IoT based smart home automation using blockchain and deep learning models

Muhammad Umer Corresp., 1, **Saima Sadiq** [2], **Reemah M. Alhebshi** [3], **Maha Farouk Sabir** [3], **Shtwai Alsubai** [4], **Abdullah Al Hejaili** [5], **Mashael M. Khayyat** [6], **Ala' Abdulmajid Eshmawi** [7], **Abdullah Mohamed** [8]

[1] Department of Computer Science & Information Technology, The Islamia University of Bahawalpur, Bahawalpur, 63100, Pakistan
[2] Department of Computer Science, Khwaja Fareed University of Engineering and Information Technology, Rahim Yar Khan, Pakistan
[3] Department of Computer Science, Faculty of Computing and Information Technology, King Abdul Aziz University, Jeddah, Saudi Arabia
[4] Department of Computer Science, College of Computer Engineering and Sciences in Al-Kharj, Prince Sattam bin Abdulaziz University, All-Kharj 1, P.O. Box 151,1942, Saudi Arabia
[5] Faculty of Computers \& Information Technology, Computer Science Department, University of Tabuk, Tabuk, 71491, Saudi Arabia
[6] Department of Information Systems and Technology, Faculty of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia
[7] Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudia Arabia
[8] University Research Centre, Future University in Egypt, New Cairo, 11745, Egypt

Corresponding Author: Muhammad Umer
Email address: umersabir1996@gmail.com

For the past few years, the concept of the smart house has gained popularity. The major challenges concerning a smart home include data security, privacy issues, authentication, secure identification, and automated decision-making of IoT devices. Currently, existing home automation systems address either of these challenges, however, home automation that also involves automated decision-making systems and systematic features apart from being reliable and safe is an absolute necessity. The current study proposes a deep learning-driven smart home system that integrates a Convolutional neural network (CNN) for automated decision-making such as classifying the device as “ON” and “OFF” based on its utilization at home. Additionally, to provide a decentralized, secure, and reliable mechanism to assure the authentication and identification of the IoT devices we integrated the emerging blockchain technology into this study. The proposed system is fundamentally comprised of a variety of sensors, a 5V relay circuit, and Raspberry Pi which operates as a server and maintains the database of each device being used. Moreover, an android application is developed which communicates with the Raspberry Pi interface using the Apache server and HTTP web interface. The practicality of the proposed system for home automation is tested and evaluated in the lab and in real-time to ensure its efficacy. The current study also assures that the technology and hardware utilized in the proposed smart house system are inexpensive, widely available, and scalable. Furthermore, the need for a more comprehensive security and privacy model to be incorporated into the design phase of smart homes is highlighted by a discussion of the risks analysis' implications including cyber threats, hardware security, and cyber attacks. The experimental results emphasize the significance of the proposed system and validate its usability in the real world.

IoT Based Smart Home Automation using Blockchain and Deep Learning Models

Muhammad Umer[1], **Saima Sadiq**[2], **Reemah M. Alhebshi**[3], **Maha Farouk Sabir**[3], **Shtwai Alsubai**[4], **Abdullah Al Hejaili**[5], **Mashael M. Khayyat**[6], **Ala' Abdulmajid Eshmawi**[7], **and Abdullah Mohamed**[8]

[1]Department of Computer Science & Information Technology, The Islamia University of Bahawalpur, Bahawalpur, 63100, Pakistan; umersabir1996@gmail.com
[2]Department of Computer Science, Khwaja Fareed University of Engineering and Information Technology Rahim Yar Khan, Pakistan; s.kamrran@gmail.com
[3]Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia; ralhebshi@kau.edu.sa, msaber@kau.edu.sa
[4]Department of Computer Science, College of Computer Engineering and Sciences in Al-Kharj, Prince Sattam bin Abdulaziz University, P.O. Box 151, Al-Kharj 11942, Saudi Arabia; Sa.alsubai@psau.edu.sa
[5]Faculty of Computers & Information Technology, Computer Science Department, University of Tabuk, Tabuk 71491, Saudi Arabia; a.alhejaili@ut.edu.sa
[6]Department of Information Systems and Technology, Faculty of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia; Mkhayyat@uj.edu.sa
[7]Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudia Arabia; aaeshmawi@uj.edu.sa
[8]University Research Centre, Future University in Egypt, New Cairo, 11745, Egypt

Corresponding author:
Muhammad Umer[1]

Email address: umersabir1996@gmail.com

ABSTRACT

For the past few years, the concept of the smart house has gained popularity. The major challenges concerning a smart home include data security, privacy issues, authentication, secure identification, and automated decision-making of IoT devices. Currently, existing home automation systems address either of these challenges, however, home automation that also involves automated decision-making systems and systematic features apart from being reliable and safe is an absolute necessity. The current study proposes a deep learning-driven smart home system that integrates a Convolutional neural network (CNN) for automated decision-making such as classifying the device as "ON" and "OFF" based on its utilization at home. Additionally, to provide a decentralized, secure, and reliable mechanism to assure the authentication and identification of the IoT devices we integrated the emerging blockchain technology into this study. The proposed system is fundamentally comprised of a variety of sensors, a 5V relay circuit, and Raspberry Pi which operates as a server and maintains the database of each device being used. Moreover, an android application is developed which communicates with the Raspberry Pi interface using the Apache server and HTTP web interface. The practicality of the proposed system for home automation is tested and evaluated in the lab and in real-time to ensure its efficacy. The current study also assures that the technology and hardware utilized in the proposed smart house system are inexpensive, widely available, and scalable. Furthermore, the need for a more comprehensive security and privacy model to be incorporated into the design phase of smart homes is highlighted by a discussion of the risks analysis' implications including cyber threats, hardware security, and cyber attacks. The experimental results emphasize the significance of the proposed system and validate its usability in the real world.

1 INTRODUCTION

The Internet of Things (IoT) refers to the network of peculiar physical objects that are embedded with sensors, software, and other technologies and are rendered virtually in a network or cyberspace Zeinab and Elmustafa (2017); Kang et al. (2015). IoT is an immaculate information rectification and gathering technique that comprises nanotechnology, smart technology, sensor machinery, RFID Darianian and Michael (2008) sensor technology and a variety of other technical advancements. IoT is not an individually superlative technology, rather, it overcomes significant technological advancement and brings forth the capabilities that are suitable in conjunction to subdue the gap between physical and virtual worlds Wang et al. (2019). With the development of technology and the world, people are living highly busy lives and they require to be facilitated in every aspect of life. IoT covers a wide area of research, and this study is not capable of covering the whole field of research. However, because of the simplicity with which people may use it, smart home and smart environment is the first domain that springs to mind. A smart home Lobaccaro et al. (2016); Abdulrahman et al. (2016) is an automated home that refers to the mechanism of automating the working of all home appliances by controlling them using a computer, tablet, or smartphone with an internet connection. In recent years, home automation has been receiving immense attention as people prefer to control and maintain the utilization of home appliances by changing their status from anywhere around the world. Eventually, home automation is becoming a necessity of the current times.

IoT improves the life of a user by providing low-cost and highly flexible solutions for problems occurring in everyday life. Although, earlier studies have proposed a variety of home automation systems by integrating a variety of combinations of sensors Gill et al. (2009); Al-Ali and Al-Rousan (2004), however, given the limitations of those researches we listed some reasons for the rationale behind proposing an effective and systematic system for home automation.

- The formerly devised systems for home automation are costly and difficult to implement.
- The Bluetooth home automation system proposed in an earlier study necessitates unwanted installation.
- Internet connectivity is required for the previously proposed home automation systems; however, the Internet is not available in some areas.
- Previous studies failed to devise a secure and safe home automation system.
- Home automation systems proposed by earlier studies are inadequate for intelligent decision-making mechanisms especially in dealing with security threats.

