Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 3): pp. 3773-3783
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.03.391

Iot: Home Technologies Of The Future

Kamelsh Chandra Purohit[1], M. Anand Kumar[2], Anuj Singh[3] , Ms Sulekha Varma[4]

[1] Associate Professor, Department of Computer Science, Graphic Era Deemed to Be University, Dehradun, India.

[2] Professor, Department of Computer Science, Graphic Era Deemed to Be University, Dehradun, India.

[3], Assistant Professor, Department of Computer Science, Graphic Era Deemed to Be University, Dehradun, India.

[4]Assistant Professor, Department of Humanities and Social Sciences, Graphic Era Hill University, Dehradun.

Purohit_kaml@rediffmail.com

Abstract—

The Internet of Things (IoT) is a collection of physical devices and things that gather, store, and analyse data. The Internet of Things (IoT) is becoming increasingly important in contemporary developments. Design, development, control, and monitoring of IoT systems in a variety of applications, including health, transportation, agriculture, and home appliances, among others. We offer a framework model for future smart home appliances based on the Internet of Things (IoT), which aids developers in creating infrastructure home automation apps that meet user standards and expectations. The advancement of technology has resulted in the automation of the surroundings, including the home. One of the benefits of technology growth is that it has raised the living standards of human civilization to new advanced levels of comfort and convenience. With 'Smart Home Technologies', we have attempted to achieve yet another milestone. The Internet of Things is used to link the system, Machine Learning is used to make the system smart and sophisticated, and an application is used to operate the system, whether it is an android based mobile application or a Web based application. This paper revies the existing IoT technologies and its future. The main goal of such a system is to centralise everything so that it can be fully automated.

Keywords—Internet of Things, smart things, home security, Smart Phone, Smart home appliances, Automation.

1. INTRODUCTION

The primary concept behind 'Smart Home Technology' is to create a relationship between home and technology in order to reduce manual human effort. It is intended particularly for disabled and elderly people throughout the world to empower them at a low cost. With the use of technologies such as the Internet of Things, Machine Learning, and Mobile application development, we want to construct a system to automate home appliances as part of this project. Temperature sensors, humidity sensors, light detection sensors, smoke detection sensors, and heat sensors will be included in the system based on customer needs and budget. Face verification will be done using a camera, and the system's major components will be Machine Learning-based apps and Internet-connected gadgets. Integration of numerous technologies and subsystems on a single platform is required for the development of a home automation system. Controlled gadgets are often connected to a central hub by a home automation system. A user interface is used to control the system.

The goal of smart Home Technologies is to make homes and appliances smarter by integrating technologies such as the Internet of Things and Machine Learning into a single application that is cost-effective, all of which is hosted on a central platform. Our research looks at how the Internet of Things is used to link different devices and how it might be deployed. It also explains how a machine-learning-based facial recognition system works and how it may be integrated into security locks [1]. Following that, it will be discussed how to centralise the entire system utilising a mobile application that can be used remotely and in person. It will also provide light on how existing technology may be made accessible to persons with diverse abilities. Finally, it will provide a quick overview of how many devices and technologies may be cast on a single platform without the user having to deal with several programmes, resulting in a single application that contains everything.

It must be built for a mobile phone app or a web interface. It may also be accessed without the use of the Internet connection [2]. You can control devices in your home using home automation. From anywhere in the globe, you may access your house with a mobile device. It's possible that the phrase thermostats and sprinklers are examples of standalone programmable devices. Home automation, on the other hand, more correctly portrays houses in which practically everything, including lights, appliances, outlets, heating, and cooling systems that are connected to a network that can be controlled remotely. This also covers your alarm system in terms of home security as well as all of the doors, windows, locks, smoke alarms, and security cameras, as well as any other sensors connected to it. The first duty it addresses is the automated locking and unlocking of doors once they have been closed [2] [3]. After verifying the user with a facial recognition algorithm.

The electronic lock will function properly. It entails creating an effective Face Recognition model to validate the user, who in this case is the home's owner. After the Face Recognition System has been implemented, it must be deployed in a centralised environment, which in our instance is an Android mobile phone application.

