University of Mohamed Khider Biskra

Faculty of Sciences and Technology
Department of Electrical Engineering

MASTER'SDEGREE

Sciences and Technology

Field: Telecommunication

Option: Network and Telecommunication

Ref:.....

Presented and submitted by:

GASMI Safa

On:04 June2025

Smart Home IOT based solution

Jury:

M. Abdesselam SALIM	MCB	University of Biskra	President
M. BOUKREDINE Salaheddine	MAA	University of Biskra	Examiner
M. AMEID Sofiane	MAA	University of Biskra	Supervisor

AcademicYear:2024–2025

University of Mohamed Khider Biskra
Faculty of Sciences and Technology
Department of Electrical Engineering

MASTER'SDEGREE

Sciences et Technologies

Field: Telecommunication

Option: Network and Telecommunication

Theme:
Smart Home IOT based solution

Presented by:
GASMI SAFA

Favorable opinion of the supervisor:
Mr.AMEID Sofiane

On: 04June 2025

Favorable opinion of the Jury President:

M. Abdesselam SALIM

Stamp and signature

Abstract

This study and project explore the development of innovative solutions based on Internet of Things (IoT) technologies for use in smart home environments. The proposed approach involves connecting various household devices through a centralized system that enables real-time monitoring and remote control, with a focus on improving energy efficiency and enhancing residential security. The system integrates a suite of sensors (such as lighting sensors, surveillance cameras, motion detectors, ambient temperature sensors, and wind speed sensors) to monitor indoor and outdoor environmental conditions.

The prototype was implemented using the Cisco Packet Tracer simulation environment to replicate realistic scenarios, including fluctuations in temperature and wind speed. This allowed testing of the system's responsiveness, reliability, and ability to detect incidents and automatically adapt operations (e.g., closing smart windows during strong winds or adjusting indoor temperature based on external conditions). Results demonstrated the system's ability to effectively integrate devices, significantly reduce energy consumption, and enhance comfort and safety.

Keywords:
Smart Home, Internet of Things (IoT), Home Automation, Remote Control, Energy Efficiency, Residential Security, Packet Tracer Simulation, Home Gateway, Sensor Integration, Real-Time Monitoring, Ambient Temperature, Wind Speed.

Résume

Cette étude et projet explore le développement de solutions innovantes basées sur les technologies de l'Internet des Objets (IoT) pour une utilisation dans les environnements de maisons intelligentes. L'approche proposée consiste à connecter divers appareils domestiques via un système centralisé permettant une surveillance en temps réel et un contrôle à distance, en mettant l'accent sur l'amélioration de l'efficacité énergétique et la sécurité résidentielle. Le système intègre un ensemble de capteurs (tels que des capteurs d'éclairage, des caméras de surveillance, des détecteurs de mouvement, des capteurs de température ambiante et des capteurs de vitesse du vent) pour surveiller les conditions environnementales intérieures et extérieures.

Le prototype a été mis en œuvre en utilisant l'environnement de simulation Cisco Packet Tracer pour reproduire des scénarios réalistes, incluant des variations de température et de

vitesse du vent. Cela a permis de tester la réactivité du système, sa fiabilité, et sa capacité à détecter des

incidents et à adapter automatiquement les opérations (par exemple, fermer les fenêtres intelligentes lors de vents forts ou ajuster la température intérieure en fonction des conditions extérieures). Les résultats ont démontré la capacité du système à intégrer efficacement les appareils, réduire significativement la consommation d'énergie, et améliorer le confort et la sécurité.

Mots-clés :
Maison Intelligente, Internet des Objets (IoT), Domotique, Contrôle à Distance, Efficacité Énergétique, Sécurité Résidentielle, Simulation Packet Tracer, Passerelle Domestique, Intégration de Capteurs, Surveillance en Temps Réel, Température Ambiante, Vitesse du Vent.

الملخص

ستكشف هذه الدراسة والموضوع تطوير حلول مبتكرة تعتمد على تقنيات إنترنت الأشياء (IoT) لاستخدامها في بيئات المنازل الذكية. يتمثل النهج المقترح في ربط مختلف الأجهزة المنزلية عبر نظام مركزي يتيح المراقبة اللحظية والتحكم عن بُعد، مع التركيز على تحسين كفاءة الطاقة وتعزيز الأمان السكني. اشتمل النظام على تكامل مجموعة من أجهزة الاستشعار (مثل أجهزة استشعار الإضاءة، وكاميرات المراقبة، وكاشفات الحركة، وأجهزة قياس درجة الحرارة المحيطة، ومستشعرات سرعة الرياح) لمراقبة الظروف البيئية الداخلية والخارجية.

