International Journal of Scientific Research in Computer Science and Engineering
Vol.**13**, Issue.**3**, pp.**84-94**, June **2025**
E-ISSN: 2320-7639
Available online at: www.isroset.org

Research Article

Design and Implementation of IoT-Based Smart Home Automation Model

GATETE Marcel[1*], HARUBWIRA Flaubert[2]

[1,2]Dept. of Business Information Technology, University of Tourism, Technology, and Business Studies, Kigali, Rwanda

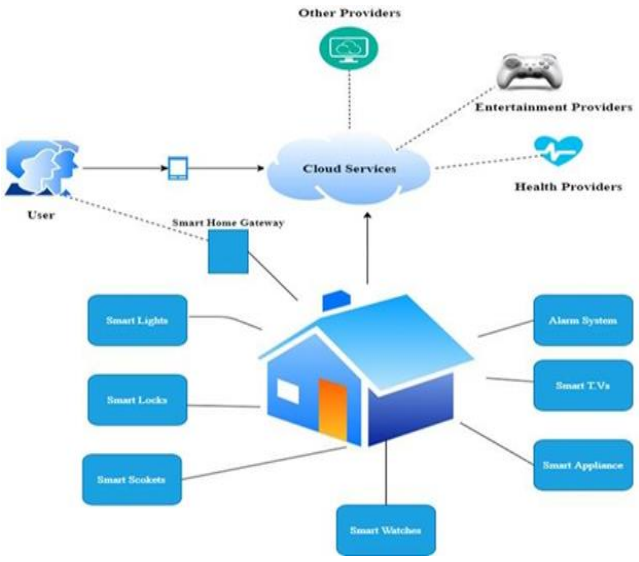
**Corresponding Author:* ✉

Received: 20/Apr/2025; **Accepted**: 22/May/2025; **Published**: 30/Jun/2025. | **DOI**: https://doi.org/10.26438/ijsrcse.v13i3.684

Abstract— Investigating the feasibility of the development of the Internet of Things and how objects are linked to the Internet to improve our daily lives through the functioning of smart homes is the primary goal of this study. The literature review chapter of this study has looked at the definition, capabilities, and present trends of the Internet of Things. The literature has enhanced our comprehension of this shift as the Internet of Things applications keep growing. We have also considered privacy and security concerns. The framework we employed was created with the aid of Cisco Packet Tracer, a technology that enabled us to establish network topologies and logical designs through visual simulation tools. Ie. The use of Python programming to integrate IoT features into Smart Homes and the IoT architecture to examine the application model. Those tools were also utilized during the feasibility study to build a network model. The primary goal of this research project has finally been accomplished, as we have demonstrated a practical solution to the manual house problem by offering a streamlined home configuration in which devices and appliances may be operated remotely or automatically via an Internet connection.

Keywords— Cisco Packet Tracer, Internet of Things, Security, Smart Home, and Privacy.

Graphical Abstract-



- IoT provides a collective databank to all devices to store their data.
- Data is sent from different sensors to the IoT platform.
- It accesses the received data from various sources.
- It analyses the data and extracts the information according to the requirement.
- In the end, the resulting information is shared between the connected devices to this IOT platform for better user experience in the future.
- Smart home devices that are connected to the network gateway.
- The user can easily control all home appliances with a smartphone or tablet.
- Smart home automation saves the time and effort of the user\owner.

1. Introduction

The world in which we live is changing rapidly; it is a truly organic phenomenon that every one of us can influence. This is an incredible opportunity; we must seize it with all of our potency. As everything becomes Internet-connected and integrated into information systems and end-user applications, our daily lives are gradually changing. This creates an infinite and interconnected universe where humans and machines work together to make our lives easier, the world safer, healthier, and more environmentally friendly. The Internet of Things is referred to as the "IoT" in the scene behind.

The phrase "Internet of Things" refers to the fusion of the first human-generated internet data and the subsequent data generated by objects. According to many panels of scientists with expertise in digital innovation, Kevin Ashton, a technological pioneer, is credited with coining the phrase "IoT" [1].

All over the world, the urban development master plan has to be modified as a significant section of the population is shifting to urban areas, and the percentage of people living in towns and cities is progressively increasing. Countries are creating a robust information technology hub and still investing in the development of enough highly qualified technicians and informaticists to meet the demands of making their countries smarter; therefore, knowledge-based technology will make the ICT industry more competitive.

Affordable housing is daily being built with a lot of dwelling units available and owned by citizens, these are inexpensive housing projects that will accelerate urbanization shortly. As a result, more modern homes with integrated technology will provide a more acceptable living environment.

People are embracing smart devices in their homes at a greater rate than ever before, and IoT devices will soon become a part of the mainstream electronics culture. By 2025, there will likely be 75 billion IoT devices installed globally and the worldwide smart home market will be worth more than US$53.45 billion, and the Internet of Things will advance to have important home and business applications that improve people's quality of life. It will be possible to remotely access and operate the gadgets installed in a home from any location at any time using the Internet of Things in a smart home.

For example, residents in smart homes will be able to operate air conditioning systems, make meals, receive real-time safety alerts, and have the ability to automatically turn on lights as they enter the house. As the world grows smaller due to the Internet of Services, companies like Xiaomi and IKEA have produced smart devices like robot vacuums, smart lighting, and smart home appliances. These products are sold online and can be bought through e-commerce and applications that can be downloaded using the iOS and Android operating systems from Apple and Google, respectively [2].

The idea behind the IoT is straightforward. It entails connecting all of the world's physical locations and objects to the internet. The Internet of Things (IoT) is a network of gadgets including cars and household appliances that have electronics, software, actuators, and connectivity that enables them to connect, communicate, and exchange data. These gadgets can also be remotely monitored and controlled [3].

IoT-enabled smart homes can enhance our quality of life by offering intelligence and comfort. A "smart home" is a house that has been automated with Internet of Things technology so that it can respond to the requirements of its occupants and offer them comfort, safety, security, and entertainment. The three main components of the smart home integration system are as follows: The third unit in the management and control of an integrated smart home system is intelligent information processing (for example, through artificial intelligence algorithms). The physical components (smart sensors and actuators) comprise the first unit, while the communication system (wired or wireless network) typically serves as the link between the physical components [4].

