of road accidents, often resulting in serious injuries, loss of life, and property damage. Most existing vehicle safety systems do not actively monitor a driver's state of alertness, making it difficult to prevent accidents caused by fatigue. There is a strong need for a cost-effective and real-time solution that can identify early signs of drowsiness and alert the driver before it's too late. This project proposes the development of a driver safety system using the Arduino Uno platform, which aims to detect fatigue symptoms—such as eye closure—and trigger immediate alerts to help drivers stay attentive and safe on the road.

TECHNOLOGY STACK

- **Circuit Design & Simulation:**

  o Proteus

Purpose: Electronic circuit design, simulation, and PCB layout design. Key Features: Real-time simulation, microcontroller support (Arduino, PIC, AVR, ARM), PCB design, 3D visualization, virtual instruments like oscilloscopes and logic analyzers.

- **PCB Layout Design:**

  o Circuit Wizard

Purpose: PCB layout design from schematic creation to board manufacturing. Key Features: Auto-routing, manualrouting, design rule checking (DRC), 3D visualization, error-free PCB designs, Gerber file export.

- Programming:

  o Arduino IDE

Purpose: Programming microcontrollers (Arduino). Key Features: Syntax highlighting, built-in examples, supports multiple Arduino boards (Uno, Mega, Nano), libraries for extended functionality, one-click upload, serial monitor for debugging.

- **Sensors:**

O **IR Sensor** Key Features: Detection of proximity of a person or object. • Message sending: o Sim Module 900A Purpose: Sending OTP to the mobile Device. Key Features: Sends the message to the user's mobile device .

- **Peripheral Devices:**

  o 4 X 4 Keypad

Purpose: To insert the OTP. Key Features: Acts as an input device allowing the user to enter the OTP.

o LCD Display

Purpose: User Interface for Displaying the messages.

Key Features: Used for Human-Machine Interaction for displaying the messages

Purpose: Proximity sensor.

IV. PROPOSED SOLUTION

The goal of the proposed system is to modernize door security by replacing traditional locks and static passcodes with a dynamic OTP (One-Time Password) verification method. Unlike conventional locking systems, which are prone to risks such as lost keys, password leaks, or unauthorized duplication, this system offers a more secure and user-friendly alternative by using a unique, time-bound OTP for every access attempt.

At the core of the design is the **Arduino UNO**, which acts as the central controller. It coordinates the communication between input devices, the GSM module, display units, and the locking mechanism. The main features and modules of the system include:

A. OTP Generation & Delivery

When access is initiated — usually triggered by an **IR sensor** — the Arduino generates a random 4-digit OTP. This code is then sent to the user's registered mobile number using the **SIM900A GSM module**. As the OTP is valid for only one session, it ensures enhanced security by preventing reuse or interception.

B. Authentication Process

The user enters the received OTP through a **4x4 keypad**. The Arduino checks this input against the stored OTP in its memory. If the input matches, a digital signal is sent to unlock the door by energizing the **solenoid lock**.

C. User Feedback

A **16x2 I2C LCD display** is used to communicate system statuses to the user. Messages like *"OTP Sent"*, *"Enter OTP"*, *"Access Granted"*, or *"Invalid OTP"* keep the user informed throughout the process, improving the interaction experience.

D. Flexibility and Integration

This system is modular and can easily be expanded to include other layers of security, such as **fingerprint scanners**, **RFID**, or **CCTV surveillance**. The framework also supports upgrades like **cloud-based OTP logging** and multi-user handling, making it ideal for home, office, or industrial setups.

E. Cost-Effectiveness

The hardware used in this project, including the Arduino, GSM module, keypad, and display, are all cost-efficient and readily available. This makes the system not only secure but also accessible for widespread deployment in both residential and commercial environments.

