Hindawi
Security and Communication Networks
Volume 2021, Article ID 9928254, 17 pages
https://doi.org/10.1155/2021/9928254

Research Article

Internet of Things-Based Intelligent Smart Home Control System

Olutosin Taiwo [1] **and Absalom E. Ezugwu** [2]

[1]*School of Mathematics, Statistics and Computer Science, University of Kwazulu-Natal, Westville Campus, Private Bag X54001, Durban 4000, South Africa*
[2]*School of Mathematics, Statistics, and Computer Science, University of Kwazulu-Natal, King Edward Avenue, Pietermaritzburg Campus, Pietermaritzburg, Kwazulu-Natal 3201, South Africa*

Correspondence should be addressed to Absalom E. Ezugwu; ezugwua@ukzn.ac.za

Received 17 July 2021; Revised 21 August 2021; Accepted 9 September 2021; Published 24 September 2021

Academic Editor: Muhammad Naveed Aman

The smart home is now an established area of interest and research that contributes to comfort in modern homes. With the Internet being an essential part of broad communication in modern life, IoT has allowed homes to go beyond building to interactive abodes. In many spheres of human life, the IoT has grown exponentially, including monitoring ecological factors, controlling the home and its appliances, and storing data generated by devices in the house in the cloud. Smart home includes multiple components, technologies, and devices that generate valuable data for predicting home and environment activities. This work presents the design and development of a ubiquitous, cloud-based intelligent home automation system. The system controls, monitors, and oversees the security of a home and its environment via an Android mobile application. One module controls and monitors electrical appliances and environmental factors, while another module oversees the home's security by detecting motion and capturing images. Our work uses a camera to capture images of objects triggered by their motion being detected. To avoid false alarms, we used the concept of machine learning to differentiate between images of regular home occupants and those of an intruder. The support vector machine algorithm is proposed in this study to classify the features of the image captured and determine if it is that of a regular home occupant or an intruder before sending an alarm to the user. The design of the mobile application allows a graphical display of the activities in the house. Our work proves that machine learning algorithms can improve home automation system functionality and enhance home security. The work's prototype was implemented using an ESP8266 board, an ESP32-CAM board, a 5 V four-channel relay module, and sensors.

1. Introduction

With the increasing prevalence of burglary and personal threats to home occupants and property damage, it is crucial to have an effective system to keep track of security in the home and environment. The safety and security of lives and properties are of great concern and should be prioritized. Therefore, a home should be equipped with an intelligent system to monitor remotely, control, and report activities to the occupant. To achieve security, safety, convenience, and control of a home, the need arises for an intelligent home automation system. A smart home is an application of the Internet of things (IoT) that enables occupants to monitor, control conveniently, and oversee their home activities from any location. According to [1], the Internet of things is an interconnected system that allows electronic devices to communicate and exchange data through network connectivity.

Smart home automation systems are therefore integral in ensuring a high quality of life by monitoring and controlling the home environment. The primary aims of a smart home automation system are safety, such as detecting harmful gases, fire or home intruders, convenience through remote monitoring and control of appliances and the physical environment, and reduction in energy and water consumption. Appliances and devices are networked through the IoT home hardware technologies of sensors and actuators for communication and automation, offering localized

or remote home control [2], thereby making the home intelligent by offering services that involve little human input or interaction. As an example, through the Internet, one could control a home from any location, the control mechanism being delivered through dedicated software or a mobile application running on a laptop, tablet, PC, or smartphone [3]. Sensors may be used in the home to monitor electricity and water usage, detect movement, and control temperature, humidity, and appliances in the house. A home populated with sensors generates a lot of readings and data. However, cloud computing services and machine learning algorithms have enhanced the smart home's functionality. Cloud computing services that benefit home automation systems are the storage of data, reduced risk of server outage and data loss, ease and efficiency of interaction with devices in the home, and automation of routine services.

Because each house may have several occupants, including human beings and animals, many movements will be detected in the home. There must, therefore, be a mechanism to distinguish between the movement of legitimate home occupants and their pets and that of an intruder. When combined with IoT technologies, a machine learning algorithm can assist in the detection and differentiation of movements in the home. Machine learning algorithms enhance security by differentiating between and classifying activities in the house. An example is the support vector machine algorithm, which can distinguish between human and animal movement in the home.

Analyzing and evaluating data to predict actions and environmental conditions and optimize automation is another advantage of using machine learning algorithms in smart home automation [4]. When the concept of machine learning is combined with IoT technologies in the design and development of a smart home automation system, the system yields exceptionally efficient performance. In this work, we present an Android mobile application-based system to control electrical appliances, monitor and measure environmental factors, movement, and capture images of possible home intruders. The system is designed to be low-cost, flexible, and extensible. The mobile application gives the command to switch OFF or ON any of the electrical home appliances for efficient use of energy. It measures the current humidity and temperature in the home and notifies the user, displays graphical readings of the home activities, and stores or retrieves the data in or from the cloud.

The objectives of this work are as follows:

(1) To develop an Android application for the remote control of basic electrical appliances, the monitoring and display of environmental factors in the home and its surroundings.

(2) To implement a sensor-based automation system for the detection of movement and intrusion in the home.

(3) To use a machine learning algorithm for distinguishing images in the home to avert false alarms by the security system.

2. Related Literature

Several research articles and existing literature have aimed at enhancing environmental control, energy management, home security, and other aspects of smart home automation systems. Machine learning algorithms have also been applied in the IoT field for classification, prediction, and analysis. This section presents articles in the field of IoT relevant to smart home automation and the use of machine learning in intelligent systems.

Govindraj et al. [5] presented a smart home automation system to replace the conventional home automation system using IoT technologies. The proposed system uses an Android application to control and monitor appliances, temperature, motion, and gases in the home environment, which is carried out via a satellite station and a radio frequency transceiver. Data generated by sensors are stored on the ThingSpeak cloud platform. A base station provides the necessary commands for home control. Also, a mobile application was designed to communicate with the satellite station, base station, and the cloud server for the overall control of the home, with a graphical display of sensor readings.

A voice-controlled home automation system was proposed by Rani et al. [6], which was based on artificial intelligence and natural language processing (NLP) techniques. To control home appliances, voice commands are issued over a mobile phone and interpreted using the predefined natural language processing medium. The system was only used to control home appliances and not extended to other aspects of home automation such as control, monitoring, and detection of environmental conditions, intruders, motion, etc.

Gladence et al. [7] proposed a client-server-based mechanism for smart home automation. The proposed system uses machine learning algorithms and NLP concepts to establish interaction between the systems and humans. The user issues command to carry out specific tasks such as controlling home appliances and doors and monitoring voice bed movement. The authors also designed a module to assist persons with disabilities through NLP and artificial intelligence techniques. Mehmood et al. [8] developed an object detection mechanism for the control of smart home appliances, in which the automation system was based on an object detection algorithm, model view controller architecture, and cloud of things. The IoT devices communicated with home appliances through the message queuing telemetry transport (MQTT) mode. This work showed that object detection algorithms combined with deep learning algorithms enhance object detection in a smart home environment.

An intelligent smart home automation system that carries out tasks based on the user's emotions was presented by Jaihar et al. [4] to control lights, sound systems, and other home devices. Several machine learning algorithms were combined and used to analyze the user's needs and the surrounding conditions to predict actions and minimize user interaction. The home appliances are switched ON or OFF according to the emotion detected by the machine

learning model. Their approach enhanced energy efficiency in the home.

An approach to controlling home appliances based on intelligent decision-making and analytics was presented by Majeed et al. [9], which used the support vector machine for its intelligent decision-making and blockchain technology for the security of IoT devices. An Android application was developed for the remote control of home appliances. The authors applied a linear kernel for decision-making about home appliances and their statuses.

A real-time algorithm for monitoring and control of the home, its environmental conditions, motion sensors, and electrical appliances was proposed by Khan et al. [10]. Lights were switched ON or OFF according to the algorithm generated inferences from the motion sensors. The proposed algorithm was also used to monitor the power consumption of various appliances in the home through the Wi-Fi module and was also applied to create an alarm based on the gas level in the home.

Detection of unusual energy consumption patterns was possible in an experiment using two deep neural network models for a smart home performed by Popa et al. [11]. The work used cloud computing services to derive a modular platform for collecting, aggregating, and storing data in the smart home environment. The authors showed that the suggested machine learning algorithms enhanced smart home automation by reducing energy consumption. Machorro-Cano et al. [12] used big data and machine learning techniques in their proposed energy-saving mechanism for appliances in a smart home environment. The system's energy efficiency was ensured using the J48 machine learning algorithm and Weka API, using techniques to classify the home energy consumption level by learning user behavior and consumption patterns. The system saved and displayed real-time records and recommendations on energy-saving in the home via the authors' developed mobile application called HEMS-IoT. Besides energy-saving, their approach also allowed the system users to interact with their homes and request the desired IoT service, addressing home comfort and the safety of both humans and devices. Along with monitoring energy consumption in the home and sending a regular notification about it, Singh et al. [13] proposed a smart home automation system for controlling electrical appliances, doors, and detection of movement in a house. The system could also send an alert to the user in response to sensors detecting low levels of gas in a cylinder or the presence of a human. A prototype implementation of the system was carried out using an Arduino Uno board, a Node MCU ESP8266, IR and LDR sensor modules.

Taiwo et al. [14] proposed a framework for controlling home appliances such as bulbs, fans, heaters, sockets. The proposed framework allows on- and off-site home control using Bluetooth and Zigbee technologies for communication and an Android mobile application for issuing commands. The communication range was, however, low because of the proposed Bluetooth technology.

A machine learning algorithm was proposed as a method in smart home automation to detect gas leakage, smoke, and fire in the home by Salhi et al. [15]. The approach presented by the authors uses a data flow model and data acquisition through sensors in the home for analytics and prediction. In conjunction with the sensed information, the data mining method was used to detect abnormalities in the air. Their approach was aimed at enhancing the safety and protection of property in smart homes. An Arduino Uno board was used to aggregate data generated by sensors, and a Raspberry Pi was used as a machine gateway to receive the sensed information.