Integrating security measures while designing a home automation system is not a simple and straightforward method and requires a formal risk analysis approach. In fact, one of the main challenges to the automation of smart homes has been recognized as the challenge of providing security in IoT environments, highlighting the complexity of this challenging but crucial task. To ensure the effective functioning of a home automation system, the key parameters that might make the system complicated must be checked. One of the important parameters that lacks in a previously devised home automation system is the absence of a Graphical User Interface (GUI) environment due to which the working of the system is not understandable by the users. Moreover, device restoration is available in the existing home automation systems which are detrimental to home appliances. In addition to this, prior home automation solutions are incapable of predicting the electricity bills and are highly expensive for the users. In consideration of this, we propose an effective and efficient solution to fill the previously discussed gap by pursuing the following objectives.

- This study proposes a cost-effective home automation system that remotely controls electrical devices and does not utilize IP-based devices.
- The proposed home automation solution is an Internet-based system. An app for smartphones has been created to assist users in creating automated homes by dragging and dropping components.
- Global System for Mobile Communication (GSM) modem is integrated into the proposed home automated system to control the home appliances including security systems, light, and conditional systems by using short text messages called SMS.

- The proposed system also facilitates the user with a device restoration feature that reinstates an electronic device such as a computer into the previous state when restored.
- The devised system involves implementations for Arduino and Raspberry Pi which have become indispensable tools for anyone who enjoys tinkering with electronics. In addition to being popular, these tools are also relatively affordable. Raspberry Pi facilitates an easy internet connection whereas, Arduino is appropriate for real-time implementation of software and hardware applications.
- Data logging is offered to assist users in improving appliance performance and energy efficiency.
- The proposed smart home automation system involves an intelligence-based decision-making mechanism for the classification of IoT devices' status.
- Blockchain technology is integrated into the suggested solution to provide secure authentication and safe identification of the users.

The rest of the paper is organized as follows: Section 2 discusses a brief literature review and the significant contributions in the domain of smart buildings and smart home solutions. Section 3 presents the proposed methodology utilized in this study to provide an effective solution, Section 4 provides an overview of the implementation of the proposed approach, as well as, the software and hardware used in the solution. Experimental results are presented in Section 5 along with a detailed discussion. Section 7 concludes the paper.

2 BACKGROUND

This section highlights the research gap in the field of smart environments and home automation systems. A considerable number of researches have been conducted in the domain of smart buildings and smart homes. For instance, the ZigBee microcontroller was utilized by Gill et al. (2009) to enable the user to connect the devices within the home. However, the system does not support long-range and the data speed is low. Along the same lines, Al-Ali and Al-Rousan (2004) utilized Personal Computer (PC) based webserver to provide remote connectivity for home appliances. The installation of the system is expensive due to the integration of wires. Another study Coskun and Ardam (1998) proposed a phone-based controller of home appliances. It did not include GUI which limited its functionality for the users. authorsBaudel and Beaudouin-Lafon (1993) devised a novel home automation system that utilized hand gestures to control the objects. However, the system failed to accurately detect the hand gestures causing inconvenience for the users.

The authors of Kumar and Pati (2016) integrated electrical switches and the Internet to provide a monitoring system for electronic devices at home. However, the system lacked secure transmission and communication between devices in a network. Researchers in Sangeetha et al. (2015) incorporated GPRS and speech recognition into their proposed home automation system but the system did not provide a secure identification and authentication for the user. Similarly, the authors of Javale et al. (2013) focused on providing the old-age and handicapped persons with a system to remotely control their home appliances using Android APK, however, the system is limited in functionality. It only automated the light controls and in turning the electronic device on and off.

Bluetooth technology was employed by Piyare and Tazil (2011) in an attempt to design a cellphone-based home automation system but the GUI only supported cell phones with Symbian OS and the range of Bluetooth was limited to 50-100m. Similarly, authors in Sriskanthan et al. (2002) utilized Bluetooth technology but the proposed system did not perform well due to the obtrusiveness of the installation. Blockchain technology is getting attention due to its reliability. The technology selection problem is solved by using blockchain in Farshidi et al. (2020). Researchers applied blockchain technology in e-government service Geneiatakis et al. (2020).

The threat to network security has gotten much worse with the rise of cyber-attacks and intrusion tactics. An effective technique for detecting anomalies was proposed in Ding and Li (2022), which takes into account the intricate communication patterns between the network topology and node attributes. Researchers looked at recent cyber-attacks that used AI-based methods, and they discovered a number of mitigation approaches that may be used to counteract such AI attacks Yamin et al. (2021). Authors designed authentication scheme for RFID system Akleylek and Soysaldı (2022). Authors investigated IoT-based cyber-attacks and discussed defense mechanisms and challenges Meng et al. (2021). A tool based on the branch and bound technique and tuned for GPU systems for block cipher security evaluation is proposed in Yeoh et al. (2022). Authors used the blockchain method to build an effective certificate-less signature framework Wang et al. (2021).

ArduinoTmega2560 and IoT technologies were utilized to help handicapped individuals to supervise and control their home appliances Abdulraheem et al. (2020). However, the proposed system failed to provide a secure authentication system for the users. Consequently, an automated system for the opening of the door in an office or home was proposed by Hoque and Davidson (2019) by integrating Elegoo Mega 2560 and a web server that required retaining information about the signals between a variety of transmitters. In an attempt to provide a smart system for home automation that enables the users to control the electronic devices at home by integrating ESP-8266, Arduino UNO, and Wi-Fi for connectivity Satapathy et al. (2018), the system consumed more time in turning on and off an appliance. Another study Pirbhulal et al. (2017) utilized a wireless sensor network to devise an energy-efficient and secure home automation system. However, the proposed system is high-priced and is only limited to the temperature.

3 PROPOSED APPROACH

The current study proposes an automation system for smart homes that facilitates the users to monitor and adjust the state of devices installed in homes such as air-conditioners, ventilation, heating, and lighting along with the operating state of the sensors. The proposed system is not limited to being time-effective but also accommodates the user with a viable energy-efficient solution by providing insight regarding the energy consumption of the devices. This energy-efficient and cost-effective solution can also be deployed in hotels, restaurants, and domestic, or industrial places. The proposed system incorporates an easy GUI environment and notification system which involves an icon-based interface that enables the user to be notified and connected with his home from anywhere around the world. This system is cost-effective due to its capability of automating the ordinarily installed electronic devices at home instead of specific IP devices like RJ-45 Chong et al. (2011). Figure 1 illustrates the operation of the proposed system for home automation.

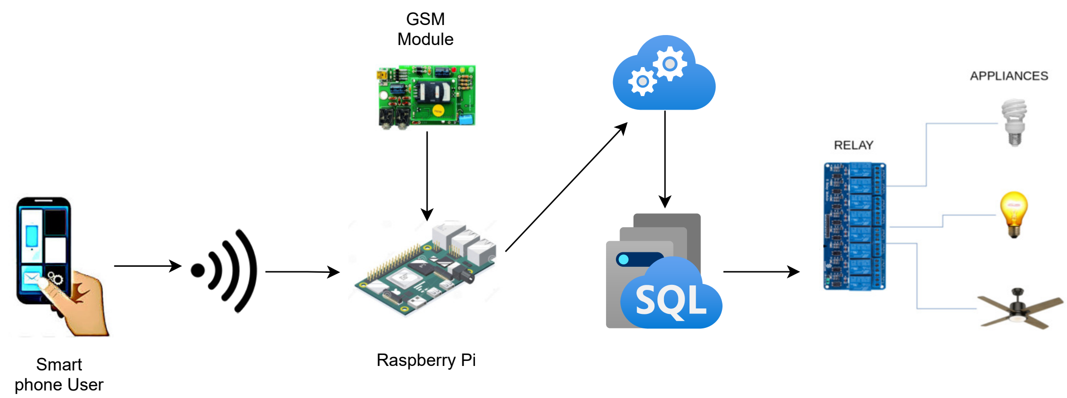

Figure 1. Workflow of home automation.

