# Smart Security Solution for Market Shop Using IoT and Deep Learning

**Talha Bin Abdul Hai[1], Wahidur Rahman[2], Md Solaiman Hosen[3], Md. Tarequl Islam[4], A H M Saifullah Sadi[5], Gazi Golam Faruque[6], Mir Mohammad Azad[7]**
[1,4,6,7]Department of Computer Science and Engineering, Khwaja Yunus Ali University, Enayetpur, Sirajganj-6751, Bangladesh
[2,5]Department of Computer Science and Engineering, Uttara University, Uttara, Dhaka
[3]Department of Computer Science, Iowa State University

**Article Info**

***Article history:***

Received May 8, 2023
Revised Dec 22, 2023
Accepted Mar 22, 2024

***Keywords:***

Convolutional Neural Network (CNN)
Deep Learning
Internet of Things (IoT)
Global System for Mobile Communications (GSM)
Amazon Echo IVA

**ABSTRACT**

Nowadays, security system in the market shop is an immense concern everywhere. The modern world is leaning towards intelligent, automated security systems instead of the traditional human-based security or CCTV surveillance system because of their limitations. A typical CCTV surveillance system is not intelligent enough to detect intruders or fire. The proposed security system in this paper is an IoT, deep learning, and GSM based innovative security solution specially designed for shops and offices. The objectives of this system are to prevent burglary and fire. For this, the proposed model focuses on fire and intruder detection through both IoT and deep learning approaches. Several IoT sensors have been utilized with a deep learning model to detect fires in shops or offices at an initial stage. The model also utilizes a current sensor for identifying electrical short-circuit to prevent unexpected damages. This system further utilizes GSM technology to send the corresponding notifications to the authorized user and play alarm sounds at the shop as well as the owner's house while detecting suspicious occurrences. The proposed solution has used two pre-trained Convolutional Neural Network (CNN) architecture, namely ResNet50 and Inception V3. This research found an accuracy of 99.49% with ResNet50 architecture in fire detection.

***Corresponding Author:***

Wahidur Rahman,
Department of Computer Science and Engineering,
Uttara University, Uttara, Dhaka.
Email: wahidtuhin0@gmail.com

## 1. INTRODUCTION

Burglary, robbery, and fire could be a sudden extensive threat to a business, and more or less, these are frequently happening all over the world every year. The amount of damage caused by such kinds of incidents is enormous. That's why ensuring security is a subject of great concern to a business.

According to the 2020 Retail Crime Survey by BRC, Figure 1 shows that the total amount of losses from crime to business is increasing day by day, and Figure 2 shows that the expenses on crime prevention are also growing over time. Every year, in the United Kingdom, £1.2BN is spent only on crime prevention [1]. Following ACS CRIME REPORT 2019, in the United Kingdom, the number of robbery incidents is 12,397, which costs around £6 million per year. On the other hand, 7,160 burglary incidents are costing around £21 million per year. They also mentioned that the top areas for investment in security purposes are CCTV. The most commonly used weapon in crime to the shops is- knife (26%), firearm (6%), and other weapons, e.g., axe, hammer (26%) [2].

Besides all, a fire can be dangerous for a business. Precious goods or whole shop can damage by the fire. Sometimes a massive fire on a large market can cause a million-dollar loss within a short time. There can be many reasons behind store fire.

Among them, the most common reason is fire from the electrical-short circuit. Detecting fire at the beginning stage can reduce the number of damages. So detecting the fire at the initial stage is very important and preventing it because it is impossible to prevent fire all the time. The research [3] on fires in mercantile properties and stores by NFPA shows that the average annual number of the structure fire is 13,570, and the number of damages from the fires is $604 million. Among them, electrical malfunctions or failure causes 22% of fires, and direct property damage is 26%. The research also shows that more fires occur during the day, but fires at customary off-hours cause more significant damages than daytime fires. On average, the property damage by each fire between 9:00 PM and 5:00 AM is $73,800, while the amount of damages from the fire that occurs between the times 5:00 AM to 9:00 PM is $33,900. These statistics indicate the importance of installing and maintaining the automated fire detection alarm system. According to the report [4], the revenue forecast in 2027 for the fire alarm and detection system's global market is $75.5 billion.

There are a lot of researchers in the field of machine learning, IoT, who put significant contributions to building more convenient security systems. The authors of the paper [5] proposed a GUI-based intelligent home monitoring system that could help disabled, old-aged, or busy people. It could notify the owner if something went wrong at the time of their absence, and the GUI was accessible from both mobile and PC. The authors also discussed smart home systems based on various technologies like Bluetooth, GSM, IoT, PIC Microcontroller to show a comparative study. In the article [6], the authors developed a WSN and GSM-based system to detect the theft, fire, and leakage of raw gas. It could send an alarm message to the user's phone over GSM. This paper [7] described a home security system using the PIR motion sensor and Raspberry Pi at a low cost. The concept of these, [8] [9] papers are almost the same. Both authors implemented an IoT-based home automation system with some security features like intruder detection. Their system could control home appliances, detect motion, play an alarm, and send notifications to the owner's phone if an intruder is detected. The paper of the ref. [10] the authors had discussed a framework built upon CNN-based techniques for detecting four kinds of threat objects: i. Knife; ii. Gun; iii. Razor-blade; iv. shuriken. Using FRCNN with RESNET, on the dataset ImageNet, they achieved 98.4% accuracy for recognizing 4-class of threat, and per image, it took 0.16 seconds. In the study of this paper [11], the authors checked the effectiveness of the pre-trained VGG16, VGG19, and AlexNet models based on CNN, to detect and classify criminal tools like knives and guns. VGG16 model based on fine-tuning for the two and three classes achieved the highest accuracy in detecting criminal devices with a rate of 99.73% and 99.67%, respectively. In the paper [12], the authors had proposed a method based on FRCNN to detect the SRoFs and not-fire using their spatial features. They showed that their proposed long-term video-based method had better accuracy in detecting fire compared with the still image-based or short-term video-based method. In this paper [13], the authors had used the optimized YOLO model for flame detection from video frames. Using the Google platform TensorFlow, they obtained up to 76% accuracy on flame detection for their proposed model.