A hybrid home automation system was proposed by Jabbar et al. [16]. The system controls electrical appliances and monitors environmental conditions, motion, and gas levels in the home, both locally and remotely, via a mobile application or laptop application. The authors developed a prototype for the system, called IoT@HoMe, for which a NodeMCU was used as a Wi-Fi-based gateway to connect different sensors in the home. Data generated by the sensors are uploaded to a cloud server (Adafruit IO) and accessed via If This Then That (IFTTT) on the user's smartphones or laptops.

Vaidya et al. [17] proposed an Android application-based smart home automation system for the elderly. The user controls the appliances in a home remotely via voice or touches commands. The door monitoring system functions through face detection by the installed camera. The system also incorporates an energy efficiency option through a module that can analyze the usage of each electrical appliance. The light intensity and fan speed can also be managed to reduce energy consumption in this approach.

Suraj et al. [18] presented a smart home automation system to sense the status of home appliances and determine if they are ON or OFF. The system is based on visual machine intelligence and discrete sensors as a substitute for sensors in a smart home. Based on the outcome of the visual monitoring, the desired home appliance is switched to the desired state, and an update is sent to the user about the status through a designated website.

A smart home metering and automation system were proposed by Mahmud et al. [19]. The system monitors, controls, and observes home appliances and electronic machines through a designated website. The system aims to provide easy monitoring of home appliances and energy efficiency. An online metering system was also included in their design for observation of anomalies in the power distribution of the household and a billing system to enhance energy efficiency. Hanumanthaiah et al. [20] proposed a smart switch home automation system for the remote control of home appliances. The power consumption was monitored through current and voltage sensors linked to a cloud platform, which provides a notification when the energy consumption in the home is higher than the threshold value.

A home security, control, and monitoring system was proposed by Kundu et al. [21], which monitors environmental conditions such as temperature, humidity, and fire and controls home appliances via multiple means. Control and monitoring are put into effect through voice, electrical switches, and the Internet. Home security involves a

notification being sent to the user when a home intruder is detected. The system is designed for wireless communication between the user and the home without a location barrier.

An Android-based smart home automation system was proposed by Rout et al. [22] for the remote observation, monitoring, and control of home appliances, the physical environment and intrusion detection via a smartphone, using cloud computing services for communication. The system uses a machine-to-machine (M2M) feature for the control. A prototype implementation was carried out using a NodeMCU, an ATMega 16, and ESP8266 IoT hardware.

A bluetooth-based smartphone application for the control of home devices, doors, and overall home monitoring was presented by Saravanan et al. [23]. Their system automatically switches off the lights at night, detects gas leakage or smoke, and controls home appliances. The system also locks and unlocks the door in the home automatically via an authentication module. Communication with the user's smartphone and the hardware is via Bluetooth.

A multifunctional system for the remote control and monitoring of home appliances, environmental conditions, and detection of movement was proposed by Liao et al. [24]. The system uses an Android application to control the home and its appliances via Wi-Fi or mobile-cellular networks. The system involves sensors, detectors, and actuators to monitor and detect motion, gases, temperature, and humidity. Data generated by sensors in the system were transmitted to a cloud platform to receive commands and for automatic control of devices and appliances.

Pujari et al. [25] developed an Android application with a Firebase database to transmit sensor data, receive commands and automatically control devices in the home. Automatic control of lights in their system is based on feedback from the passive infra-red (PIR) and light dependant resistors (LDR) sensors in the home. The work also incorporates detection of motion, gas leakage, and environmental conditions.

The services of the ThingSpeak cloud platform are proposed by Akhtar et al. [26] to automate the control and monitoring of electrical appliances, water sprinklers, door locks, and other appliances in the home. The presented method also incorporates a reduction in home energy consumption through automated behavior programmed into the system using fuzzy logic.

Hoque and Davidson [27] presented a smart home security system framework, which uses a smart door sensor with radiofrequency transceivers for communication. The user receives an alert about the opening or closing of the door through an Android application. A prototype was presented using an Elgoo mega 2560 board, an RF receiver-transmitter, and Raspberry Pi. The presented technique did not cover a wide communication range. A device patching framework for IoT devices' security and the network was presented by Aman et al. [28]. The system ensures the security of IoT networks, data, and devices in various application areas against malware attacks. An IoT smart home environment is heterogeneous [29], and the security of devices must be ensured. Also, energy efficiency in smart homes involves the transmission of data [30]. The data generated must be secured to prevent loss of data. The framework in [28] uses a remote attestation for detecting devices that have been comprised in an IoT environment and traces the source of the malicious activities. Several levels of security were proposed for achieving a secured network. A model was also developed to act as access control and cub the spread of device-to-device malware spread in an IoT environment.

Durani et al. [31] based their home management system on IoT technologies and Blynk mobile. Their work aims to control devices and multiple sensors in a house through the Internet. Their proposed system is designed to operate in both manual modes, via a phone, and an automatic mode, via a desktop computer. The proposed system incorporates sensors to monitor temperature and humidity and detects a fire, gas leakage, or intruders in the house.

Garg et al. presented [32] a home automation system for sensing and maintaining appropriate environmental home conditions and to provide security from theft or hazard using sensors and controlling home appliances. It uses a cloud database to retrieve commands that control the home over the Internet. The cloud database is also used to store time-based parameters from various sensors in the home.

3. Motivation and Conceptualization

Home security and safety are important to human health, welfare, mental stability, and peace of mind. For instance, people who have experienced home-intrusion might be distracted by this concern while away at work and so be less productive or efficient in their duties, which could, in turn, affect their health or advancement at work. So, being reassured that one's home is secured while he is away would allow the owner to concentrate on the work at hand. On the other hand, while the owner is at home, a security system that alerts the owner of an impending danger would afford them ample time to alert security agencies and avoid the worst consequences. Such scenarios have motivated us to contribute to the smart home automation field of the Internet of Things. We are, firstly, motivated to design and develop a system that controls home appliances, monitors environmental conditions, detects motion, and alerts the homeowner of an intrusion.

An efficient smart home automation system is described as a set of methods intended to make a traditional home intelligent through the use of IoT technologies for enhanced home security [32], energy efficiency [12], remote control of home appliances [16, 33], comfort [34], convenience, and detection of movement in the house [27]. The second motivation for this work arises from the issue of false alarms from a home security system. A home will house several occupants, both human and animals, usually pets, all of which would be sensed as moving from time to time, although the nature of the movement may differ. An efficient home security system should be able to distinguish between the home occupant(s) and pets and an intruder before an alert is sent to the user and the alarm is raised. If such a mechanism is not put in place, the efficiency of the system will be low. To this end, we are motivated to contribute to

knowledge in the field of smart home automation by using machine learning techniques to enhance security in a home with a system that can differentiate between regular home occupants and an intruder before an alarm is raised. To address this issue of differentiation and averting false alarms in a smart home automation system, we propose the support vector machine (SVM) learning algorithm for classifying, learning, and detecting an intruder in a smart home environment. The SVM concept for this study is further described in the next subsection.

3.1. Identity Detection in Smart Home Environment. This section focuses on using (support vector machine) SVM machine learning algorithms, which we propose for the classification and extraction of unique features from an image captured by the camera in the smart home environment. The classification algorithms will enable the system to distinguish between occupants and intruders before an alarm is raised. To achieve this, we propose a support vector machine to classify our images efficiently. A support vector machine is defined as a supervised and linear machine learning algorithm used for classification and regression problems [35]. SVMs are applicable in text recognition, handwriting recognition, face detection, motion detection, image classification, and so on [36, 37]. SVM is a machine learning algorithm used to classify data that is linearly or nonlinearly separable. It works by finding the optimal separating hyperplane that best discriminates the data. The support vector machine is fast, accurate, and reliable for analysis prediction with a small amount of data [38, 39]. This forms the justification for its use in our study. In our work, the SVM is used to classify and automatically extract features from the images to identify persons or objects in the home. The unique features considered for the image processing include features of a human face such as the eye color, shape of the face, skin color or tone, shape of the nose. In our chosen home environment, the motion sensor detects movement and sends a signal to the camera to capture a picture of the object whose motion was detected. Since there are many occupants in the home, each with its own unique features, the machine learning algorithm is used to process the detected image to ensure its identity before the system raises a security alarm.

The support vector machine works by applying a supervised learning algorithm to find the optimal hyperplane that best separates the feature planes of the labeled data. Basic mathematical definitions for the binary classifier in SVM are given as follows:

Let $\mathbb{H}$ be a real Hilbert space with the inner product $\langle \cdot, \cdot \rangle$ and induced norm $\| \cdot \|$. Let $\mathbb{R}^n$ be the n-dimensional Euclidean space and ϕ: $\mathbb{R}^n \longrightarrow \mathbb{H}$ be a mapping. Given a training dataset

$$D_k \coloneqq \{(\mathbf{x}_i, y_i) | x_i \in \mathbb{R}^n, y_i \in \{-1, 1\}\}_{i=1}^k, \tag{1}$$

where y_i is the label of $\mathbf{x}_i$, the functional margin d_k is defined as follows:

$$d_k(\mathbf{x}) = \langle \boldsymbol{\omega}, \phi(\mathbf{x}) \rangle + \theta, \quad \mathbf{x} \in \mathbb{R}^n, \tag{2}$$

where θ is called the bias term. The optimal ω and θ for the given training dataset will yield the optimal hyperplane for the SVM. To obtain the optimal ω and θ, one has to solve the following optimization problem [1]:

$$\begin{cases} \text{Minimize:} & g(\boldsymbol{\omega}, \theta) = \dfrac{1}{2}||\boldsymbol{\omega}||^2 + C\sum_{i=1}^{k}\xi_i, \\ \text{Subject to:} & y_i(\boldsymbol{\omega}, \phi(\mathbf{x}_i) + \theta) \geq 1 - \xi_i, \\ & \xi_i \geq 0, i = 1, 2, \ldots, k, \end{cases} \tag{3}$$

where $C > 0$ is the regularization parameter, which needs to be specified *a priori*.