From the admin panel, the user can draw a complete layout of his/her home by utilizing an easy-to-use drag-and-drop interface. To begin with, the interface of the proposed system allows users to add the floors of the house. Afterward, he/she can add the rooms on the particular floor by selecting the corresponding added floor. Then, the user can add appliances to the room and can position them in accordance with the real-time structure of the room. The interface also provides additional functionality to add custom devices, rooms, or floors to the layout of the house. Once the user is finished setting up the home layout from the admin panel, the database of the user's home structure is synced with our server in JSON Haq et al. (2013) format where it is updated using VOLLEY Hang and Kim (2018). The user will be able to fetch the home structure from the admin panel after 30 seconds of syncing the database by logging in using the credentials. The interface of the application allows the user to see the details regarding the floor, as well as, the electronic devices placed at the home. Apart from this, the application involves other three tabs as well on the bottom of the main screen. The second tab displays the state of the sensors. The third tab shows the history of the device as well as the individual's name who changed the status of that particular device. The fourth tab enables the user to log out of the application. Credentials are controlled via shared preferences, and the data is preserved.

Furthermore, the status of the devices being utilized in the home is classified into two categories such as “OFF” and “ON” using a supervised learning classifier based on the usage of the device. The input data contains categorical as well as continuous numeric values. The input data contains floor_id, room_id, device_id, room_temperature, room_light, device_time, and status. We also performed a comparative analysis of the predictive model utilized in this study with other conventional models and selected the model with maximum performance. Moreover, the system provides authentication and secure communication between IoT devices and the user requesting the change in the device’s status by integrating blockchain technology. It assures the secure transmission of data between applications, servers, devices, and users of the proposed smart home.

3.1 Blockchain Technology for Secure Home Automation System

The primary goal of an automated system for homes is to provide IoT devices with safe, trustworthy authentication, and identification. We employed blockchain technology in order to ensure these goals. In 2008, Nakamoto introduced blockchain technology Nakamoto (2008). The significant features of this technique include decentralization, anonymity (anonymity), and security Christidis and Devetsikiotis (2016). Blockchain technology can be leveraged by IoT to provide a highly secure central server resulting in reduced dependency. Additionally, this technology incorporates timestamp and data encryption which ensures a moderate data structure. The proposed approach implements the blockchain module in Java by utilizing hash as the unique identifier of the block’s contents. To compute a block hash, each block is utilized which then computes the hash SHA-256 from it. When a threshold is reached, the block is created by granting permission for connectivity by means of managing the blockchain. The hash value of the preceding block is verified against the hash value of the succeeding block in order to validate the whole blockchain. Whenever a user generates a connection request, it is authenticated following the steps illustrated in Figure 2. Algorithm 1 elaborates on the working of blockchain technology works. A flowchart illustrating the blockchain implementation process is presented in Figure 2.

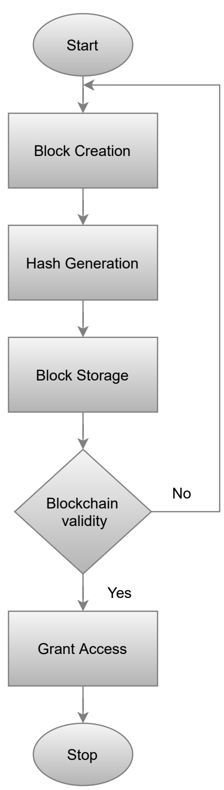

Figure 2. Workflow of blockchain implementation.

To begin, a block is constructed by utilizing a block class that has been implemented in Java which calculates the hash value based on the preceding hash, data string, and timestamp. Following the creation of a block, a hash is created by integrating the SHA256 algorithm. Afterward, the generated blocks are stored. Finally, the blockchain is validated to evaluate whether the value of the hash is equal to the calculated value. The user will be granted access if the preceding and succeeding hash is equal, otherwise, the entire procedure is repeated from the beginning.

4 IMPLEMENTATION DETAIL

Figure 1 depicts the complete functionality of the proposed model along with the integration of various devices with each other to get an in-depth understanding of the working of the proposed smart home solution. The flow of the project is represented by the arrows from an application on the user's smartphone to switching the electronic device's state. There are two different modules in which the user can communicate with the Raspberry Pi server Maksimović et al. (2014); Leccese et al. (2014) depending on the user's location. The first module allows the user to interact with the IoT devices without connecting to the Internet given the user is residing inside the house and using a local network resulting in high-speed communication between the user and devices. The second module requires the user to connect to the Internet and is employed if the user is located outside of the house, at any place around the world. The connection request is then processed and forwarded to the Azure Cloud Wei et al. (2010). Afterward, the user inputs his/her credentials which are coordinated with the help of the Azure database and directed to the corresponding Raspberry Pi server for further processing. The Microsoft Azure Cloud databases maintain the account of each user separately. Each user is provided with the services in accordance with the inputted credentials by the user to initiate the request. APIs are accessed from the cloud if the user is not connected to the home. However, the Raspberry P server stores similar APIs if the user is residing in the house i.e., having a home network connection.

The data is shared between the user and the server in JSON format. A variety of hashing techniques are utilized to secure the APIs. Raspberry Pi GPIO Brock et al. (2013) pins are utilized to modify the status of any electronic device in the system. The server's request is received by the Raspberry Pi which responds to the devices in accordance with the user's request which is being maintained in a database at the cloud servers. This enables the user to view the entire history by inputting the time period on his/her smartphone. The sensors which are installed in the house update their status after every 30 sec and adapt accordingly to the Raspberry Pi server. Regarding this, the Raspberry Pi server synchronizes the entire database data saved in the cloud server and updates the values on the mobile application.

4.1 Hardware Components

A variety of sensors and electronic components are utilized in the proposed system as shown in Figure 1. This section presents a complete description of the hardware components integrated into the system which are also summarized in Table 1.

Table 1. Performance of Machine Learning Models.

Components	Specification
Raspberry Pi 2B	40 GPIO pins, 1 GB RAM A 900 MHz quad-core ARM Cortex-A7 CPU, operational voltage 7–12 V
Relay circuit pack	The 5 V operational 8-relays circuit pack
L293D motor control shield	Supply-voltage range: 4.5–36 V; output current: 600 mA/channel
Smartphone mobile	Android supported
DS18B20 temperature sensor	Temperature range: -55 to 125°C (-67°F to +257°F)
LM393 LDR sensor	Digital switching outputs (0 and 1), external 3.3 V–5 V vcc
MQ2 smoke sensor	Combustible gas, smoke

The Raspberry Pi is an inexpensive compact single-board computer (SBC) that is designed to assist educational institutions and underdeveloped countries teach the fundamentals of computer science. It comprises a quad-core ARM Cortex-A7 CPU running at 900 MHz in addition to 1 GB RAM, which supports Ethernet (100 Mbps) and includes a card interface, 4 USB ports as well as 40 GPIO-pins, complete HDMI compatibility with the camera along with SD card compatibility. It supports composite video and consists of a 3.5 mm-sized audio jack.

A relay is operated using electricity and is often utilized in the control circuit which is automatic. Relay has an input circuit (also known as a control system or input contractor) and an output circuit (also known as a controlled system or output contractor). It is an automated switching device that utilizes a low-current signal to control a high-current circuit.

L223D Quadri and Sathish (2017) is a 4-channel, high-current, high-voltage, and monolithic integrated driver. This implies that by using L293D, we can integrate power supplies and DC motors with a voltage of up to 16 V, that is, quite large motors, and per channel. The chip circuit can deliver a current of a maximum of 600 mA. The L293D chip is a series of H-Bridge that is an electrical circuit that supplies the voltage across a load in any output direction such as the motor.

The DS18B20 is a temperature sensor comprised of a 1-wire which enables the user to record the temperature using a very convenient interface. It utilizes a bus to communicate which allows the user to connect multiple devices and use only a single Raspberry Pi GPIO pin to read their values.

