International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

IOT-BASED SMART KITCHEN WITH ENHANCED AND AUTOMATED SAFETY MEASURES

[1] Dr. M. Senthil Kumar, [2] Teppala Manoj, [3] V Sirisha, [4] Katakam Bhavyasree, [5] Chikatla Srikar, [6] Dr S Venkata Achuta Rao
[1]Principal, [2345] B. Tech Students, [6] Professor
[12345]Department of Electronics and Communication Engineering
[6]Department of Computer Science and Engineering
[12345]Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, 501510, Telangana, India
[6]Sree Dattha Institute of Engineering and Science, Sheriguda, Hyderabad, Telangana,India-501510,
sreedatthaachyuth@gmail.com

ABSTRACT

The IoT-Based Smart Kitchen with Enhanced and Automated Safety Measures is a modern solution designed to improve kitchen safety, efficiency, and convenience through intelligent automation and IoT connectivity. Kitchen accidents, such as gas leaks, fire hazards, and appliance malfunctions, pose significant risks to households. This system integrates sensors, microcontrollers, and IoT technologies to monitor cooking appliances, detect hazardous conditions, and take preventive actions automatically. Gas leakage is detected using MQ2 or MQ5 gas sensors, while smoke detection is achieved via smoke sensors. Temperature sensors monitor stovetop and oven temperatures to prevent overheating and fire incidents. Smart relays connected to appliances enable automatic switching OFF in hazardous conditions. Motion sensors or proximity sensors detect human presence to ensure operational safety. The ESP32/ESP8266 microcontroller processes sensor inputs and communicates with cloud servers using MQTT or HTTP protocols. Real-time alerts and notifications are sent to users via mobile apps or dashboards in the event of unsafe conditions, gas leaks, or smoke detection. The dashboard provides live monitoring of appliance status, historical data on safety incidents, and remote control for appliances. IoT integration allows users to control kitchen devices from anywhere, enhancing convenience and operational control. Safety mechanisms include automatic shutdown of gas stoves or ovens in emergencies, alert notifications, and integration with smart locks for kitchen access. Data analytics enables trend analysis, predictive maintenance, and identification of recurring hazards. Modular design allows expansion to include additional smart appliances, cameras, or sensors. Security is ensured through encrypted communication, authentication, and device-specific credentials. Overall, this IoT-based smart kitchen system reduces risks, prevents accidents, enhances operational efficiency, and provides a safer cooking environment for households. The system combines embedded electronics, IoT connectivity, cloud monitoring, and automated safety mechanisms to create a modern, intelligent, and user-friendly kitchen environment.

I. INTRODUCTION

1.1 Introduction

The kitchen is one of the most essential and frequently used areas in any household. It involves continuous interaction with gas cylinders, electrical appliances, high temperatures, and flammable substances. Due to these factors, kitchens are also one of the most accident-prone environments in residential buildings. Incidents such as gas leakage, fire outbreaks, smoke accumulation, and overheating of cooking appliances can lead to severe injuries, loss of life, and property damage.

With the rapid growth of technology, traditional kitchens are gradually evolving into smart kitchens that focus on automation, safety, and efficiency. The Internet of Things (IoT) plays a vital role in this transformation by enabling devices to communicate, monitor conditions, and take automated decisions without constant human intervention.

The **IoT-Based Smart Kitchen with Enhanced and Automated Safety Measures** is designed to create a safer and more intelligent kitchen environment. This system continuously monitors hazardous parameters such as gas leakage, smoke, temperature, and human presence using various sensors. In the event of any abnormal or dangerous condition, the system automatically performs safety actions such as turning OFF appliances and sending real-time alerts to the user through IoT platforms.

1.2 Motivation for the Project

The motivation behind developing this project comes from real-life incidents and increasing concerns about kitchen safety. Many kitchen accidents occur due to simple human mistakes such as forgetting to turn off the gas stove, leaving cooking unattended, or delayed response during emergencies. These issues become even more critical in households with elderly people, children, or working professionals who may not always be present in the kitchen.

Existing safety devices like gas alarms or smoke detectors are limited in functionality. They only provide alerts but cannot take corrective actions or inform users remotely. With IoT integration, it becomes possible to design a system that not only detects hazards but also responds intelligently and proactively.

This project aims to bridge the gap between traditional safety mechanisms and modern smart automation by providing a reliable, affordable, and scalable smart kitchen safety solution

NEED OF THE PROJECT

1. **Increasing Kitchen Accidents**
   Modern households experience a high number of kitchen-related accidents such as gas leaks, fires, and overheating of appliances. These incidents often occur due to human negligence, busy lifestyles, or delayed response. A smart and automated safety system is essential to detect hazards early and prevent accidents before they become life-threatening.
2. **Lack of Real-Time Monitoring**
   Traditional kitchen safety devices operate independently and provide only local alerts. They do not offer real-time monitoring or remote access when users are away from home. There is a strong need for an IoT-enabled system that continuously monitors kitchen conditions and provides instant alerts to users and caregivers from any location.
3. **Human Dependency and Error**
   Many accidents occur due to forgetfulness, such as leaving gas stoves ON or overheating appliances. Manual supervision is unreliable, especially for elderly people or individuals with disabilities. An automated smart kitchen system reduces dependency on human intervention and minimizes errors through intelligent control.
4. **Rising Demand for Smart Homes**
   With the growth of smart home technologies, users expect intelligent systems that enhance safety, convenience, and energy efficiency. Integrating kitchen safety into smart home ecosystems is necessary to meet modern lifestyle demands.
5. **Need for Preventive Action, Not Just Alerts**
   Existing systems mostly focus on detection and alerting but do not take preventive actions such as turning OFF appliances or gas supply. The proposed system fulfills the need for automated preventive mechanisms that actively reduce risk.
6. **Remote Healthcare and Elderly Care Support**
   Elderly individuals and patients living alone require continuous safety monitoring. The smart kitchen system supports caregivers by providing remote

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

alerts and usage data, ensuring safer independent living.