تم تنفيذ النموذج الأولي باستخدام بيئة محاكاة **Cisco Packet Tracer** لمحاكاة سيناريوهات واقعية تشمل تقلبات درجة الحرارة وسرعة الرياح، وذلك لاختبار استجابة النظام وموثوقيته في الكشف عن الحوادث وتكييف العمليات تلقائيًا (مثل إغلاق النوافذ الذكية عند هبوب رياح قوية أو ضبط درجة الحرارة الداخلية وفقًا للظروف الخارجية). أظهرت النتائج قدرة النظام على تحقيق التكامل الفعّال بين الأجهزة، وتحسين استهلاك الطاقة بنسبة ملحوظة، بالإضافة إلى تعزيز الراحة والأمان.

الكلمات المفتاحية:

المنزل الذكي، إنترنت الأشياء(IoT) ، الأتمتة المنزلية، التحكم عن بُعد، كفاءة الطاقة، الأمان السكني، محاكاة Packet Tracer، بوابة المنزل، تكامل المستشعرات، المراقبة اللحظية، درجة الحرارة المحيطة، سرعة الرياح

.

Dedication

In conclusion, all praise is due to Allah, Lord of the Worlds.
Praise be to Him at the beginning and praise be to Him at the end.

This journey has been long and transformative, marked by moments of failure that shaped me and successes that inspired me. Today, I stand proud of what I have achieved — the realization of a dream that has accompanied me for years.

It is a moment I have long awaited — the closing chapter of a story written with emotion, effort, and perseverance.

I extend my deepest gratitude:
To those who surrounded me with love, and who supported me with unwavering care, To those who stood by me through every stage of life,
To my honorable father — for his sacrifices, guidance, and the selfless lessons in giving.
May Allah prolong his life and preserve him as a source of pride.
To my beloved mother — the heartbeat of my soul, whose prayers were a silent pillar of strength. May Allah protect and bless her.
To my dear siblings — companions of my upbringing and a constant source of encouragement and joy,
To all who supported and motivated me — whether near or far,
To the friends who accompanied me on this journey — each of whom holds a unique and cherished place in my heart,
To my grandmother, my aunts, my cousins, my maternal aunts and uncles — for their kindness and encouragement,
To those who have passed on, whose words still resonate within us, strengthening and uplifting our spirits,
To every teacher who shared knowledge with me throughout my academic journey, To the innocent souls lost unjustly in lands deprived of peace,
To the martyrs of truth, in a homeland worn down by sorrow,
And to myself — for holding onto hope, trusting in patience, and persevering until the goal was achieved.

Though the road ahead remains long, today I pause to express my sincere appreciation.
I dedicate this humble achievement to everyone who holds a place in my heart, even if this page could not contain all your names.

With heartfelt gratitude and deep respect —

May Allah reward you all generously on my behalf.

Acknowledgments

In the name of Allah, the Most Gracious, the Most Merciful,

All praise is due to Allah alone, the Lord of the worlds, who granted me the strength and patience to complete this work.

I extend my sincere thanks and deep gratitude to my supervising, Mr. AMEID Sofiane, for the effort he exerted and the guidance and advice he provided throughout the course of this work. His continuous support and encouragement had a great impact in helping me overcome difficulties and achieve this accomplishment.

I would also like to express my heartfelt thanks to all my esteemed professors and the members of the committee for the knowledge and expertise they shared, and for their tireless efforts in educating and guiding us throughout our university years.

I must also extend special thanks and appreciation to my dear sister Ms FORTAS Amira, who never hesitated to offer me her help and support whether through advice, participation, or simply standing by my side throughout the different stages of this project. You have my deepest appreciation and gratitude.