MQ2 or chemiresistor is a widely used Metal Oxide Semiconductor smoke sensor in the series of MQ2 sensors. When the smoke comes in contact with the sensor it works by detecting the variation in resistance of the sensing element. The concentration of the smoke can be sensed by using a primary voltage divider network. MQ2 can detect carbon monoxide, methane, hydrogen, propane, alcohol, smoke, and LPG in the range of 200 to 10,000 ppm. It operates at 5V DC and consumes roughly 800 mW.

GSM module has a dual mode that is typically utilized for creating embedded applications and IoT. It operates between frequencies of 900 MHz and 1800 MHz. It does not require high-power consumption and includes a multislot class feature, for instance, class 8, and class 10th. The data is received and transmitted using the TXD and RDX pins. It consumes low voltage within the range of 3.4 V to 4.5 V and might be damaged if the voltage is increased.

4.2 Software Components

Many platforms have emerged for mobile application development such as Windows Mobile, IOS, Android, and Symbian. In the current study, we utilized the Android platform to develop the entire project. The use of the Android platform in this study is mainly motivated by its extensive use around the world. Android applications are supported by nearly every manufacturing brand of smartphones. Android applications. To develop and implement the proposed smart home system, an Android development kit called SDK is utilized in Java.

Android studio Esmaeel (2015) is utilized to create Android APK since it involves the tools which are necessary for mobile application development such as handset emulators, libraries, and debuggers. For the services of all sensors, the Volley library is integrated. Android application is made more interactive by incorporating a material design library.

LAMP which is an acronym of Linux, Apache, MySql, and PHP is utilized to offer complete backend functionalities for server-side development on the cloud within the Raspberry Pi.

4.3 Mobile Applications

The mobile application has two modules for the operation. In the admin module, the user can utilize a simple interface (drag-and-drop) to draw a prototype of his/her home. A Raspberry Pi pin is allocated to the devices in order to regulate the operation of the electronic devices at the backend.

Whereas, the user module allows the users to visualize the home prototype which he/she designed in the admin panel. This module also enables the user to operate the electronic devices based on the pin that he/she configured on the admin module as illustrated in Figure 3. The mobile application's main screen displays information regarding the names of floors, the number of rooms inside a particular floor, and devices placed or installed in the home. Switching between the mobile application services is carried out via tab layout.

Figure 4 demonstrates a well-designed and interactive graphical user interface with appealing icons which facilitates the user in the understanding of its working. The icons are programmed to change according to the electronic device's present state along with an active touch button to switch the status of the device. The app also enables the user to set the brightness of light or fan speed with an interactive intensity bar. The status of working devices is shown as "active" and the passive state is displayed as "active ago". The second tab of the mobile application's home screen enables to user to view the status of each sensor as well as their current values. Sensors are refreshed after every 30 seconds and the values are

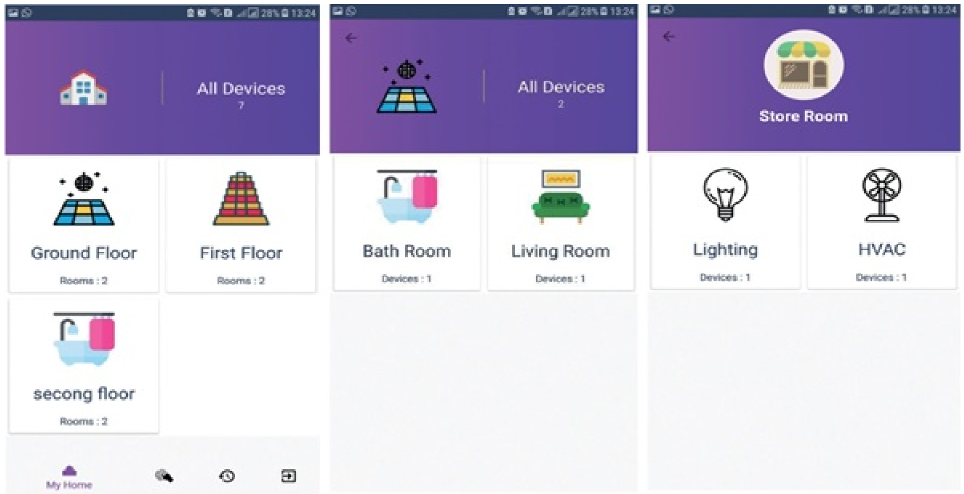

Figure 3. Workflow of home appliances.

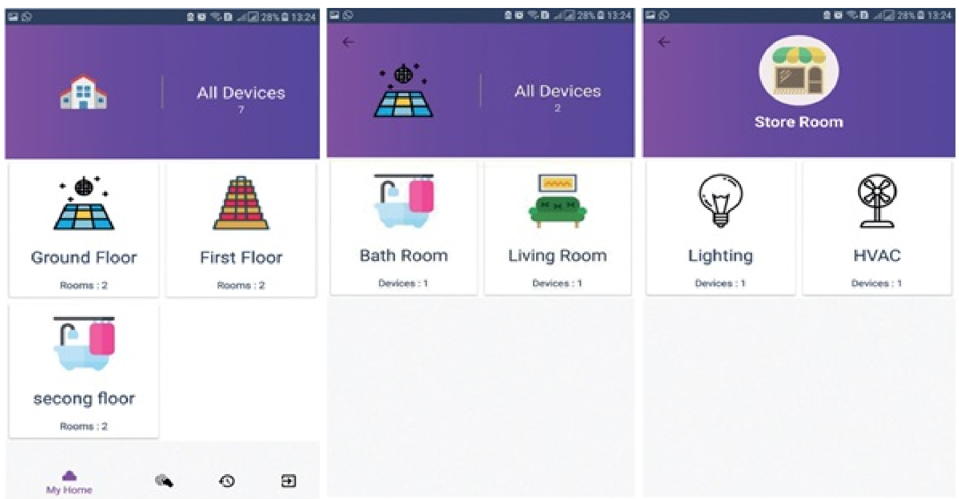

Figure 4. Graphical User Interface of User screen.

updated in the mobile application by integrating the backend services as illustrated in Figure 5. Currently, we deployed two sensors such as temperature and light to visualize their live status. Figure 6 shows that the value of the light sensor is 0.0 indicating the "OFF" state of the sensor and that currently, daylight is present. The third tab n the home screen enables the user to view comprehensive information regarding the device's history. Complete information regarding the user who modifies the state of the device is maintained in the form of a log along with the time-stamped details. It also enables the user to see the active and inactive duration of electronic devices. Another prominent aspect of the proposed system is that it notifies the user if any device is in an "ON" state for more than two hours. It functions similarly as a reminder or an alarm for the user to monitor and maintain the electricity usage of each device in either the case of a person being in a room or the case of electricity waste as displayed in Figure 7. The mobile application also facilitates the user by calculating the electricity based on the power consumption by the electronic devices and the duration for which the power was consumed.

4.4 Predictive Models

In this study, extensive experiments have been performed to make decisions about the status of appliances using state-of-the-art models. Various machine learning and deep learning models employed for this purpose are discussed below.