The authors of the papers from [5-9] had mainly developed smart home automation and security systems based on IoT or WSN or both technologies for controlling home appliances, detecting intruders, fires, gas leakages and in the papers of these references [10-13], authors had mainly focused on detecting fire and threatful objects like firearms, knives, et cetera from cameras using deep learning technology. On the other hand, by combining technologies like deep learning, IoT, and GSM, we have focused on developing such a complete security solution for shops capable of monitoring several things like intruders, fire, electrical short-circuits, and threatful objects. Along with the detection system, our proposed system also had multiple notifying systems like local alarm, remote alarm, and sending notification to the phone to notify the owner in case of emergency.

From the facts and statistical analysis above, it is clear that an intelligent solution can be very beneficial for shops to ensure security, minimize the shop-crime, and prevent sudden damages from fire and burglary. Modern technologies can play a significant role here. So, we proposed such an intelligent system based on some modern technologies, namely IoT, deep learning, and GSM, that can overcome these kinds of problems mentioned above. The research contributions of this paper are as follow:

- An architectural design has been presented to ensure security for shops and other places like offices, banks, etc.
- An intelligent system has been proposed to detect fire, electrical short-circuit, and intruders using several techniques. The proposed system can also detect some threatful objects like knives, firearms, hammers with the mechanism of deep learning.
- A real-time monitoring system for shops, offices from remote places has been implemented through the app. Local and remote alarm facilities are also integrated. Different sensors and security cameras collect data, and NodeMCU, Raspberry Pi is used to process them.
- Here we tried to provide such a solution that can cover various aspects to provide complete, reliable security. This solution has dedicatedly designed for market shops or offices rather than other home security solutions.

The primary goals of this security solution for market shops are to prevent burglary and fire. A sensor-based system is proposed to detect intruders in a closed shop by detecting movement, sound, light intensity, and door status. The system can generate sharp noise to force intruders to leave shop. Electrical short circuits can cause massive fires, so the system intelligently detects high electricity flow and cuts off electricity if necessary. If a fire occurs, it is detected as soon as possible and notified to the owner and corresponding personnel. Camera image analysis and sensor data are used for fire detection. Beside app & SMS-based notification, remote alarm system is also used for ensure informing the owner.

The proposed sensor-based security system utilizes different sensors to detect a wide range of threats beyond just visual cues, including motion, sound, temperature changes, and electrical short circuits. This comprehensive approach provides early detection of potential risks, enabling faster response and requires less bandwidth and storage. Overall, the proposed system offers privacy-conscious, more efficient, and versatile threat detection than conventional CCTV surveillance.

This article is organized into four sections, where section II describes the proposed methodology with its operating principles. Then in section III, the performance evaluation of the developed solution has been interpreted with results and the related discussions. Finally, section IV reveals the conclusion of this manuscript.

## 2. RESEARCH METHOD

Our proposed methodology is consists of three parts: IoT-enabled sensor-based monitoring system, fire & harmful objects detection using deep learning, and remote alarm and monitoring system. We are going to discuss all of them in detail. Here, Figure 3 represents the overall proposed methodology. It is also depicts an overview of how each part of the system is connected to the other parts.

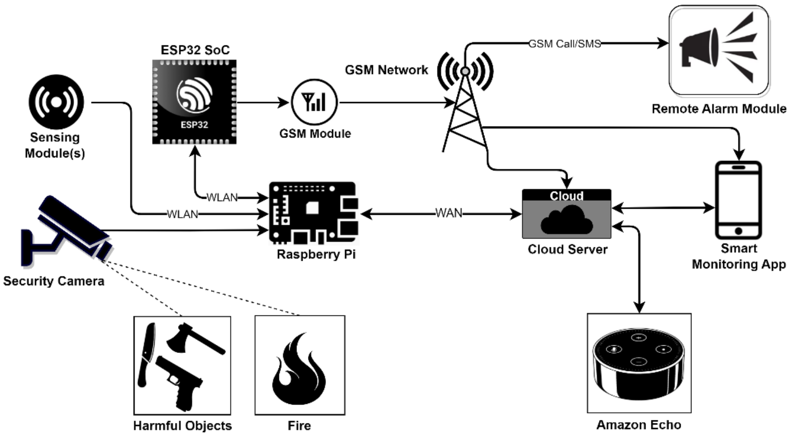

Figure 3. A block diagram of the proposed intelligent security solution

The sensor based monitoring system is a combination of several sensing modules connected to the MQTT broker running on the Raspberry pi via Wi-Fi. Each sensing module is equipped with different types of sensors that are directly connected to an ESP8266 SoC [14].