The opportunity to manage a smart home and improve the quality of life for citizens and the environment is being brought about by the integration of IoT technologies. IoT will make it feasible to remotely monitor, access, and operate the objects, gadgets, and sensors that are connected throughout the house at any time and from any location. In a similar situation, a smart house would allow its residents to schedule necessary maintenance, prepare food and coffee, regulate air conditioning systems, monitor for intruders, protect their homes, and control door access. To create a "smart home," smart devices will be automated and everything will be connected. It must be able to transmit, receive, or both to regulate these systems. This ability to transmit and receive data comes from the matters of connecting to the internet and connecting things [5].

For controlling an automation system in a smart home. A home typically has automated infrastructure systems like smart lighting that can be turned on and off, sensors for windows and doors, sophisticated automatic systems that can be programmed, and security systems like biometric locking, video surveillance, authentication, identification, detector devices, and smart multimedia systems. Demonstrating home automation, streamlining energy management, and minimizing environmental emissions are the goals of this smart home research. When evaluating a smart home setting, energy usage, and occupant comfort are important considerations [6].

Three key elements make up the design of an IoT smart home: To manage and control an equipped smart home system, the first entity consists of physical components for sensing and identification (IoT actuators and smart sensors); the second entity is the gateway communication systems (wired/wireless network), which typically connects the first entity and can be classified as either locally or remotely connected. The third entity is intelligent information processing at the end-user level [7].

IoT-based homes must strictly adhere to security standards to safeguard the residents' living spaces, which hold vital and sensitive private information. Using IoT technology to operate a smart home presents security issues. People are empowered by contemporary technology, but there are risks involved as well. As a result, an IoT-based smart home needs to have a high level of security and the right safeguards in place to protect users' data and privacy. Technology opportunities must reduce risks and vulnerabilities and safeguard systems from hackers, attacks, and cybercrime. If smart devices are compromised, the attacker can gain access

to citizens' privacy, take control of the infrastructure, steal citizens' information, or commit cybercrime inside Smart Home systems. For this reason, security and privacy should be properly measured during implementation [8].

Building a workable IoT design that operates a smart house and evaluating IoT security and privacy using an IoT simulator tool have been the main goals of the research work. Cisco Packet Tracer is the appropriate tool for the simulation; its most recent version 7.2, which includes IoT functionalities, enables network topology creation, simulates the configuration and programming of smart devices and sensors, and mimics a contemporary IoT-based smart home [9].

1.1 Statement of the Problem

People will inevitably continue connecting things to the Internet to make life more intelligent, user-friendly, effective, and efficient. In 2050, there will be about 8 billion connected "things" in use (AL MOGBIL, 2020). Developing and developed countries are working to empower their citizens to use IT technologies more effectively by implementing complex modern homes that will improve citizens' quality of life. For example, some houses in cities are well-equipped with fiber connectivity, but some life transitions in some countries reveal that there is a lack of integrating technology in infrastructure. Some life changes reveal that the home's infrastructure does need an integration technology to create a "smart home".

Smart home systems allow the home's owner to operate and monitor things like security systems, door locks, air conditioners, IoT coffee machines, entertainment systems, etc [10]. Some problems related to this integration may arise; attackers may compromise the user's privacy by stealing private information and monitoring the whole building if they manage to penetrate the IoT technology using some advanced tools. It is important to note that a smart home is a prime target for hackers looking to launch security breaches as sensitive or personally identifiable information is easily accessible via the internet.

Things in conventional homes are not monitored, managed, or secure but when connected to the Internet, a smart home is then created. In this research work, we have evaluated the information security and privacy in IoT-based smart homes, seeing the sights of information security threats in IoT connectivity, improved security, and provided some recommendations. We have conducted our findings using simulation by designing a smart home and exploring the capabilities and features of sensors/devices referring to IoT technology.

This research work is divided into the following parts: Chapter One provides the General introduction while Chapter Two provides the literature review. Chapter Three presents the framework and methodology used in this research paper whereas Chapter Four presents simulation environments of IoT structures, tests, and analysis. Chapter five which is the last chapter provides the conclusions and recommendations.

1.2 Objective of Study

i. To examine the effect of IoT sensors/actuators devices on running an IoT smart home.
ii. To establish the effect of IoT network connectivity on running an IoT smart home.
iii. To assess the effect of end-users data processing and manipulation on running an IoT smart home
iv. To examine the effect of Security and privacy having a statistical influence on running an IoT smart home.

2. Related Works

2.1 Introduction

By focusing on their application areas, theoretical academic review, structures, architectures, model creation, conceptual framework, and IoT security ideas, this section mainly aims to provide a general overview of IoT-based smart home environments. Concepts of IoT of Smart Home

IoT will transform how people work and live. There will be a ton of linked devices in smart homes that could make our lives more comfortable, convenient, and easy. A smart home will allow its occupants to manage more tasks using smart application devices and operate their home from anywhere at any time. The potential for Internet of Things (IoT) smart home gadgets is endless, and home automation appears to be the way of the future. Smart house solutions will become increasingly prevalent in increasing residential energy efficiency and convenient, connected living, and smart home technology will be used to give users greater freedom and a higher quality of life [11].

2.2 Application area of Smart Home Automation System

The Internet of Things offers a scalable, adaptable, and user-friendly platform that can support a wide range of applications. Smart homes are one of the many application categories that have emerged with the rise of the Internet of Things. The primary use of SHAS is that it provides us with automated, remotely controlled appliances that operate well. For example Locks, air conditioners, personal safety systems for emergency systems, device detectors, automated heating and cooling systems, security cameras that control and verify who is at your home and keep an eye on the house while you are away, and manageable lighting that dims and turns on and off are just a few examples of the various items that can be equipped with SHAS. Applications for smart homes fall into several categories, including those for security, family care such as eldercare, childcare, healthcare, etc. [12].

2.3 Theoretical academic review

We used the Technology Acceptance Model (TAM) theory and developed a prototype for the IoT-based smart home model that has been carefully scrutinized using the collected data.

TAM theory

An information systems theory called the technology acceptance model (TAM) simulates how people adopt and

utilize new technologies. As change agents, it's a potent tool that may help us understand why people embrace or reject new technology and encourage them to use it [12].

