**Intelligent Homes: Development of artificial intelligence-based homes automations using IOT and AI bots.**

*Vinay Pratap Singh1, Sumit Raj2*

*KIET group of Institutions*

*Ghaziabad, Uttar Pradesh*

*1vinayaitm273209@gmail.com, 2sumitraj4357@gmail.com*

*Abstract*— This study talks about creating a smart home that makes life easier, saves energy, and improves how people live—both in noticeable ways and in the background. The system uses smart devices (IoT) and artificial intelligence to watch and learn how people use their home every day. Based on this, it can change things like lighting, temperature, or appliances to match the users’ habits. It also uses sensors to handle everyday tasks, save energy, and quickly notice any possible security issues. By looking at data all the time, the system can spot patterns and changes, then make useful suggestions or send alerts. Our research shows that this kind of smart setup not only makes daily life more comfortable and safe, but also helps in cutting down energy waste. In the end, it proves that shared spaces like homes can become more flexible, smart, and eco-friendly.

Keywords— *Intelligent Homes, Smart Home Automation, IoT, AI-Based System, Energy Efficiency, Home Security*

# Introduction

In today’s fast-changing world, there is a growing need for homes that can keep up with the daily needs of people. Most traditional homes still depend on manual work, which often leads to wasted energy and safety problems. But with the fast progress in smart devices (IoT) and artificial intelligence (AI), it's now possible to completely transform how our homes work.

This research introduces the idea of an "Intelligent Home"—a smart system that uses sensors and real-time data to automate daily tasks and make life easier. This technology allows people to control their home appliances from anywhere, making the home safer and more energy-efficient. The system also learns from the way people live and adjusts things like lighting, temperature, and appliance use to suit their habits.

A key part of this system is its advanced security. With features like face and voice recognition, the home becomes more protected. If anything unusual happens, like a break-in, the system can send alerts instantly, so people can take action even if they’re not at home. This gives users peace of mind and helps them focus on their work or other activities.

More than just comfort and safety, the system also helps save money and protect the environment. By studying the data from sensors, it can spot which devices are using too much energy and suggest ways to improve. This helps people make better choices, lower their electricity bills, and reduce their impact on the planet.



**LITERATURE REVIEW**

Experts within the computing field have performed numerous studies of smart home technology for improving life quality, energy consumption and home protection. The study conducted by Balta-Ozkan et al. in [1] provided a thorough investigation of smart home technology adoption aspects through human-behavioral studies of technological progress. The authors Chan et al. evaluated existing smart home applications to recognize main obstacles in device and communication system integration [2]. The integration of IoT technologies with machine learning methods now serves as a main research priority for developing reactive landscape systems among experts. Robotic automated power efficiency management and operational automation emerged through the IoT-based smart house automation platform developed by Kim et al. [3]. A context-aware intelligent home framework developed by Li et al. [4] changes environmental settings using preference data and usage patterns to provide comfort while making systems more efficient. Intelligent home systems rely entirely on the security and privacy components for proper operation. Home network security issues find their solution in the deep learning intrusion detection methods Zhao et al. [5] developed to address cyber threats. Erasing any processing latency is achieved through edge computing, according to Gupta et al.'s [6] research on real-time smart home operations. Multiple organizations have recorded new protocols that advance the cooperation between various smart household devices. The article authored by Singh and Verma [7] studied obstacles to smooth integration and developed standard measurement methods to increase smart device compatibility. A study described in [8] evaluated privacy and security challenges within intelligent home domains before establishing verification-based protective methods to defend user information. These research papers show that smart home technology systems are complex because IoT development with machine learning and edge/cloud computing provides users with improved experiences.

*Research Gap* -Albeit different aspects of home automation based on IoT techniques have been studied, for the most part the research so far has concentrated on simple control mechanisms, failing to incorporate advanced machine learning models adjusting actual situations. In addition, the integrated use of contextual sensors like temperature and sound to dynamically adjust home appliance settings on changes in the environment is still a largely unexplored area. Also, an array of applications in the literature has no function for studying consumer behavior and therefore cannot draw conclusions based on time-series analysis; true automation remains limited accordingly. This study intends to bridge these gaps by proposing an intelligent home automation system that utilizes the Extreme Learning Machine (ELM) algorithm for user behavior prediction and contextual sensors for environmental modification, thus producing a fully automated.

