IoT-based Fire Alarm: Design and Approach

Pinaki Pritam Singha and Professor Dr. Sandip Mandal, University of Engineering and Management, Kolkata, West Bengal

***Abstract*— The Internet of Things (IoT) describes the network of physical objects— "things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025.**

Our main objective is to use this technology to build a working fire alarm that would not only work like a regular alarm but will also send a notification to cloud connected devices.

***Index Terms*— Fire Alarm, Notification, Cloud Alert, Security.**

I. Introduction

The **Internet of things** (**IoT**) describes physical objects (or groups of such objects) with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. Internet of things has been considered a misnomer because devices do not need to be connected to the public internet, they only need to be connected to a network and be individually addressable.

The field has evolved due to the convergence of multiple technologies, including ubiquitous computing, commodity sensors, increasingly powerful embedded systems, and machine learning. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), independently and collectively enable the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems, cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. IoT is also used in healthcare systems.

The main concept of a network of smart devices was discussed as early as 1982, with a modified Coca-Cola vending machine at Carnegie Mellon University becoming the first ARPANET-connected appliance, able to report its inventory and whether newly loaded drinks were cold or not. Mark Weiser's 1991 paper on ubiquitous computing. In 1994, Reza Raji described the concept in *IEEE Spectrum* as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1997, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned device-to-device communication as a part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999. The term "Internet of things" was coined independently by Kevin Ashton of Procter & Gamble, later of MIT's Auto-ID Centre.

A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, wearable technology, connected health, and appliances with remote monitoring capabilities. IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems and camera systems. Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off or by making the residents in the home aware of usage.

II. Literature Survey

IoT system architecture, in its simplistic view, consists of three tiers: Tier 1: Devices, Tier 2: the Edge Gateway, and Tier 3: the Cloud. Devices include networked things, such as the sensors and actuators found in IoT equipment, particularly those that use protocols such as Modbus, Bluetooth, Zigbee, or proprietary protocols, to connect to an Edge Gateway. The Edge Gateway layer consists of sensor data aggregation systems called Edge Gateways that provide functionality, such as pre-processing of the data, securing connectivity to cloud, using systems such as WebSockets, the event hub, and, even in some cases, edge analytics or fog computing. Edge Gateway layer is also required to give a common view of the devices to the upper layers to facilitate in easier management. The final tier includes the cloud application built for IoT using the microservices architecture, which are usually polyglot and inherently secure in nature using HTTPS/OAuth. It includes various database systems that store sensor data, such as time series databases or asset stores using backend data storage systems (e.g., Cassandra, PostgreSQL). The cloud tier in most cloud-based IoT system features event queuing and messaging system that handles communication that transpires in all tiers. Some experts classified the three-tiers in the IoT system as edge, platform, and enterprise and these are connected by

proximity network, access network, and service network, respectively. WSNs comprise of the Tier 1: Devices.

A wireless sensor network (WSN) is a self-configuring wireless network with minimal infrastructure that monitors physical or environmental conditions including temperature, sound, vibration, strain, motion, or contaminants and transmits data via the network's first place. Or a receiver that can observe and analyse data. The receiver or base station serves as the interface between the user and the network. By entering a query and collecting the results from the recipient, you can get the information you need from the Internet. A wireless sensor network usually has thousands of sensor nodes. Sensor nodes can communicate with each other via radio signals. Wireless sensor nodes are equipped with sensitive equipment and computing equipment, radio transmitters and power supply components. Each node in a wireless sensor network (WSN) is resource constrained in some way: processing speed, storage space, and communication bandwidth are all restricted. After installation, the sensor nodes are in charge of self-organizing the necessary network infrastructure and frequently communicate with them through multi-hop communication. Then, the built-in sensors begin to collect information of interest. Wireless sensor devices also respond to requests from "checkpoints" to follow specific instructions or provide samples for testing. The sensor node can operate in either a continuous or event-driven mode. To calculate your location, you can use the Global Positioning System (GPS) and local positioning algorithms. Actuators may be added to wireless sensor systems to make them "work" in specific situations. Wireless sensor and actuator networks are a more generalized term for these networks. New technologies can be supported by wireless sensor networks (WSNs). Protocol architecture necessitates unconventional paradigms due to a variety of constraints. Due to the requirements for low device complexity and low power consumption (i.e., long network life), a reasonable balance needs to be struck between communication and signal/data processing capabilities. This has stimulated tremendous efforts in the field of research, standardization and wireless sensor networks.