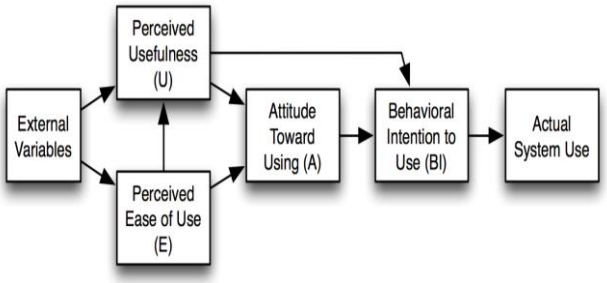


Figure 1: The Technology Acceptance Model

In this paper, we have revised the TAM theory as it focuses on how people use technology in their homes to create a comfortable living environment. By determining what is needed and when, IoT can help you save time, energy, and money. In addition to making your house more comfortable, IoT can make it safer or more secure.

1) The Internet of Things.
The authors in[14] first used the term "Internet of Things" in 2018, and it quickly became widely used to describe physical objects that can connect and share data.

3) The Internet of Everything
The Internet of Everything (IoE) is a process that combines people, information, and objects to increase the value and relevance of networked interactions.

4) The distinctions between IoE and IoT
IoE resides in the intelligent connection, whereas IoT mostly concentrates on physical devices connecting. Network intelligence is utilized to connect all the ideas into a more cohesive system instead of actual items interacting. IoE is regarded as an extension of IoT.

2.4 Enabling Technologies Use in IoT
The Internet of Things, which enables ubiquitous information transmission and content sharing across smart devices with little to no human contact, is a crucial enabler for many applications. To make smart IoT better than current IoT, smart gadgets must have more than just sensors, actuators, and RFID tags. The physical layer should be redesigned from the ground up, followed by the application layer. While the traditional-sense IoT paradigm, which includes the current narrowband IoT (NB-IoT) proposal, aims to provide low-rate, short-range, and relatively stationary connections to the wireless sensors, the new architecture is expected to support higher data rates, longer communication ranges, and more flexible mobility for smart devices with the aid of some new caching, communication, and computing technologies and/or RFID tags. According to Al-Turkistani and AlSa'awi, these also make it possible for smart IoT to be used in a wider range of application areas, such as crowd sensing, crowdsourcing, AR/VR, UAV, etc., to create smarter grid, health, and transportation systems.

2.5 IoT Architecture
Depending on the IoT applications we plan to develop, IoT architecture differs from application to application. The four primary layers of IoT technology are framed by architecture [12].

From a technical perspective and IoT architecture conventional, a home automation system consists of five building blocks:

Devices Under Control
All components, including consumer electronics and household appliances, that are linked to and managed by the home automation system are considered devices under management. A growing number of components (such as Web servers, WLANs, Bluetooth, Z-Wave interfaces, etc.) have built-in features that provide direct access to the control network. To integrate them with the smart home infrastructure, additional components must have adapters installed [12].

2.6 Sensors and Actuators
The home network's eyes and ears are sensors. Sensors can be used for a variety of tasks, including detecting movement or noise and measuring temperature, humidity, light, liquid, and gas. The home network's hands are actuators. These represent the real-world capabilities of the smart network. Electrical motors and pumps are examples of mechanical actuators, while dimmers and electric switches are examples of electronic actuators, depending on the kind of interaction needed. Sensor-equipped IoT devices will function as collectors, while actuator-embedded devices will function as performers. A gadget that has both sensors and actuators will be able to see and do [12].

2.7 Control Networks
On the one hand, the control network connects the controller, sensors, actuators, and devices under control; on the other hand, it also connects remote control devices. Today, there are two primary technological choices for control networks for home and building automation: Systems that are remotely and locally operated [12].

2.8 Controller, Web server, and database
A controller is the computer system that serves as the brain of the automated infrastructure. It uses sensors to collect various data and remote control devices to accept and process commands. Using actuators and communication channels such as a loudspeaker, email, or phone, it responds to various commands or a set of present rules. A web server connects the database to a user interface. Every home device's information and current state are included in the database. Through the web server, a user can remotely access their house and retrieve the device's status data from the database. Every function and communication within the home network is controlled by the microcontroller [12].

2.9 Remote control devices
The widespread use of smartphones and tablets has eliminated the need for specialized automation control

devices which is one of the primary causes of the growing adoption of home automation systems in the domestic market. The home-controlling application can be accessed using remote-controlled devices such as smartphones, tablets, laptops, and PCs. Additionally, speech-based control is now available in various smart homes thanks to advancements in voice recognition technology. As a result, using smartphones as home remote controls enables remote building control using the Internet or a mobile phone network's data feature that is built into smart devices [12].

3. Theory

The model canvas has been strategically used to pre-structure the IoT application model that runs a smart home.

Figure 2: Canvas model for IoT Smart home

3.1 Conceptual Framework of IoT

The conceptual framework of the proposed IoT system is provided below:

Sensors/Devices

First, environmental data is collected by sensors or other equipment. As sensors can be packed together or might be a part of a device that does more than merely sense things, those equipment can be termed as "sensors/devices." The mobile phone, for instance, is a gadget consisting of several sensors (camera, accelerometer, GPS, etc.) and yet, it is more than just a sensor because it is capable of performing various operations and functions [12].

3.2 IoT Connectivity

After data has been collected, it is then transferred to a database or cloud, a gateway is required for this purpose. Depending on how and where the sensors and equipment are connected, there are several types of connections namely cellular, satellite, Wi-Fi, Bluetooth, router/gateway, or directly connected to the Internet [12].

3.3 Data processing

Concept of user interface

The information can then be used by the end-user in human languages that have been interpreted. The user may receive an alert (email, text, notice, etc.) or may have access to an interface that facilitates proactive system monitoring. For example, a customer might need to monitor the video feeds using a web browser or a mobile app. However, it's not always a one-way street. Depending on the IoT application, she may also have the ability to perform some operations that might affect the whole system. According to predetermined protocols, some actions can be automatically performed and triggered [12].