Alternatively, using the Lagrange multiplier method, the optimal vector ω is obtained as follows:

$$\begin{cases} \omega = \sum_{i=1}^{k}\alpha_i y_i \phi(\mathbf{x}_i), \\ \text{subject to: } \sum_{i=1}^{k}\alpha_i y_i = 0, \end{cases} \tag{4}$$

where $\alpha_i, i = 1, 2, \ldots, k$ are the solution of the Wolfe dual of the optimization problem (2) [40]. Substituting (3) in (1) then yields that for a test datum $\mathbf{x}_0$,

$$\begin{aligned} d_k(\mathbf{x}_0) &= \langle \omega, \phi(\mathbf{x}_0) \rangle + \theta \\ &= \left\langle \sum_{i=1}^{k}\alpha_i y_i \phi(\mathbf{x}_i), \phi(\mathbf{x}_0) \right\rangle + \theta \\ &= \sum_{i=1}^{k}\alpha_i y_i \langle \phi(\mathbf{x}_i), \phi(\mathbf{x}_0) \rangle + \theta. \end{aligned} \tag{5}$$

Let K: $\mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$ be a kernel function defined as follows:

$$K(\mathbf{x}_i, \mathbf{x}_j) = \langle \phi(\mathbf{x}_i), \phi(\mathbf{x}_j) \rangle. \tag{6}$$

Then, according to (5),

$$d_k(\mathbf{x}_0) = \sum_{i=1}^{k} \alpha_i y_i K(\mathbf{x}_i, \mathbf{x}_0) + \theta. \quad (7)$$

The SVM is denoted as $f_k(\mathbf{x}_0)$, is defined as follows:

$$f_k(\mathbf{x}_0) = \operatorname{sgn}(d_k(\mathbf{x}_0)) = \begin{cases} 1 & \text{if } d_k(\mathbf{x}_0) \geq 0, \\ -1 & \text{if } d_k(\mathbf{x}_0) < 0. \end{cases} \quad (8)$$

Support vectors are the training data with nonzero α. Thus, by specifying the kernel K and the penalizing coefficient C, we can classify the data. There are several kernel types for classifying data. A commonly used technique for selecting the optimal kernel and regularization coefficient is cross-validation [41, 42], which is also applicable in this work.

4. Overview of the Proposed System

Smart home automation is an application area of IoT for remote home control, comfortable and healthy living, energy efficiency, safety, security, and social benefits. IoT technologies have made it possible for home occupants to remotely have total control over their homes, appliances, environmental conditions, and activities in their homes and their surroundings, regardless of the current location of the home occupant. Several commercial products such as Amazon Echo, Google Nest Hub, Wink Hub2, Samsung SmartThings, and Apple HomeKit have been developed, tested, implemented, and used for the intelligent control of a home. As discussed in Section 2, different approaches have been proposed and presented in the literature by several researchers. However, interoperability, security of data, data analytics, security of communication, and the home remain prominent challenges in smart home automation [43–47]. To address some of these existing challenges in smart home automation, we present an intelligent home automation system, which we have named the intelligent home control and security system (iHOCS). The next subsection describes our system and indicates its overall functionality.

4.1. The iHOCS System. The iHOCS system is an IoT-based intelligent home automation system for controlling basic home appliances using daily monitoring of environmental factors around the house and detecting harmful gases and motion in it. Our iHoCS is designed to contribute to the field of home automation in IoT by providing comfort, convenience, security, and safety for home occupants. We introduce a system that uses the support vector machine algorithm as a machine learning tool to classify images detected from movements in the home, distinguish between regular occupants or their pets, and an intruder. In our presented system, the user monitors, controls, and oversees the house through an Android-based mobile application. The iHOCS integrates six modules for its functionality and presentation: namely, the intelligent device module, the communication and gateway module, the management and decision module, the cloud computing module, the presentation module, and the security module. These are discussed in turn in the subsections that follow.

4.1.1. Intelligent Device Module. The intelligent module of the system describes the smart devices that function in the home, including light bulbs, heaters, a microwave, fans, the television, air-conditioners, sensors, etc. The home appliances are integrated with a level of smartness for intelligent responses when receiving commands. The sensors are used for data gathering, monitoring, and detection in the home. They are motion sensors for movement detection, gas, smoke, and fire detectors; temperature and humidity sensors for measuring and monitoring environmental factors; and a smart camera to capture images of an intruder.

4.1.2. Communication and Gateway Module. This module is needed for interaction and communication between the home devices and sensors and the outside world. In a smart home environment, Gateways allow local and external networks to connect and communicate with one another. The devices and sensors in the home are connected to a gateway for interaction among themselves and communication with the user. Our design uses an ESP8266 Wi-Fi board as the gateway for wider network coverage and extended communication. The system connects to the Internet via this gateway and communicates with all appliances and devices in the home. The communication protocols used are Wi-Fi, which is one of the primary operating standards for home automation technology, TCP/IP, and HTTPS/IP.

4.1.3. The Management and Decision Module. The iHOCS is a system that provides safety and security alongside the usual control of appliances. To strengthen the level of security, the SVM is used to classify some features in the home before sending an alert to the user about the detected motion. We give a scenario wherein the user is far from home, but other occupants are at home, or the home security has been switched on at night. In these two situations, movements would still be detected in the home and its surroundings. A motion sensor would only detect movement and could then send an alert to the user. However, these frequent alerts would most often be false alarms due to the movement of the legitimate home occupants, which would obviously be annoying. The use of machine learning algorithms enhances the system to correctly classify images and distinguish whether there is an intruder in the house or the movements sensed were those of regular home occupants. This module classifies the features of the image captured and analyses it to notify the user and save the picture of the intruder.

4.1.4. Cloud Computing Module. A smart home involves applications and portals that offer efficient and cost-effective solutions to track, connect, and manage anything from any location and at any time [48]. Our design for the iHOCS environment includes a DHT11, PIR motion sensor, and ESP32 camera that generate data at intervals set by the user. The generated data need to be stored for monitoring of the

home, for analysis, and for future prediction. The cloud infrastructure is needed for real-time storage of the data, processing, communication, and monitoring in a smart home. Therefore, in our work, a cloud computing module is used to store data generated, display it graphically, and process it.

4.1.5. Presentation and Control Module. The presentation module describes the interface that remotely controls the home. Through the mobile application, it allows the user to select the desired appliance to control or monitor. The screens and tabs for carrying out various tasks are designed in this module, along with the graphical display of output generated by the sensors in the home. The iHOCS system displays temperature and humidity, and output of the PIR motion sensor on the mobile application screen to allow the user to see any changes in the status of the home and surroundings.

4.1.6. System Security Module. The system security module ensures that the user has some level of security over the system. In iHOCS, an authentication mode is used to ensure that the platform user is the person intended. In the setup of the mobile application, the user's profile and configuration require a unique authentication code, which is sent to the user's e-mail address. The correct authentication code is required for programming the system to control and monitor devices and appliances. Without the correct authentication code, the mobile application will not be able to communicate with the home and control devices.

4.2. Architectural Design. Figure 1 above shows the architectural design of iHOCS system. As depicted in the architectural design, the system includes the user, home appliances, sensors, a Wi-Fi module, and the cloud platform. The ESP8266 Wi-Fi module does the dual work of communication and a microcontroller. This work uses a wireless mode of communication between the user, the home, and its devices. The ESP8266 collects data from the sensors and relay board and transmits the data over the Internet to the user. The user sends and receives commands and information to and from home through an Android mobile application, which in turn communicates with the microcontroller (ESP8266). The functional aspects of the system are home monitoring and control, together with home security. The flow of processes and actions in the iHOCS environment are presented using a flowchart in Figure 2.

The setup of iHOCS involves electrical sockets and other basic home appliances to be controlled, such as light bulbs, television, cooling, and heating apparatus. As stated earlier, it also measures environmental conditions around the house. Lastly, it detects movement and captures an image of the person detected. The sockets and home appliances are connected to the relay board module, and the relay module is connected to the ESP8266 for the Android application to receive and send commands. A DHT11 sensor is used to measure the humidity and temperature, and the values are displayed on the screen of the user's smartphone. The home is enhanced with greater security and safety of the occupants. A PIR motion sensor is used to detect movement in the house, and once detected, a notification is generated on the Android mobile application to keep track of the graphs. The SVM does a background check before sending an alert to the user and ringing the alarm. The cloud storage embedded with the mobile application stores all the data generated from all the sensors. The sensors are interfaced with the Wi-Fi module for wireless transmission to the cloud platform via the mobile application. Steps involved in the operations, services, communication, and transmission of data in the iHOCS system are stated in Algorithm 1. Based on the SVM algorithm, intelligent decisions are taken by the system for efficient monitoring and security of the home. Abbreviations used in the algorithm are given in italics below:

EHA: Electrical Home Appliances
HSD: Home sensors and detectors
NC: Network Connectivity
HC: Come control
M: Motion
CS: Cloud storage
HO: Home Occupant
PE: Pet
HP: Home premises
D: Darkness
LDR: Light Dependent Resistor
IM: Image

5. Results and Discussion

As shown in the architectural design, our iHOCS is set up using IoT hardware and software tools to achieve the desired intelligent home control, monitoring, and security system. We implemented a prototype of the iHOCS system using the following hardware components: DHT11 sensor, HC-SR501 PIR motion sensor, ESP8266 Wi-Fi board, 5 V four-channel relay module, breadboards, LEDs, LDR, and an ESP32 camera. A full description of the components is given below. After successful registration and configuration of the iHOCS Android mobile application, the user can perform the following basic functions:

(1) Control of electrical home appliances
(2) Monitor home environmental conditions (temperature and humidity)
(3) Automatic switch lights ON and OFF, based on the home condition
(4) Detection of movement in the home
(5) Receiving notifications about the home
(6) View graphical data of home sensors.