Table of Content

LIST of FIGURES

List of Tables

List of Abbreviations

IoT: Internet of Things

ICT: Information and communication technologies

TIA/EIA: Telecommunications industry association/electronic industries alliance

COM port : Communication port

AP : Access point

MCU: Microcontroller

SBC: Single boarded computers

LED: Light emitting diode

AC: Air conditioning

ISP: Internet service provider

DHCP: Dynamic host configuration protocol

HVAC: heating ventilation and air conditioning

RAM: Random access memory

CO: Coaxial

WAN: Wide Area Network

CLI: Command Line Interface

Co: Central Office

PT: Packet Tracer

QoS: Quality of service

IT: Information Technology

HTTPS: Hypertext transfer protocol secure

SSID: Service set identifier

WPA2-PSK : wi-fi protected access 2-pre-shred

NIC: network interface card

AAA: Authentication authorization and account

IP: Internet protocol

CAN: controller area network

PSTN: public switched telephone network

LTE: long-term evolution

DSL digital subscriber lines

FCAPS: Fault, Configuration, Accounting, Performance Security

CoAP: Constrained Application Protocol

MQTT: Message Query Telemetry Transport

IEEE: Institute of Electrical and Electronics Engineers

UDP: User datagram Protocol

TCP: Transmission Control protocol

P2P: Peer to peer

HTTP: Hypertext Transfer Protocol

HAM: Home appliance management

ESD: Emergency shutdown

RFID: Radio frequency identification

ID: Identification

HI: Home Intelligence

AI: Artificial intelligence

DNS: Domain Name System

ATM: Asynchronous transfer mode

EMI: Electromagnetic interference

LAN: Local area network

RF: Radio frequency

BLE: Bluetooth low energy

API: Application Programming Interface

OSI: Open systems interconnection

TV: Television

GENERAL INTRODUCTION

The twenty-first century has witnessed an unprecedented acceleration in digital transformation, driven by the growing integration of key technologies that have reshaped the global information and societal infrastructure. Rapid advancements in communication networks, cloud computing, and artificial intelligence have led to the emergence of interconnected digital systems characterized by real-time interaction, intelligent data processing, and autonomous adaptation to environmental changes.

Within this context, the concept of Cyber Physical Systems has emerged as a theoretical and practical framework for integrating digital infrastructure with physical components. This framework has facilitated the development of advanced applications across various domains, including smart cities, automated industrial facilities, connected healthcare systems, and smart homes. The Internet of Things (IoT) serves as the foundational layer of these systems, providing an integrated environment that relies on distributed sensors, embedded controllers, and high- performance communication networks that enable real-time data exchange and autonomous control.

Despite the broad potential of smart home technologies, their practical implementation faces a number of technical and operational challenges. These include limited interoperability among devices from different manufacturers, inadequate energy efficiency due to the absence of adaptive control mechanisms, and security vulnerabilities arising from network interruptions or cyber threats. Furthermore, the complexity of managing a large number of IoT devices in real time presents a barrier to widespread adoption, particularly in the absence of unified, centralized systems that allow full control and remote access. This project aims to address these challenges by designing a smart home-based solution that integrates IoT devices through a unified Home Gateway connected to a centralized IoT server, enabling centralized management and remote accessibility.

Based on this general context, Chapter One of this project examines the fundamental principles of IoT, including its architectural components, communication protocols, and enabling technologies. Chapter Two focuses on smart homes as one of the key applications of IoT, analyzing their structure, core functionalities, and possible use-case scenarios, in addition to defining the simulation environment in Which the system will be tested. Chapter Three presents the practical implementation of the smart home system using Packet Tracer simulation software, with the aim of translating theoretical concepts into a working model and analyzing system behavior within a controlled virtual environment.

I Chapter One

IOT Ecosystem: history and application

I.1 Introduction

Our world has evolved dramatically from manual processes to digital systems, fundamentally changing how we work and live. The emergence of computers transformed data management and operational efficiency across industries, reducing human error and accelerating task completion. The internet revolution followed, connecting previously isolated digital systems and enabling unprecedented information exchange. This global connectivity created new opportunities for collaboration, commerce, and communication that transcended geographical boundaries. Taking this evolution a step further, the rise of the Internet of Things (IoT) represents the next significant technological leap.

By embedding sensors and connectivity into everyday objects, IoT extends digital intelligence into the physical world. From smart homes—where lighting, heating, and security systems coordinate automatically to industrial environments where machines predict and prevent breakdowns, IoT is creating responsive, intelligent systems that adapt to our needs in real time. In this chapter, we will explore the Internet of Things (IoT) in depth examining its history, precise definition, key components, how it functions, its impact across various sectors, as well as its advantages and potential drawbacks.

I.2 Definition Internet of things

From the perspective of technical standardization, the IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT) [1].

Internet of things or internet of everything refers to the idea of things (object)that are readable, recognizable, locatable, addressable through information sensing devices (sensor) and controllable via the internet. Things are physical objects with unique identifiers that are able to transfer data over the network. Examples of physical objects include vehicles, smart phones, home appliances, toys, cameras, medical instruments and industrial systems, animals, people, buildings, etc [2].

The Internet of Things is a new revolutionary and advanced technology where any object becomes a smart object, and where they can communicate information about themselves without human intervention. The Internet of Things is expected to make a huge change in our lives it will help us to perform our tasks and duties in a better way.