Furthermore, the electrical appliances must be connected to a controlling system, which is accomplished through the use of a system on chip and a relay that acts as an electrical switch to connect or disconnect the power supply to the household appliances, including the electric lock. Using a local server, all of these appliances will be connected to a local Wi-Fi network. The automation system will allow users to turn on/off house gadgets straight from their cell phone, which will operate as a remote control. Other benefits include watering the home plants without the need for physical labour, which is accomplished by moving the water pump's controls to the local Wi-Fi. The complete automation will be achieved by introducing a system that will automatically determine whether the soil is hydrated or not and respond appropriately, i.e., designing an intelligent system to sense the soil's moisture demands [3]. The system's most complicated aspect is its ability to avert life-threatening scenarios such as fire mishaps. In the event of a fire, a flame detection system is installed to inform the residents in a timely manner. More features, such as a gas leak alarm system and a smoke detection system, may be added to make it more advanced. A socket is also supplied so that the user may suit the gadget to their needs, making it more user-friendly and convenient. We created an android mobile application for user interaction with the system, which is connected to two servers to integrate it with home devices and a face verification enabled locking system. The programme uses a two-level security scheme to verify the user's identity [4]. To launch the programme and validate the user, the first level requires a security password.

The second phase assures security by taking a real-time photograph of the user and determining whether or not the user is recognised. Only if the individual passes the face verification test will the door be unlocked, and the gadgets will be operational once the two security levels have been crossed. As a result, our home automation system provides both security and convenience in terms of accessing gadgets from any location in the house. To use the device outside of the home, the local server is moved to the internet rather than local Wi-Fi to allow connectivity everywhere and at any time.

This will allow the user to check the status of their household appliances and turn them on and off as desired. Our study demonstrates how multiple technologies and systems may be combined to create an intelligent and user-friendly automation system. Our study is focused on the goal of having all of the systems and models function together on a single platform without colliding.

2. Related Work

Home automation has become a vital focus for innovation, research, and design due to its huge potential and demanding global market. There are various systems available now that can manage home appliances via mobile or online applications with unique capabilities. However, these systems have flaws that prevent them from effectively utilising the architecture and resources available, such as high implementation costs, security flaws, lack of centralization, and a user-unfriendly user interface. We have attempted to address the aforesaid problems in our system by utilising a machine learning-based security system, a user-friendly Android-based mobile application, low-cost devices, and a centrally connected and tailored system. In this part, we'll talk about several cutting-edge home automation systems. An IoT-based paradigm for using technologies and protocols to advance urban houses [5]. The model covers the technology solutions and approaches utilised in the Padova Smart City project, which is a real-time IoT application intended at transforming Padov, an Italian city, into a smart city. Pavitha.D demonstrates how the Internet of Things (IoT) may be used to administer and monitor equipment through the internet in a cost-effective and efficient manner. Both online and local servers can be used to control devices [6]. The IoT-based concept incorporates a security mechanism that sends alert text messages to mobile phones linked to the system's server and raises an alarm if suspicion is detected in the event of intrusion.

The prototype uses a TICC3200 microcontroller and a Wi-Fi module to send notifications to the user's smartphone, independent of whether or not it has internet connection. Vamsikrishna Patchava's approach emphasises the growth of security features employing Computer Vision Technique via video cameras and motion sensors for monitoring, detecting and recognising intruders' presence, all of which are controlled by Raspberry Pi [7]. The study "Internet of Things Business Models, Users, and Networks" delves into several types of IoT-based protocols and their applications. It is advantageous for picking protocols based on the security model used. N. Mohire presented a home automation system that combines wireless communication, mobile devices, and a cloud-based network to allow users to control things both within and outside the home.

3. Home Automation System Spinal Cord - Internet of Things (IoT)

Although this technology allows linking the different components of the system and enabling fast communication between them, the Internet of Things is referred to as the spinal cord for home automation systems. The term "Internet of Things" refers to the interconnection of objects in a network. The items might be inanimate objects or live organisms with a unique identity supplied by a chip with logical addressing integrated in them. It becomes possible to transfer/receive data and act on things once they have a virtual identity [8]. Other significant components include sensors embedded in objects to create relevant data, databases and servers to store this data, and devices with specialised functions to build a network that might be web-based. In a nutshell, the Internet of Things entails creating a network of things with unique virtual identities, similar to a computer network, but without the need for human intervention, while humans can instruct or check the status of the IoT-based system based on the architecture and requirements of the system.