7. **Data Logging and Safety Analysis**
   There is a growing need to analyze safety incidents to improve future prevention. Cloud-based data logging enables long-term analysis of hazardous events, helping improve system reliability and user awareness.

1.3 Need for Smart Kitchen Safety Systems

The need for an IoT-based smart kitchen system is driven by several important factors:

- **Increasing domestic accidents:** A significant number of household accidents originate from kitchen-related hazards.
- **Human negligence:** Forgetfulness and lack of attention are common causes of gas leaks and fire accidents.
- **Lack of automation:** Traditional kitchens rely heavily on manual supervision.
- **Busy lifestyles:** Modern lifestyles reduce the ability to constantly monitor cooking activities.
- **Elderly and child safety:** Automated systems help protect vulnerable individuals.
- **Remote monitoring requirement:** Users need to be informed about emergencies even when they are not at home.
- **Smart home adoption:** Growing interest in smart homes demands intelligent kitchen solutions.

The proposed system fulfills these needs by combining automation, IoT communication, and intelligent decision-making.

1.4 Problem Statement

In conventional kitchen environments, safety management is largely manual and reactive. Gas leakage, smoke generation, or overheating are often detected only after they reach dangerous levels. Existing safety systems operate independently and lack coordination, remote accessibility, and automatic control capabilities.

There is a lack of an integrated system that can continuously monitor kitchen safety parameters, automatically control appliances during emergencies, and notify users in real time using IoT technology. This limitation increases the risk of severe accidents and delays preventive action.

Hence, there is a strong requirement for an IoT-based smart kitchen system that ensures proactive safety monitoring, automated response, and remote alerting to minimize kitchen-related risks.

1.5 Objectives of the Project

The primary objectives of the proposed system are:

- To design an IoT-based smart kitchen safety system.
- To detect gas leakage using gas sensors such as MQ2 or MQ5.
- To monitor smoke levels using smoke sensors.
- To measure temperature variations using temperature sensors.
- To automatically switch OFF appliances during unsafe conditions.
- To provide real-time alerts and notifications to users.
- To enable remote monitoring through cloud platforms.
- To enhance safety and reduce kitchen accidents.
- To support future expansion and scalability.

1.6 Scope of the Project

The scope of this project defines the boundaries and functionality of the smart kitchen system. The project focuses on safety-oriented automation rather than full kitchen automation.

The scope includes:

- Continuous monitoring of gas leakage, smoke, and temperature.
- Automatic control of kitchen appliances using relay modules.

- IoT connectivity through ESP32/ESP8266 microcontrollers.
- Cloud-based monitoring and alert notifications.
- Data storage for historical safety analysis.
- Integration with mobile or web dashboards.
- Modular design for future sensor or appliance expansion.
- Application in homes, apartments, hostels, and assisted living facilities.

The project does not include advanced cooking automation or robotic cooking systems.

II. LITERATURE SURVEY

2.1 Introduction

IoT in Smart Home Kitchens

IoT technology has enabled smart home appliances with automated control and monitoring. Traditional kitchens rely on manual operation of appliances, posing safety risks such as gas leaks, fires, and accidental overheating. Studies show that IoT-enabled kitchen appliances improve safety, energy efficiency, and convenience. Sensors for gas, temperature, smoke, and motion are integrated with microcontrollers to enable real-time monitoring and automatic actuation. Research highlights the use of cloud platforms for remote control, monitoring, and historical data analysis. IoT dashboards provide live status updates, alerts, and operational control to users. Automated systems reduce human errors and enhance household safety.

Safety Mechanisms in Smart Kitchens

Kitchen safety is a major concern due to fire hazards, gas leaks, and unattended cooking. Existing studies demonstrate that sensors such as MQ series gas sensors, smoke detectors, and temperature sensors are effective in detecting hazardous conditions. Automated relays and actuators can switch off appliances or gas valves when unsafe conditions are detected. Motion and proximity sensors ensure that appliances operate only when users are present, preventing accidental operation. IoT integration enables sending alerts to mobile devices, allowing users to respond immediately. Research emphasizes the importance of integrating multiple sensors for accurate hazard detection and reducing false alarms.

Microcontroller-Based IoT Systems in Kitchen Automation

ESP32 and ESP8266 microcontrollers are widely used for IoT-based smart kitchen systems due to their Wi-Fi connectivity, low power consumption, and real-time processing capabilities. Studies show that microcontrollers can monitor multiple sensors, control relays, and communicate with cloud platforms efficiently. OTA updates simplify firmware upgrades, while secure protocols like MQTT ensure safe data transmission. Microcontroller-based systems allow modular expansion for additional appliances, sensors, or smart devices. Real-time dashboards provide users with live monitoring, alerts, historical logs, and analytics. Integration with mobile apps ensures remote control and supervision, enhancing safety and convenience.