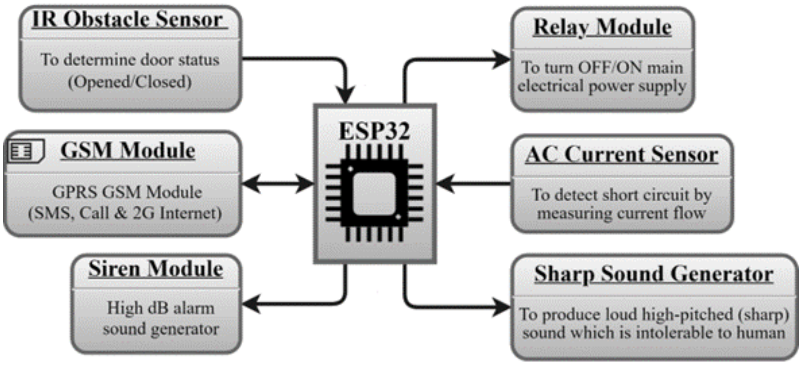
IR Obstacle Sensor
To determine door status (Opened/Closed)
GSM Module
GPRS GSM Module (SMS, Call & 2G Internet)
Siren Module
High dB alarm sound generator
ESP32
Relay Module
To turn OFF/ON main electrical power supply
AC Current Sensor
To detect short circuit by measuring current flow
Sharp Sound Generator
To produce loud high-pitched (sharp) sound which is intolerable to human

Figure 4. A block diagram and working principle of sensor-based monitoring system (main module)

ESP8266 acts like the heart of each sensing module. It collects data from the sensors, processes them, and finally publishes the updated data to the MQTT broker. In addition, one or several cameras connect to the

Raspberry Pi to detect harmful objects by analyzing the surveillance video in real-time [15]. The Raspberry Pi always send data to the cloud, and users can fetch data from there to monitor the system remotely using a smartphone application over the internet.

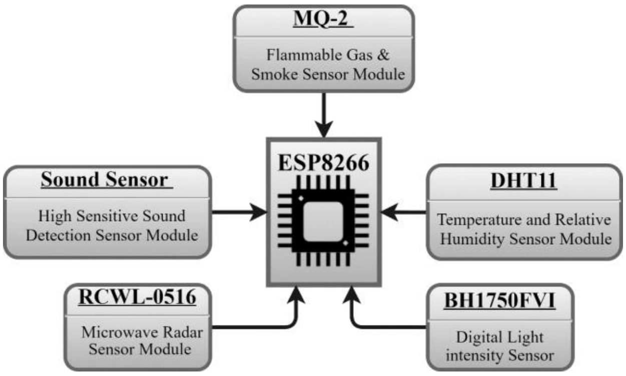
MQ-2
Flammable Gas & Smoke Sensor Module
ESP8266
Sound Sensor
High Sensitive Sound Detection Sensor Module
DHT11
Temperature and Relative Humidity Sensor Module
RCWL-0516
Microwave Radar Sensor Module
BH1750FVI
Digital Light intensity Sensor

Figure 5. A block diagram of a sensing module

Moreover, to make the interaction easier between our system and its user, Amazon Echo [16], a smart speaker with a virtual assistant called Alexa has added to the system. Amazon Echo connects to an app server running on Raspberry pi through AWS Lambda. When the user commands something to Amazon Echo, it sends the voice data to Amazon's web server, and their web services process the user's voice data into text format. After converting voice data to text, AWS Lambda returns necessary commands to the app server running on Raspberry Pi in JSON data format. Using voice commands, users can do many things quickly and easily, such as disarm/arm a group of sensors or the whole system. Users also can utilize it to activate the alarm system before leaving the shop. For this, they have to provide a command like this "activate alarm after 1/2/4/5 minute(s)". Moreover, Amazon echo can also be used to call emergency contacts in case of any emergency. For some sensitive tasks like disarming sensors/system, the user might need to authorize themselves by providing a verbal password. This simple authentication system will help to prevent unauthorized access to the system.

### 2.1. Working procedure of IoT-enabled sensor-based monitoring system

The proposed sensor-based monitoring system is a sensor-based modular system to detect intruders and short-circuits in a closed place (such as a locked market shop or office). The system uses seven types of sensors to detect intruders, fire, and electrical short circuits in a closed shop or office. IR obstacle sensors, microwave radar sensors, sound sensors, and light intensity sensors are used to detect intruders. Local and remote alarms are activated if loud sounds, bright lights, door openings, or movement are detected. The presence of smoke or flammable gas can also trigger alarms, and the electric supply is cut off automatically if the system detects any unwanted high electricity flow.

Figure 4 represents the block diagram and working principle of the system. Figure 5 shows that how each sensing module consists of five different types of sensors (Appendix A). Among five of them, we have used three sensors (microwave radar sensor, light sensor, and sound sensor) to detect intruders in the monitoring area. Another two types of sensors (flammable gas & smoke sensors and temperature sensors) have been used for fire detecting purposes. The intruder and short-circuit detection system will be activated only if the user manually activates the security system (after closing shop/office) or chose to activate the system automatically when the main door is closed. To monitor the main door's status, we have used an infrared obstacle sensor. The user will be able to activate the system manually by sending a phone call/SMS from an authorized phone number to the system's GSM module or can use voice commands to the Amazon Echo. Anyone must have to deactivate the sensor-based intruder detection system before entering the monitoring area. Otherwise, the system will trigger the alarm and will take further steps. To deactivate the system, the user will need to send a voice command to Amazon Echo along with the set verbal password or send an SMS with a secret code (table 1.1) from an authorized phone number to the system's GSM module.

To detect intruders in a monitoring area, we have focused on several things like motion detection, measurement of light and sound intensity. There are three different sensors for intruder detection in each sensing module. First, we have used a microwave radar sensor for motion detection [17], which can detect a slight movement of any objects within its range- which is 7 meters, 360° angle. Then sound and light intensity measurement sensors have been used to get additional information for intruder detection, and this will also help prevent false alarms in some cases.

MQ-2 sensor has used to detect fire by measuring the amount of smoke and flammable gas in the monitored environment. It can detect smoke and LPG, Propane, Methane, Carbon Monoxide, Hydrogen concentrations from 200 to 10000 ppm [18]. A current sensor (AC) has been used to monitor the main's current flow to detect short-circuit and electrical sparking. If it detects a sudden increase of current flow from the defined threshold level to another level through the main power supply line of a shop/office, and if it exceeds a certain level, then the system will shut down the AC power supply by turning off the power relay switch. It will do the same thing to prevent fire from electrical sparking; if a tremendous amount of current flow keeps fluctuating frequently. If the primary AC source goes off, the system will keep itself alive using backup battery power.