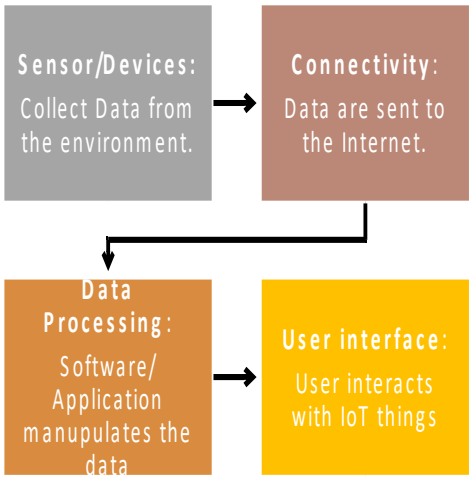


Figure 3: How an IoT system works

3.4 Energy-efficient

Smart home design and development mainly aims at providing energy management as the IoT sensors continuously monitor energy patterns of consumption by other devices in the network, the same operation is applied to those devices themselves as they consume energy too. IoT sensors are equipped with the ability to make some adjustments for optimal usage of the network's devices.

This helps the system to automatically control illumination and HVAC levels as per real-time occupation and environment considerations. Using such technology, IoT users' comfort is improved considerably, while energy is saved substantially. Sustainable living methods will be encouraged and overall energy consumption will be decreased with the use of energy-saving techniques and technologies. Additionally, users will learn more about their consumption habits, which will inform and encourage them to use energy more efficiently.

3.5 Security and privacy issues with IoT systems

This section explains various privacy and security issues related to the protection of a smart home system. It also covers the main ideas outlined in the conceptual framework above, including sensors/devices, connectivity, data processing, and user interface, as well as the architecture and technologies namely controllers and remote controls.

3.6 Security with IoT

To provide security and privacy for the smart home automation system, we use blockchain technology which is used for creating a decentralized ledger holding all the ongoing transactions and communication passing through the interconnected devices, this helps ensure the integrity of the data and that it is protected from unauthorized access. The blockchain then makes sure that each device is authentic and gives it access to the network. These security measures eliminate risks associated with data breaches and unauthorized control of devices, which in turn results in improving overall system security. Ensuring that these security measures are achieved, we therefore create a safe environment where we can manage and share sensitive data as the blockchain's immutability and transparency are achieved [12].

3.7 Energy-saving with IoT devices

Energy management is one of the key aspects being aimed at by the smart home system. IoT sensors will continuously monitor energy patterns of consumption; therefore, data will be available which AI algorithms work through to make some adjustments for optimal usage of the devices. For instance, the system will automatically control illumination and HVAC levels as per real-time occupation and environment considerations. In such a dynamic control, user comfort will be improved significantly, while energy will be saved substantially. The incorporation of energy-saving practices and technologies will help reduce overall energy consumption and promote sustainable living practices. Users will also be enlightened about their usage patterns and thus will be informed and nudged to consume energy with more efficiency [12].

4. Experimental Methodology

In this section, we discuss the methods used to design and implement the proposed IoT framework ie. Rapid Application Development which consists of the following phases: requirements gathering, tool analysis (Cisco Packet Tracer), simulation model development, and, finally, testing, analysis, and feedback. We used Cisco Packet Tracer as the IoT simulator to test and analyze the model running a smart home.

4.1 IoT Actuators in Smart Home

With the use of an IoE cable, IoT actuators can be connected to a Multipoint Control Unit or Session Border Controller board, or they can be connected to a gateway over the network. The smart network can accomplish tasks in the real world thanks to actuators. Electrical motors and pumps are examples of mechanical actuators; electric switches are examples of electronic actuators [12].

4.2 IoT Sensors in Smart Home

Parts of smart gadgets that detect responses to stimuli or the surroundings are called sensors. These devices are based on the smart kits and conduct a single task that can be connected to an MC or SBC board which can subsequently be connected to the network. The home network allows sensors to see and hear. There are sensors for a wide range of applications, such as detecting movement or noise and measuring temperature, humidity, light, liquid, and gas[12].

4.3 Connecting things to IoT home gateway

Logical connectivity or cabling is the process of connecting devices with the proper cables and creating sophisticated network configurations using a command-line interface. It can also be used to link single-boarded computers (SBC-PT) or microcontrollers (MCU-PT) to the home gateway.

Controllable gadgets are necessary for setting up a smart home. These gadgets are made up of every part that is connected to and managed by the home automation system, including consumer electronics and household appliances. For direct communication to the control network, a variety of connecting technologies are used, including WLAN, Bluetooth, Switch port analyzers (SPAN), and an extension of SPAN known as RSPAN [12].

4.4 Prototype Cycle (Pilot)

Once the requirements have been identified, we build out the prototype of the network topology by ensuring that the connectivity between all the networking devices and components is logically set.