In recent years, the rapid growth of embedded systems and Internet of Things (IoT) technologies has paved the way for intelligent and connected home environments. Among various applications, kitchen safety has emerged as a critical area of research due to the high frequency of domestic accidents involving gas leaks, fire hazards, and appliance malfunctions. Traditional kitchen safety solutions, such as standalone gas detectors and smoke alarms, function independently and lack intelligent interaction with users or automated preventive measures. The literature reveals that integrating IoT with embedded sensing and intelligent control can significantly enhance kitchen safety and usability. This chapter reviews existing research works on smart kitchen systems, IoT-based monitoring, automated safety mechanisms, and related technologies,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

highlighting their contributions and limitations, and setting the stage for the proposed system.

2.2 Traditional Kitchen Safety Systems

Early approaches to kitchen safety relied predominantly on manual or discrete devices such as mechanical gas regulators, audio alarms, flame failure devices, and smoke detectors. These systems primarily acted as warning mechanisms rather than preventive solutions. Researchers like Gupta and Singh (2018) noted that while these devices provide essential alerts, they often fail to intervene during emergencies or inform users remotely. Moreover, such systems are isolated and lack integration with modern communication networks, making them ineffective in scenarios where users are away from home. A study by Sharma et al. (2017) highlighted that conventional kitchen safety mechanisms cannot automatically control appliances or mitigate risks proactively.

2.3 Early Smart Kitchen Systems

The concept of a "smart kitchen" initially focused on convenience, energy efficiency, and remote monitoring of appliances. Early research by Lee et al. (2019) presented embedded systems that automatically switch OFF stoves or ovens based on timer functions or user input. However, these systems lacked real-time environmental sensing and did not consider hazardous scenarios like gas leakage or smoke. Efforts by Rao and Patel (2020) introduced microcontroller-based kitchen automation, but these were limited to scheduling and remote control functionality without integrated safety measures. These implementations laid the groundwork for more sophisticated designs but emphasized that safety was still an underdeveloped aspect.

2.4 IoT Integration in Home Safety

The emergence of IoT transformed domestic safety systems by enabling networked devices to communicate and respond intelligently. IoT frameworks allow sensors, actuators, and control units to interact over wireless networks, with cloud platforms providing remote access and data analytics. Research by Zanella et al. (2014) and Gubbi et al. (2013) established foundational IoT architectures suitable for smart environments. Subsequently, studies such as those by Patel and Mehta (2018) explored IoT-enabled safety systems for homes. They demonstrated real-time monitoring and alerting using cloud dashboards and mobile notifications.

In kitchen environments, IoT facilitates sensor data collection, real-time anomaly detection, and automated response. Unlike traditional solutions, IoT systems can transmit alerts to users regardless of their physical location, supporting remote intervention. However, many early IoT implementations focused on single parameters such as temperature or motion detection, without holistic safety strategies.

2.5 Sensor Technologies for Kitchen Safety

Effective kitchen monitoring requires a combination of multiple sensing technologies. Gas sensors like MQ2, MQ5, and semiconductor detectors are widely used to detect combustible and toxic gas concentrations. Studies by Singh et al. (2020) highlighted the effectiveness of MQ-series sensors in real-time gas leak detection. Smoke sensors and optical particle detectors are employed for fire detection. Research by Chen and Huang (2019) showed that smoke sensors combined with temperature data provide robust early warning for fire scenarios.

Temperature monitoring is essential for detecting overheating incidents. Thermocouples, digital temperature sensors, and infrared temperature sensors have been integrated into various smart home projects to observe appliance temperatures and prevent thermal hazards. A study by Kumar and Dixit (2021) presented a system combining gas, smoke, and temperature sensors for comprehensive safety monitoring but did not include automated appliance control or IoT connectivity.

III. SYSTEM ANALYSIS

System analysis is a crucial step in understanding the strengths and limitations of existing kitchen safety mechanisms and defining the improvements offered by the proposed IoT-based smart kitchen system. It involves examining current safety approaches, identifying deficiencies, and determining how a modern automated and connected solution can enhance safety, convenience, and efficiency.

3.1 Existing System

Traditional kitchens rely heavily on human supervision and manual safety mechanisms to prevent accidents. Safety devices such as gas leak detectors, smoke alarms, and fire extinguishers exist independently but are limited in scope and functionality.

EXISTING METHOD

Traditional kitchen setups rely on manual monitoring of appliances and gas usage. Users are responsible for turning off stoves, ovens, and other devices. Accidents such as gas leaks, fire, or overheating are often only detected after damage occurs. Some basic electronic devices exist, like standalone smoke detectors or gas alarms, but they lack automation and integration with appliances. Manual monitoring is prone to human error, and emergency alerts are delayed. Data logging, historical analysis, and remote monitoring are generally absent. Current kitchens do not provide adaptive control, automated safety shutdown, or IoT-enabled monitoring. As a result, the risk of accidents remains high, and operational efficiency is limited.