5.1. DHT11 Sensor. DHT 11 is a temperature and humidity sensor used for measuring environmental conditions. A DHT11 has an embedded negative temperature coefficient to

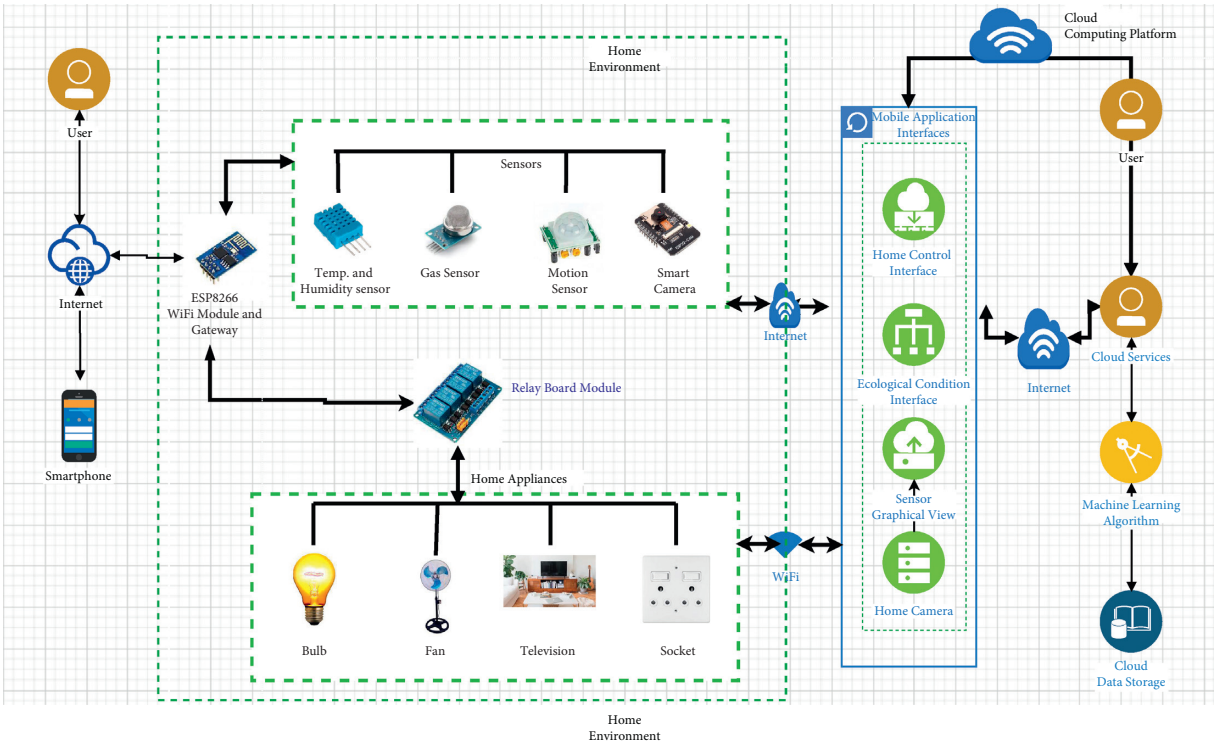


Figure 1: The iHOCS architecture.

measure temperature and an 8-bit microcontroller to give the temperature and humidity output as serial data. The sensor is easy to interface with microcontrollers. The advantages of a DHT11 sensor are that it is low-cost, small in size has a high sampling rate and can capture readings every second. The DHT11 possesses four pins: the VCC pin for power supply, data pin for communication between the sensor and the microcontroller, NC pin not connected, and the GND pin for connection to the ground. We use the DHT11 sensor to capture humidity and temperature readings in the home environment, and the values are displayed on the user's smartphone via the Android application. Knowing the current humidity and temperature of the home allows the user to take necessary actions for comfort.

5.2. HC-SR501 PIR Motion Sensor. An HC-SR501 is a motion-sensing IoT device used in prototypes with microcontrollers. It is highly reliable, sensitive, and can function in an ultralow-voltage operating mode. Other features of this motion sensor are its wide-range communication and an easy-to-use interface. It is used to detect a movement by an intruder and so is applicable in security systems, automatic garage doors, dryers, automatic washing machines, automatic lighting, and alarm systems. This PIR motion sensor has three pins (VCC, output and ground). An in-built voltage regulator can be easily powered by any DC voltage between 4.5 and 12 volts. The HC-SR501 PIR motion sensor is used in our work mainly to detect unauthorized movement in the home. However, it also sends a signal to the ESP32-CAM module for capturing the image. The SVM algorithm can perform a check to classify the features and determine if the movement is due to an intruder or not before the system raises the alarm.

5.3. ESP8266 Wi-Fi Development Board. The ESP8266 is a Wi-Fi Internet development with an integrated TCP/IP protocol stack that enables communication with the Wi-Fi network. It can also be used to set up a local network of its own to allow other devices to be connected to it directly. It is cost-effective with on-board processing and storage capabilities for integration with sensors and other IoT devices. Version 2.2.0 was used in this work, and it entails an ESP-12s Wi-Fi module with excellent antenna performance. The features are 11 digital input and output pins and analog pins. Our work uses the ESP8266 as a Wi-Fi module and development board for connection with sensors and the 5 V four-channel relay module, which triggers the electrical appliances.

5.4. 5 V Four-Channel Relay Module. A four-channel relay module is a board used to control high voltage and high current loads. It is designed for easy interfacing with a microcontroller board or sensors. It has 5 V relay channels for switching and isolating components. Each channel of the relay board has a LED indicator to depict when the relay is powered ON. The LED indicators brighten when the respective relay channel is energized. Our work uses a 5 V four-channel relay module to power on LEDs, which serve as fan, bulb, socket, and an additional unit for an extra appliance.

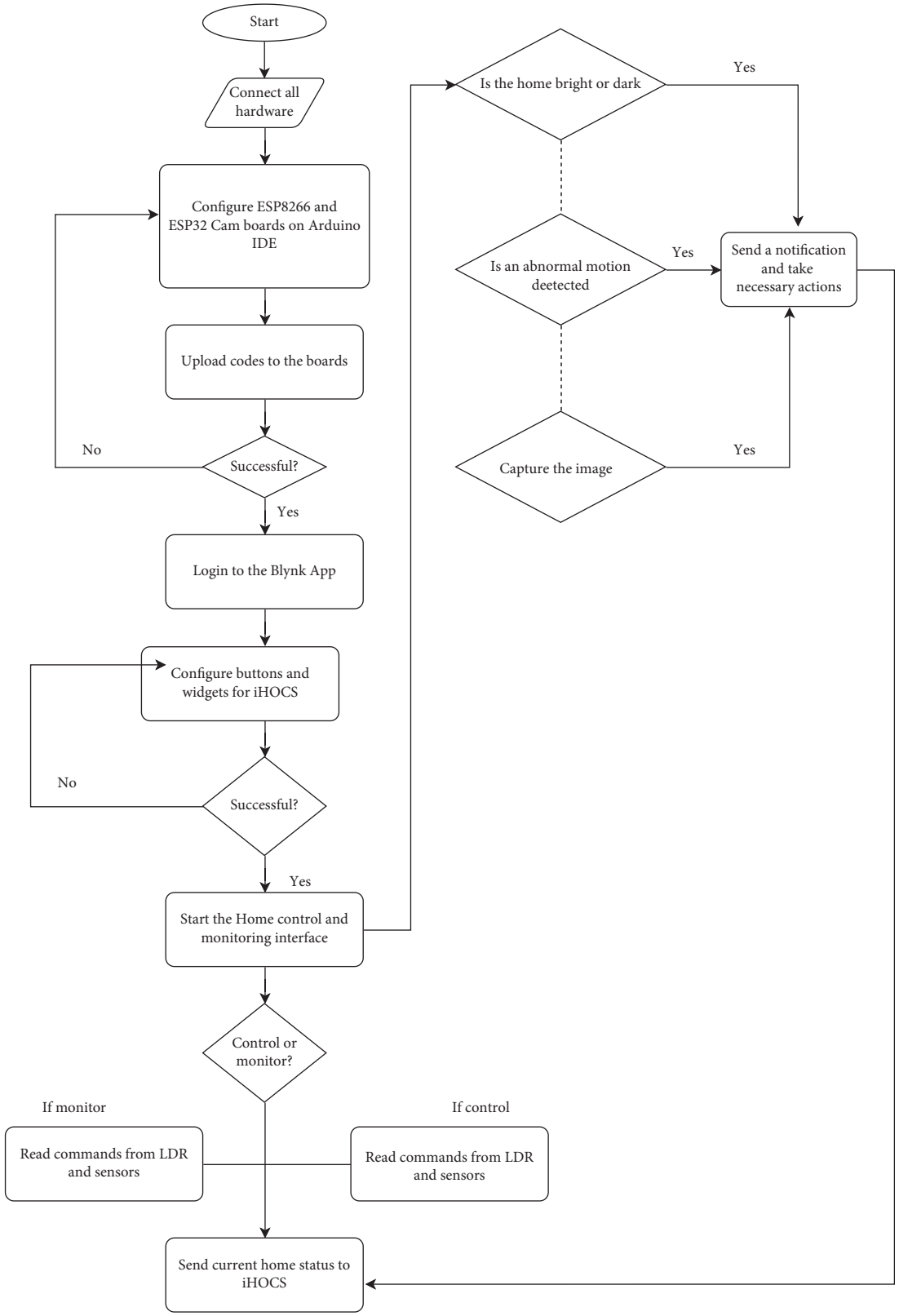


Figure 2: Flowchart of iHOCS.