Since devices need to interact with one other and with the controller, the Internet of Things is the backbone of every automation system [9]. This network should be able to store, retrieve, transfer, or fetch data according to the system's requirements without the need for human intervention. They deploy servers and data storage virtual clouds for sophisticated systems for this purpose. To link home appliances with each other and with remote control, we utilise a NodeMCU with ESP8206 chip as a microcontroller and Wi-Fi module in our Internet of Things-based home automation system. The network creates an Intranet by linking devices linked to a local Wi-Fi network. By linking the Wi-Fi to the World Wide Web, the network may be upgraded to Internet. Sensors are also employed in subsystems, such as a flame detection subsystem and a humidity sensor in a plant irrigation system, and they may be customised further. There are two servers that enable for easy data fetching, transfer, and retrieval inside the system, namely from and to the face verification subsystem [11]. The servers are local, but they may be updated to internet servers depending on how much consumers want to spend on a home automation system and what they need. Home appliances such as lights, fans, and power sockets, as well as a plant watering subsystem, a fire alert subsystem, and a mobile phone acting as a central remote control (the mobile should be the network's centralised component), all of which involve humans in this Internet of Things-based automation system.

We make it easy for users to send commands to equipment and verify their status using their smart phones.

4. Security System with Face Verification

The face verification security system's primary task is to match users' faces with photographs of genuine individuals in the dataset. To do this, we developed a quick, accurate, and efficient face identification method. To improve verification reliability, we used a mix of algorithms and models in our face verification system. Deep learning (a subset of machine learning) approaches are mostly used in the algorithms [12]. When compared to conventional approaches, Deep Learning models can do complicated calculations such as data mapping, feature extraction, and so on in a fraction of the time. The goal of implementing such a system is to improve accuracy while lowering mistake rates.

To provide accurate findings, the face verification security system employs a variety of algorithms. The system has an accuracy rate of around 80%.

There are three phases to our face verification algorithm:

The acquired real-time picture is fetched in the algorithm for processing in the first step. Only important information from the picture pixels is sent on to the next stage, which in this case is the user's frontal face. The pixels of the frontal face are carefully retrieved from the image since the output of the subsequent models is highly dependent on them. In the second stage, they are fed into two different models for evaluation.

The following are the steps for retrieving and processing data for frontal face detection:

1. To obtain pixel format, convert the picture into byte arrays.
2. Crop the pixels such that just the frontal face pixels are visible.

```
If pixel value! = frontal face:
Discard
Else:
```

3. Create tiny and big models from the byte arrays.
4. Come to an end

The face verification algorithm's second step is the major computing stage, which generates probability of face matching from two independent machine learning models that function in parallel without impacting each other's output. Both models analyse picture pixels at the same time and give probability for the person who matches the legitimate user. One model is little, while the other is huge and performs more sophisticated calculations than the first. The tiny model using Hog Face Detector to determine if the user's image matches any other image in the legislative user dataset. On the frontal face, the 'Hog Face Detector' maps 68 landmarks. This is accomplished by computing distances between pixels on the frontal face (for example, the distance between the forehead and the chin). The distances are saved as vectors, which are compared to the vectors of the valid photos, and the subsequent probabilities are returned as output. The tiny model accomplishes this by normalising the test data with the real user data, yielding a % likelihood of the user being legitimate as a consequence.

Steps for comparing facial landmarks on a miniature model:

1.Using the Hog Face Detector, plot 68 land marks on the frontal face.
2. For comparison, feed the terrain markings to a miniature model.
3. Landmarks comparison with a real user dataset using normalising procedures.
4. Keep the model's output in a safe place.