3.1.1 Features of Existing Systems

- Manual gas stove and appliance operation
- Conventional standalone gas detectors
- Smoke alarms with local audio alerts
- Manual monitoring of temperature and fire hazards
- No integration with internet or mobile platforms
- Isolated operation of each safety device

In conventional kitchens, hazards such as gas leakage or smoke generation are typically noticed only when they reach dangerous levels or when an individual is present to detect them. This makes traditional kitchen safety highly dependent on human attention and presence, which is not always reliable.

3.1.2 Disadvantages of Existing Systems

1. **High Human Dependency**
   The existing systems require constant user supervision. Forgetting to turn off appliances or leaving cooking unattended can easily lead to accidents.
2. **Reactive, Not Preventive**
   Conventional gas detectors or smoke alarms only provide alerts but do not take preventive actions such as shutting off the gas supply or switching OFF appliances automatically.
3. **No Remote Monitoring**
   Users cannot monitor kitchen conditions while away from home. In case of emergencies, they are unaware until it is too late.
4. **Delayed Emergency Response**
   Manual intervention leads to slower responses, increasing the severity of accidents.
5. **Independent and Isolated Devices**
   Gas, smoke, and temperature sensors work separately without centralized control or integration, reducing overall efficiency.
6. **No Data Storage or Analysis**
   Existing systems do not maintain historical logs, making it impossible to analyze safety incidents or identify recurring hazards.
7. **Limited Support for Vulnerable Users**
   Elderly, disabled, or single-person households cannot rely on manual safety mechanisms alone, increasing risk.
8. **Limited Scalability**
   Conventional safety devices cannot easily

integrate additional sensors or smart appliances.

These limitations highlight the need for a comprehensive, intelligent, and automated kitchen safety solution.

3.2 Proposed System

The IoT-Based Smart Kitchen with Enhanced and Automated Safety Measures addresses all shortcomings of traditional systems. It provides a holistic safety solution by integrating multiple sensors, IoT communication, automated appliance control, and cloud monitoring.

PROPOSED METHOD

The proposed IoT-Based Smart Kitchen integrates sensors, microcontrollers, and cloud connectivity for automated safety and monitoring. Gas sensors (MQ2/MQ5) detect leaks, smoke sensors detect fire, and temperature sensors monitor appliance overheating. ESP32/ESP8266 microcontrollers process sensor data and trigger relays to automatically switch off gas stoves, ovens, or other appliances in hazardous conditions. Motion and proximity sensors ensure safe operation when users are present. Real-time alerts are sent via mobile app or dashboard notifications for immediate response. Cloud integration allows remote monitoring, historical data tracking, and analytics. Dashboards display live appliance status, safety alerts, and operational logs. Modular design allows integration of additional smart appliances or sensors. Security mechanisms include encrypted communication, device authentication, and restricted access to prevent unauthorized control. The system reduces human error, prevents accidents, enhances operational efficiency, and provides a safer, intelligent kitchen environment.

3.2.1 Features of the Proposed System

- Gas leak detection using MQ2 or MQ5 sensors
- Smoke detection using smoke sensors
- Temperature monitoring using temperature sensors (DHT11, LM35, or DS18B20)
- ESP32 / ESP8266 microcontroller for data processing
- Relay modules to automatically switch OFF appliances
- Wi-Fi-enabled IoT communication using MQTT/HTTP
- Cloud storage for historical data
- Real-time dashboards for monitoring
- Mobile notifications and alerts
- Modular design for adding more sensors and appliances
- Encrypted communication for security

3.2.2 Advantages of the Proposed System

1. **Automated Safety Actions**
   In hazardous situations, appliances and gas supply are automatically turned OFF, reducing accident risks.
2. **Real-Time Monitoring**
   Continuous monitoring ensures early detection of gas leaks, smoke, or overheating appliances.
3. **Remote Monitoring**
   Users can check appliance status and safety conditions from anywhere using a mobile or web interface.
4. **Immediate Alerts**
   Instant notifications through mobile apps, buzzer alarms, and LED indicators ensure timely intervention.
5. **Reduced Human Error**
   Automation minimizes risks caused by forgetfulness or inattention.
6. **Data Logging and Analysis**
   All events and sensor data are stored in the cloud for historical analysis, trend identification, and system improvement.
7. **Enhanced Safety for Vulnerable Users**
   Supports independent living for elderly, disabled, or busy individuals.
8. **Scalability and Modular Design**
   Future integration with additional sensors, smart appliances, or AI-based predictive safety algorithms is possible.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

9. **Energy Efficiency**
   Automated switching reduces energy wastage and prevents appliance damage from overheating.
10. **Secure Communication**
    Encrypted data transmission prevents unauthorized access to system controls.

IV. HARDWARE

4.1 ARDUINO UNO

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

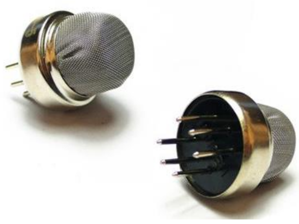
The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. Uno board has a resistor pulling the 8U2 HWB line to ground, making it easier to put into DFU mode.Arduino board has the following new features:

- 1.0 pinout: added SDA and SCL pins that are near to the AREF pin and two other new pins placed near to the RESET pin, the IOREF that allow the shields to adapt to the voltage provided from the board. In future, shields will be compatible both with the board that use the AVR, which operate with 5V and with the Arduino Due that operate with 3.3V. The second one is a not connected pin, that is reserved for future purposes.
- Stronger RESET circuit.
- Atmega 16U2 replace the 8U2.

"Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform; for a comparison with previous versions, see the index of Arduino boards.

Fig: ARDUINO UNO

MQ2- SENSOR



DESCRIPTION

MQ2 flammable gas and smoke sensor detects the concentrations of combustible gas in the air and outputs its reading as an analog voltage. The sensor can measure concentrations of flammable gas of 300 to 10,000 ppm. The sensor can operate at temperatures from -20 to 50°C and consumes less than 150 mA at 5 V.

Connecting five volts across the heating (H) pins keeps the sensor hot enough to function correctly. Connecting five volts at either the A or B pins causes the sensor to emit an analog voltage on the other pins. A resistive load between the output pins and ground sets the sensitivity of the detector. Please note that the picture in the datasheet for the top configuration is wrong. Both configurations have the same pin out consistent with the bottom configuration. The resistive load should be calibrated for your particular application using the equations in the datasheet, but a good starting value for the resistor is 20 kΩ.

DHT11 Sensor

DHT11 Sensor and Its Working

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Humidity is the measure of water vapour present in the air. The level of humidity in air affects various physical, chemical and biological processes. In industrial applications, humidity can affect the business cost of the products, health and safety of the employees. So, in semiconductor industries and control system industries measurement of humidity is very important. Humidity measurement determines the amount of moisture present in the gas that can be a mixture of water vapour, nitrogen, argon or pure gas etc… Humidity sensors are of two types based on their measurement units. They are a relative humidity sensor and Absolute humidity sensor. DHT11 is a digital temperature and humidity sensor.

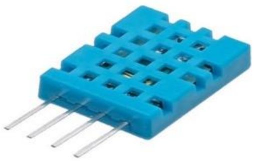
Working Principle of DHT11 Sensor

DHT11 sensor consists of a capacitive humidity sensing element and a thermistor for sensing temperature. The humidity sensing capacitor has two electrodes with a moisture holding substrate as a dielectric between them. Change in the capacitance value occurs with the change in humidity levels. The IC measure, process this changed resistance values and change them into digital form.

For measuring temperature this sensor uses a Negative Temperature coefficient thermistor, which causes a decrease in its resistance value with increase in temperature. To get larger resistance value even for the smallest change in temperature, this sensor is usually made up of semiconductor ceramics or polymers.

The temperature range of DHT11 is from 0 to 50 degree Celsius with a 2-degree accuracy. Humidity range of this sensor is from 20 to 80% with 5% accuracy. The sampling rate of this sensor is 1Hz .i.e. it gives one reading for every second. DHT11 is small in size with operating voltage from 3 to 5 volts. The maximum current used while measuring is 2.5mA.

DHT11 sensor has four pins- VCC, GND, Data Pin and a not connected pin. A pull-up resistor of 5k to 10k ohms is provided for communication between sensor and micro-controller.



WIFI:

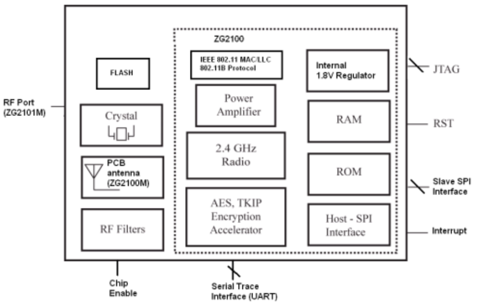
Description

The ZG2100M & ZG2101M modules are low-power 802.11b implementations. All RF components, the baseband and the entirety of the 802.11 MAC reside on-module, creating a simple and cost-effective means to add Wi-Fi connectivity for embedded devices. The module(s) implement a high-level API, simplifying design implementation and allowing the ZG2100M or ZG2101M to be integrated with 8- and 16-bit host microcontrollers.

Features

- Single-chip 802.11b including MAC, baseband, RF and power amplifier
- Data Rate: 1 & 2 Mbps
- 802.11b/g/n compatible
- Low power operation
- API for embedded markets, no OS required
- PCB or external antenna options
- Hardware support for AES and RC4 based ciphers (WEP, WPA, WPA2 security)
- SPI slave interface with interrupt
- Single 3.3V supply, operates from 2.7V to 3.6V (see section 5)
- 21mm x 31mm 36-pin Dual Flat pack PCB SM Package
- Wi-Fi Certified, RoHS and CE compliant
- FCC Certified (USA, FCC ID: W7O-ZG2100-ZG2101)
- IC Certified (IC: 8248A-G21ZEROG)
- Fully compliant with EU & meets the R&TTE Directive for Radio Spectrum

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



Alphanumeric LCD

Liquid Crystal Display also called as LCD is very helpful in providing user interface as well as for debugging purpose. The most commonly used Character based LCDs are based on Hitachi's HD44780 controller or other which are compatible with HD44580. The most commonly used LCDs found in the market today are 1 Line, 2 Line or 4 Line LCDs which have only 1 controller and support at most of 80 characters, whereas LCDs supporting more than 80 characters make use of 2 HD44780 controllers.

Pin Description

BUZZER

What is a Buzzer: Working & Its Applications

There are many ways to communicate between the user and a product. One of the best ways is audio communication using a buzzer IC. So during the design process, understanding some technologies with configurations is very helpful. So, this article discusses an overview of an audio signaling device like a beeper or a buzzer and its working with applications.