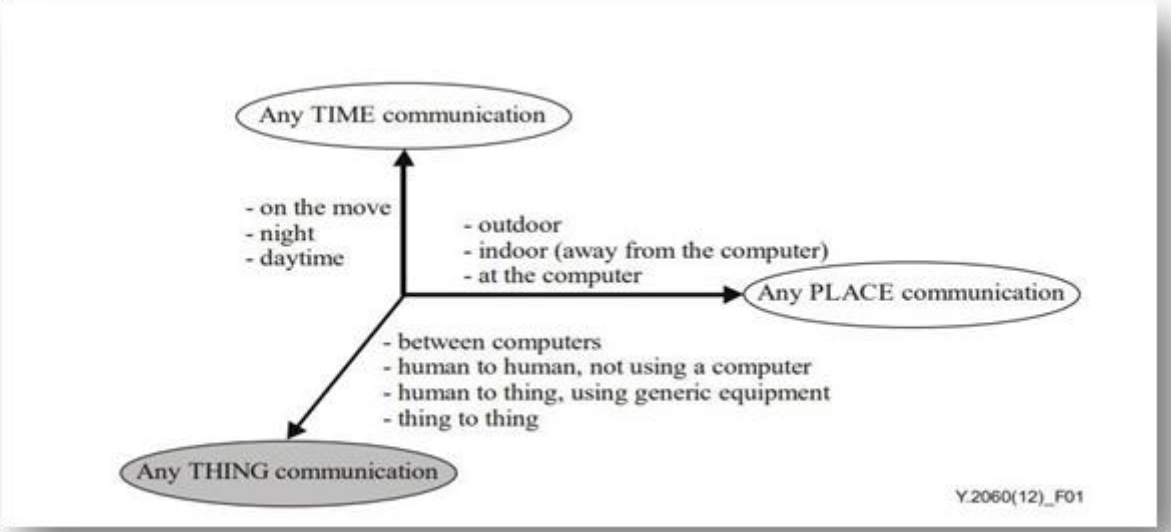


*Figure I-1:*The new dimension introduced in the Internet of things [b-ITU Report] [1].

As shown in figure, the IoT adds the dimension "Any THING communication" to the information and communication technologies (ICTs) which already provide "any TIME" and "any PLACE "communication [3].

I.3 History and Evolution of Iot

The emergence of IoT is widely recognized to have occurred between 2008 and 2009, when the number of internet-connected devices surpassed the global human population marking the beginning of a new technological era. The term ″Internet of Things″ was first introduced in 1999 by Kevin Ashton, who used it while working at Procter & Gamble to describe a concept of integrating the company's supply chain with the Internet.

Ashton later elaborated on the concept, explaining that IoT effectively adds "senses" to computers. Unlike in the twentieth century, when computers relied entirely on human input for data, IoT enables machines to gather information from the physical world independently through sensors. This shift represents a fundamental transformation in computing and data interaction. Today, IoT is regarded as a significant technological milestone with broad implications, raising questions about its scale, role, and importance in the continuing evolution of the Internet [4].

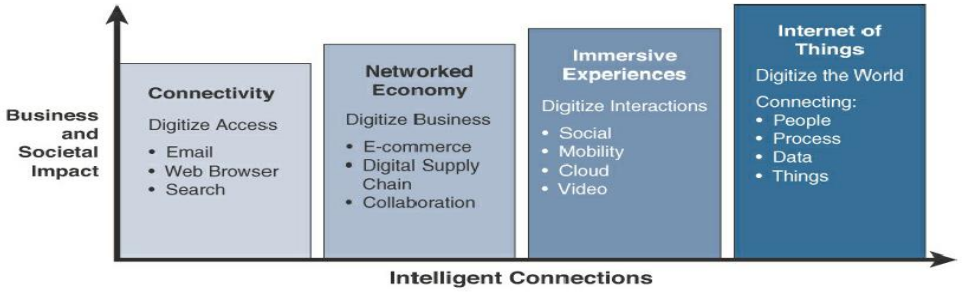


Figure I-2:Evolutionary Phases of the Internet (cisco) [4].

Figure shows the evolution of the Internet can be categorized into four phases. Each of these phases has had a profound impact on our society and our lives.

The **first phase**, Connectivity, emerged in the mid-1990s. At that time, internet access was limited primarily to universities and corporations, with the general public relying on dial-up connections. While access gradually expanded and improved, the focus eventually shifted from basic connectivity to how that connectivity could be leveraged.

This shift marked the **second phase**, known as the Networked Economy. It was defined by the rise of e-commerce and digitally integrated supply chains. Businesses became more interconnected, enabling streamlined operations and widespread online shopping, which significantly disrupted traditional brick and mortar retail models.

The **third phase**, Immersive Experiences, brought about the growth of social media, collaboration tools, and the proliferation of mobile devices. Connectivity became ubiquitous across platforms phones, tablets, and computers enabling seamless communication and person-to-person interaction through various digital channels.

Currently, we are entering the **fourth phase**, the Internet of Things (IoT). Despite extensive attention, IoT is still in its early stages, with the vast majority of physical objects yet to be connected. This phase is characterized by machines and objects communicating with one another and with humans, generating vast amounts of data and enabling new levels of automation, insight, and efficiency. As this phase develops, IoT is expected to drive transformative changes across industries and daily life, much like the previous phases of internet evolution.

I.4 Fundamental characteristics

The fundamental characteristics of the IoT are as follows [1]:

- **Interconnectivity:** With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

- **Things-related services:** The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing- related services within the constraints of things, both the technologies in physical world and information world will change.