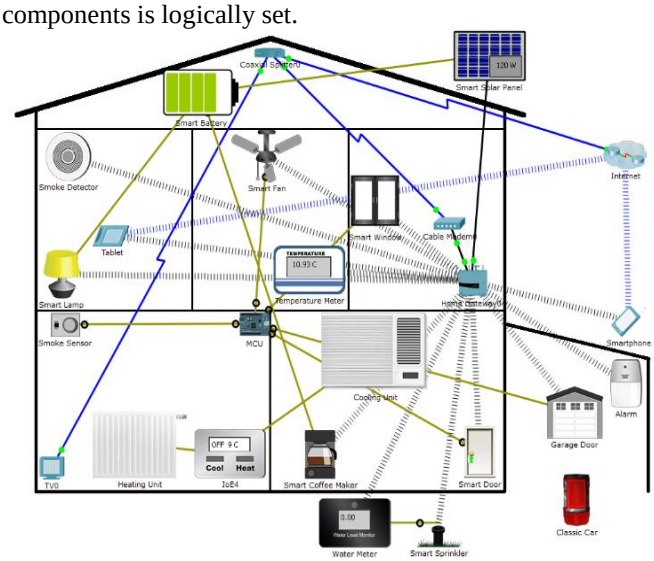


Figure 4: IoT-based Integrated Smart Home Automation System

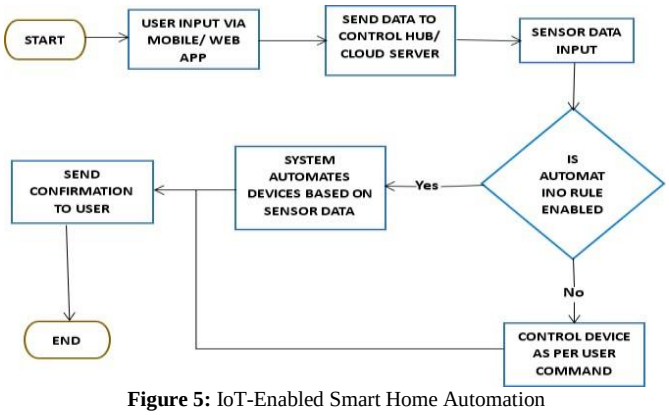


Figure 5: IoT-Enabled Smart Home Automation Workflow

4.5 System Testing & Validation

A thorough testing and validation process is applied to the smart home automation system, ensuring that all criteria and design standards are met. To evaluate the prototype system's dependability, security, energy efficiency, and end-user experience, it is tested in real-world scenarios. Testing can involve evaluating performance in a variety of scenarios, identifying any possible issues, fixing them, and ensuring that every part functions as a whole. During this testing phase, user input is gathered to make necessary adjustments before a full-scale deployment. Subsequently, the most rigorous validation procedures are used to guarantee that the final system is robust, secure, and capable of meeting the given needs.

5 Results and Discussion

5.1 Testing model and analysis findings

This chapter's resolution examined how IoT sensors and devices affected positively smart homes, how connectivity was established, and how data was processed and altered at the end-user level. Through the simulated environment, a model running an IoT smart home was built using the Cisco Packet Tracer. To efficiently break security breaches in smart homes, another approach to IoT security has been evaluated. In the proposed model, we simulated various functions in the smart home using Signal Board Computers SBC-PT, a network access factor, sensors, detectors, and an actuator. Using an IOT-based system, were able to keep an eye on and manage those devices. The home gateway interface of the home automation system connects to portable devices, thus serving as an operator interface, and finally, a summary of the results was provided.

5.2 IoT Smart Home Model Viewpoint

The registration servers are home gateways that control and keep an eye on IoT motions, sensors, actuators, and household items like smart coffee makers, smart lights, smart doors, smart fans, etc., made up of the proposed model framework. As a single central network access component, the microcontroller's network interface (MCU-PT) was used to link the smart objects. And because of the amount of data these sensors produced, an Internet of Things (IoT)-based home automation system was built and connected to a cluster of Internet servers, enabling users to operate their smart devices using gadgets such as tablets, smartphones, or remote controls.

5.3 IoT Smart home System functions

The following are key features of various smart devices that our proposed IoT model consists of. A smoke detector that can detect the environment's variable smoke level, a garage door that can detect car carbon for a garage opener, a smart door that can open, close, unlock, or lock the door, a temperature meter that can monitor and detect the temperature from the environment, a smart coffee maker, a home appliance that can electronically switch devices on/off, a smart fan switch which can turn the fan on/off, set the fan's speed low or high, a smart lamp which can turn on/off, dim, or emit light into the environment, and many more. Those advanced features help house residents manage and keep an eye on interconnected devices inside their homes.

5.4 IoT Smart Home Gateway Layout

Smart gadgets are connected to and registered with a Home Gateway server to provide users with remote home access, programming, and setup. This Home Gateway makes it easier to use wireless router features and gives different local network devices the ability to connect to the Home Gateway router automatically. The Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) authentication process has been used to set it up. It consists of a complex security encryption of words or phrases made up of 8–63 American Standard Code for Information Interchange, or "ASCII" characters.

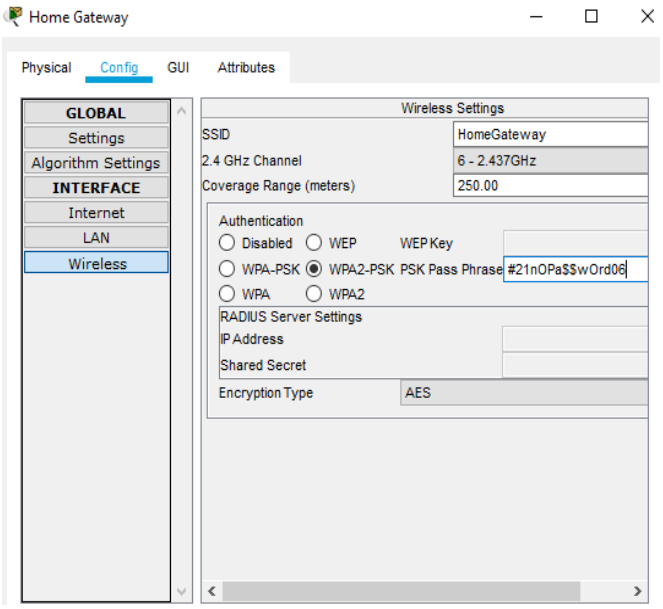


Figure 2: Home Gateway Settings

In Figure 8, for security reasons, the home gateway's password was toughened using a complex passphrase.

Through the use of a cable modem that connects to an external network, the Home Gateway has enabled remote access and built connectivity between the devices inside the Home environment. We have also set up a firewall to separate the internal resources so they can be accessed directly from the outside and ensure that vital security measures are not overlooked.

5.5 IoT Smart Home Network Layout

As seen in Figure 9, the Network was logically partitioned and a Home network was connected to the Internet via the Home Gateway to also allow direct remote access to the internal resources.

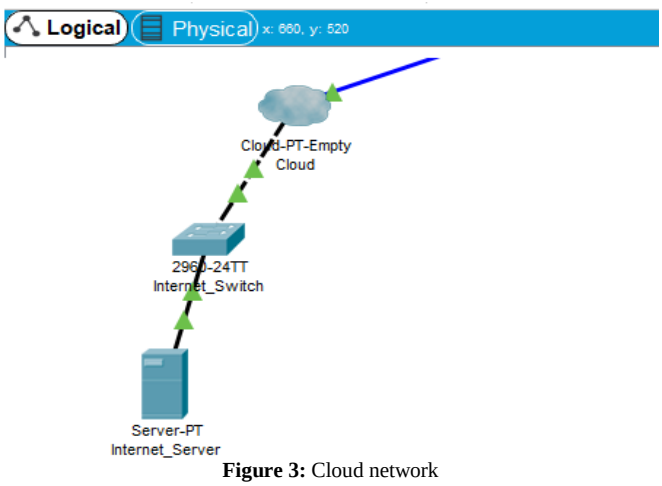


Figure 3: Cloud network

Figure 10 depicts the situation in which through the Internet connection, the server's network settings were set up to link the coaxial cable from the home LAN network to the Ethernet, and the DHCP services were used to establish communication via an external interface.