What is a Buzzer?

An audio signaling device like a beeper or buzzer may be electromechanical or piezoelectric or mechanical type. The main function of this is to convert the signal from audio to sound. Generally, it is powered through DC voltage and used in timers, alarm devices, printers, alarms, computers, etc. Based on the various designs, it can generate different sounds like alarm, music, bell & siren.

RELAYS

What is a relay?

We know that most of the high end industrial application devices have relays for their effective working. Relays are simple switches which are operated both electrically and mechanically. Relays consist of a n electromagnet and also a set of contacts. The switching mechanism is carried out with the help of the electromagnet. There are also other operating principles for its working. But they differ according to their applications. Most of the devices have the application of relays.

Why is a relay used?

The main operation of a relay comes in places where only a low-power signal can be used to control a circuit. It is also used in places where only one signal can be used to control a lot of circuits. The application of relays started during the invention of telephones. They played an important role in switching calls in telephone exchanges. They were also used in long distance telegraphy. They were used to switch the signal coming from one source to another destination.

Relay Design

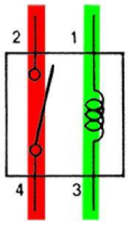
There are only four main parts in a relay. They are

- Electromagnet
- Movable Armature
- Switch point contacts
- Spring

Relay Basics

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

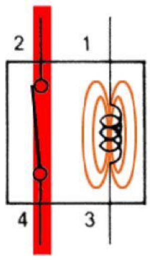
The basics for all the relays are the same. Take a look at a 4 – pin relay shown below. There are two colours shown. The green colour represents the control circuit and the red colour represents the load circuit. A small control coil is connected onto the control circuit. A switch is connected to the load. This switch is controlled by the coil in the control circuit. Now let us take the different steps that occour in a relay.



relay operation

- **Energized Relay (ON)**

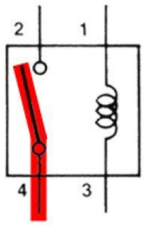
As shown in the circuit, the current flowing through the coils represented by pins 1 and 3 causes a magnetic field to be aroused. This magnetic field causes the closing of the pins 2 and 4. Thus the switch plays an important role in the relay working. As it is a part of the load circuit, it is used to control an electrical circuit that is connected to it. Thus, when the relay in energized the current flow will be through the pins 2 and 4.



Energized Relay (ON)

- **De – Energized Relay (OFF)**

As soon as the current flow stops through pins 1 and 3, the switch opens and thus the open circuit prevents the current flow through pins 2 and 4. Thus the relay becomes de-energized and thus in off position.



De-Energized Relay (OFF)

V. METHODOLOGY & IMPLEMENTATIONS

The methodology describes the systematic approach used to design and implement the IoT-Based Smart Kitchen System. It includes the hardware and software setup, data flow, sensor integration, cloud connectivity, and automated control mechanisms.

5.1 Block Diagram and Its Working

5.1.1 Block Diagram

The block diagram of the proposed smart kitchen system consists of the following major components:

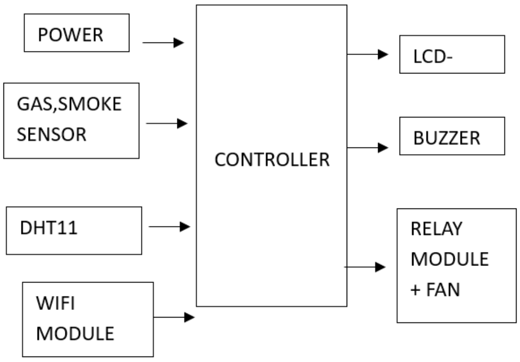
1. **Sensors**
   - **Gas Sensor (MQ2/MQ5):** Detects combustible gas leakage.
   - **Smoke Sensor:** Detects smoke generated from fire or overheating.
   - **Temperature Sensor (DHT11/LM35/DS18B20):** Monitors stovetop and appliance temperature.
   - **Motion/Proximity Sensor:** Detects human presence in the kitchen to ensure operational safety.
2. **Microcontroller**
   - **ESP32/ESP8266:** Acts as the central processing unit, receiving data from all sensors and making decisions based on predefined thresholds.
3. **Actuators/Control Devices**
   - **Relay Modules:** Control appliances and gas valves automatically.
   - **Buzzer and LED Indicators:** Provide instant audible and visual alerts.
4. **IoT & Cloud Connectivity**

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- **Wi-Fi Module:** Sends real-time data to the cloud.
- **Cloud Dashboard:** Stores historical data, visualizes real-time metrics, and provides remote access.

5. **User Interface**
    - **Mobile App / Web Dashboard:** Allows users to monitor appliance status, receive alerts, and control kitchen devices remotely.