V. METHODOLOGY

The core of the system's authentication process revolves around generating a unique four-digit OTP (One-Time Password) using the **Arduino microcontroller**. Once generated, the OTP is temporarily stored in the Arduino's memory (RAM) and sent to the user's registered mobile number via the **GSM module** (SIM900A).

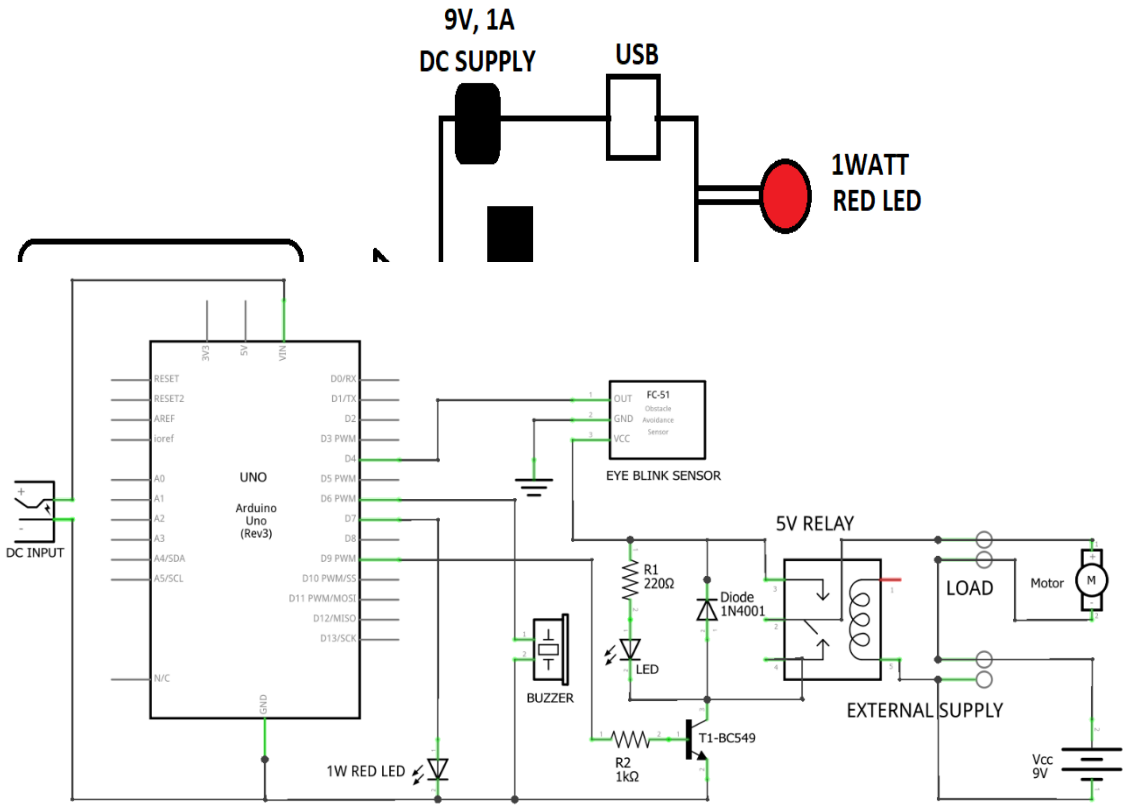
The user then enters the received OTP using a **4x4 keypad** connected to the system. The Arduino continuously monitors input from the keypad and compares it against the OTP stored in memory.

If the entered OTP matches the one stored, the Arduino sends a signal to activate the connected hardware—typically a **solenoid lock**—which unlocks the door.

Additionally, a **16x2 LCD display (I2C enabled)** provides real-time feedback throughout the process. It informs the user when the OTP is sent, prompts for OTP input, and indicates whether access has been granted or denied based on the entered code.

This method ensures a secure and responsive user experience while maintaining simplicity in implementation.