- **Heterogeneity**: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

- **Dynamic changes:** The state of devices changes dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

- **Enormous scale**: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

I.5 IoT reference model

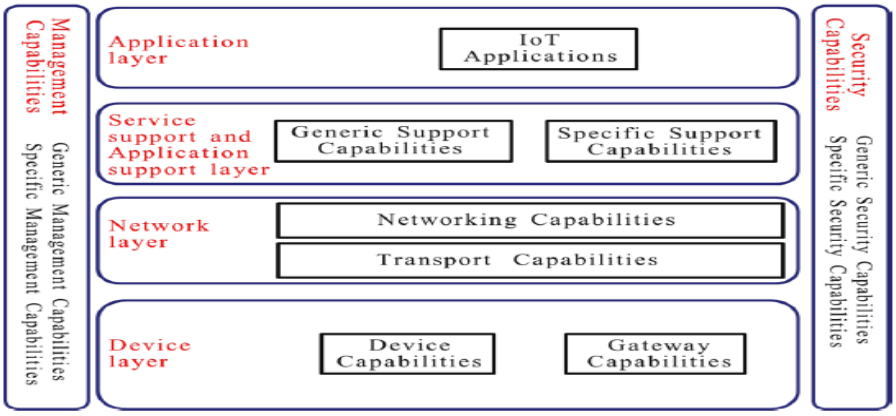


Figure I-3:IoT reference model [1] .

The figure shows the IoT reference model. It is composed of four layers as well as management capabilities and security capabilities which are associated with the four layers.

The four layers are as follows [1]:

– application layer

– service support and application support layer

– network layer

– device layer.

I.5.1 Application layer

The application layer contains IoT applications.

I.5.2 Service support and application support layer

The service support and application support layer consist of the following two capability groupings:

- **Generic support capabilities**

The generic support capabilities are common capabilities which can be used by different IoT applications, such as data processing or data storage. These capabilities may be also invoked by specific support capabilities, e.g., to build other specific support capabilities.

- **Specific support capabilities**

The specific support capabilities are particular capabilities which cater for the requirements of diversified applications. In fact, they may consist of various detailed capability groupings, in order to

provide different support functions to different IoT applications.

I.5.3 Network layer

This consists of the following two types of capabilities:

- **Networking capabilities**

Provide relevant control functions of network connectivity, such as access and transport resource control functions, mobility management or authentication, authorization and accounting (AAA).

- **Transport capabilities**

focus on providing connectivity for the transport of IoT service and application specific data information, as well as the transport of IoT- related control and management information.

I.5.4 Device layer

The device capabilities include but are not limited to:

Direct interaction with the communication network: Devices are able to gather and upload information directly (i.e., without using gateway capabilities) to the communication network and can directly receive information (e.g., commands) from the communication network.

Indirect interaction with the communication network: Devices are able to gather and upload information to the communication network indirectly, i.e., through gateway capabilities. On the other side, devices can indirectly receive information (e.g., commands) from the communication network.

Ad-hoc networking: Devices may be able to construct networks in an ad-hoc manner in some scenarios which need increased scalability and quick deployment.

Sleeping and waking-up: Device capabilities may support "sleeping" and "waking-up ‘‘mechanisms to save energy. Network and indirect interaction with the communication network is not mandatory.

- **Gateway capabilities**

The gateway capabilities include but are not limited to:

Multiple interfaces support: At the device layer, the gateway capabilities support devices connected through different kinds of wired or wireless technologies, such as a controller area network (CAN) bus, ZigBee, Bluetooth or Wi-Fi. At the network layer, the gateway capabilities may communicate through various technologies, such as the public switched

telephone network (PSTN), second generation or third generation (2G or 3G) networks, long-term evolution networks (LTE), Ethernet or digital subscriber lines (DSL).

Protocol conversion: There are two situations where gateway capabilities are needed. One situation is when communications at the device layer use different device layer protocols., ZigBee technology protocols and Bluetooth technology protocols, the other one is when communications involving both the device layer and network layer use different protocols e.g., a ZigBee technology protocol at the device layer and a 3G technology protocol at the network layer.

I.5.5 Management capabilities

In a similar way to traditional communication networks, IoT management capabilities cover the traditional fault, configuration, accounting, performance and security (FCAPS) classes, i.e., fault management, configuration management, accounting management, performance management and security management.

The IoT management capabilities can be categorized into generic management capabilities and specific management capabilities. Essential generic management capabilities in the IoT include:

– device management, such as remote device activation and de-activation, diagnostics, firmware and/or software updating, device working status management.

– local network topology management.

– traffic and congestion management, such as the detection of network overflow conditions and the implementation of resource reservation for time-critical and/or life-critical data flows.