BLOCK DIAGRAM

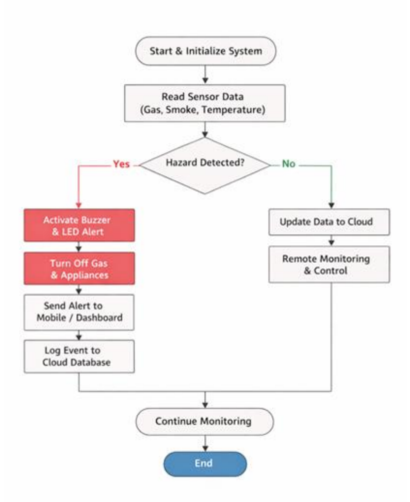


5.1.2 Working of Block Diagram

1. Sensors continuously monitor kitchen conditions for gas leakage, smoke, or abnormal temperature.
2. Sensor data is sent to the **ESP32 microcontroller**, which compares readings with safety thresholds.
3. If a hazardous condition is detected:
    - The **relay module** automatically shuts off the gas supply or electrical appliances.
    - The **buzzer and LEDs** alert users immediately.
    - IoT connectivity sends notifications to the user's **mobile app or web dashboard**.
4. All sensor readings and safety events are **stored in the cloud** for future reference, trend analysis, and predictive insights.
5. Users can **remotely monitor and control appliances** via the dashboard or mobile app, ensuring continuous safety even when away from home.

This block diagram ensures **proactive kitchen safety**, real-time monitoring, and minimal human intervention.

5.2 Flowchart



5.2.1 Flowchart Description

The flowchart represents the step-by-step process of the smart kitchen system:

1. **Start / System Initialization**
    - Initialize microcontroller, sensors, and relay modules.
    - Connect to Wi-Fi and cloud platform.
2. **Sensor Data Acquisition**
    - Continuously read data from gas, smoke, and temperature sensors.
3. **Check Safety Conditions**
    - Compare sensor readings with predefined thresholds for gas, smoke, and temperature.
4. **Hazard Detected?**
    - **Yes:** Trigger emergency protocols.
        - Switch OFF appliances and gas supply via relay.
        - Activate buzzer and LEDs.
        - Send notifications to mobile app/dashboard.
        - Log event in the cloud.
    - **No:** Continue monitoring.
5. **Cloud Communication**
    - Transmit sensor data to cloud for storage and real-time visualization.

- Update dashboard with live appliance and safety status.

6. **Remote User Interaction**
   - Users can monitor system status and control appliances remotely.
7. **Repeat Loop**
   - The process continues indefinitely to ensure continuous kitchen safety.

The flowchart ensures **real-time hazard detection, automated intervention, and cloud-based monitoring**, providing a seamless and intelligent kitchen safety system.

VI. CONCLUSION & FUTURE SCOPE

Conclusion

The IoT-Based Smart Kitchen with Enhanced and Automated Safety Measures presents a comprehensive solution to modern kitchen safety challenges. The system integrates gas, smoke, temperature, and motion sensors with a microcontroller (ESP32/ESP8266), relays, and IoT connectivity to ensure real-time monitoring, hazard prevention, and automated control of appliances.

Key outcomes of this project include:

1. **Enhanced Safety**:
   The system detects gas leaks, smoke, and overheating appliances, providing automatic shutdowns and alerts. This proactive approach significantly reduces the risk of fire accidents and other kitchen hazards.
2. **Automation and Convenience**:
   Appliances and gas supply can be automatically controlled, reducing the dependency on human supervision and improving convenience for users, particularly elderly or disabled individuals.
3. **Real-Time Monitoring and Alerts**:
   IoT integration allows users to monitor kitchen conditions remotely via mobile apps or web dashboards. Notifications and alerts ensure timely intervention.
4. **Data Logging and Analytics**:
   All sensor data and events are logged in the cloud, providing valuable insights for predictive safety analysis, trend monitoring, and maintenance planning.
5. **Scalability and Modularity**:
   The system design allows easy integration of additional sensors, smart appliances, or AI-based safety algorithms in the future.
6. **Energy Efficiency**:
   Automated appliance control prevents unnecessary power consumption and reduces risks associated with unattended cooking.
7. **Security**:
   Encrypted communication and authentication mechanisms ensure that only authorized users can access or control the system, protecting against tampering and unauthorized access.

Overall, the proposed system combines **IoT, cloud computing, embedded electronics, and automation** to deliver a modern, intelligent, and reliable kitchen safety solution. It addresses the limitations of conventional kitchens, providing enhanced safety, efficiency, and user convenience.

Future Scope

The IoT-based smart kitchen system can be expanded and enhanced in multiple ways:

1. **AI Integration for Predictive Safety**:
   Machine learning algorithms can analyze historical data to predict potential hazards or appliance malfunctions before they occur.
2. **Voice Control Integration**:
   Incorporating voice assistants like Google Assistant or Alexa allows users to control appliances and monitor kitchen safety hands-free.
3. **Smart Energy Management**:
   Integration with smart meters can monitor energy usage and optimize appliance operation for energy efficiency.
4. **Integration with Smart Home Ecosystems**:

The system can be connected to other smart home devices like smart locks, cameras, and lighting systems to provide a holistic home safety environment.

5. **Automated Fire Suppression Systems**:
   Advanced versions can trigger fire suppression mechanisms automatically if smoke or fire is detected.
6. **Enhanced Mobile App Features**:
   Users can receive predictive maintenance suggestions, appliance health reports, and safety analytics through mobile dashboards.
7. **Multiple User and Role Management**:
   Different access levels for family members, caregivers, or maintenance personnel can enhance usability and security.
8. **Industrial and Commercial Kitchen Applications**:
   The system can be scaled for restaurants, hotels, and cafeterias, monitoring multiple appliances and zones simultaneously.
9. **Integration with Wearable Devices**:
   Wearable alerts for elderly or disabled users can improve immediate response to kitchen hazards.
10. **Environmental Monitoring**:
    Addition of humidity, CO2, and particulate matter sensors can help maintain indoor air quality and enhance overall kitchen health.