5.5. ESP32-CAM. The ESP32-Cam is a low-cost development board with a Wi-Fi camera for image capturing and video streaming in IoT prototyping. The ESP32-CAM is a system on chip module with Wi-Fi and Bluetooth connectivity, camera, micro-SD card connector, and an in-built PCB antenna. The ESP32 is used to ensure security in a smart

(1) **Begin**
(2) Define N_c parameters
(3) Initialize *EHA* and *HSD*
(4) Establish and confirm the status of N_c
(5) **If** $N_c = 1$
(6) Evaluate the initial state of *EHA*; $\forall EHA \in N_C$
(7) **while** $EHA = n$ (where n = number of configured home appliances)
(8) Start *HC*
(9) **Else**, go to step 4
(10) **End if**
(11) **While** N_c&&$HC = 1$; continue action till the desired state is reached
(12) Evaluate the initial state of *HSD*; $\forall HSD \in N_C$
(13) **If** $HSD = n$ (where n = number of home sensors and detectors)
(14) Connect *iHOCS* to the Internet
(15) Acquire sensor data to *iHOCS* via the *ESP8266*
(16) **Else**, go to step 4
(17) For each round do
(18) Get the values for T, H, M and IM
(19) Upload data to *CS* via *iHOCS*
(20) Update status of *HSDs* in *iHOCS*
(21) Display graphical status of *HSDs* in *iHOCS*
(22) Synchronize data to *CS*
(23) **Else**, go to step 12
(24) **Case 1: (LDR)**
(25) **if** $(D = 1)$ **then**
(26) Notify the user "*It's DARK, Turn on the LIGHTS*"
(27) **Else**
(28) Notify the user "*Its BRIGHT, Turn off the LIGHTS*"
(29) **break;**
(30) **Case 2: (PIR Sensor)**
(31) **If** M is detected, **then**
(32) Notify user via e-mail "TOSIN: Motion detected"
(33) **break;**
(34) **Case 3: (ESP Cam)**
(35) **If** M is detected, capture *IM*
(36) Notify via iHOCS and apply *SVM*
(37) **If** $IM \in (PE_1, PE_2, PE_3, HO_1, HO_2, \cdots HO_n)$
(38) Mute alarm
(39) **Else**,
(40) Raise alarm and send picture to e-mail
(41) **end if**
(42) User monitors EHA and HSD via iHOCS app
(43) Remotely control the home
(44) **End**

Algorithm 1: Intelligent home control, monitoring, and security algorithm.

home automation prototype. It is used here with an FTDI programmer because the ESP32-Cam does not have a USB connector. Therefore, the FTDI is used to upload code written on the Arduino IDE to the ESP32-CAM module to receive instructions for the image capturing.

5.6. Software Components. The control and monitoring of the home, its devices, appliances, and sensors can only be carried out through a set of predefined instructions, procedures, and programs. Our iHOCS system uses specific software packages to function and communicate properly. The major software packages used for the configuration, coding, design, and development of the iHOCS system are the Arduino IDE and Blynk software.

5.6.1. Arduino IDE. The Arduino integrated development environment is a cross-platform software based on C and C++ programming languages for Windows, Linux, and MAC operating systems. The Arduino IDE is used to develop code that can be uploaded to boards. It is used to configure microcontroller boards in IoT prototyping. Code to control home appliances and sensors in iHOCS is written using the Arduino IDE and uploaded to the ESP8266 and ESP32-Cam boards.

5.6.2. Blynk Application. The Blynk application is a cross-platform application that works on both iOS and Android operating systems. It is an interface builder for the design of projects in the Internet of Things and its applications. It is used to design and develop a mobile application to control hardware, display, store, and visualize data generated by sensors. The Blynk platform comprises three major components: the Blynk app to allow individuals to create desired interfaces for projects using the available widgets; the Blynk server as a mode of communication between various pieces of hardware and the smartphone; and the Blynk libraries to enable communication between the hardware platforms, the server, and processes of incoming and outgoing commands. We use the Blynk application to design the graphical user interface, widgets, and graphical reading interfaces of our iHOCS system. Our work also uses the cloud computing services of the Blynk app as a cloud database for the real-time storage of sensor data and its parameters.

5.7. Results. This subsection presents a detailed explanation of the prototype functionality, configuration, and setup of all the components involved in the design and development of the iHOCS system. The training of the dataset for the machine learning image classification is also presented. The iHOCS system controls electrical home appliances (such as lights, fan, sockets, and one other electrical appliance), measures environmental conditions in the home (temperature and humidity), monitors movement and captures images after sensing a motion and sends the picture to the user via the mobile application on an Andriod-based smartphone anytime and anywhere. The code to configure the boards was written on the Arduino IDE, and after successful compilation, the programs were uploaded to the board via a USB cable. During the programming, the home network credentials were specified, stating the service set identifier (SSID) and password to have smooth connectivity. The authentication code generated during the setup of the mobile application in Blynk was also specified. An Android-based smartphone was used to issue commands that switch appliances OFF or ON. As described in the architecture, data generated from sensors in the home are acquired, stored in a cloud database, and displayed on the screen of the mobile application. The system has an advantage over previous works that made use of ThingsSpeak, and other web-based applications, because the user can visualize the trend of data right on the mobile application page without having to close or minimize the home control mobile application.

5.7.1. Image Classification. The images were processed to ascertain the validity of the SVM for the classification of images, as discussed in Section 3. As discussed earlier, the SVM algorithm supports a small amount of data for effective performance. Since the home environment in our work does not involve a large number of people or pets, a training dataset consisting of images of human beings and animals (dogs and cats) were downloaded from Kaggle to form the three classes that were to be differentiated by the algorithm; namely, human beings, dogs, and cats. The training dataset was imported into the MATLAB application of the R2017a version to determine if the intended SVM model gives the required and the best accuracy for our intended approach. We evaluated the performance of the machine learning algorithms using five-fold cross-validation. The SVM classifier determines the intelligent classification of images captured by the user. The downloaded dataset contains twenty images, and for the training, we divided the images into two main classes (home occupants and intruders). The home occupants class contains six images (four persons and two dogs), while the intruder class contains fourteen images (five cats, three dogs, and six persons). This segregation is justified because we believe intruders might be of a higher number than home occupants. Also, a pet can be an intruder. Figure 3 shows the SVM scatter plot alongside the legend. The blue color represents the occupant in the scatter plot, while the red color is used for an intruder. Figure 4 shows the confusion matrix, and Figure 5 shows the receiver operating characteristic (ROC) curve with an area under curve (AUC) value of 0.72619. The SVM algorithm yielded the best accuracy value of 80.0%, which is higher than other classifiers we compared with. We compared with K-Nearest neighbor (KNN) and decision tree classifiers with an accuracy of 70.0% and 65.0%, respectively.

(1) Performance Evaluation Metrics. A dataset contains data points for each class specified in a training model. These data points might lead to a biased classification if a class is of higher data points than the other class. For instance, in our work, we present two classes (home occupants and intruders). Suppose the data points of the intruder class are higher than the occupants' class. In that case, the algorithm will be biased towards the intruders' class if the evaluation is based on accuracy only. To correctly evaluate the performance of our model, we calculate the precision, recall, and $F1$-score values of the SVM algorithm and compare them with KNN and decision tree algorithms. Precision and recall values are useful in understanding the performance of an algorithm and the production of results based on the requirements, while the F1-Score provides a standardized representation of values [49]. Table 1 shows the effectiveness of the SVM classifier in comparison with other classifiers using the precision, recall, and $F1$-score metrics.

Precision: Precision is defined as the fraction of relevant instances among the retrieved instances. It is also referred to as positive predictive values. In other words, precision is the percentage of the positive predictions that the model rightly made. Precision is calculated as follows:

$$\text{Precision} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Positives (FP)}}. \tag{9}$$

Recall means the percentage of actual positive predictions that were rightly classified. Recall is calculated as follows:

$$\text{Recall} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Negatives (FN)}}. \tag{10}$$

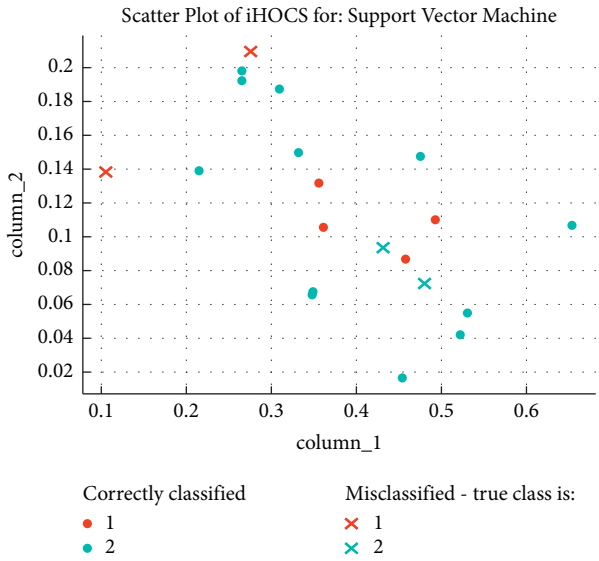


Figure 3: SVM scatter plot diagram.

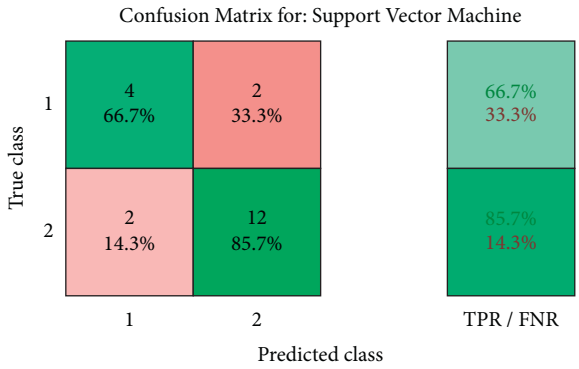


Figure 4: SVM confusion matrix.