I.6 Protocol and addressing

In the context of the Internet of Things (IoT), the seamless exchange of data between heterogeneous devices requires well-defined communication protocols and robust addressing mechanisms. Protocols in IoT govern how data is formatted, transmitted, and received across constrained networks and devices with limited resources. Addressing, on the other hand, plays a fundamental role in uniquely identifying devices and ensuring accurate data delivery. Due to the vast number of interconnected devices and the diversity of communication technologies, the selection and implementation of appropriate protocols and addressing schemes are critical for

achieving interoperability, scalability, and efficiency in IoT systems. [5]

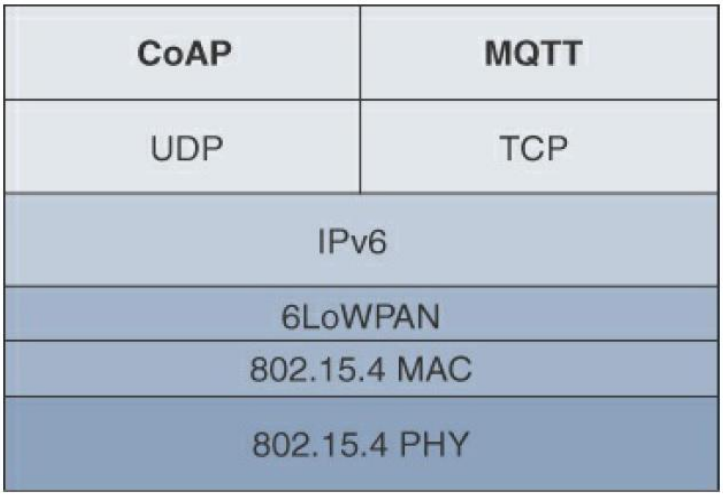


Figure I-4::High-Level IoT Protocol Stack for CoAP and MQTT [4].

In figure CoAP and MQTT are naturally at the top of this sample Io stack, based on an IEEE 802.15.4 mesh network. While there are a few exceptions, you will almost always find CoAP deployed over UDP and MQTT running over TCP. The following sections take a deeper look at CoAP and MQTT.

I.6.1 TCP / IP

TCP / IP (RFC 1180) is a transport model that sends data as an unstructured stream of bytes. TCP / IP represents in a way all the rules of communication on the Internet and is based on the concept of IP addressing, which means providing an IP address to each machine on the network in order to be able to route data packets. This model is based on the Internet protocol IPv4 which works on the Internet layer. Its role is to identify the hosts based on their logical addresses and to do the routing of the data. But nowadays or in a few years IPv4 will no longer be able to address a huge number of devices due to the growth of connected devices, which leads us to use version 6 of the Internet protocol (IPv6); In IoT, the TCP / IP protocol guarantees reliable routing between the source and the destination [4].

I.6.2 MQTT

MQTT (RFC 9431) stands for Message Query Telemetry Transport. It is an extremely simple and lightweight publish / subscribe messaging protocol designed for constrained devices and low bandwidth networks, high latency or unreliable networks. The design principles are to minimize network bandwidth and device resource requirements while attempting to ensure reliability and some degree of assurance in delivery. These principles are also proving ideal for the protocol of the

emerging world of machine-to-machine (P2P) or the Internet of Things, and for mobile applications where bandwidth and battery power are paramount. The operation of MQTT is described as follows: An MQTT session is divided into four stages: connection, authentication, communication and termination. A client begins by creating a TCP / IP connection to the broker using a standard port or a custom port defined by the operators. When creating the connection, it is important to recognize that the server can continue an old session if it is provided with a reused client identity [4].

I.6.3 CoAP

CoAP (RFC 7252) stands for " Constrained Application Protocol ", it is a simple protocol designed especially for low power constrained devices in the Internet of Things. CoAP works much like an HTTP protocol for constrained devices, allowing equipment as basic as sensors or actuators to communicate over the IoT, being controlled and transmitting their data as part of a system [4] [5].

I.7 Applications of IoT

IoT has found its applications in almost all domains of computing and other societal domains. presents the various applications of IoT.

I.7.1 The Smart Home

Future smart homes will be conscious about what happens inside a building, mainly impacting three aspects: resource usage (water conservation and energy consumption), security and comfort [6].

I.7.2 Smart Cities

Smart city is an urban area which creates sustainable development and high quality of life. The characteristics of smart city are: encompassing economy, people, governance, mobility, environment and living. Outperforming in these key areas can be achieved through strong human or social capital and/or ICT infrastructure [6].

I.7.3 Transport/Logistics

In transport logistics, IoT improves not only material flow systems but also the global positioning and automatic identification of freight. It also increases energy efficiency and thus decreases energy consumption [6].

I.7.4 E-Health

Control and prevention are two of the main goals of future health care. Already today, people have the option of being tracked and monitored by specialists even if the patient and specialist are

not in the same place. In this domain, IoT makes human interaction much more efficient because it permits not only localization, but also tracking and monitoring of patients. Providing information about the state of a patient makes the whole process more efficient, and also makes people much more satisfied [6].