All the data from the sensors is continuously sent to the cloud. Internal communication with sensing modules happens over the MQTT messaging protocol. If anything abnormal is detected anytime, depending on the situation, the system notifies the user via text message/phone call, turns on the local alarm, or both local and remote alarms along with the sharp sound generator.

### 2.2. Fire & harmful objects detection using deep learning

Sensor-based fire detection systems have limitations, such as missing slow-burning fires and not detecting fires in their early stages. To address this, a camera-based fire detection system using deep learning models is combined with the sensor-based system, ensuring timely fire detection, and minimizing damage.

This subsection will present the working principles of fire and harmful objects detection utilizing the deep learning paradigm. Figure 6 shows the block diagram of the corresponding proposed working principles. The figure is classified into two phases. In the first phase, the system will perform image acquisition through a camera module connected with raspberry pi. When the camera module finds any unauthorized movement with harmful objects or fire flames, it will automatically focus on the suspected objects. As we have already referenced that, knives and firearms are the most used weapon in retail shop's crimes, that's why our system marks handheld guns and open knives as highly suspected harmful objects. Like guns and knives, the system also might suspect some other things like axes and hammers as harmful objects.

After focusing on the suspected objects, the detected information will be sent to the raspberry pi for image processing with the deep neural network. In the second phase, the system will store the captured images. Then, the images will be fed to the already trained model to find the detected information. The system procedures will continuously repeat and safeguard live monitoring with robust security in the market shops.

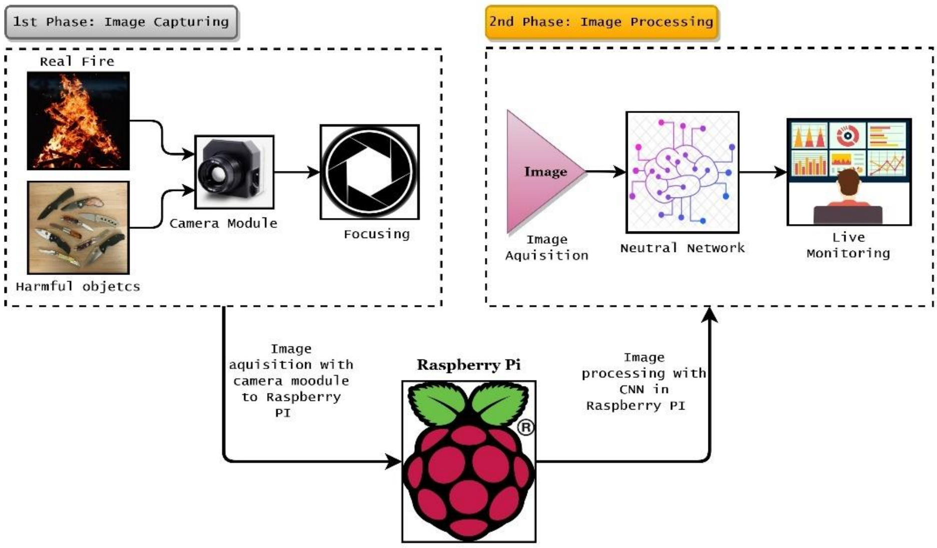
1st Phase: Image Capturing
Real Fire
Camera Module
Focusing
Harmful objetcs
2nd Phase: Image Processing
Image
Image Aquisition
Neutral Network
Live Monitoring
Image aquisition with camera moodule to Raspberry PI
Raspberry Pi
Image processing with CNN in Raspberry PI

Figure 6. A block diagram of fire and harmful object detection with deep learning

### 2.3. Remote alarm and monitoring system

The remote alarm system is a way to notify the user in case of an emergency that something happens wrong with their shop/office. If the user fails to get notified from their phone, it can be very beneficial in this case. This module will be installed in the user's house. It has three main components: an ESP8266 (NodeMCU), a GSM Module to receive calls/SMS, and an alarm sound generator. If it receives any call/SMS from the central system's GSM module, it will trigger the alarm. The user can stop the alarm by pressing a push-button along with the module or sending a call/SMS from the authorized phone number.

The remote monitoring system allow users to monitor all the sensor's data in real-time in a dashboard. Users can also see the history of past sensor data log in the app. After installing the app, a user must need to log in with valid credentials. Then the app will fetche sensors data from the cloud and displays them in the app's dashboard.

## 3. RESULTS AND DISCUSSION

This section represent results analysis of the proposed system with relevant discussion, and it is divided into five sections. The first section presents the experimental data analysis of some sensors used in the sensor-based monitoring system. The second section describes the deep learning approach used for fire detection with its accuracy result on a test dataset. Finally, the last section provides a short comparison among existing security system related work with our proposed security system.

### 3.1. Experimental data analysis of IoT-enabled sensor-based monitoring system

Several experiments have been performed on the sensors, such as microwave radar sensor, sound measurement sensor, light intensity sensor, gas/smoke sensor, temperature sensor, current sensor, and IR obstacle sensor used in this system. A Single microwave radar sensor, light intensity sensor, and sound sensitivity measurement sensor is utilized in this integration to detect intruders. Here, the RCWL-0516 radar sensor module detects movement that emits microwave frequencies employing "Doppler Radar". For unauthorized movement within its range, the output pin of it goes HIGH.

An IR obstacle sensor is utilized to determine whether the door status is open or closed. We have set up the IR obstacle sensor so that it could detect the closed door as an obstacle; otherwise, if the door opened, there will be nothing in front of the sensor. That means a HIGH value from its output represents an open door. The experimental data for the four sensors are illustrated in Table 1.