Convolution Neural Network Mmode Detector, a Deep Learning-based model, is used in the huge model. This model accepts frontal picture pixels as input and uses layers of convolutional neural networks to extract face characteristics. The extracted face features, which are in the form of vectors, are then compared with the legitimate users' vectors of facial features. The probability is the proportion of facial features that seek to match with the genuine user as a consequence of the process. The following are the steps for extracting face characteristics from a huge model:

1. Using the Mmode facial detector, extract face characteristics.
2. Use the neural network's convolution layer to match the features.
3. Using a thick layer, convert the result of a multidimensional array to a single-dimensional array result.
4. Save the huge model's outcome.

The algorithm's third and final step commences after the production of match probabilities. To derive tolerance from the consequent probability from both big and small models, we now use another machine learning model. The Resnet Convolution Neural Network Model uses probability from small and big models to provide a tolerance value for legitimate user or invader identification. We've specified a tolerance value of at least 40%, which means that if the value hits or surpasses this threshold, the user is deemed legitimate and permission to lock/unlock the door for a single time is provided. After that, the Face Verification Security System authentication is accomplished.

5. Servers for sending requests and retrieving responses

A server may be defined as a programme that provides functionality to another programme or device. For our Internet of Things concept, we deployed dedicated local servers that only handle a few specific requests. Additional functionality may be added to the servers by converting them from local to online. Two servers are used in 'Comfy Smart Home with IoT' to fulfil distinct objectives. The server that sits between the mobile application and the face verification model is written in the Flask programming language, while the one that sits between the NodeMCU system on chip and the mobile application is written in C. To interface with the image verification server and the NodeMCU server, the Android mobile application employs Restful APIs (Application Program Interfaces). An API is a piece of code that allows two or more programmes or devices to interact with one another by specifying a format that they must follow. API is a significant toolset for developing Internet of Things-based systems that provide connectivity between various tools. The goal of employing Restful APIs in the home automation system is to provide a stable and adaptable environment [34]. APIs' capacity to add functionality gives resilience and customisation, while their ability to communicate with a variety of apps and tools regardless of programming language provides flexibility, which aids in the preservation of Internet of Things technology.

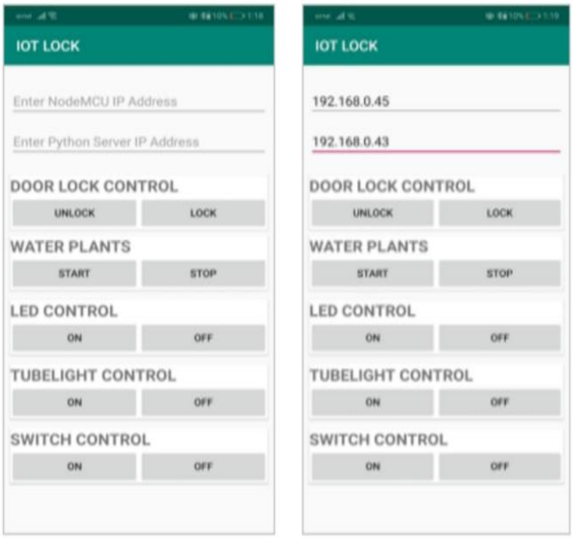
Servers' Generalized Working Algorithm:

1. A system application sends a request to the server via the Application Program Interface (API)
2. The server saves your request and sends it to the backend system application for processing.
3. Another system processes the request and produces results.
4. Sends the ensuing outcome to the server.
5. Receives the result and sends it to the front end application system as a response to the request.

We employ a Web API, also known as a Restful API, that communicates and exchanges data via URLs. It is the API that asks servers to perform a certain function and records their replies in accordance with the request's outcome. An API can utilise multiple ways to make requests or obtain responses from the server; ours uses the Post method to submit requests since the data is sent in encrypted form, which protects it from malicious usage, and the Get method to retrieve responses from the servers. The NodeMCU server, which is implemented in C programming language, accepts the URL (Universal Resource Locator) and IP address technically logical address from the mobile application written in Java, while the Python Face verification system server, which is implemented in Flask programming language, accepts the URL and logical address from the mobile application written in Java.