I.7.5 Smart retail

Retail IoT realizes both customer needs and business needs: price comparison of a product, looking for other products of the same quality at lower prices; with shop promotions, giving information not only to customers but also to shops and businesses. Having this information in real time helps enterprises to improve their business and to satisfy customer needs [6].

I.7.6 Smart farming

The Internet of Things could revolutionize the way farmers work. Smart farming will become the important application field in the predominantly agricultural-product exporting countries [6].

Figure I-5:The paradigm of the Internet of things application [3]

I.9 Conclusion

In conclusion, this chapter provided a comprehensive introduction to the Internet of Things (IoT) and its growing significance. It explained how IoT connects devices to enable automation and real-time decision making. Applications across sectors like smart homes, healthcare, agriculture, and transportation were explored.

The chapter detailed the interaction between the physical and digital worlds through sensing and data processing. It emphasized how IoT enables smarter environments through continuous data exchange and control. Key characteristics such as interconnectivity, scalability, context-awareness, and autonomy were discussed. Overall, IoT is shown as a transformative force shaping modern industries and daily life.

II Chapter Two

Study of Iot smart homes and cisco packet tracer simulator

II.1 Introduction

In recent years, the concept of smart homes has transformed from an innovative idea into a practical and essential aspect of modern living. Smart home technologies offer users greater control over their environments, improving convenience, security, and energy efficiency. By integrating various devices through centralized control systems, smart homes have significantly enhanced daily life and comfort.

To support the design, simulation, and deeper understanding of these smart home networks, tools such as Packet Tracer are increasingly used. Packet Tracer provides a virtual environment where users can build smart home models, test the interaction between devices, and identify potential issues without relying on physical hardware. It also includes support for Internet of Things (IoT) simulations, enabling users to integrate sensors, actuators, and smart devices into their network designs. By simulating IoT environments, users can explore how smart devices communicate, respond to conditions, and interact within a connected home system. This chapter will examine the fundamentals of smart home technologies, the communication protocols they utilize, and the application of Packet Tracer as a practical platform for network simulation.

II.2 Definition of smart home

A smart home is a home equipped with different smart objects, such as a smart fan, smart light, coffee maker, and smart windows that can be remotely controlled via a smartphone or computer through an internet connection. Smart homes offer the homeowners convenience, savings, safety, and comfort.

Saving because the use of some smart objects, such as smart thermostats and smart lights, can help save energy (reduce energy consumption) and reduce bills. It is convenient because every task is done automatically.

Safety is one of the biggest benefits of a smart home because you can remotely control the devices and see if there is a danger at any time in your home.

Comfort because of the possibility it offers: imagine that you have the possibility to turn on your air conditioner to cool down the place before you reach your home and also the possibility to check if there is food in your refrigerator or even to check if some food inside your refrigerator is expiring or finishing. Smart homes allow homeowners to manage all the home devices anywhere at

any time [7].

There are some main features for smart homes as follows [8]**:**

- The smart home can realize the interaction between the user and the power grid enterprise, obtain the information of electricity consumption and electricity price, set the electricity consumption plan, and so on, guide the scientific and rational electricity use, and advocate the family's consciousness of energy saving and environmental protection.
- Smart homes can enhance the comfort, safety, convenience, and interactivity of home life and optimize people's lifestyles.
- Smart homes can support remote payment.
- Smart homes can monitor and interact with the home through telephones, mobile phones, and remote networks and discover abnormal and timely processing.
- The smart home realizes the real-time meter reading and security service of water meters, electric energy meters, and gas meters, which provide more convenient conditions for high-quality service.
- Support "triple networks" business and the perfect intelligent service.

II.3 Smart home services

II.3.1 Measuring home conditions

A smart home uses sensors to monitor temperature, humidity, light, and proximity. Some sensors handle multiple measurements, like temperature and humidity, while others track light levels and object distances. The data is stored and visualized in real time via a signal processor, communication interface, and cloud- based system, allowing users to access it anytime, anywhere [9].

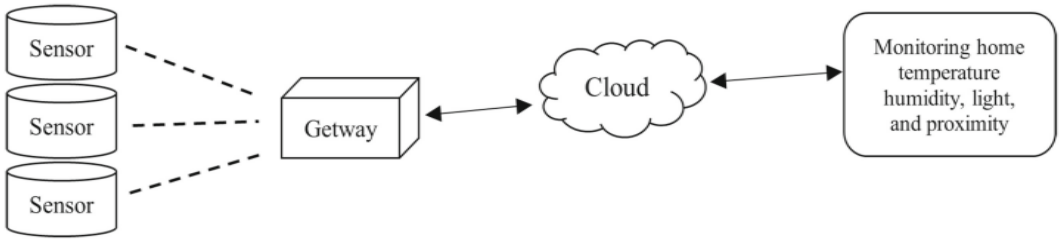


Figure II-1:Smart Home Systems Based on Internet of Things [9].