Table 1. Experimental data of the intruder detection system (when the system is activated)

| Test No. | IR obstacle sensor | MW radar sensor (=<6m, 360°) | Light sensor Value (lux) | Sound sensor value (dB) | Door status | Human presence in monitoring range | Light intensity in monitoring range | Sound intensity in monitoring range | System's returned status code | Actions | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | GSM Call/SMS | Alarm | | Sharp sound |
| | | | | | | | | | | | Local | Remote | |
| 1. | High | Low | 1.3 | 55 | Closed | No | No (dark) | Very low | 0-N | Void | Void | Void | Void |
| 2. | Low | Low | 2.1 | 58 | Open | No | Very low | Low | 3-U | Yes | Yes | Yes | Void |
| 3. | Low | High | 5.7 | 59 | Open | Yes | Low | Low | 4-I-D | Yes | Yes | Yes | Yes |
| 4. | High | High | 20.0 | 65 | Closed | Yes | Medi-um | Medi-um | 4-I-O | Yes | Yes | Yes | Yes |
| 5. | High | Low | 0.0 | 78 | Closed | No | No (dark) | Loud | 1-I-T | Yes | Void | Void | Void |
| 6. | High | Low | 31 | 57 | Closed | No | Bright | Low | 0-N | Void | Void | Void | Void |
| 7. | High | High | 1.5 | 56 | Closed | Yes | No (dark) | Low | 1-I-Q | Yes | Void | Void | Void |

Table 1.1. The system returned status codes with their meanings

| Code | Meaning |
|---|---|
| 0-N | Everything is OK; no action is required. |
| 3-U | Someone might open the door without deactivating the alarm |
| 4-I-D | Someone entered the shop/office through the door |
| 4-I-O | Someone entered the shop/office without using the door |
| 1-I-T | Someone might be trying to enter the shop/office by breaking the wall or something, or it could be just a thunder strike |
| 1-I-Q | It might be the radar sensor's noise or something non-living moving things. |

To detect fire, an MQ-2 sensor is also used in each sensing module to detect smoke and flammable gases. Besides the MQ-2 sensor, there is also a temperature sensor to monitor the room temperature. The MQ-

2 sensor module triggers HIGH voltage to its output pin if smoke or gases such as LPG, CH4 appear to the sensor. Table 2 represents the respective experimental data on it.

Table 2. Experimental data for the fire detection system (sensor-based)

| Test No. | Smoke | Gas Leakage (LPG, Propane and Hydrogen) | MQ-2 sensor's digital output | Actions | | | |
|---|---|---|---|---|---|---|---|
| | | | | Power supply | GSM Call/SMS | Local alarm | Remote alarm |
| 1. | Yes | No | HIGH | Shutdown | Yes | Yes | Yes |
| 2. | Yes | Yes | HIGH | Shutdown | Yes | Yes | Yes |
| 3. | No | No | LOW | Void | Void | Void | Void |
| 4. | No | Yes | HIGH | Shutdown | Yes | Yes | Yes |
| 5. | Yes | No | HIGH | Shutdown | Yes | Yes | Yes |

The proposed security system has been enriched by adding short-circuit detection technique with a low trigger current. For this, a current measurement sensor named ACS712-30A has been attached to this integration. This sensor module utilizes a hall sensor to measure the current flow. When current flows through this module, the value of Vcc changes according to the current flow. Therefore, the current flow in amperage has been calculated from the ADC value using the Eq. (1) & (2).

$$\text{ADC\_Voltage} = (\text{ADC\_Value} \div 1024) \times \text{Vcc} \times 1000 \tag{1}$$

$$\text{Current\_Value} = \left((\text{ADC\_Voltage} - \text{Offset\_Voltage}) \div \text{Sesnor\_Sensitivity}\right) \tag{2}$$

Where, *ADC_Value* = 10-bit read value from analog pin, *1024* is to get the ratio of full 10-bit width, *Vcc* is the supply voltage for the module (*1000* to convert it in mV), *Offset_Voltage* = half of the Vcc, and *Sesnor_Sensitivity* = 66 mV/A (for ACS712-30A Sensor).

Table 3 provides the corresponding experimental data for this sensor used for short-circuit detection by assuming no heavy electrical appliance runs after closing shop/office (such as air conditioner, fridge, heater, etc.)

Table 3. Experimental data of the short-circuit detection system (when the system is activated)

| Test No. | Current Sensor value (Amp) | Time duration (sec) | Actions | |
|---|---|---|---|---|
| | | | Relay switch (Main power supply status) | GSM SMS notification |
| 1. | 3 | 1 | Relay state unchanged | void |
| 2. | 3 | 2 | Off, shutdown power supply | Yes, sent |
| 3. | 5.5 | 2 | Off, shutdown power supply | Yes, sent |
| 4. | 5.5 | 1 | Relay state unchanged | void |
| 5. | 1 | 10 | Relay state unchanged | void |

From the experimental data presented in table 3, we can see that the system turns off the main power supply (for short-circuit) if it detects 3A or more current flowing through the mainline for 2 seconds or more when almost all power appliances are turned off.

The system is designed for individual shops. Each shop needs to install separate systems. However, it might not be possible to cover an entire shop area with the sensors of a single sensing module. So, a user might need to install multiple sensing modules in the same shop. The MQTT messaging protocol is used to ensure secure communication among all modules. This lightweight and efficient protocol can handle a large number of devices efficiently. If more nodes (publishers and subscribers) are added to an existing MQTT network, the network can scale to accommodate increased data flow. In our tests, the Mosquitto broker was used on a Raspberry Pi 4B (8GB RAM) with 8 sensing modules and 1 main module connected to the broker. The CPU utilization was between 1% to 5%, and the free memory percentage was 84. At QoS level 0, the message loss rate was 0.13%, which is considerable for the proposed system. The MQTT protocol is designed to handle communication between millions of devices, so adding double, triple, or more sensing nodes (than the number of nodes used for testing) should not cause problems if the broker's hardware is powerful enough.