6. The role of mobile applications in the 'Smart Home Technologies Using IoT'

The mobile application that has been utilised to link every single device in the system to a central control is the most important aspect of our home automation system. For mobile phones, the android application is based on a native platform and programmed in Java. The user can connect to the NodeMCU by supplying the IP address of the server running on the NodeMCU, as well as connect to the flask server by entering its IP address. The user can then use that app to control all of the devices mentioned in it, as well as unlock the door using the face unlock functionality enabled by Flask server and Face Verification System. The mobile application uses the IP address of the Flask server to access the face verification subsystem. The mobile application connects to the Flask server attached to the face verification subsystem by supplying the server's IP address. For authentication, the mobile application uses the phone's camera to take a real-time image of the user. The Rest APIs then use the server to deliver the request to the validation system. The application's features are opened for legitimate users; otherwise, it will keep requesting for user authorisation. To monitor and access the devices, the application requires a logical address, which is the IP address of the server operating on the NodeMCU, which is also linked to the Flask server. The mobile application makes a request to the NodeMCU mentioned in the app's menu to lock or unlock the door. It has a long list of capabilities, including automatic plant watering, home appliance switching on/off, fire alarm, and other features, all of which are housed in an easy-to-use user interface. The mobile application is sturdy, secure, and user-friendly all at the same time. The user interface was likewise created using native Android, with the idea that the user may be of any age. It has a basic user interface with large buttons that can be used by people of all ages. The user interface is also designed in such a way that it may be adapted to be used by visually or physically handicapped people in the future 1.



192.168.0.45

192.168.0.43

Figure 1. Screenshots of Android Mobile Application for IOT LOCK

7. <u>Smart Home Technologies Using IoT: Results and Findings</u>

It has been proven through the prototype that a home automation system can be developed utilising the Internet of Things and Artificial Intelligence, with a mobile android application functioning as a central control. Because the system is offline, web-based threats are implicitly forbidden, and only the Wi-Fi network has to be protected against unauthorised or external access. The technology only functions while the authenticated Mobile device is within Wi-Fi signal range, preventing any remote access assault. The system is constructed with the bare minimum of hardware support and equipment, emphasising its cost efficiency, and it is a personalised home automation system, unlike other systems. The system's versatility allows users to add or remove features based on their needs and budgetary resources. The Android application was created only for the purpose of user validation and system control, and it was built using open source APIs and frameworks. Furthermore, the mobile application only operated when the right Wi-Fi and NodeMCU microcontroller IP addresses were known, and the mobile application's GUI (Graphical User Interface) was also user-friendly.

The Face Verification algorithm's True Positives success rate was 9 out of 10, confirming the algorithm's resilience and efficacy. The typical server response time for verification/validation is 3 to 5 seconds, thanks to the Face Verification System's Machine Learning algorithms. On the other hand, the Microcontroller's response time to requests is less than 0.1 second, which appears to be device dependant. As a result, once a user has been authorised, the operating cost is minimal in terms of time.

From the standpoint of actual implementation, the following table summarises the state of the concepts and components of the 'Smart Home Technologies utilising IoT' given in this paper:

Table.1 Status of components

Components of Smart Home Technologies	**Current Status**
Face Verification System	Practically Implemented
Centralized Control via Mobile App	Practically Implemented
Offline Servers	Practically Implemented
Intermodular Connectivity	Practically Implemented
Online Servers Implementable	Conceptual but Practically

As a result, the concept given was realistic and could be completely executed. Internet of Things, Machine Learning, Android Application Development, Microcontroller Programming, and Server Architecture are the most important domains to know.