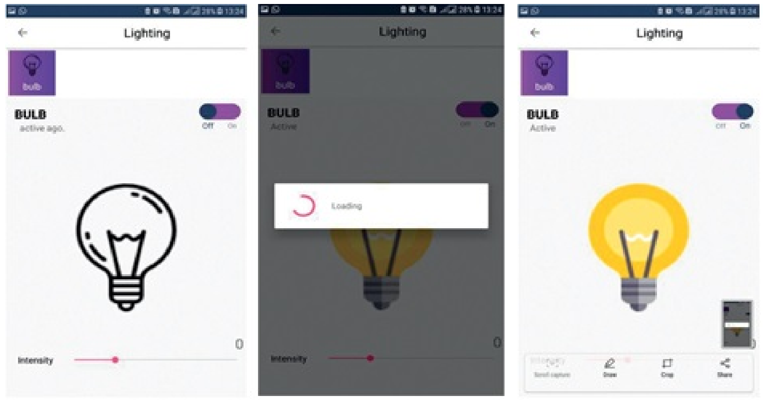

Figure 5. State of home appliances

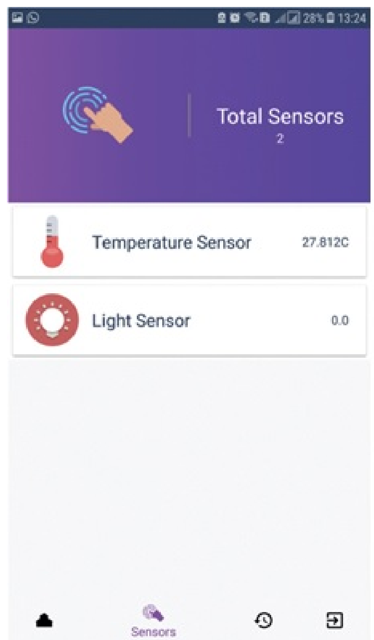

Figure 6. Sensor data

4.4.1 Random Forest

Random Forest works using decision trees and building numerous trees to avoid variance. RF has been widely used in literature in solving regression and classification problems. The bagging technique is used by RF in predicting final results based on majority voting. A bootstrap dataset is used by RF which is a subset of original data Breiman (1996). The workflow of RF is presented as follows.

$$p = mode\{T_1(y), T_2(y), \ldots, T_m(y)\} \tag{1}$$

$$p = mode\left\{\sum_{m=1}^{m} T_m(y)\right\} \tag{2}$$

Here p represents the final output, calculated by majority voting T_1, T_2, and T_m trees.

4.4.2 Support-vector machine

The support-vector machine is a machine learning algorithm that can be applied for regression as well as classification problems. It transforms data using kernel trick and determines the optical border line between output. Borderline is called hyperplanes, these planes distinguish one type of data from other.

Figure 7. History log

4.4.3 Logistic Regression

Logistic Regression Wright (1995) is mostly used to solve classification problems. It is a statistical model and analysis algorithm based on the probability concept. It finds output using one or more variables with binary data. It uses a sigmoid function to produce a connection between categorical data.

4.4.4 Stochastic Gradient Descent

Stochastic Gradient Descent Gardner (1984) joins various classifiers in the one-versus-all technique. It uses all samples of data in each iteration and is more suitable for large-sized datasets. It is very easy to implement because of its basic principle. It is highly sensitive in feature scaling and hyperparameters require suitable values.

4.4.5 Decision Tree

Decision Tree Breiman et al. (1984)is simple tree bases supervised machine learning algorithm that shows good results on both numerical and categorical data. A decision tree is very easy in terms of implementation and has been extensively used in various fields.

4.4.6 Gradient Boosting Machine

In a Gradient Boosting Machine Friedman (2001) various weak classifiers are combined to make a strong learning classifier. It works on the decision tree and creates independent trees and takes more time for execution. It improves the working after several tweaks to it that improves the algorithm which is called PAC (probability approximately correct learning). It shows good results on un-processed data and handles missing values of data efficiently.

4.4.7 Extra Trees classifier

Extra Trees classifier Sharaff and Gupta (2019) works like a random forest but creates trees in a different way and constructs trees from the original sample data instead of the bootstrap data sample. Decisions are made on random data samples of the k-best feature. Selection of the top feature to split the tree is done by the Gini index.

4.4.8 Long Short Term Memory

Long Short Term Memory (LSTM) is a deep learning model and is an extended variant of Recurrent neural network (RNN) Sherstinsky (2020). LSTM comprises three gates; one is input gate i_k, the second is output gate o_k and the third is forget gate f_k. Data is passed through these gates, important information is retained by the gates and unimportant is forgotten according to dropout value. Important information is saved in a memory block named C_k. LSTM has different variants, the one used in this study is presented in eq. 3, 4 and 5.

$$i_k = \sigma(W_i s_k + V_i h_{k-1} + b_i) \tag{3}$$

$$f_k = \sigma(W_f s_k + V_f h_{k-1} + b_f) \tag{4}$$

$$o_k = \sigma(W_o s_k + V_o h_{k-1} + b_o) \tag{5}$$

$$c_k = tanh(W_c x_k + V_c h_{k-1} + b_c) \tag{6}$$

where W and V presents associated weights with matrix elements. h presents the hidden state up to $k-1$ time step,whereas s_k shows the input of specific time and b presents the bias. c is the memory block cell which is updated at $k-1$ time steps. In the output layer of LSTM, all neurons are connected to every neuron of the dense layer.

4.4.9 Convolutional Neural Network

Convolutional Neural Network (CNN) is a deep neural model and its convolution layers and pooling layers learn complex features Yamashita et al. (2018). Most of the time CNN is used in image classification and image segmentation tasks. The end-to-end training of the layered CNN model makes it more robust. Features are mapped by applying filters on the output of the layers as it is a feed-forward network model. Moreover, the CNN model consists of activation layers, hidden layers drop out and fully connected layers. The output of the previous layers is fed to the fully connected layers for determining the final result. Pooling layers play a role in feature selection by reducing them and it can be max-pooling or average pooling. ReLU function is utilized as an activation function and presented in eq. 7.

$$y = max(0, i) \tag{7}$$

where y shows the output of activation and i is the input. High-level features for training are extracted by convolutional layers using weights. Cross entropy is a loss function that is computed as presented in equation 8.

$$crossEntropy = -(i\ log(p) + (1-i)\ log(1-p)) \tag{8}$$

where i presents class labels and p is the predicted probability. As CNN is an extended version of the backpropagation model output is predicted using the sigmoid error function. CNN model generates output for two target classes. For the ON status of the device, the output will be 1 for the first neuron and 0 for other neurons. In the case of OFF status, the values of neurons will be reversed.

5 EXPERIMENTS AND RESULTS

The functionality of the project is elaborated in figure 8. The proposed framework consists of two scenarios. The first scenario deals with remote access of the users outside the home and uses a cloud database by Microsoft Azure. The request of the user is sent on the cloud according to the user's APIs. The second scenario deals with the users inside the home directly connected to Raspberry Pi. Requests of users are sent to the server (Raspberry Pi) rather than on the cloud or internet as shown in figure 9. Local processing makes the process fast without the implication of the cloud.

5.1 Data Collection and Visualization

Data is collected using the developed app and stored in an excel sheet. Data is further analyzed to explore the relationship between different attributes. The attribute data include light, temperature, and smoke. Whereas, in the status column 0 means "OFF" and 1 means "ON".

Figure 10 presents the scatter plot of temperature with smoke and temperature. Different readings, if the temperature is presented on X-axis while smoke is along Y-axis and with temperature are given on