BLOCK DIAGRAM:



FLOW CHART

VIII. FUTURE SCOPE

Although the current OTP-based smart door lock system effectively improves upon traditional security methods, there is still a lot of room for enhancement and new features that can boost its usability, reliability, and overall performance. The following ideas highlight the potential future developments of this system:

1. **Biometric Integration**

Future versions can include fingerprint or facial recognition sensors to enable multi-factor authentication. This combination of OTP and biometrics will significantly strengthen access control and reduce the risk of unauthorized entry.

2. **IoT and Cloud Connectivity**

Connecting the system to the Internet of Things (IoT) will enable users to manage access remotely using a mobile app or web interface. Additionally, shifting OTP generation and verification to cloud platforms can improve scalability and flexibility.

3. **Mobile Application**

A custom-built mobile app could allow users to receive OTPs via push notifications, manage access permissions, review entry history, and get real-time alerts for suspicious activity or failed access attempts.

4. **Access Logs and Analytics**

By maintaining a record of each access attempt, the system can provide detailed entry logs. These logs can be used for analysis, monitoring, or even generating security reports—whether stored locally or on the cloud.

5. **Power Backup and Emergency Access**

To ensure the system functions during power failures, backup solutions such as rechargeable batteries or solar panels can be introduced. Emergency override features, like manual keys or reset codes, can also be added for extra reliability.

6. **Multi-User and Role-Based Access**

The design can be expanded to support multiple users with different permission levels. For example, admins could manage system settings, while guests are granted temporary or limited access.

7. **Secure Data Transmission**

To protect the system against hacking or data interception, future implementations should include robust encryption techniques like AES or RSA, ensuring all user credentials and OTP data are transmitted securely.

By integrating these features, the OTP-based door locking system can grow into a smart, future-ready solution tailored for homes, offices, and industrial facilities where safety and controlled access are paramount.

Conclusion

This paper presents the design and implementation of a secure and budget-friendly OTP-based door locking system, built around the Arduino UNO and GSM technology. By replacing static passwords and traditional keys with dynamic, single-use codes, the system significantly reduces common security risks like unauthorized duplication or key loss.

Through the integration of key components—including a GSM module for communication, a keypad for input, an LCD for feedback, and a solenoid lock for physical access control—the setup ensures real-time, reliable, and user-friendly operation. The results validate the system's ability to deliver enhanced security, adaptability, and convenience over standard locking systems.

Designed with scalability in mind, this solution is highly applicable in environments requiring controlled access, such as smart homes, offices, and secure zones. Its modular nature also opens the door for future upgrades like biometric verification, cloud-based management, and support for multiple users with role-specific permissions.

In conclusion, the proposed system offers an effective and modern alternative for access control, blending affordability with improved safety and functionality.

References

1. Mohammed, S. A., & Alkeelani, A. H. (2019). *Locker Security System Using Keypad and RFID*. Proceedings of the International Conference on Computer Science and Renewable Energies (ICCSRE), pp. 1–5.
2. Jalapur, S., & Maniya, A. (2017). *Door Lock System Using Cryptographic Algorithm Based on IoT*. International Journal of Modern Trends in Engineering and Research (IJMTER), Vol. 4, Issue 2. ISSN (Online): 2349-9745.
3. Ahtsham, M., Yan, H., & Ali, U. (2017). *IoT-Based Door Lock Surveillance System Using Cryptographic Algorithms*. International Journal of Current Multidisciplinary Studies (IJCMES), Special Issue 1. ISSN: 2455-5304.
4. Hossain, M. A., Hossain, N., Shahid, A., & Rahman, S. M. S. (2016). *Security Solution of RFID Card Through Cryptography*. Presented at the International Conference on Explorations and Innovations in Engineering and Technology.
5. Nehete, P. R., & Rane, K. P. (2016). *A Paper on OTP-Based Door Lock Security System*. International Journal for Emerging Trends in Engineering and Management Research (IJETEMR), Vol. II, Issue II, June 21. ISSN: 2455-7773.