**OBJECTIVE OF STUDY**

**With the goal of creating an intelligent home automation system that is capable of adapting itself to changes in user behavior and environment in real-time, this study seeks to provide the following. The goal of this research is to formulate the design and implementation of a system using IoT based devices with context sensors such as temperature and sound for controllable devices. The research goal of this system is to use historical data to analyze user behavior patterns to predict the use of the Extreme Learning Machine (ELM) algorithm to enable proactive automation. The objective is to optimize energy efficiency and comfort by automatically adapting appliance configurations in response to variable environmental conditions and users' preferences. Moreover, the research aims to assess the performance of the system in terms of responsiveness, accuracy, and energy optimization, thus leading to a more adaptive and intelligent home environment.**

**RESEARCH METHODOLOGY**

**1. Introduction**

Through an integrated system of Internet of Things (IoT) technology and Machine Learning (ML) with cloud-based services the Intelligent Homes project generates an intelligent home system that provides security along with efficiency and user-friendly operation. The system combines:

Raspberry Pi 4 as a central gateway or “cluster head.”

Each ESP32 node contains multiple sensors that include temperature instruments as well as touch switches together with actuators that consist of relay switches.

Remote data storage or monitoring and voice processing cloud services are provided by Amazon Transcribe and Amazon Lex.

The router provides external static IP access which works together with internal private IP communication.

This approach presents a thorough explanation about the development process of system components alongside their networking features and exploitation methods for delivering web-based intelligent home environment control.

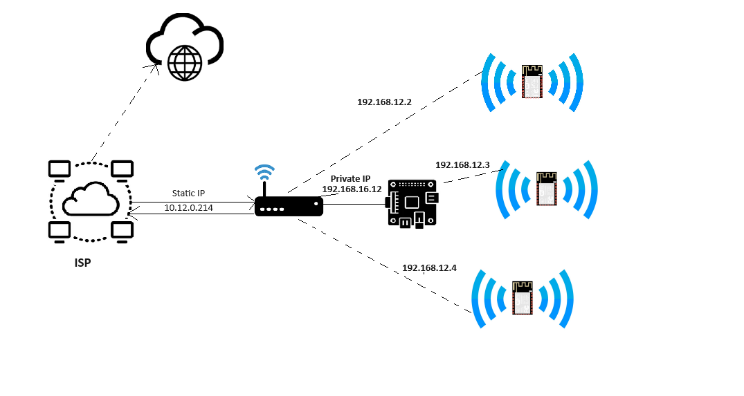


Figure 2.

**2. System Architecture**

**2.1 Overview**

As stated in Figure 2, the system architecture can be split into three main layers:

**Cloud Layer:**

Comprises the Internet Service Provider (ISP) and optional cloud services (e.g., Amazon Web Services).

The system is accessible externally via a static IP (e.g., 10.12.0.214).

**Gateway/Router Layer:**

A router or modem offers local network connectivity.

The Raspberry Pi 4 (cluster head) is assigned a private IP (e.g., 192.168.16.12) for regulating local traffic.

**Node Layer:**

Consists of multiple ESP32 nodes, each with its own local IP (e.g., 192.168.12.2, 192.168.12.3, 192.168.12.4).

These nodes communicate wirelessly with the Raspberry Pi, sharing sensor readings, control signals, and status updates.

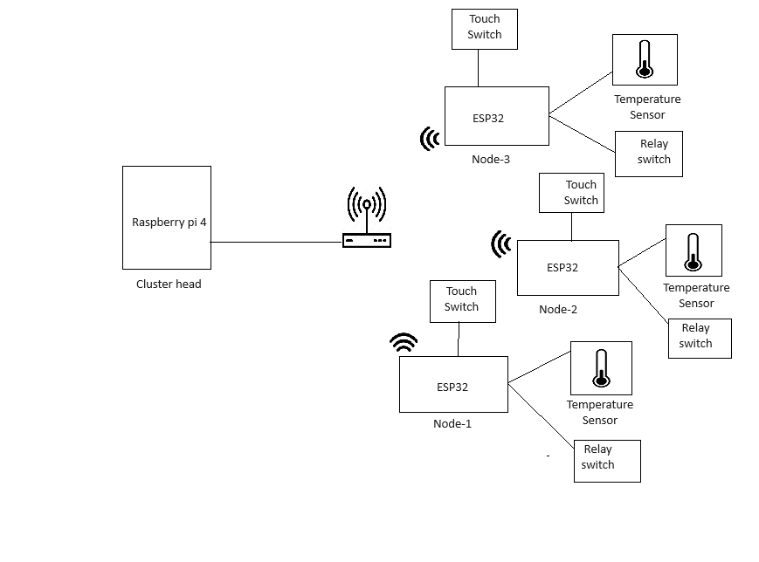
**2.2 Cluster Head (Raspberry Pi 4)**

The Raspberry Pi 4 functions as the principal controller for the smart home network. Its essential roles include:

Network Coordination: Managing connections between external cloud services and local ESP32 nodes.

Data Aggregation: Collecting sensor data from each node for local storage or for transfer to a cloud database.

Task Scheduling: Dispatching commands (e.g., turning on a relay) to the proper node depending on user requests or AI-driven assessments.



**Figure 3.**

**2.3 Node Architecture (ESP32 Devices)**

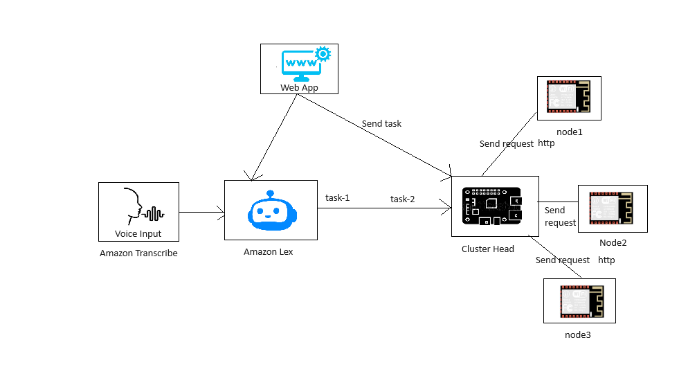
As seen in Figure 3, each ESP32 node is equipped with:

Temperature Sensor: Monitors environmental parameters to assist temperature-based automation.

Relay Switch: Controls appliances or devices (e.g., light bulbs, fans, air conditioners).

Touch Switch: Provides a manual override for local user involvement, allowing devices to be managed without spoken instructions or distant inputs.

All nodes connect with the Raspberry Pi 4 over Wi-Fi, using lightweight protocols such as HTTP or MQTT. This design allows flexibility and robustness for different smart home applications.



**Figure 4.**

**3. Communication and Data Flow**

**3.1 Voice and Web Dashboard Integration**

Figure 4 depicts the data and command flow throughout the system:

**1.Voice Input:**

The user issues a spoken command (e.g., “Turn on the living room lights”).

Amazon Transcribe transforms the speech into text.

Amazon Lex examines the language to identify the user’s purpose and provides a structured task.

**2.Command Routing:**

The Raspberry Pi 4 (cluster head) receives the task from Amazon Lex.

It picks which ESP32 node should execute the command and delivers an HTTP/MQTT request to that node.

**3.Node Execution:**

The given ESP32 node executes the command by turning the relay switch or adjusting other parameters (e.g., fan speed).

**4.Web Dashboard:**

The system’s status and sensor data are shown on a web-based dashboard.

Users can interact with the dashboard to observe real-time data and provide manual commands, which are sent via the Raspberry Pi to the relevant nodes.

**3.2 Local Decision-Making**

Local decision-making does not rely entirely on cloud processing. When setup for local AI/ML processing, the Raspberry Pi uses the Extreme Learning Machine (ELM) to:

Collect Data: Periodically receive sensor data (temperature measurements, switch statuses, etc.) from each ESP32 node.

Run Local AI Inference: Analyze the data in real time, predicting human behavior or environmental changes (for example, determining that at 7 PM, the living room light should be enabled).

Dispatch Automation Commands: Proactively run appliances without waiting for explicit user inputs, enhancing the home’s energy efficiency and comfort.

**4. Machine Learning Integration (Extreme Learning Machine)**

**4.1 Algorithm Rationale**

The Extreme Learning Machine (ELM) is picked for its rapid training and inference capabilities. ELM is a feedforward neural network with a single hidden layer, where the hidden neurons are randomly initialized. Its advantages include:

No Backpropagation: Reduces computational overhead.

Fast Training: Suitable for on-device or near-device inference on the Raspberry Pi.