### 3.2. Fire detection approach using deep learning

This research is experienced with a deep learning mechanism to detect fire and unauthorized access in the shop. The system also capable of detecting harmful objects, but this section will only depicts fire detection with transfer learning [19]. The training of the model is performed with the dataset retrieved from

Kaggle [20]. After that, the image augmentation process has been applied to enrich the dataset. The training of the model was taken place in Google Colab.

The proposed system has utilized two pre-trained Convolutional Neutral Network (CNN) architectures such as ResNet50 and InceptionV3. There are around 2 million parameters in ResNet50's architecture. The ResNet50 model is made up of various components. It has a max-pooling layer, a convolutional layer, and a fully connected layer. Enhancement layers enable deterioration issues and remove disappearing issues. There is a super-pathway in the skip connection. The ResNet50 is only used for feature extraction in this study, not for classification purposes. When given a fire image with dimensions of 248 by 248 by 3, the model generates 4096 features for each image (the result of the final layer of the feature extraction section). Figure 7 shows the corresponding architecture of the ResNet-50 model for fire detection mechanism. In these figures, two types of shortcut modules are utilized in the implementation of ResNet, such as identity block and convolution block. The identity block has no convolution layer but has the exact dimensions as output. On the sharp opposite, the convolution block has a convolution layer at shortcut. Also, the convolution block has input dimensions that are smaller than output dimensions. In both blocks, 1x1 convolution layers are attached to the start and endpoint of the network.

On the other hand, GoogleNet is the name given to Inception V3, and the model is a pre-trained network model. The inception model consists of 22 layers with 5M parameters and filter sizes of 1x1, 3x3, and 5x5 to extract features at different scales using max pooling. Following the implementation of Inception v3, the 5x5 convolutional filters are replaced with two 3x3 filters to reduce computation while maintaining network performance. To minimize overfitting, the conception v3 has 48 layers and a fine-tuned structure. Figure 8 depicts the architecture of the inception v3 model for extracting deep features from fire data.

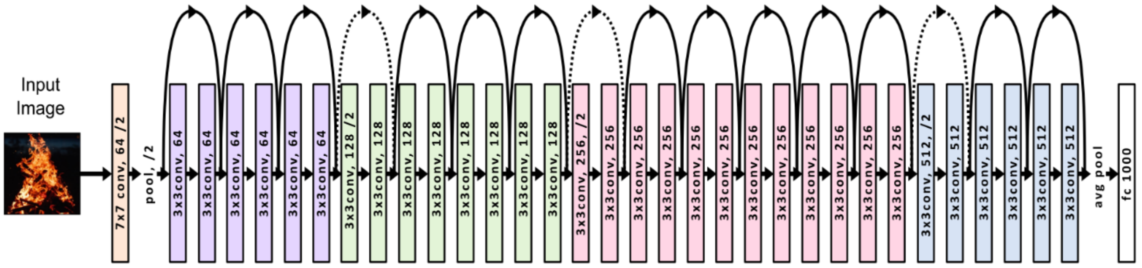

Figure 7. The fire detection mechanism with ResNet-50 Architecture

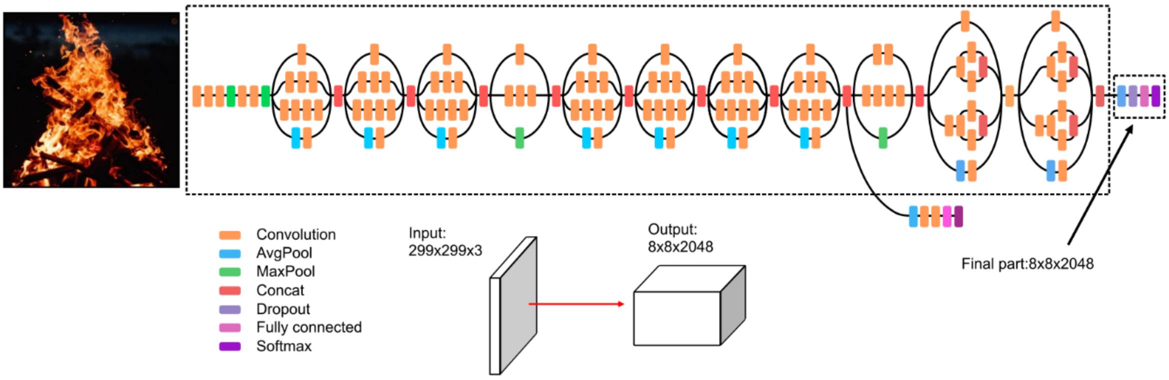

Figure 8. The fire detection mechanism with Inception V3 Architecture

The training data are fed to extract features of the images. After that, feature engineering was performed with pre-trained CNN architecture such as ResNet50 and Inception V3 [21] to build the model for fire detection. The model classifies the images into two classes, fire and neutral. After that, test data is fed to the model to predict the classification and enumerate the experimental data accordingly. This study experienced better accuracy with the configuration of 90% training and 10% test data. The experiment also includes the Principle Component Analysis (PCA) [22] to reduce the dimension of the dataset and optimize interpretability. Table 4 presents the data analysis with ResNet50 pre-trained CNN architecture. The experiment also considers the accuracy with the corresponding precision and recall. This research found an accuracy of 99.49% with ResNet50 architecture in fire detection.