8. Conclusion and Prospect

Smart Home Technologies is a cost-effective, smart home automation solution that includes all of the required functions. Our home automation has achieved its goal of producing a higher level of comfort and convenience in people's living standards. As of now, it is a successful and stable working model of comfortable and smart automation, and we have achieved our goal of developing a home automation to make users' lives more comfortable, easier, and in line with advanced technological standards, but there is still room for improvements and add-on services. After creating a centralised automation system for a normal user, the system's assistance could be expanded by including voice assistants, emergency triggers, and music/tone recognition controllers for physically challenged people, allowing the system's benefits to reach a larger group of people and making it truly useful for those who need it the most. Not only that, but it can be made more safe and useful in emergency scenarios, such as by building a system that would warn the user and their trusted ones when they are in danger. The next objective would be to make it more convenient by offering a smart voice and sound control with an add-on function that is a speech system that informs the user of the tasks that the system has completed thus far. Security sensors such as smoke detectors, Gas Leak Detectors to detect natural gas leaks in the house, and an Intrusion Detection system employing smart security cameras and Artificial Intelligence algorithms may be added to the 'Comfy Smart Home' for the protection of the house and its residents. Users will be able to get timely message notifications thanks to the mobile application's connection. Smart Home Technologies with IoT is a customizable home automation system that can be tailored to the user's needs and security requirements. As a result, the long-term goal is to make the system more resilient and advanced by adding new features. The next stage would be to make the network dynamic by connecting the servers to the World Wide Web using Heroku, an online server building platform. Encryption techniques and cryptosystems can be used to improve the security of dynamic web servers by ensuring the secrecy and conciseness of picture data and commands to the microcontroller when sending and fetching requests. Efforts can be made to build a technique that allows home automation to be easily customised based on the preferences of the user. Updates to mobile phone applications can include things like improving the Graphical User Interface for easier understanding and availability in multiple languages, evolving it for platforms other than Android, increasing security against web attacks, ensuring data privacy, and improving performance. As previously said, the 'Comfy Smart Home' has a wide range of potential for innovation and development; however, as technology advances and the capacity to create grows, the future vision will expand even more.

REFERENCES

[1]. Al-Ali, A.R. ; Dept. of Comput. Eng., American Univ., United Arab Emirates ; AL-Rousan, M., "Java-based home automation system"2004.

[2]. M.-T. Chen, C.-M. Lin, "Standby power management of a smart home appliance by using energy saving system with active loading feature identification", IEEE Trans. Consum. Electron., vol. 65, no. 1, pp. 11-17, Feb. 2019.

[3]. P. Bertoldi, "Code of conduct on energy consumption of broadband equipment—Version 6.0", Feb. 2017.

[4]. B. Taji, A. D. C. Chan, S. Shirmohammadi, "Effect of pressure on skin-electrode impedance in wearable biomedical measurement devices", IEEE Trans. Instrum. Meas., vol. 67, no. 8, pp. 1900-1912, Aug. 2018.

[5]. L. Lombardo, S. Corbellini, M. Parvis, A. Elsayed, E. Angelini, S. Grassini, "Wireless sensor network for distributed environmental monitoring", IEEE Trans. Instrum. Meas., vol. 67, no. 5, pp. 1214- 1222, May 2018.

[6]. P. Ferrari, A. Flammini, E. Sisinni, S. Rinaldi, D. Brandão, M. S. Rocha, "Delay estimation of industrial IoT applications based on messaging protocols", IEEE Trans. Instrum. Meas., vol. 67, no. 9, pp. 2188-2199, Sep. 2018.

[7]. M. Raspopoulos, "Multidevice map-constrained fingerprint-based indoor positioning using 3-D ray tracing", IEEE Trans. Instrum. Meas., vol. 67, no. 2, pp. 466-476, Feb. 2018.

[8]. F. Al Machot, A. H. Mosa, M. Ali, K. Kyamakya, "Activity recognition in sensor data streams for active and assisted living environments", IEEE Trans. Circuits Syst. Video Technol., vol. 28, no. 10, pp. 2933-2945, Oct. 2018.

[9]. G. Azkune, A. Almeida, "A scalable hybrid activity recognition approach for intelligent environments", IEEE Access, vol. 6, pp. 41745-41759, Aug. 2018.

[10]. V. Bianchi, P. Ciampolini, I. De Munari, "RSSI-based indoor localization and identification for ZigBee wireless sensor networks in smart homes", IEEE Trans. Instrum. Meas., vol. 68, no. 2, pp. 566-575, Feb. 2019.

[11]. H. Wang, D. Zhang, Y. Wang, J. Ma, Y. Wang, S. Li, "RT-Fall: A real-time and contactless fall detection system with commodity WiFi devices", IEEE Trans. Mobile Comput., vol. 16, no. 2, pp. 511-526, Feb. 2017.

[12]. Tiwari, A., Sharma, N., Kaushik, I., & Tiwari, R. (2019). Privacy Issues & Security Techniques in Big Data. International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). IEEE, 2019.