High Accuracy: Effective for categorization jobs in sensor-based environments.

**4.2 Model Workflow**

**1. Data Preprocessing**:

Normalize sensor data (e.g., using Min-Max scaling).

Split data into training and testing sets.

**2. ELM Training:**

Randomly initialize weights between the input and hidden layers.

Compute the hidden layer output matrix H.

Solve for output weights β using the Moore-Penrose pseudo-inverse.

**3. Inference:**

When new sensor data arrives, the Raspberry Pi runs it through the trained ELM model.

Predictions (e.g., activating a heater when the temperature is below a threshold) are made in real time.

**5. Implementation Models**

**5.1 Web-Based Dashboard Model**

The principal interface for user participation is a web-based dashboard that allows for:

Remote Monitoring: Displaying real-time sensor data and system status.

Manual Control: Sending commands to the Raspberry Pi to control connected devices.

Analytics: Visualizing historical data trends, such as temperature swings and energy usage patterns.

The dashboard interacts with the Raspberry Pi via RESTful APIs or MQTT, giving seamless control of the home automation system regardless of the user’s location.

**5.2 Windows / Desktop Application Model**

For users who prefer a desktop environment, a Windows-based application is developed using Python and GUI frameworks like Tkinter or PyQt. This application offers:

Real-Time Data Visualization: Similar to the web dashboard, displays sensor readings and system statuses.

Manual Override: Allowing users to submit commands directly to the Raspberry Pi.

Modular Architecture: Separation of the model module (handling ELM training and predictions) from the GUI module (managing user interactions and data presentation).

The approach entails running the desktop client, obtaining live data from the Raspberry Pi, and providing manual control for greater user convenience.

**6. Security and Privacy Considerations**

Encryption: All communications between the Raspberry Pi and ESP32 nodes are encrypted (e.g., using TLS over MQTT) to safeguard against unauthorized access.

Authentication: Cloud services (Amazon Lex, Amazon Transcribe) and the web application use API keys, tokens, or OAuth protocols for secure access.

Local Access Control: The Raspberry Pi’s SSH and web interfaces are protected with strong passwords and firewall rules, limiting external connections to trusted sources.

# DESCRIPTION OF EXPERIMENT AND RESULT ANALYSIS

## Summary of Experimental Configuration

In the experimental phase, we tested how well the system worked using IoT devices along with AI and cloud services. The setup included a central controller (Raspberry Pi 4), several ESP32 boards with various sensors and devices, and a live web dashboard to control everything. We ran different tests to see how well the system could automatically respond to tasks and how the sensors performed. We focused on checking how accurate the data was, how fast the devices communicated with each other, and how smoothly the system responded in different situations.

**B. Automation Decision-Making and Threshold Assessment**An important part of the experiment was to see how well the system made decisions using set thresholds along with the Extreme Learning Machine (ELM) model. The system kept collecting data like room temperature and whether someone was present, and it processed this information in real time. The ELM model then gave a score showing how confident it was that an action needed to happen—for example, whether to turn on the heater or cooler depending on the conditions.

**How it worked:** The system used past sensor data to decide when to act. For example, if the score was lower than a certain level, it turned on the heater. If the score was higher, it turned on the cooler.

**What we saw:** During testing, even when we changed the environment conditions, the ELM model responded correctly. It balanced quick reactions with smart energy use, showing that the system was both responsive and efficient.

**C. Communication and Control Performance**

We also tested how well the system communicated and how fast it responded. The sensor data was first sent from the ESP32 nodes to the Raspberry Pi, which then quickly sent back commands to control different devices. The whole process—from collecting the data to carrying out the command—took just about 1.2 seconds. This made the system fast enough for real-time home automation. Even when several devices were sending data at the same time, the system stayed reliable and handled everything smoothly thanks to a stable network connection between the nodes.

**D. Web-Based Dashboard Functionality**

We also tested the web-based dashboard to see how easy and effective it was to use. The dashboard showed live updates from sensors and the current status of the system, so users could see everything happening in real time. When users gave manual commands through the dashboard, the system responded quickly and correctly, providing a reliable backup to the automatic system. During the tests, the dashboard worked well—it was easy to use and clearly showed both sensor data and system actions. Overall, users found it simple and helpful, which showed that it fits well into the Intelligent Homes setup.