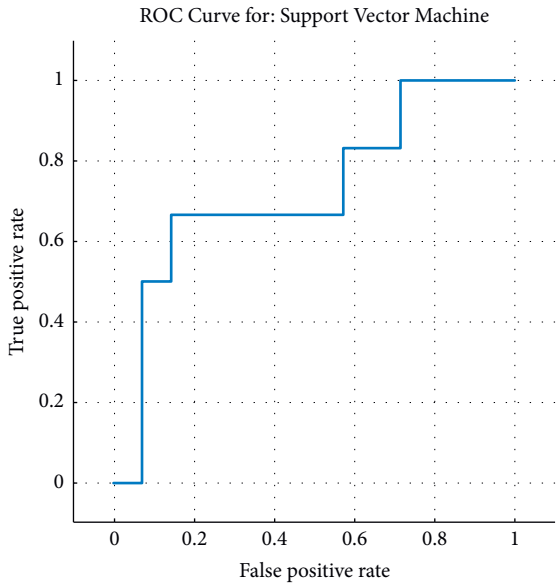


Figure 5: SVM ROC curve.

F1-Score: *F*1-Score is a measure of the accuracy of a test. It is calculated from the precision and recall of a test. The *F*1-Score metric takes the precision and recall values to provide a standardized value representation. *F*1-Score is calculated as follows:

$$F1\text{–Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}. \quad (11)$$

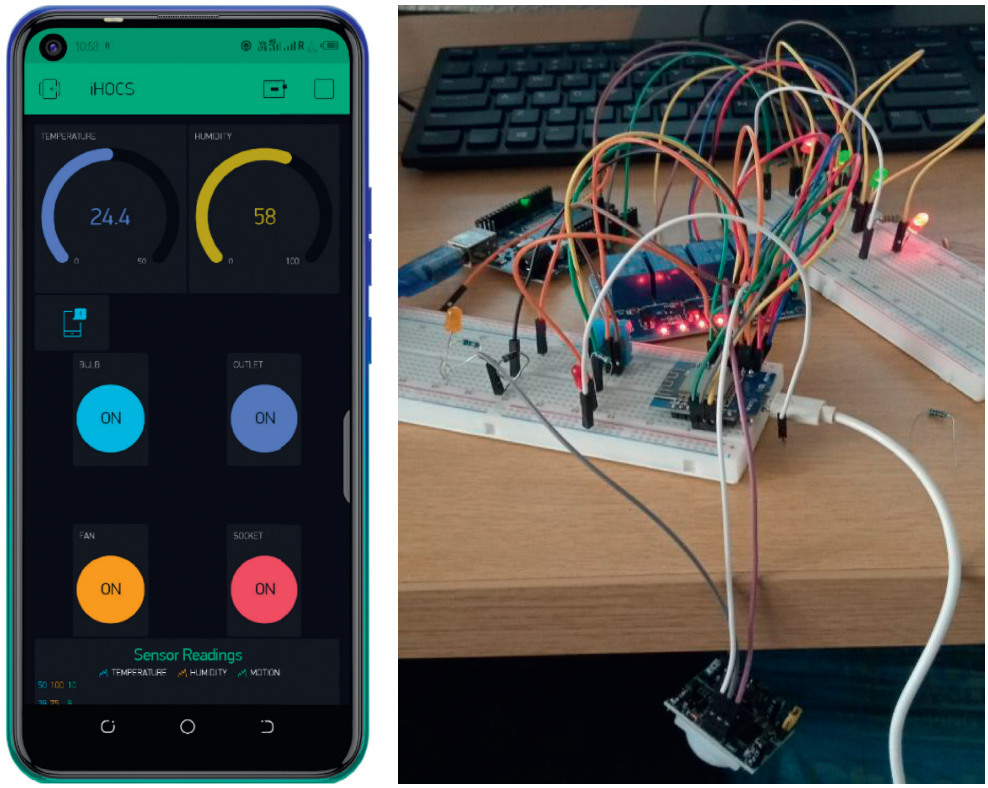
5.7.2. Prototype Implementation. The prototype implementation integrates an ESP32-CAM board, an FDTI serial converter, breadboards to link the various hardware components to each other, an HC-SR501 PIR sensor, a DHT11 temperature, and humidity sensor, several jumper cables, an Arduino board, LEDs, resistors (10k, 1k and 220 ohms), NPN transistor, and 5 V four-channel relay module. Jumper cables (male to male, female to female, male to female) were used to establish links on the breadboards for communication between the respective hardware components and also direct communication between the components. The ESP8266 served as both the Wi-Fi module and the microcontroller. It connects the home appliances (represented by LEDs) wirelessly and sensors to the Internet and connects the various hardware components to a gateway (microcontroller). The output units of the 5 V four-channel relay board were connected to the specified pins of the ESP8266 board, amd the DHT11 and PIR motion sensors were also connected to the microcontroller board using the appropriate jumper cables and pins. Different LEDs were used to indicate our electrical appliances (bulb, fan, socket, and an outlet for additional home appliances). The lights of the LEDs turn ON or OFF as specified by the command from the smartphone. Figure 6(a) shows the command to switch ON all four appliances in the home, while Figure 6(b) shows the corresponding lights from the LEDs. In Figures 7(a) and 7(b), three appliances were switched ON, and one appliance was turned OFF.

The values of the temperature and humidity sensed around the home are displayed on the mobile application screen, as shown in Figures 8(a) and 8(b). The mobile application is designed to capture a reading from the DHT11 sensor every five seconds and display these. The cloud computing service and real-time cloud database rendered through the Blynk platform allow the DHT11 to gather the temperature and humidity values of the home and display them as a graphical output on the interface of the iHOCS application. Figure 8(a) shows the minimized graphical sensor readings on the screen, while Figure 8(b) shows the full screen of the graphical display of the readings.

As explained earlier, the iHOCS system also ensures the safety and security of the home. The ESP32-CAM board and a PIR motion sensor are used for prototyping the system's home security module. The motion sensor is used to detect movement in the house, while the ESP32-CAM is used to capture images of the object, person or animal captured. The motion sensor captures movements and sends a notification to the user via the mobile application (Figure 9(a)); a real-time graphical display of the motion sensor values is also

Table 1: Result metrics.

Model	Accuracy %	TP%	FP%	FN%	Precision	Recall	*F*1-Score
SVM	80	66.7	14.3	33.3	0.823	0.667	0.737
KNN	65	50.0	28.6	50.0	0.636	0.5	0.56
Complex decision tree	65	33.3	21.4	66.7	0.609	0.333	0.431



(a) (b)

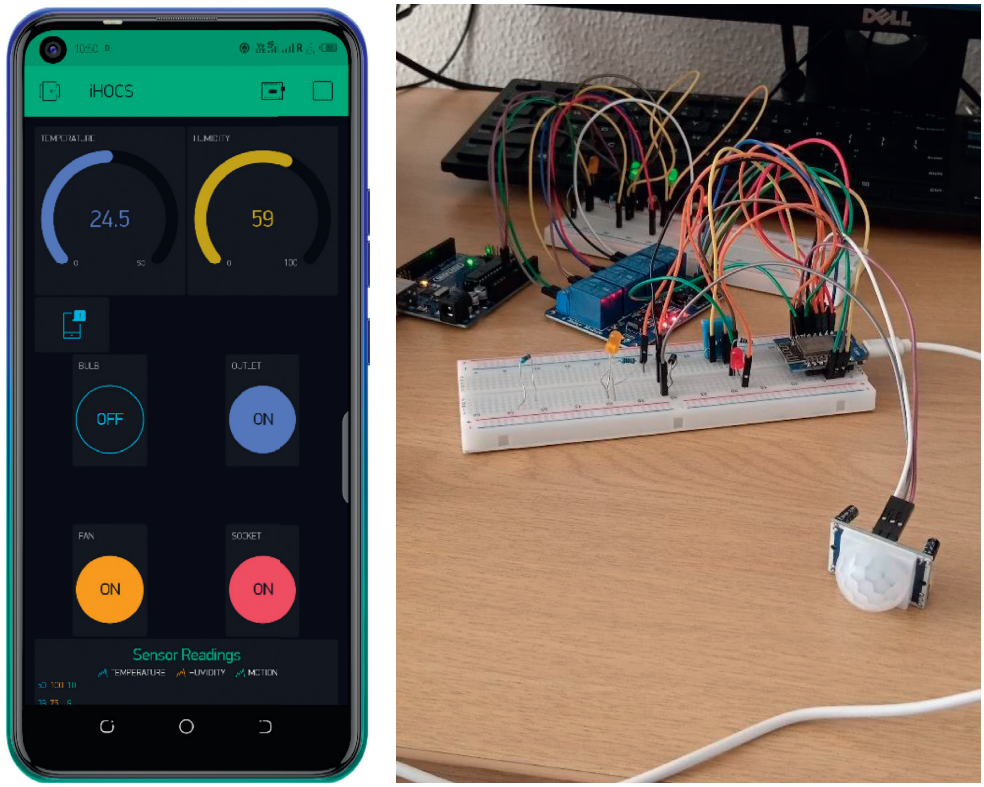
Figure 6: (a) All appliances ON. (b) Corresponding light indicators.

displayed alongside the temperature and humidity values (Figures 8(a) and 8(b)). Figure 9(a) depicts the notification sent to the user about a motion sensed in the home premises before capturing the image. Although our system automatically saves all images of the person responsible for the movement, our system is also enhanced by being designed to allow the user to capture the image of the person immediately so that the user may act proactively. The user may, if inside the premises, thus decide to ignore the notification or, if outside, would have an immediate view of the situation at home. Figure 9(b) depicted the captured image of the person in the house when the motion sensor sensed the movement. The ESP2-CAM has a light that makes it possible for it to capture an image even when it is dark.