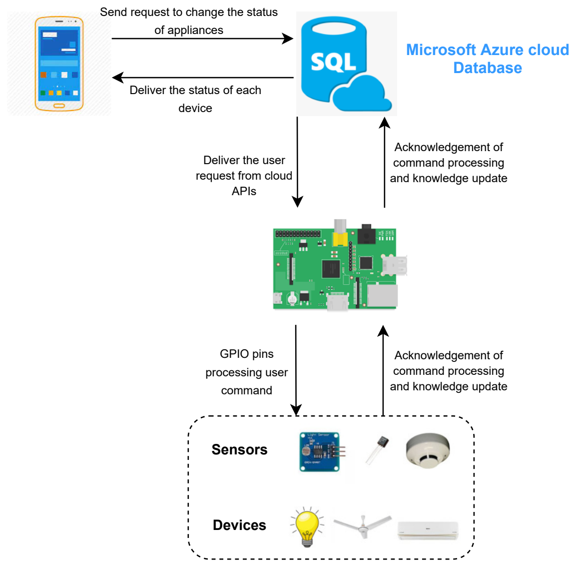

Figure 8. Microsoft Azure cloud database

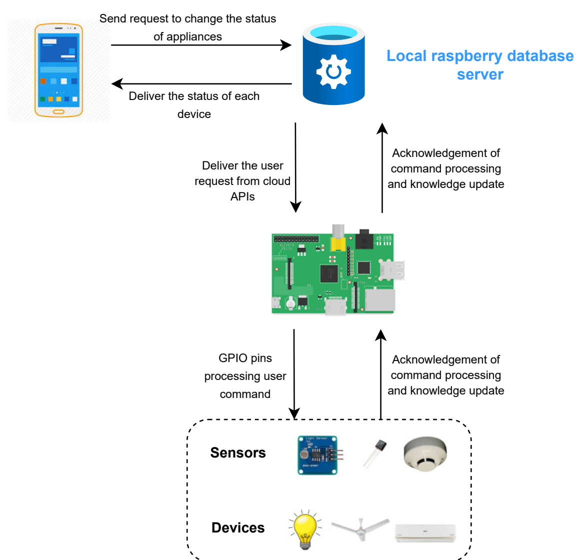

Figure 9. Local database server

the y-axis and values of light, are given along the x-axis. Figure 11 presents a scatter plot between light and smoke. Values of smoke are shown along the x-axis and the value of light is shown along the y-axis. The kernel density plot is presented in figure 12. The status of light and smoke and smoke is presented in figure 13, where 1 represents ”ON” and 0 represents ”OFF”. Status is presented on the x-axis and relevant values are along the y-axis.

All devices are set in a way that these devices are set to the previous state in case of an electricity outage or restart of Raspberry Pi. Device states are maintained by involving a database server. The last state of each device is retained accordingly from the server. Installed in the home will make updates at regular intervals. In situations like the rising of home temperature to a specific threshold will cause the starting of ventilation fans. Light sensors are installed to control the on and off timings of lights according to day and night. Features like sensor updates, data logs, Raspberry support, cloud database, and deep learning models make the project robust and unique. Customized design of devices according to the house makes the system flexible and easy to operate.

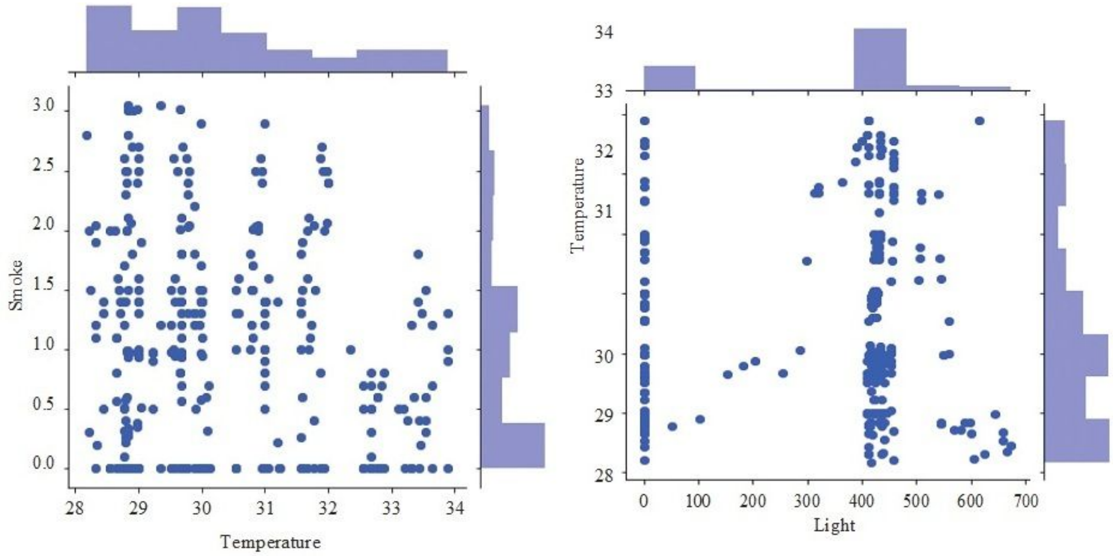

Figure 10. Scatter plot of temperature with smoke and temperature.

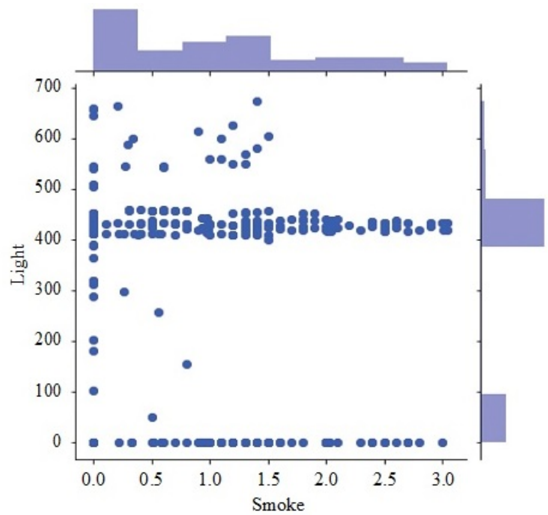

Figure 11. Scatter plot between light and smoke.

5.2 Results

Extensive experiments have been performed to make decisions about the status of appliances in a smart home using state-of-the-art classifiers. Classifiers used in experiments include Random Forest, Support Vector Machine, Logistic Regression, Decision Tree, Gradient Boosting Machine, Extra Tree Classifier, Voting Classifier (that combines Support Vector Machine and Logistic Regression), Long Short Term Memory (LSTM), and Convolutional Neural Network (CNN). Recorded data has been divided into train and test sets in a 70:30 ratio. All the experiments are carried out on a $2GB$ Dell PowerEdge $T430$ GPU on $2x$ Intel Xeon 8 Cores $2.4Ghz$ machine which with 32 GB $DDR4$ RAM. Python programming language by Anaconda using the Jupyter notebook environment has been used to perform experiments. Classifiers are implemented using Tensorflow, sci-kit learns, and Keras. Table 2 presents the result of the classifier in predicting "ON" and "OFF" classes for home appliances. Random Forest, Support Vector Machine, Logistic Regression, Stochastic Gradient Descent, Voting Classifier (that combines Support Vector Machine and Logistic Regression), Decision Tree, Gradient Boosting Machine, and Extra Tree Classifier have achieved 93.9%, 91.4%, 93%, 90.8%, 92.6%, 92.7%, 87.7% and 93.8% accuracy values respectively. Deep learning models LSTM and CNN have achieved 91.6% and 96.6% respectively. It

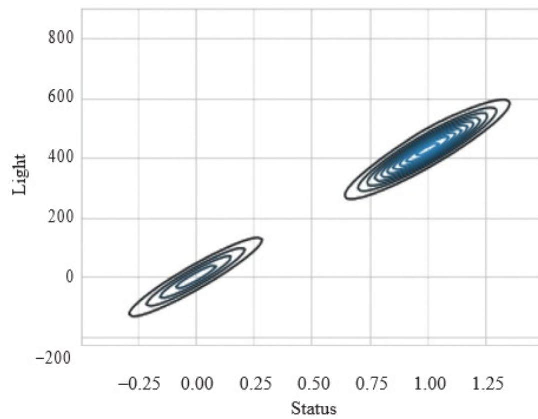

Figure 12. Scatter plot between light and smoke.

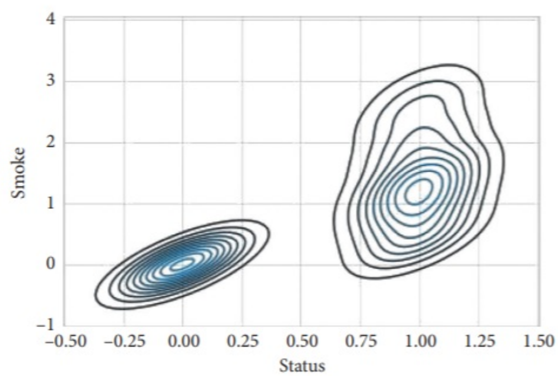

Figure 13. Scatter plot between light and smoke.