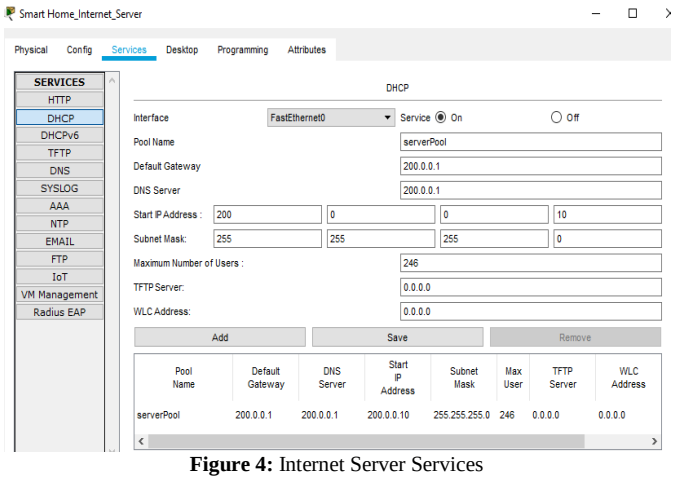


Figure 4: Internet Server Services

5.6 IoT Smart Home Sensors and Actuator Devices

As seen in Figure 11, throughout the simulation time, IoT client devices and servers were connected to the same Local Area Network, and IoT logic connectivity was established resulting in IoT devices being accessible by the home server gateway.

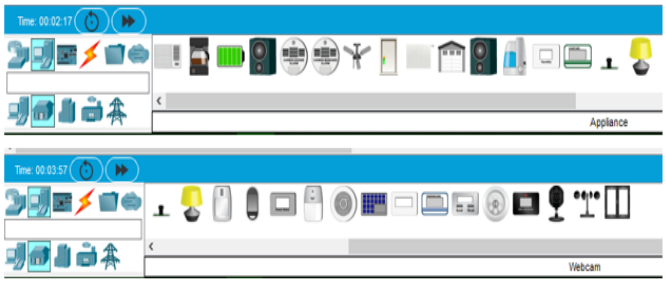


Figure 5: IoT Logic Connectivity

Figure 10 depicts various IoT Actuators and Sensors used throughout the simulation time.

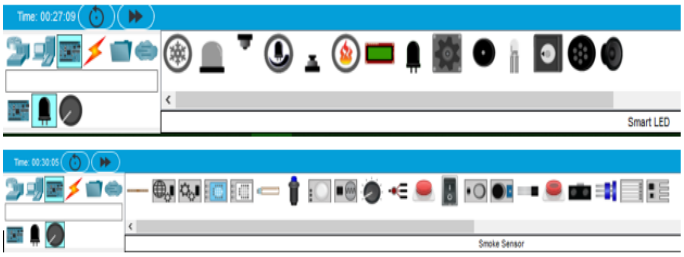


Figure 6: IoT Actuators and Sensors

5.7 IoT programming components

In Figure 13, the simulation mimics programming using JavaScript and Python languages to create centralized connectivity of the smart objects. The input from IoT sensors, actuators, and detectors is connected to an MCU packet tracer using an IoT custom cable.

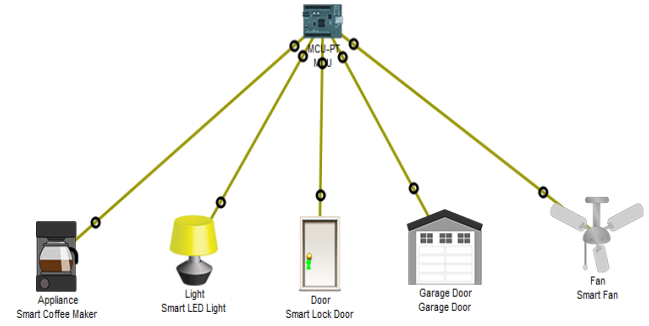


Figure 7: Appliance, sensors, actuators, and sensors in Smart Home

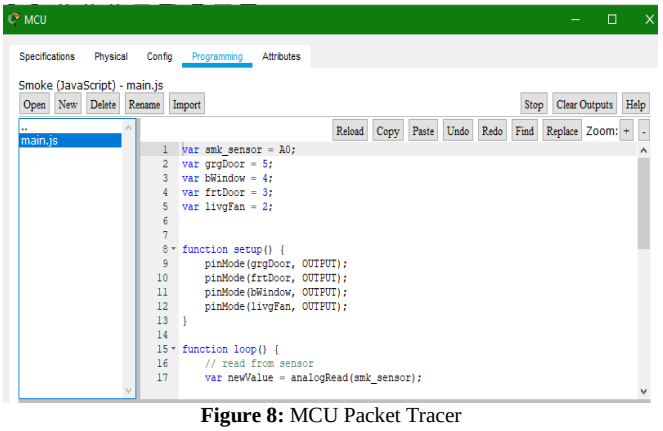


Figure 8: MCU Packet Tracer

An Internet of Things programming editor is part of the Home Gateway online interface (Figure 14). The MCU-PT microcontroller may be programmed using Python and Javascript. The web interface is used to write the code before it is published to the MCU board. The LED connected to the digital0 port blinks when the sample code below is run.

5.7 Testing the model of IoT smart home

As seen in Figure 15 all of the devices were added to Home Gateway using an authenticator so that the IoT server could locate them, allowing us to remotely control the devices' mechanisms via the browser or an IoT monitor. The IoT monitoring platform presented information on all linked

smart devices, such as sensors, detectors, and actuators. When you log into the console, you may see their current condition, which is ON/OFF, open/lock, low/high, or dim. The sensors and actuators listed below were used in this dissertation lab to stimulate reactions, including a ceiling fan, home gateway, garage door, smart door, and home appliances such as a smart lamp, smart coffee maker, temperature monitor, smoke detector, and smart solar panel connected wirelessly to the home gateway.