Table 4. Experimental data analysis with ResNet50 pre-trained CNN architecture

| Number | Training - Test | PCA | Accuracy | Precision | Recall |
|---|---|---|---|---|---|
| 1 | 90% -10% | 80 | 0.9949 | 1.000 | 0.99 |
| 2 | 90%-10% | 100 | 0.9949 | 1.000 | 0.99 |
| 3 | 90%-10% | 200 | 0.9949 | 1.000 | 0.99 |
| 4 | 80%-20% | 80 | 0.9874 | 0.995 | 0.98 |
| 5 | 80%-20% | 100 | 0.9896 | 0.995 | 0.98 |
| 6 | 80%-20% | 200 | 0.9849 | 0.984 | 0.98 |
| 7 | 70%-30% | 80 | 0.9882 | 0.986 | 0.99 |
| 8 | 70%-30% | 100 | 0.9916 | 0.990 | 0.99 |
| 9 | 70%-30% | 200 | 0.9865 | 0.986 | 0.98 |
| 10 | 50%-50% | 200 | 0.9869 | 0.983 | 0.98 |

Table 5 depicts the performance analysis of two CNN architectures, namely ResNet50 and Inception V3. This table data indicates that ResNet50 offers better performance than the Inception V3 model. Again, the confusion matrix is also illustrated with the normalization technique [23] to present the proficiency of the proposed model. Figure 9 shows the confusion matrix with the normalization technique.

Table 5. Performance analysis between two CNN architectures.

| Model | Training - Test | PCA | Accuracy | Precision | Recall |
|---|---|---|---|---|---|
| ResNet50 | 90%-10% | 200 | 0.9949 | 1.000 | 0.99 |
|  | 80%-20% | 200 | 0.9849 | 0.984 | 0.98 |
|  | 70%-30% | 200 | 0.9865 | 0.986 | 0.98 |
|  | 50%-50% | 200 | 0.9869 | 0.983 | 0.98 |
| Inception V3 | 90%-10% | 200 | 0.7750 | 0.761 | 0.80 |
|  | 80%-20% | 200 | 0.8095 | 0.830 | 0.80 |
|  | 70%-30% | 200 | 0.8095 | 0.830 | 0.79 |
|  | 50%-50% | 200 | 0.7530 | 0.755 | 0.76 |

On the other hand, the proposed also experienced a cross-validation technique to ensure the efficacy of the proposed architecture [24]. Figure 10 shows the corresponding validation curve that indicates 10-fold cross-validation with the false-positive rate in the horizontal axis and true-positive rate in the vertical axis. This figure shows that the prediction accuracy of the proposed model is almost 100%.

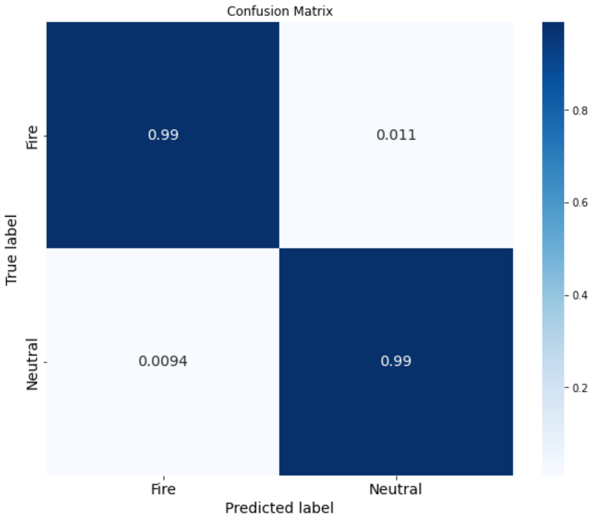

Figure 9. Confusion matrix with normalization of ResNet50

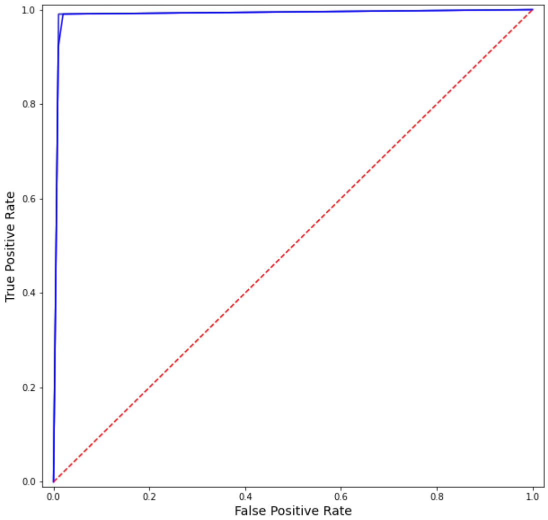

Figure 10. K-fold cross-validation curve

### 3.3. Comparison among existing systems

In this section, a comparison of our proposed work with previous similar types of security-related work has been shown. The comparison criteria are divided into three categories. The first one is the used methods of AI/ML techniques, the second one is the presence of IoT/WSN technology, and the last one is notification and remote monitoring system. If we look at table 6, we can see that our proposed work is the most enriched featureful system compared to others.

Table 6. A comparison among the same types of previous work and our proposed system

| Ref. No. | AI/ML Techniques Methods | | Detection | | | IoT/WSN Based Detection | | | Notification/ Remote Monitoring | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Alarm | |
| | Best performed method's name | Highest Accuracy | Fire | Firearms | Knives | Intruder | Smoke (Fire) | Short-Circuit | **GSM Call/SMS** | **App/Web-based** | Local | Remote |
| [5] | AI/ML is not used | | N/A | | | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |
| [6] | AI/ML is not used | | N/A | | | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ |
| [7] | AI/ML is not used | | N/A | | | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| [8] | AI/ML is not used | | N/A | | | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ |
| [10] | ResNet | 98.40% | ✗ | ✓ | ✓ | Not used | | | ✗ | ✗ | ✗ | ✗ |
| [11] | VGG16 | 99.73% | ✗ | ✓ | ✓ | Not used | | | ✗ | ✗ | ✗ | ✗ |
| [12] | Faster R-CNN | 97.92% | ✓ | ✗ | ✗ | Not used | | | ✗ | ✗ | ✗ | ✗ |
| [13] | YOLO | 76.00% | ✓ | ✗ | ✗ | Not used | | | ✗ | ✗ | ✗ | ✗ |
| **Proposed** | ResNet50<br>(for fire detection) | 99.49% | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