Table 2. Classification report of supervised learning models.

Classifiers	Accuracy	Precision	Recall	F-score
Random Forest	93.9%	89.69%	90.67%	90.11%
Support Vector Machine	91.4%	85.17%	87.74%	86.29%
Logistic Regression	93.0%	91.29%	93.44%	92.54%
Stochastic Gradient Descent	90.8%	83.33%	84.77%	84.32%
Voting Classifier	92.6%	91.34%	92.66%	91.97%
Decision Tree	92.7%	89.59%	90.57%	90.01%
Gradient Boosting Machine	87.7%	80.97%	83.35%	81.99%
Extra Tree Classifier	93.8%	89.89%	90.87%	90.34%
Long Short Term Memory (LSTM)	91.6%	89.17%	90.74%	90.09%
Convolutional Neural Network (CNN)	96.6%	95.57%	97.74%	96.45%

can be noticed that CNN outperforms in predicting the status of home appliances with 96.6% accuracy. Random forest is less complex in terms of computation and mostly shows better performance using an interpretation of decision trees. Deep neural networks require more data for training to show better results. CNN has high feature compatibility when compared with RNN. RNN performs better in arbitrary input or output while CNN performs better in input and out of fixed size. LSTM handles sequential data while CNN explores spatial correlation among features and shows better results in categorical data. Therefore, CNN is the most suitable classifier for predicting the status of home appliances and can be effectively used for decision-making.

6 RISK ANALYSIS

Smart home automation is seen as a crucial component of the Internet of the future. Investigating possible computer security attacks and their effects on occupants is necessary as houses become more computerized and loaded with gadgets like smart TVs and home energy management systems. Jacobsson et al. Jacobsson et al. (2016) categorized risks into five categories that are: software, hardware, information, communication, and human-related risks. In software risk, the in-house gateway's insufficient accountability, or the fact that system events are not logged so they may be traced afterward, poses the most likely challenge. The worst effect is related to the API's insufficient authentication. The greatest risk value relates to unauthorized changes being made to system operations in mobile apps, which means that end users may access system resources without the necessary authorization. Hardware risk involves unauthorized modification or tampering with physical sensors. Information risks include the insufficient distinction between user accounts' privileges. Communication risks involve the deletion of the server. Human-related risks relate to poor or weak passwords and gullible end-users.

The issue of privacy risk points to the necessity of integrating security throughout the design stage of developing smart home systems, i.e., a model for security and privacy in design. The question that arises next is how such a model should be created, including what the key elements should be to maintain privacy and security. This study leads the readers to recommend that the model should at the very least contain the following steps:

- In smart homes, personal data in transit is identified and categorized.
- The key privacy and security threats are analyzed and described.
- Finding and implementing risk-reduction strategies that are proactive, investigative, and reactive
- A plan for managing information in smart homes while protecting privacy.

To specify a mechanism for categorizing the personal data that is produced, saved, updated, and disseminated in conjunction with the smart home, further work is still required. The design of a user-generated information management strategy for smart homes and its link to the digital ecosystems they interact with both fall under this category.

6.1 Performance Comparison of the Proposed System

The proposed system is described in relation to the earlier proposed models of the home automation system. For performance comparison, a number of significant factors are taken into account. One crucial component that determines a system's cost-effectiveness and convenience of installation, for instance, is the sort of devices or sensors employed. Similarly, useful controls are real-time sensor data, data logs of sensors for optimization, automatic implementation of the user-set preferences, system recovery, and remote access. Table 3 highlights the benefits of the proposed system over competing home automation systems and displays the performance criteria utilized for the comparison. The proposed system stands out from other systems due to all the characteristics and functionality listed in Table 3. It is simpler for a user to use an electronic device by creating a model of their own home and putting each piece of equipment up in accordance with the layout of their rooms.

7 CONCLUSION

In this study, a project of complete home automation is explained along with its functionality. The main aim is to design a user-friendly and flexible design in making decisions about the status of home appliances. The proposed framework comprises two modes; the admin mode makes the user able to design a house and the other is user mode which makes the user able to control each home appliance using the graphical user interface. The status of each device is controlled by users based on previous track records.

A CNN-based deep learning model is applied for decision-making about the "ON" and "OFF" status of the home appliances. The proposed approach also authenticates the use of blockchain in IoT devices. Intelligent and flexible decision-making in home automation is the need of the current time. Overall, it has also been determined by risk analysis that a model's security and privacy are necessary for smart home design. Furthermore, this home automation project is a simple, flexible, reliable, and affordable

Table 3. Performance evaluation of the proposed system against previously proposed systems.

Features	**Automation systems**								
	Patchava V. and P.R. (2015)	Jabbar et al. (2018)	Hadwan and Reddy (2016)	Mahamud et al. (2019)	Jabbar et al. (2019)	Dey et al. (2016)	Vishwakarma et al. (2019)	Singh et al. (2019)	**Proposed**
App to make home prototype	✗	✗	✗	✗	✗	✗	✗	✗	✓
Device status data logging	✗	✗	✗	✗	✓	✗	✗	✗	✓
Real time sensors data display	✓	✗	✓	✓	✓	✓	✗	✗	✓
Use of micro-processor (Raspberry Pi)	✓	✗	✓	✗	✗	✓	✗	✗	✓
Internal network in case of gateway failure	✗	✗	✗	✗	✗	✗	✗	✗	✓
Sensors recent state recovery	✓	✗	✓	✗	✗	✗	✗	✗	✓
Light and fan intensity control using pulse wave modulation	✗	✗	✗	✗	✗	✗	✗	✗	✓
Use of blockchain security	✗	✗	✗	✗	✗	✗	✗	✗	✓
Predictive model based on usage of appliances and sensor data	✗	✗	✗	✗	✗	✗	✗	✗	✓
Use of ordinary electrical appliances	✓	✗	✓	✗	✗	✗	✗	✗	✓

system. In the future, more deep learning models will be tested in decision-making steps to improve the efficiency of the system.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Abdulraheem, A. S., Salih, A. A., Abdulla, A. I., Sadeeq, M., Salim, N., Abdullah, H., Khalifa, F. M., and Saeed, R. A. (2020). Home automation system based on iot. *Technology Reports of Kansai University*, 62(5).

Abdulrahman, T., Isiwekpeni, O., Surajudeen-Bakinde, N., and Otuoze, A. O. (2016). Design, specification and implementation of a distributed home automation system. *Procedia Computer Science*, 94:473–478.

Akleylek, S. and Soysaldı, M. (2022). A new lattice-based authentication scheme for iot. *Journal of Information Security and Applications*, 64:103053.

Al-Ali, A.-R. and Al-Rousan, M. (2004). Java-based home automation system. *IEEE Transactions on Consumer Electronics*, 50(2):498–504.

Baudel, T. and Beaudouin-Lafon, M. (1993). Charade: remote control of objects using free-hand gestures. *Communications of the ACM*, 36(7):28–35.

Breiman, L. (1996). Bagging predictors. *Machine learning*, 24(2):123–140.

Breiman, L., Friedman, J., Olshen, R., and Stone, C. (1984). Classification and regression trees. statistics/probability series.

Brock, J. D., Bruce, R. F., and Cameron, M. E. (2013). Changing the world with a raspberry pi. *Journal of Computing Sciences in Colleges*, 29(2):151–153.

Chong, G., Zhihao, L., and Yifeng, Y. (2011). The research and implement of smart home system based on internet of things. In *2011 International Conference on Electronics, Communications and Control (ICECC)*, pages 2944–2947. IEEE.

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, 4:2292–2303.

Coskun, I. and Ardam, H. (1998). A remote controller for home and office appliances by telephone. *IEEE Transactions on Consumer Electronics*, 44(4):1291–1297.