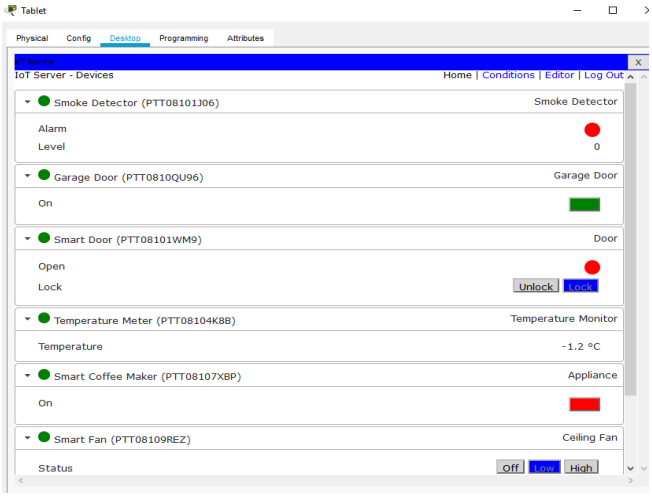


Figure 9: IoT Home Page Monitoring

Testing the connectivity

As you can see in Figure 16, through remote-control devices such as smartphones, tablets, laptops, and PCs, we were able to test the connectivity from the end-user application and the lab network environment.

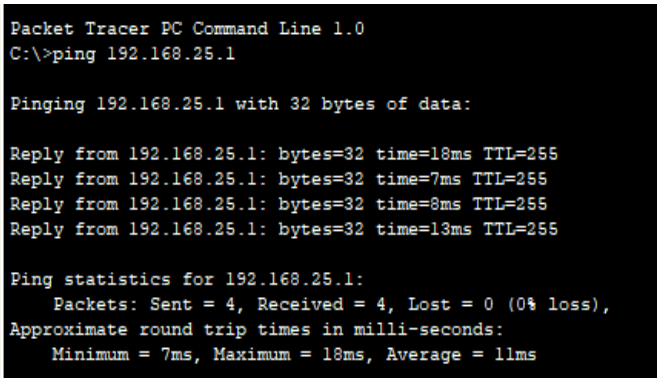


Figure 10: Packet tracer, pinging results

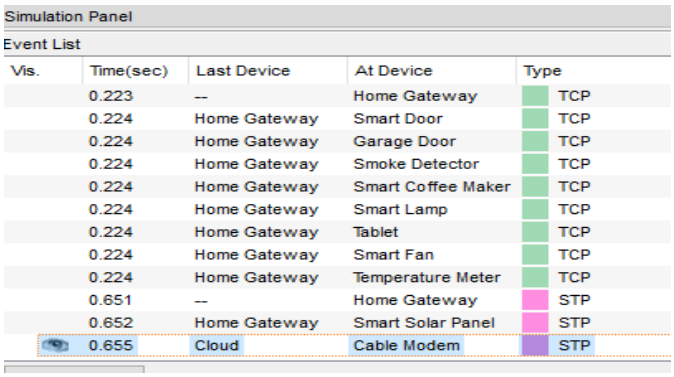


Figure 11: Connection Outputs

Figure 17 revealed that the connection results in no packet loss (0%), this means that the connection was successfully established from the internal LAN network to external networks.

5.8 Analysis

Based on the simulation results and the study's objectives, we concluded that smart things such as sensors, detectors, and actuators play an important role in the creation of a smart home, connectivity among devices within the network infrastructure has a significant impact on the operation of a smart home, and human intervention is required to manipulate and control the data generated by smart things.

5.9 Results

1. Energy Efficiency Enhancement (EEE):
Smart home automation systems revealed that energy waste could be drastically reduced by monitoring and fine-tuning equipment such as lighting and HVAC while they were in operation. This environmentally friendly element improves sustainability at an optimal level while incurring higher expenditures. Energy must be used only when necessary.

2. Increased Safety (IS):
AI guards and motion sensors with AI can provide additional security features to homes by identifying and alerting homeowners in real-time when there is a potential threat. The fact that this system can warn the homeowner of such suspicious activities 95% of the time suggests that it has some strong protection built into its levels of tranquility and proactive security management.

3. Faster Data Processing Time (FDPT):
Smart homes' innovative edge computing technology can provide results up to 40% faster and respond faster to user commands, allowing for ideal real-time automation of lighting, temperature, and other household services.

4. User Customization and Control (UCC):
A convenient mobile app made it simple for homeowners to customize their home automation experience. More than 80% thought the app was simple enough to set up personalized routines and get additional control over home appliances, lighting, and temperatures.

5. AI Predictive Automation (APA):
The smart home system's AI capabilities automate common chores by predicting user behavior, reducing the need for human intervention. It demonstrated how the deployment of AI skills increased customer satisfaction by 20%, as homeowners could perceive that it anticipated their needs and simplified home administration.

6. Common User Experience (CUE):
The smart home system delivered a comprehensive experience that improved energy efficiency, security, data processing speed, customization, and AI-based automation

throughout. Finally, this resulted in comfort, efficiency, and security in living on one's terms.

Table 1: Summary of Enhancements in Percentage provided by the Smart Home Automation

EEE	IS	FDPT	UCC	APA	CUE
18%	23%	17.8%	30%	35%	43.2%

6. Conclusion, Recommendation, and Future Work

6.1 Conclusion

The main objective of this research work was to make known the topic of the Internet of Things (IoT) and its application area by creating a smart home simulation, to provide an outlook of components that make smart home intelligence, comfortable and to improve the quality of life of end-users (citizens). Integrating IoT technology into the results of our home is a new security challenge, therefore IoT-based smart homes require very stringent security have been advisory taken into consideration to put in place appropriate measures and a vigilant assessment of security risks must precede any security to make the home-based more secure, appropriate and relaxed live in.

6.2 Recommendation and Future Works

Based on our findings, we would recommend the following to future researchers:

1. Autonomous Smart Home:
As AI technology advances, future smart houses will be able to function autonomously with minimum human intervention. The next level of development will be to create residences that can automatically configure their lighting, temperature, security, and energy usage using real-time data and predictive algorithms.