The proposed system performs multiple functions of home control and energy conservation. Figure 10 shows the intelligent response from the environment to the switch on of the light. The system assists in conserving energy by sending a reminder notification to either turn OFF the light when it is bright or turn ON the light when it is dark. This enhances energy conservation and management in the home.

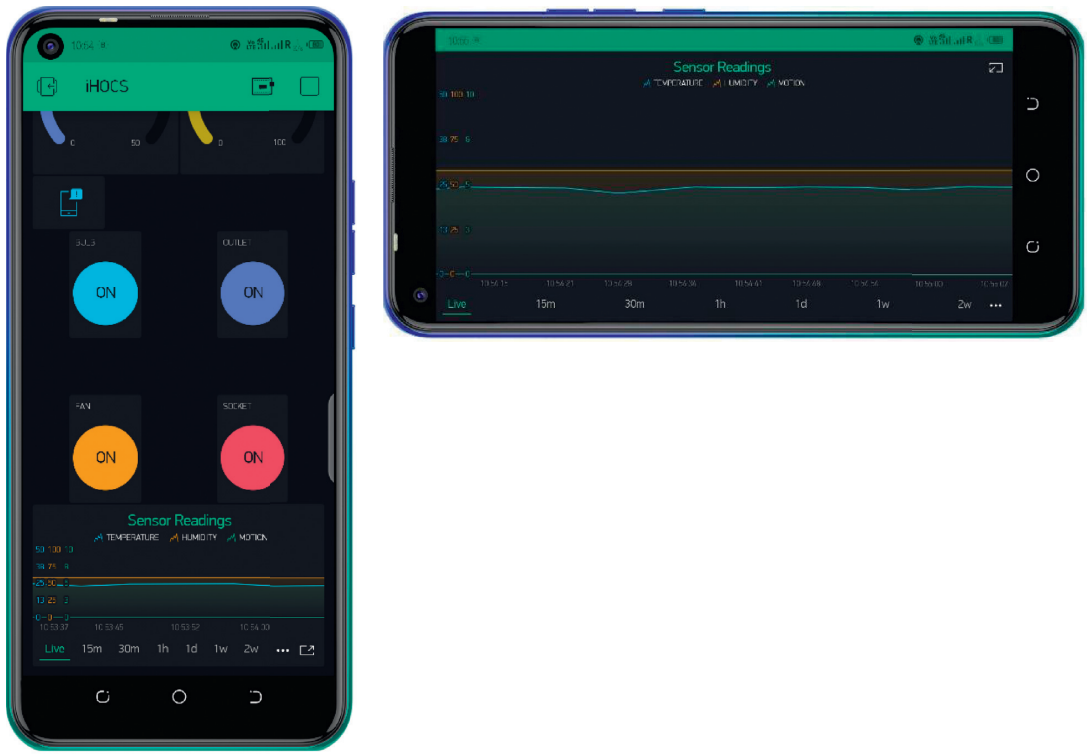
As noted with smart home automation systems, the system also gives convenience in allowing remote control of the home from any location. Thus, the home can be monitored and controlled remotely from any location. Monitoring of environmental conditions is also needed around the home for safety. For instance, if an older person, a handicapped, or a young one, is left at home, the user can monitor the temperature of the home from his remote location and assist the person at home to switch ON or OFF the fan or heater in the home to give the desired temperature. This promotes healthy living.

An added advantage of iHOCS is the security of the home and the proposed SVM algorithm for user notifications. With the aid of an SVM algorithm, false alarms and unnecessary notifications would be averted. Though all images sensed by the system would still be captured for future reference, the user will only be notified when the system classifies the image as that of an intruder.



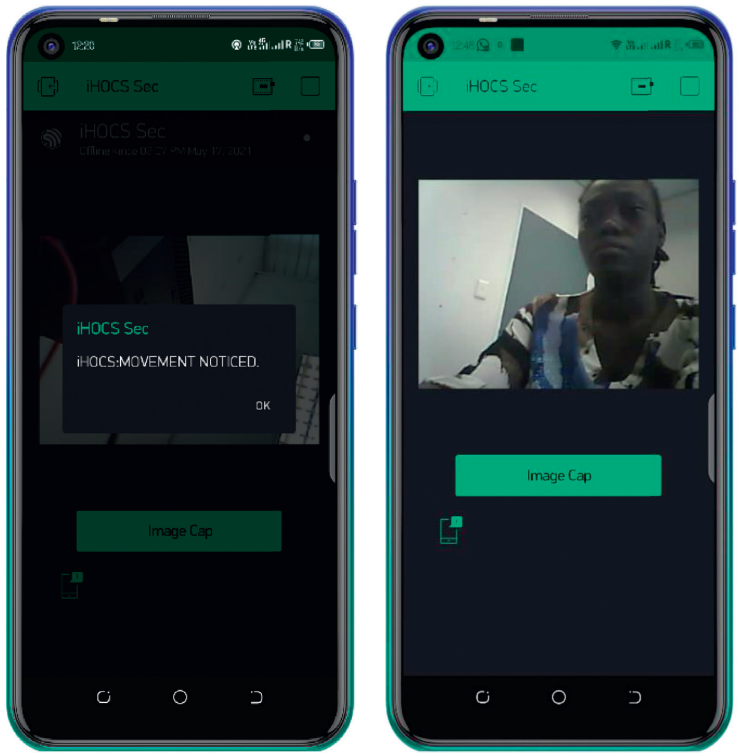
(a) (b)

Figure 7: (a) Three appliances ON. (b) Corresponding three LED indicators ON.



(a) (b)

Figure 8: (a) In-app graphical readings. (b) Full screen of graphical readings.



(a) (b)

Figure 9: (a) Movement notification. (b) Captured image.

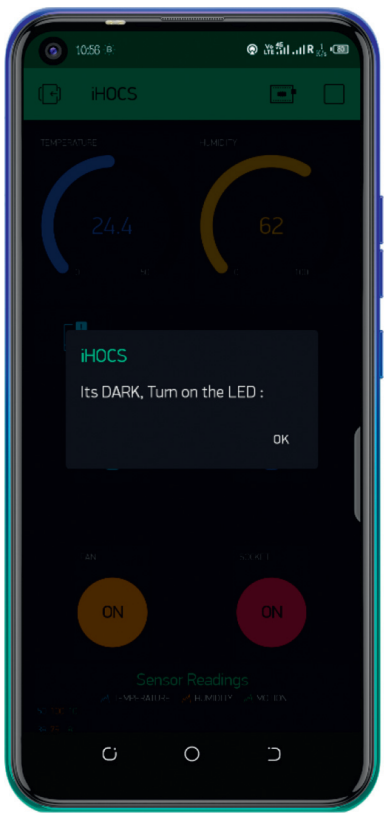


Figure 10: Intelligent home response.

6. Conclusion

This work has presented an intelligent home automation system based on IoT technologies, cloud computing, and a machine learning algorithm. The home automation system allows remote and local control of the home via an Android-based mobile application. The system controls electrical home appliances, monitors environmental conditions through temperature, humidity, and light sensors, and ensures home security through a motion sensor and an IoT camera. The system makes intelligent decisions to automatically turn ON or OFF lights and allow the user to view a picture of the person captured by the camera and decide whether to save it. The system is scalable, and the application allows additional appliances with an extra configured point, simply named outlet in our work. Also, the mobile application uses a real-time cloud database to record data gathered. It also displays the trend of the readings graphically on the screen of the mobile application. These data can be analyzed and used for future prediction. The next phase of the work will be to use a dataset of several real-life images captured by the camera from the system or sourced from relevant datasets in the field of home automation and train a machine learning algorithm to classify them so that the system could differentiate between an intruder and the home occupants. Also, we plan to enhance the system such that the user will only receive captured images of an intruder, and other captured images will be saved in real-time into the

cloud-based database of the system. This will remove the limitation on the encumbrance of a load of images on the mobile application. In addition, machine learning will also be used to enhance the PIR sensor's performance to differentiate between an animal, the occupant, and an intruder. This will reduce the notification from the PIR sensor to the user. The machine learning algorithm will also be applied to classify detected images to work with several occupants and a larger data set of intruders.

As a future direction, we plan to broaden our horizons to integrate machine learning into a mobile application to classify images captured by the camera and notify the user about the exact identity of the captured object. Also, we intend to extend the mobile application to function on the iOS platform. The approach presented in this work can also be applied to security systems in large communities like smart cities, office areas, hotels, malls, and university environments to enhance the security system of the specific environment. It is also believed that with machine learning, prediction is made easy. Machine learning can also be applied to the environmental module of smart home automation to predict weather and home conditions [50].

Data Availability

The experimental data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] K. Ashton, "That "internet of things" thing," *RFiD Journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] C. J. Diane, "How smart is your home?" *Science*, vol. 335, no. 6076, pp. 1579–1589, 2012.

[3] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, "Benefits and risks of smart home technologies," *Energy Policy*, vol. 103, pp. 72–83, 2017.

[4] J. Jaihar, N. Lingayat, P. S. Vijaybhai, G. Venkatesh, and K. P. Upla, "Smart home automation using machine learning algorithms," in *Proceedinfs of the International Conference for Emerging Technology*, IEEE, Belgaum, India, June 2020.

[5] V. Govindraj, M. Sathiyanarayanan, and B. Abubakar, "Customary homes to smart homes using internet of things (IoT) and mobile application," in *Proceedings of the International Conference on Smart Technologies for Smart Nation*, IEEE, Bengaluru, India, Aug 2017.

[6] P. J. Rani, B. Jason, K. U. Praveen, K. U. Praveen, and K. Santhosh, "Voice controlled home automation system using natural language processing (NLP) and internet of things (IoT)," in *Proceedings of the Third International Conference on Science Technology Engineering and Management*, IEEE, Chennai, India, March 2017.