Darianian, M. and Michael, M. P. (2008). Smart home mobile rfid-based internet-of-things systems and services. In *2008 International conference on advanced computer theory and engineering*, pages 116–120. IEEE.

Dey, S., Roy, A., and Das, S. (2016). Home automation using internet of thing. In *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 1–6. IEEE.

Ding, Q. and Li, J. (2022). Anogla: An efficient scheme to improve network anomaly detection. *Journal of Information Security and Applications*, 66:103149.

Esmaeel, H. R. (2015). Apply android studio (sdk) tools. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(5).

Farshidi, S., Jansen, S., España, S., and Verkleij, J. (2020). Decision support for blockchain platform selection: Three industry case studies. *IEEE Transactions on Engineering Management*, 67(4):1109–1128.

Friedman, J. H. (2001). Greedy function approximation: a gradient boosting machine. *Annals of statistics*, pages 1189–1232.

Gardner, W. A. (1984). Learning characteristics of stochastic-gradient-descent algorithms: A general study, analysis, and critique. *Signal processing*, 6(2):113–133.

Geneiatakis, D., Soupionis, Y., Steri, G., Kounelis, I., Neisse, R., and Nai-Fovino, I. (2020). Blockchain performance analysis for supporting cross-border e-government services. *IEEE Transactions on Engineering Management*, 67(4):1310–1322.

Gill, K., Yang, S.-H., Yao, F., and Lu, X. (2009). A zigbee-based home automation system. *IEEE Transactions on consumer Electronics*, 55(2):422–430.

Hadwan, H. H. and Reddy, Y. (2016). Smart home control by using raspberry pi and arduino uno. *Int. J. Adv. Res. Comput. Commun. Eng*, 5(4):283–288.

Hang, L. and Kim, D.-H. (2018). Design and implementation of intelligent fire notification service using ip camera in smart home. *International Journal of Control and Automation*, 11(1):131–142.
Haq, Z. U., Khan, G. F., and Hussain, T. (2013). A comprehensive analysis of xml and json web technologies. *New Developments in Circuits, Systems, Signal Processing, Communications and Computers*, pages 102–109.
Hoque, M. A. and Davidson, C. (2019). Design and implementation of an iot-based smart home security system. *International Journal of Networked and Distributed Computing*, 7(2):85–92.
Jabbar, W. A., Alsibai, M. H., Amran, N. S. S., and Mahayadin, S. K. (2018). Design and implementation of iot-based automation system for smart home. In *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6. IEEE.
Jabbar, W. A., Kian, T. K., Ramli, R. M., Zubir, S. N., Zamrizaman, N. S., Balfaqih, M., Shepelev, V., and Alharbi, S. (2019). Design and fabrication of smart home with internet of things enabled automation system. *IEEE Access*, 7:144059–144074.
Jacobsson, A., Boldt, M., and Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, 56:719–733.
Javale, D., Mohsin, M., Nandanwar, S., and Shingate, M. (2013). Home automation and security system using android adk. *International journal of electronics communication and computer technology (IJECCT)*, 3(2):382–385.
Kang, B., Park, S., Lee, T., and Park, S. (2015). Iot-based monitoring system using tri-level context making model for smart home services. In *2015 IEEE International Conference on Consumer Electronics (ICCE)*, pages 198–199. IEEE.
Kumar, P. and Pati, U. C. (2016). Iot based monitoring and control of appliances for smart home. In *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pages 1145–1150. IEEE.
Leccese, F., Cagnetti, M., and Trinca, D. (2014). A smart city application: A fully controlled street lighting isle based on raspberry-pi card, a zigbee sensor network and wimax. *Sensors*, 14(12):24408–24424.
Lobaccaro, G., Carlucci, S., and Löfström, E. (2016). A review of systems and technologies for smart homes and smart grids. *Energies*, 9(5):348.
Mahamud, M. S., Zishan, M. S. R., Ahmad, S. I., Rahman, A. R., Hasan, M., and Rahman, M. L. (2019). Domicile-an iot based smart home automation system. In *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pages 493–497. IEEE.
Maksimović, M., Vujović, V., Davidović, N., Milošević, V., and Perišić, B. (2014). Raspberry pi as internet of things hardware: performances and constraints. *design issues*, 3(8):1–6.
Meng, W., Lopez, J., Xu, S., Su, C., and Lu, R. (2021). Ieee access special section editorial: Internet-of-things attacks and defenses: Recent advances and challenges. *IEEE Access*, 9:108846–108850.
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260.
Patchava V., K. H. and P.R., B. (2015). A smart home automation technique with raspberry pi using iot. In *International Conference on Smart Sensors and Systems (IC-SSS)*, pages 1–4. IEEE.
Pirbhulal, S., Zhang, H., E Alahi, M. E., Ghayvat, H., Mukhopadhyay, S. C., Zhang, Y.-T., and Wu, W. (2017). A novel secure iot-based smart home automation system using a wireless sensor network. *Sensors*, 17(1):69.
Piyare, R. and Tazil, M. (2011). Bluetooth based home automation system using cell phone. In *2011 IEEE 15th International Symposium on Consumer Electronics (ISCE)*, pages 192–195. IEEE.
Quadri, S. A. I. and Sathish, P. (2017). Iot based home automation and surveillance system. In *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, pages 861–866. IEEE.
Sangeetha, S. B. et al. (2015). Intelligent interface based speech recognition for home automation using android application. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pages 1–11. IEEE.
Satapathy, L. M., Bastia, S. K., and Mohanty, N. (2018). Arduino based home automation using internet of things (iot). *International Journal of Pure and Applied Mathematics*, 118(17):769–778.
Sharaff, A. and Gupta, H. (2019). Extra-tree classifier with metaheuristics approach for email classification. In *Advances in Computer Communication and Computational Sciences*, pages 189–197. Springer.
Sherstinsky, A. (2020). Fundamentals of recurrent neural network (rnn) and long short-term memory

(lstm) network. *Physica D: Nonlinear Phenomena*, 404:132306.
Singh, H. K., Verma, S., Pal, S., and Pandey, K. (2019). A step towards home automation using iot. In *2019 Twelfth International Conference on Contemporary Computing (IC3)*, pages 1–5. IEEE.
Sriskanthan, N., Tan, F., and Karande, A. (2002). Bluetooth based home automation system. *Microprocessors and microsystems*, 26(6):281–289.
Vishwakarma, S. K., Upadhyaya, P., Kumari, B., and Mishra, A. K. (2019). Smart energy efficient home automation system using iot. In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pages 1–4. IEEE.
Wang, I., Smith, J., and Ruiz, J. (2019). Exploring virtual agents for augmented reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12.
Wang, W., Xu, H., Alazab, M., Gadekallu, T. R., Han, Z., and Su, C. (2021). Blockchain-based reliable and efficient certificateless signature for iiot devices. *IEEE transactions on industrial informatics*.
Wei, Z., Qin, S., Jia, D., and Yang, Y. (2010). Research and design of cloud architecture for smart home. In *2010 IEEE International Conference on Software Engineering and Service Sciences*, pages 86–89. IEEE.
Wright, R. E. (1995). Logistic regression.
Yamashita, R., Nishio, M., Do, R. K. G., and Togashi, K. (2018). Convolutional neural networks: an overview and application in radiology. *Insights into imaging*, 9(4):611–629.
Yamin, M. M., Ullah, M., Ullah, H., and Katt, B. (2021). Weaponized ai for cyber attacks. *Journal of Information Security and Applications*, 57:102722.
Yeoh, W.-Z., Teh, J. S., and Chen, J. (2022). Automated enumeration of block cipher differentials: An optimized branch-and-bound gpu framework. *Journal of Information Security and Applications*, 65:103087.
Zeinab, K. A. M. and Elmustafa, S. A. A. (2017). Internet of things applications, challenges and related future technologies. *World Scientific News*, 2(67):126–148.