2. Greater In-Situ Incubation of More Sophisticated AI and ML Models:
Advanced smart homes could be powered by more advanced AI and machine learning models capable of learning and gathering data from a wider range of user behavior and environmental factors. Such models may improve the prediction and automation of more complex processes, resulting in more personalized and intuitive user experiences.

3. Improved Security:
Future generations of smart home systems will incorporate more complex anomaly detection algorithms capable of sending out clearer signals to identify threats and respond faster. Facial recognition and other biometric security solutions have the potential to dramatically improve home security by reducing false alarms and unauthorized access.

4. Scalability to Large Settings:
Smart home automation's scalability will increase dramatically with larger homes or even workplace space. In the future, performance will be efficient and responsive across multiple devices, larger environments, and diverse user requirements.

5. Integration with Emerging Technologies:
As the Internet of Things (IoT) evolves, more work is required to integrate smart homes with emerging technologies such as 5G, blockchain for secure data transfers, and augmented reality (AR) for an immersive control experience. This would enable significantly more dynamic, secure, and engaging home automation experiences.

6. Sustainability Goals:
Future research will continue to focus on improving energy efficiency. As environmental concerns grow, more research will be performed to develop smart homes that can help achieve global sustainability goals by optimizing renewable energy consumption and reducing carbon footprints.

7. User Behavior Analytics:
The system might grow to be far more sophisticated for analytics purposes, supplying users with data on their daily routines, energy consumption, and other things. Such analytics can be used to give homeowners personalized recommendations on how to save energy or increase home security.

Contribution to Knowledge: This study makes significant contributions the smart home automation by addressing the limitations of traditional home buildings by providing a modern smart home automation solution, uniquely combined with AI, blockchain, and IoT, addresses all the security, privacy, and energy management challenges**.**

Conflict of Interest

This unique replica is not being considered for publishing anywhere and has not been disseminated. There are no conflicts of interest to declare as a result.

Funding Source: There was no external funding for this study.

Authors' Contributions

Each author made an equal contribution to this research dissertation. They all looked over and verified the original manuscript's final draft.

Acknowledgments

We praise God and offer him all the glory. We also thank our families, the entire staff of the Department of Management and Information Technology, UTB, and for their encouragement in making our study a success**.**

References

[1] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, & S. Elkhediri, "CyberSecurity: a review of Internet of things (IoT) security issues, challenges, and techniques", *In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS),* pp. **1-6, 2019.**

[2] M. Al-Enazi & S. El Khediri, "Advanced Classification Techniques for Improving Networks' Intrusion Detection System Efficiency", *Journal of Applied Security Research*, pp. **1-17., 2021.**

[3] A.K. Ray & A. Bagwari, "Study of smart home communication protocols and security & privacy aspects", *In 2017 7th International Conference on Communication Systems and Network Technologies (CSNT)*, pp. **240-245, 2017.**

[4] M. Sultan & K. Nabil, "Smart to smarter: smart home systems history future and challenges", *In The 34th Annual ACM Conference on Human Factors in Computing Systems, Future of Human-Building Interaction Workshop*, **2020.**

[5] Y. Mittal, P. Toshniwal, S. Sharma, D. Singhal, R. Gupta & VK. Mittal, "A voice-controlled multi-functional smart home automation system", *In 2015 Annual IEEE India Conference (INDICON)*, pp. **1-6, 2015.**

[6] Alohali, B., Merabti, M., & Kifayat, K. (2014, September). A cloud of things (cot) based security for home area network (han) in the smart grid. In 2014 eighth international conference on next-generation mobile apps, services, and technologies (pp. 326-330). IEEE.

[7] A.S. Al-Qahtani & M.A. Khan, "Predicting Internet of Things (IoT) Security and Privacy Risks–A Proposal Model", **2021.**

[8] K. Karimi, K., & S. Krit, "Smart home-smartphone systems: Threats, security requirements and open research challenges", *In 2019 International Conference of Computer Science and Renewable Energies (ICCSRE)*, pp. **1-5, 2019.**

[9] R. AL MOGBIL, M. AL ASQAH & S. EL KHEDIRI, "IoT: Security challenges and issues of smart homes/cities", *In 2020 International Conference on Computing and Information Technology (ICCIT-1441)*, pp. **1-6, 2020.**

[10] Y. Wen, & T. Liu,"|WIFI Security Certification through Device Information", *In 2018 International Conference on Sensor Networks and Signal Processing (SNSP)*, pp. **302-305, 2018.**

[11] J. A. Al-Fahdi1, H. Fadhil Al-Yahyaai2, B. Rashid Al-Rashdi & Annamalai. "Muthu4Smart Home Automation Based On Bluetooth with IR Receiver", " *International Journal of Scientific Research in Computer Science and Engineering*, Vol. **11,** Issue. **4,** pp. **1-7, 2023.**

[12] F. Aziz, S. Kumar, "Preventing Salmonella: Integrating Data Analytics With Electronic Health Records In Smart Cities," *International Journal of Scientific Research in Multidisciplinary Studies*, Vol.**10,** Issue. **5**, pp.**1-10, 2025.**

AUTHORS PROFILE

Dr. GATETE Marcel received a Doctor of Philosophy degree in Computer Science and Applications from Periyar Maniammai University in India between 2012 and 2018. In 2010–2011, he received a Master of Philosophy (MPhil) in Computer Science from PRIST University in India. He received a Master of Science in Information Technology from Bharathidasan University in India between 2008 and 2010. He received a Bachelor of Science in Computer Science and Engineering from the Institut Superieur Pedagogique de Gitwe in Rwanda between 2002 and 2006. He has been employed at the University of Tourism, Technology, and Business Studies in Kigali, Rwanda, since 2021 as a Senior Lecturer in the Department of Business and Information Technology. Computer programming and mobile ad hoc networking are areas of interest.

HARUBWIRA Flaubert received a Bachelor of Science in Computer Science and Engineering from Institut Superieur Pedagogique de Gitwe in Rwanda from 2003 to 2007, a Master of Science in Banking and Insurance Management from Annamalai University in India from 2012 to 2013, and a Master of Science in Information Technology from Bharathidasan University in India from 2011 to 2013. He is now the Deputy Vice-Chancellor of the University of Tourism, Technology, and Business Studies in Kigali, Rwanda, where he has been since 2021. The area of interest is networking.