The first fire alarm was discovered by accident in 1980 by Francis Robbin Upton, an associate of Thomas Edison to create a device to automatically detect poison gas electrically.

A modern-day fire alarm warns people when there is smoke, fire, carbon dioxide or other fire related, general emergencies. The device automatically detects the presence of smoke or fire and sets an alarm off electrically through the circuit.

However, with the use of present-day smartphones, Wi-Fi and globally connected devices, it has become an importance for a device to take use of the notification system and be remote controlled without always the requirement of an external physical contact for application of appliances especially those which are necessary during emergencies.

III. PROBLEM STATEMENT

IOT Based Fire Alerting System uses two Sensors, namely, Temperature and Smoke sensors. Arduino has an inbuilt ADC converter, which converts the analog signals received at the sensor end to digital. The Arduino is programmed to turn on the buzzer when the temperature & the smoke reach a threshold value.

At the same time, Arduino sends the data to the Wi-Fi module ESP8266. ESP8266 is a chip that is used for connecting micro-controllers to the Wi-Fi network. ESP8266 will then the following data to the IOT website, where, authorized people can take appropriate measures in order to curb the fire.

1. Temperature (in Degree Celsius)
2. Smoke Value (in Percentage)
3. Device ID
4. Date and Time Stamp

The device ID is the unique ID given to a device, which would help the person get information related to the location, where the fire is detected.

The Prerequisite for this IoT-based fire alarming system is that the Wi-Fi module should be connected to a Wi-Fi zone or a hotspot. This project is also implemented without the IOT module. In place of the IOT module, we have used the GSM module, by which an SMS is triggered when the buzzer is turned ON.

IV. PROPOSED SOLUTION

1. Study the working principles of smoke and fire alarm systems.
2. Design a cheap fire alarm system based on microcontroller.
3. Design an automatic fire alarm system to protect users and the environment.
4. Create a simple fire alarm system. Use a fire alarm system.
5. Make people's lives easier.
6. Design a prototype fire alarm system with smoke detector as input and buzzer and text message as output. Arduino Uno card, embedded system: NodeMCU, cable connection, buzzer etc.

V. EXPRERIMENTAL SETUP AND RESULT ANALYSIS

A. Components:

1) NodeMcu Board

It is an open-source firmware that uses the LUA scripting language.

2) Flame Sensor

A Flame Sensor or a Flame detector is a device designed to detect and respond to the presence of a flame or fire, allowing flame detection.

3) Jumper Wires

A jumper is an electrical wire, a group of them bundles with pins or connector attached at the end. Wires are fitted by using the pins by putting them on a breadboard.

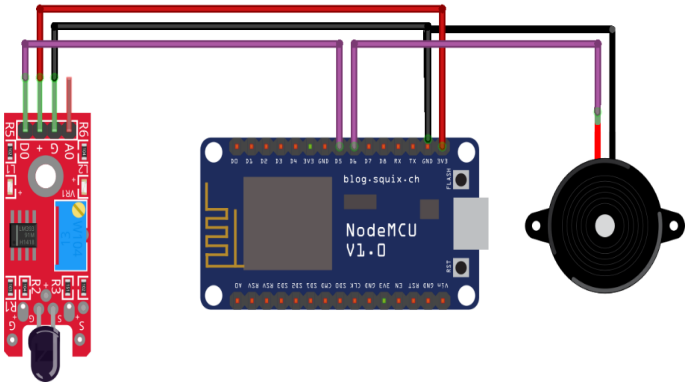
4) Breadboard

A Breadboard is a temporary construction base used to build electronic circuits and basic technological device.

5) Buzzer

A Buzzer for making a sharp noise upon detection of fire by the circuit.

6) Circuit Diagram:



VI. CONCLUSION & FUTURE SCOPE

The model continuously monitors fire alarms and sends alarms to users. The reception and system we propose can achieve its main goal, mainly to build an IoT-based fire alarm system. Call them when you find the fire. The answer is sent to the user via notification. Using this product can help these people quickly learn about the incident and the nearest fire department. You will receive a valid notification. It is cheap and easy to install.

REFERENCES

Book Referred:

1. International Journal of Computer Applications
2. Oracle Industries IoT Report

Websites Referred:

1. Wikipedia [https://en.wikipedia.org/wiki/Internet_of_things : 7-11-22 19:44]
2. StackOverflow [https://stackoverflow.com/search?q=fire+aLARM&s=9023917d-b2b2-4f70-8174-5de0f447c5ef : 7-11-22 20:11]
3. Blynk [https://blynk.io/ 1-11-22 8:31]