## 4. CONCLUSION

This paper represents a prototype of an intelligent security solution for shops and offices which is based on IoT-enabled sensors. The whole system utilizes three different technologies (IoT, deep learning, and GSM) to provide security from burglary, fire, and electrical short-circuit., the research has gone through a set of development processes to ensure the optimum outcome from this work. The proposed methodology is divided into three significant parts. The first one is sensor-based monitoring system where all sensors work together to detect intruder, fire, and electrical short-circuit. The second one is the fire detection approach using deep to detect fire at an earlier stage. The last one is the remote alarm and monitoring system, which can be very useful to warn the user in case of an emergency or to monitor the sensor's data and status in real-time. The proposed solution has used two pre-trained Convolutional Neural Network (CNN) architectures, namely ResNet50 and Inception V3. This research found an accuracy of 99.49% with ResNet50 architecture in fire detection. While working with the proposed methodology, two limitations have been observed. Firstly, the short-circuit detection system only works when the shop or office is closed, which means night time. Secondly, the sound sensor cannot identify any sound; the sensor can only measure the sound level in dB. For this limitation, the system may trigger a false alarm for an external sound such as a lightning strike sound, which is should not be a valid subject to concern. In the future, the research will try to fix these issues. Moreover, deep learning will be used here to detect various harmful objects like knives, guns, axe, etc., from the surveillance camera's video in real-time. However, the proposed security solution will be beneficial to the users to address optimized security at shops and offices with many exclusive features.

## REFERENCES

[1] H. Dickinson, "Retail Crime Survey: March 2020," 2020.

[2] J. Lowman, "ACS Crime Survey 2019," 2019.

[3] R. Campbell, "Structure Fires in Stores and Other Mercantile Properties," 2015.

[4] "Fire Alarm And Detection Market Size, Share & Trends Analysis Report By Product (Fire Detectors, Fire Alarms), By Type (Heat, Smoke Detectors), By Application (Commercial, Residential), And Segment Forecasts, 2020 - 2027," 2020.

[5] V. D. Vaidya and P. Vishwakarma, "A comparative analysis on smart home system to control, monitor and secure home, based on technologies like gsm, iot, bluetooth and pic microcontroller with zigbee modulation," in 2018 International Conference on Smart City and Emerging Technology (ICSCET), 2018, pp. 1-4.

[6] H. Huang, S. Xiao, X. Meng, and Y. Xiong, "A remote home security system based on wireless sensor network and GSM technology," in 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010, pp. 535-538.

[7] S. Tanwar, P. Patel, K. Patel, S. Tyagi, N. Kumar, and M. S. Obaidat, "An advanced internet of thing based security alert system for smart home," in 2017 international conference on computer, information and telecommunication systems (CITS), 2017, pp. 25-29.

[8] S. Somani, P. Solunke, S. Oke, P. Medhi, and P. Laturkar, "IoT based smart security and home automation," in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018, pp. 1-4.

[9] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, "IoT based smart security and home automation system," in 2016 international conference on computing, communication and automation (ICCCA), 2016, pp. 1286-1289.

[10] D. K. J. p. r. l. Jain, "An evaluation of deep learning based object detection strategies for threat object detection in baggage security imagery," vol. 120, pp. 112-119, 2019.

[11] M. T. Ağdaş, M. Türkoğlu, S. J. S. U. j. o. c. Gülseçen, and i. sciences, "Deep neural networks based on transfer learning approaches to classification of gun and knife images," vol. 4, pp. 131-141, 2021.

[12] B. Kim and J. J. A. S. Lee, "A video-based fire detection using deep learning models," vol. 9, p. 2862, 2019.

[13] D. Shen, X. Chen, M. Nguyen, and W. Q. Yan, "Flame detection using deep learning," in 2018 4th International conference on control, automation and robotics (ICCAR), 2018, pp. 416-420.

[14] D. R. J. I. J. o. A. R. i. C. S. Patnaik Patnaikuni, "A Comparative Study of Arduino, Raspberry Pi and ESP8266 as IoT Development Board," vol. 8, 2017.

[15] K. Kardas and N. K. J. E. S. w. A. Cicekli, "SVAS: surveillance video analysis system," vol. 89, pp. 343-361, 2017.

[16] (November, 18). Amazon Echo. Available: https://www.amazon.com/dp/B07XKF5RM3

[17] L. S. J. A. a. S. Manchineella, "Motion Detection Using Microwave Radar Sensor," 2021.

[18] R. C. Pandey, M. Verma, L. K. Sahu, S. J. I. J. o. E. D. Deshmukh, and Research, "Internet of things (IOT) based gas leakage monitoring and alerting system with MQ-2 sensor," vol. 5, pp. 2135-2137, 2017.

[19] J. Wen-ping, J. J. F. S. Zhen-cun, and Technology, "Research on early fire detection of Yolo V5 based on multiple transfer learning," vol. 40, p. 109, 2021.

[20] "Fire Detection Dataset," C. Ganteng, Ed., 1.0 ed, 2021.

[21] M. Islam, N. Tasnim, and J.-H. J. I. Baek, "Human gender classification using transfer learning via Pareto frontier CNN networks," vol. 5, p. 16, 2020.

[22] M. J. N. b. Ringnér, "What is principal component analysis?," vol. 26, pp. 303-304, 2008.

[23] S. Patro and K. K. J. a. p. a. Sahu, "Normalization: A preprocessing stage," 2015.

[24] K. J. T. T. i. A. C. Baumann, "Cross-validation as the objective function for variable-selection techniques," vol. 22, pp. 395-406, 2003.