[7] M. V. Gladence, M. V. Anu, R. Rathna, and E. Brumancia, "Recommender system for home automation using IoT and artificial intelligence," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–9, 2020.

[8] F. Mehmood, I. Ullah, S. Ahmad, and D. Kim, "Object detection mechanism based on deep learning algorithm using embedded IoT devices for smart home appliances control in CoT," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–17, 2019.

[9] R. Majeed, N. A. Abdullah, I. Ashraf, Y. B. Zikria, M. F. Mushtaq, and M. Umer, "An intelligent, secure, and smart home automation system," *Scientific Programming*, vol. 2020, Article ID 4579291, 14 pages, 2020.

[10] S. A. Khan, A. Farhad, M. Ibrar, and M. Arif, "Real TIme algorithm for the smart home automation based on the internet of things," *International Journal of Computer Science and Information Security*, vol. 14, no. 7, pp. 94–99, 2016.

[11] D. Popa, F. Pop, C. Serbanescu, and A. Castiglione, "Deep learning model for home automation and energy reduction in a smart home environment platform," *Neural Computing & Applications*, pp. 1–21, 2018.

[12] I. Machorro-Cano, G. Alor-Hernandez, M. A. Paredes-Valverde, L. Rodriguez-Mazahua, J. L. Sanchez-Cervantes, and J. O. Olmedo-Aguirre, "HEMS-IoT: a big data and machine learning-based smart home system for energy saving," *Energies*, vol. 13, no. 1097, pp. 1–24, 2020.

[13] H. Singh, V. Pallagani, V. Khandelwal, and U. Venkanna, "IoT based smart home automation system using sensor Node," in *Proceedings of the Fourth International Conference on Recent Advances in Information Technology*, IEEE, Dhanbad, India, March 2018.

[14] O. Taiwo, A. E. Ezugwu, N. Rana, and S. i. M. Abdulhamid, "Smart home automation system using ZigBee, Bluetooth and Arduino technologies," in *Proceedings of the Computational Science and its Applications – ICCSA 2020*, vol. 12254, pp. 587–597, Springer, Cagliari, Italy, July 2020.

[15] L. Salhi, T. Silverston, T. Yamazaki, and M. Takumi, "Early detection system for gas leakage and fire in smart home using machine learning," in *Proceedings of the 2019 IEEE International Conference on Consumer Electronics*, ICCE, Las vegas, NV, USA, Jan 2019.

[16] W. A. Jabbar, T. K. Kian, R. M. Ramli et al., "Design and fabrication of smart home with internet of things enabled automation system," *IEEE Access*, vol. 7, pp. 144059–144074, 2019.

[17] B. Vaidya, A. Patel, A. Panchal, R. Mehta, K. Mehta, and P. Vaghasiya, "Smart home automation with a unique door monitoring system for old age people using Python, OpenCV, Android and Raspberry pi," in *Proceedings of the International Conference on Intelligent Computing and Control Systems*, ICICCS, Madurai, India, June 2017.

[18] I. K. Suraj, D. Kumar, and S. Barma, "Visual machine intelligence for home automation," in *Proceedings of the 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages*, IoT-SIU, Bhimtal, India, February 2018.

[19] S. Mahmud, S. Ahmed, and K. Shikder, "A smart home automation and metering system using internet of things (IoT)," in *Proceedings of the International Conference on Robotics,Electrical and Signal Processing Techniques*, ICREST, Dhaka, Bangladesh, January 2019.

[20] A. Hanumanthaiah, D. Arjun, M. L. Liya, and A. Gopinath, "Integrated cloud based smart home with automation and remote controllability," in *Proceedings of the 2019 International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Coimbatore, India, July 2019.

[21] D. Kundu, M. E. Khallil, T. K. Das, A. A. Mamun, and A. Musha, "Smart home automation system using on IoT," *International Journal of Scientific Engineering and Research*, vol. 11, no. 6, pp. 697–701, 2020.

[22] K. K. Rout, S. Mallick, and S. Mishra, "Design and implementation of an internet of things based prototype for smart home automation system," in *Proceedings of the International Conference on Recent Innovations in Electrical*, IEEE, Bhubaneswar, India, July 2018.

[23] S. K. Saravanan, A. M. Nainar, and S. V. Marichamy, "Android based smart automation system using multiple authentications," *IRE Journal*, vol. 3, no. 6, pp. 60–65, 2019.

[24] L.-D. Liao, C.-C. Chuang, T.-R. Ger et al., "Design and validation of a multifunctional android-based smart home control and monitoring system," *IEEE Access*, vol. 7, pp. 163313–163322, 2019.

[25] U. Pujari, P. Patil, N. Bahadure, and M. Asnodkar, "Internet of things based integrated smart home automation system," in *Proceedings of the International Conference on Communication and Information Processing (ICCIP)*, Tokyo, India, November 2020.

[26] A. Akhtar, T. Ahmad, N. Sabahat, and S. Minhas, "IoT based home automation system using ThingSpeak," in *Proceedings of the 2019 International Conference on Computing*, Electronics & Communications Engineering (iCCECE), London, UK, Aug 2019.

[27] M. A. Hoque and C. Davidson, "Design and implementation of an IoT-based smart home security system," *International Journal of Networked and Distributed Computing*, vol. 7, no. 2, pp. 85–92, 2019.

[28] M. N. Aman, U. Javaid, and B. Sikdar, "IoT-proctor: a secure and lightweight device patching framework for mitigating malware spread in IoT networks," *IEEE Systems Journal*, pp. 1–12, 2021.

[29] U. Javaid, M. N. Aman, and B. Sikdar, "Defining trust in IoT environments via distributed remote attestation using blockchain," in *Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (Mobihoc '20)*, New York, NY, USA, October 2020.

[30] U. Javaid and B. Sikdar, "Lightweight and secure energy trading framework for electric vehicles," in *Proceedings of the 021 International Conference on Sustainable Energy and Future Electric Transportation*, SEFET, Hyderabad, India, Jan 2021.

[31] H. Durani, S. Mitul, M. Vaghasia, and S. Kotech, "Smart automated home application using IoT with Blynk app," in *Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies*, Coimbatore, India, April 2018.

[32] S. Garg, A. Yadav, S. Jamloki, A. Sadana, and K. Tharani, "IoT based home automation," *Journal of Information and Optimization Sciences*, vol. 41, no. 1, pp. 261–271, 2020.

[33] A. E. Amoran, A. S. Oluwole, E. O. Fagorola, and R. S. Diarah, "Home automated system using Bluetooth and android application," *Scientific African*, vol. 11, pp. 1–8, 2021.

[34] O. Taiwo and A. E. Ezugwu, "Smart healthcare support for remote patient monitoring during covid-19 quarantine," *Informatics in Medicine Unlocked*, vol. 20, no. 100428, pp. 100428–100512, 2020.

[35] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

[36] X. Qi and J. Liu, "Comparison of support vector machine and softmax classifiers in computer vision," in *Proceedings of the Second International Conference on Mechanical, Control and Computer Engineering*, Harbin, China, December 2017.

[37] C. Garcia and M. Delakis, "Convolutional face finder: a neural architecture for fast and robust face detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 26, no. 11, pp. 1408–1423, 2004.

[38] H. Basly, W. Ouarda, F. E. Sayadi, B. Ouni, and A. M. Alimi, "CNN-SVM learning approach based human activity recognition," in *Proceedings of the Image and Signal Processing ICISO 2020*, Marrakesh, Morocco, June 2020.

[39] S. Siddiqui, F. Azam, K. Bashir, M. Y. Javed, M. Khan, and M. Y. Javed, "Human action recognition: a construction of codebook by discriminative features selection approach," *International Journal of Applied Pattern Recognition*, vol. 5, no. 3, pp. 206–228, 2018.

[40] V. N. Vapnik, *Statistical Learning Theory*, Wiley, New York, NY, USA, 1998.

[41] D. Cao, O. T. Masoud, D. Boley, and N. Papanikolopoulos, "Human motion recognition using SUpport vector machines," *Computer Vision and Image Understanding*, vol. 113, no. 10, pp. 1064–1075, 2009.

[42] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, Wiley-Interscience, New York, NY, USA, 2000.

[43] W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, "IoT based smart home: security challenges, security requirements and solutions," in *Proceedings of the 23rd International Conference on Automation & Computing*, ICAC, Huddersfield, UK, September 2017.

[44] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: challenges and solutions," *Journal of Cleaner Production*, vol. 140, no. 3, pp. 1454–1464, 2017.

[45] O. Taiwo, L. L. Gabralla, and A. E. Ezugwu, "Smart home automation: taxonomy,Composition, challenges and future direction," in *Computational Science and its Applications – ICCSA 2020*, O. Gervasi et al., Ed., Springer Nature Switzerland, Switzerland, 2020.

[46] A. A. Zaidan and B. B. Zaidan, "A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations," *Artificial Intelligence Review*, vol. 53, no. 1, pp. 141–165, 2020.

[47] F. Hall, L. Maglaras, T. Aivaliotis, L. Xagoraris, and L. Kantzavelou, "Smart homes: security challenges and privacy concerns," pp. 1–6, 2020, https://arxiv.org/pdf/2010.15394.pdf.

[48] P. Sharma and P. kantha, "'Blynk' cloud server based monitoring and control using 'NodeMCU'," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 10, pp. 1362–1366, 2020.

[49] P. Shivaprasad, "Understanding confusion matrix, precision-recall and F1 score," 2020, [Online]. Available: https://towardsdatascience.com/understanding-confusion-matrix-precision-recall-and%20f1-score-8061c9270011.

[50] S. V. Gunge and S. P. Yalagi, "Smart home automation: a literature review," in *Proceedings on National Seminar on Recent Trends in Data Mining RTDM*, vol. 1, pp. 6–10, IJCA, 2016.