The future scope demonstrates that this system is not only a solution for domestic safety but also a platform for **smart, connected, and energy-efficient kitchens**, capable of integrating advanced AI, automation, and IoT technologies.

REFERENCES

[1] Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.

[2] Gajula, S. (2026, March). Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

[3] Maturi, S. Y. (2024). Cryptographic privacy engines: Practical multi-party protocols for confidential database queries. Nanotechnology Perceptions, 20(S13), 2770–2785.

[4] Maturi, S. Y. (2024). Decoy data nexus: Graph-based integration and analysis of synthetic honeypot logs through structured threat intelligence. International Journal of Computational and Experimental Science and Engineering (IJCESEN), 10(4), 4255–4261. https://doi.org/10.22399/ijcesen.5010.

[5] Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2465.

[6] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

[7] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Innovative Engineering and Management Research (IJIEMR).

[8] Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of Enhanced Research in Science, Technology &Amp; Engineering, 10(07), 61–72. https://doi.org/10.55948/ijerste.2021.0708.

[9] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

[10] Pavan Kumar Adabala. (2026). IoT-Driven Digital Twins for Manufacturing Optimization: Hybrid Modelling, Reinforcement Learning and Sustainable Operations. International Journal of Computational and Experimental Science and Engineering, 12(1). https://doi.org/10.22399/ijcesen.5050.

[11] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. Eudoxus Press Journal.

[12] Pavan Kumar Adabala. (2026). Smart Retail Fuel Systems: IoT-Enabled Solutions for Loss Prevention and Environmental Safety. Computer Fraud and Security, 868–875. https://doi.org/10.52710/cfs.995.

[13] Pavan Kumar Adabala. (2026). Best Practices for Enterprise System Integration in Modern Organizations. Journal of Information Systems Engineering and Management, 11(2s), 1137–1146. https://doi.org/10.52783/jisem.v11i2s.14558.

[14] Srikanth Kavuri. (2025). AI-DRIVEN TEST AUTOMATION FRAMEWORKS: ENHANCING EFFICIENCY AND ACCURACY IN SOFTWARE QUALITY ASSURANCE. International Journal of Applied Mathematics, 38(10s), 699–710. https://doi.org/10.12732/ijam.v38i10s.990.

[15] Kavuri, S. (2025). Critical Review of Software Testing Problems in the Current Decade. International Journal on Science and Technology, 16(2). https://doi.org/10.71097/ijsat.v16.i2.9469.

[16] Srikanth Kavuri. (2024). Probabilistic Generative Modeling for Synthesizing High-Coverage Test Data in Safety-Critical Software Applications. Computer Fraud and Security, 633–642. https://doi.org/10.52710/cfs.838.

[17] Kavuri, S. (Ed.). (2024). Shift-left and shift-right testing approaches: A practical roadmap for continuous quality in agile and DevOps. Journal of Information Systems Engineering and Management, 9(4). https://doi.org/10.52783/jisem.v9i4.127.

[18] Srikanth Kavuri. (2023). Machine Learning Approaches for Security Vulnerability Detection in Software Testing. Computer Fraud and Security. https://doi.org/10.52710/cfs.837.

[19] Srikanth Kavuri. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud and Security. https://doi.org/10.52710/cfs.836.

[20] Venkata Pavan Kumar Gummadi. (2023). MuleSoft Batch Processing: High-Volume Streaming Architecture. Computer Fraud and Security, 50–57. https://doi.org/10.52710/cfs.886.

[21] Venkata Pavan Kumar Gummadi. (2026). Infrastructure Optimization Techniques for Enterprise Integration Platforms: A Comprehensive Analysis. Computer Fraud and Security, 37–44. https://doi.org/10.52710/cfs.875.

[22] Venkata Pavan Kumar Gummadi. (2024). API Design and Implementation: RAML and OpenAPI Specification. Journal of Electrical Systems, 16(4), 76–85. https://doi.org/10.52783/jes.9329.

[23] Venkata Pavan Kumar Gummadi. (2025). MuleSoft's Role in Advancing Sustainable Digital Infrastructure: An Enterprise Integration Perspective. Journal of Information Systems Engineering and Management, 10(62s), 1313–1321. https://doi.org/10.52783/jisem.v10i62s.13783.

[24] Venkata Pavan Kumar Gummadi. (2025). MuleSoft Architectural Paradigms and Sustainability: A Comprehensive Technical Analysis. Journal of Computer Science and Technology Studies, 7(12), 534–540. https://doi.org/10.32996/jcsts.2025.7.12.59.

[25] Harshitha, G. K., & Rajashekar, K. K. (2025). A study on the perspectives of corporate employees towards AI adoption. Journal of International Commercial Law and Technology, 6(1), 699–706.

[26] Kandula, S. T. R., Susarla, R. S., & Boyapati, P. K. (2025, July). Enhanced Cyber Security Using Global Local Artificial Neural

Network Based Intrusion Detection in Big Data Environment. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 426-431). IEEE.

[27] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219