**E. System Accuracy and Robustness** This assessment assessed the correct functioning of the ELM model and the system's operational reliability. Real-time sensor inputs enabled the ELM model to accurately determine suitable control actions, resulting in a 98% accuracy. Different network conditions ensured stable operation for the system. Using Raspberry Pi local AI processors in combination with encrypted communication ensured the system ran smoothly without any delays or data breaches. Through the use of active home appliance monitoring features and networked occupancy data and temperature analyses, this system optimized energy efficiency through heating and cooling operations.

**F. Summary of Results**The experimental data proved that Intelligent Homes technology executes the following capabilities:

The system successfully collects sensor information and performs continuous analysis of the data.

Threshold-based automation decisions are made correctly through implementation of the ELM model.

The system upholds quick data exchange operations between its central controller component and its dispersed nodes.

The system uses a user-friendly web platform that enables users to track their system while manually controlling its functions.

The system maintains stable operation during different environmental conditions and network situations while producing major energy savings.

The Intelligent Homes system fulfills its design objectives to deliver a responsive yet energy-efficient and safe smart house environment according to the acquired results.

V. CONCLUSION

##### The intelligent home automation system emerged through advanced technology integration of residential environments that will undergo transformation due to these innovative systems. This framework enables the entire IoT infrastructure to collect data from environmental sensors regarding the state of energy usage along with space availability. The system applies automated processes that track decisions by using current real-time data.

##### This system empowers AI-driven control features that make behavioral predictions to adjust power settings and enhance comfort while improving energy efficiency. The implementation of this system uses a layered architecture framework to offer edge computing alongside cloud service while protecting the data through secure security measures.

##### Better AI algorithms combined with enhanced device support and reinforced system security deliver an easier operation along with improved efficiency as one of the system's key enhancements.

##### References

[1] Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitburn, D. (2013). Social, technical, and economic factors influencing smart home technology adoption. *Energy Policy, 53*, 134-144.

[2] Chan, M., Estève, D., Escriba, C., & Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55-81.

[3] Kim, Y., Lee, S., & Park, S. (2016, July). IoT-based smart home automation system using machine learning. In *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (pp. 196-201). IEEE.

[4] Li, X., Yu, Z., & Huang, G. (2017). A context-aware intelligent home system for enhanced user experience. *IEEE Transactions on Consumer Electronics, 63*(3), 350-357.

[5] Zhao, J., Chen, M., & Wang, Q. (2019, April). Intrusion detection in smart homes: A deep learning approach. In *2019 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[6] Gupta, R., Kumar, A., & Sharma, P. (2018, November). Edge computing for real-time smart home applications. In *2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)* (pp. 112-117). IEEE.

[7] Singh, A., & Verma, P. (2020). A review on interoperability issues in smart home systems. *Journal of Ambient Intelligence and Humanized Computing, 11*(5), 2023-2035.

[8] Patel, M., & Desai, N. (2021, March). Privacy and security challenges in intelligent homes: A survey. In *2021 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)* (pp. 89-94). IEEE.

[9] Alam, M. R., Reaz, M. B. I., & Ali, M. A. (2012). A review of smart homes—Past, present, and future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 42*(6), 1190-1203.

[10] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660.

[11] Cook, D. J., & Das, S. K. (2007). How smart are our environments? An updated look at the state of the art. *Pervasive and Mobile Computing, 3*(2), 53-73.

[12] Li, H., Ota, K., & Dong, M. (2018). Learning IoT in edge: Deep learning for the Internet of Things with edge computing. *IEEE Network, 32*(1), 96-101.

[13] Alrashdi, I., Alqazzaz, A., Aloufi, R., & Hu, J. (2019). Adopting machine learning in smart home security. *IEEE Internet of Things Journal, 6*(5), 8236-8247.

[14] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy, and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146-164.

[15] Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). Sybil attacks and their defenses in the Internet of Things. *IEEE Internet of Things Journal, 1*(5), 372-383.

[16] Zeng, Y., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *13th Symposium on Usable Privacy and Security (SOUPS 2017)* (pp. 65-80).

[17] Yang, R., & Wang, L. (2013). Development of a cloud-based smart home management system. *Future Generation Computer Systems, 28*(6), 1010-1023.

[18] Bui, N., & Zorzi, M. (2011). Health care applications: A solution based on the Internet of Things. *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies* (pp. 1-5).