II.3.2 Managing home appliances

Home appliance management (HAM) provides the user with an interface that the user can use to manage appliances and monitor system data. This leads us to wonder why a person needs to perform these tasks of managing and monitoring device usage data. [10]. What can be done to replace human intervention and automate the entire end-to-end system, from reading and analyzing usage data to planning and taking appropriate action based on user preferences IoT, more precisely home appliance management (HAM), plays a very important role in this goal of automating a process where two goals are to be achieved: energy savings and user preferences. Monitoring smart devices by the user can help the user achieve the first goal - preventing energy losses during the day. On the other hand, I believe that reinforcement learning can allow us to find a solution to the second goal - user preference management. Creates the cloud service for managing home appliances, which will be hosted on a cloud infrastructure. The smart home cloud service offers a simple, flexible, and inexpensive way to store and access data from smart home devices. The managing service allows the user to control the outputs of smart actuators associated with home appliances, such as lamps and fans. Smart actuators are devices, such as valves and switches, that perform actions such as turning things on or off or adjusting an operational system. Actuators provide a variety of functionalities, such as on/off valve service and positioning to percentage open, modulating to control changes in flow conditions, and emergency shutdown (ESD). To activate an actuator, a digital write command is issued to the actuator [9].

II.3.3 Controlling home access

Home access control systems enhance security by verifying individuals against a database of authorized credentials. These systems often use cloud-based infrastructure for centralized data collection and processing, especially in large or distributed environments. Authentication methods include RFID, facial recognition, fingerprints, and proximity cards. In a typical setup, an RFID card is scanned at an entry point, and the ID is sent to a cloud service for verification. Access is granted if the ID matches an authorized entry [10].

II.4 Functions of Smart Home

A smart home system comprises applications developed on top of an IoT infrastructure.

These smart home applications may perform the following primary functions[5]:

– **Alert**

The smart home system is capable of sensing its surrounding environment and, accordingly, sending alerts to the user via a registered device or account. Each alert contains information related to environmental conditions, which may include gas levels, temperature, humidity, light intensity, and other relevant parameters. Alerts can be scheduled to be sent to the user at predefined intervals. They may be delivered through various channels such as email, text messages, tweets, or other social media platforms.

– **Monitor**

This is one of the most critical functions of a smart home system. A smart home is capable of monitoring its surroundings using various sensors and camera feeds. Monitoring plays a vital role as it continuously tracks all activities within the smart home, forming the foundation upon which further actions can be taken or decisions can be made. For instance, the system can monitor the room temperature and send an alert to the user to switch on the air conditioner if the temperature exceeds a predefined threshold.

– **Control**

This function of the smart home system enables the user to manage and control various activities within the home. These activities may include switching lights, air conditioners, and appliances on or off; locking or unlocking doors; and opening or closing windows and doors, among others. The user can exercise control either locally from within the home or remotely from any location. Furthermore, this function supports automation, allowing activities such as automatically turning the air conditioner on or off based on the room's temperature conditions.

– **Intelligence**

Intelligence, often referred to as Home Intelligence (HI), represents the most critical function of a smart home, reflecting the intelligent behavior of the smart home environment. This function involves the automatic decision-making process in response to various events. HI relies on the artificial intelligence (AI) mechanisms embedded within the smart home system. Beyond providing the "brain" of the smart home, HI also plays a crucial role in enhancing home security[9].

HI creates an integrated environment in which the AI system can recognize and appropriately respond to changing conditions and events. By identifying abnormal or unexpected occurrences, HI can alert the user and initiate immediate automatic responses if necessary. Examples include automatically preparing coffee upon the user's arrival, sending alerts when suspicious activity is

detected at the door or inside the home, automatically ordering groceries when shortages are detected in the refrigerator, and notifying an electrician or plumber whenever maintenance is required[1].

II.5 IoT-Based Architecture Model for Smart Homes|

Figure 2 shows the smart-home and IoT-based main components and their interconnectivity. Here in the smart home environment, we can see the typical devices connected to a local area network (LAN). Nowadays it might be ZigBee, BLE, Wi-Fi, or other proprietary RF communication, as shown in Table 1. This enables communication among the sensors, actuators, and outside of it. Connected to the LAN are a server and its database. The server controls the devices, logs its activities, provides reports, answers queries, and executes the appropriate commands. For more comprehensive or common tasks, the smart home server transfers data to the cloud and remotely activates tasks in it using APIs, application programming interface processes. Besides, IoT home appliances are connected to the internet and the LAN, and so expand smart homes to include IoT. The connection to the internet allows the end-user application to communicate with smart home, enabling resident to get information and remotely activate tasks [11].

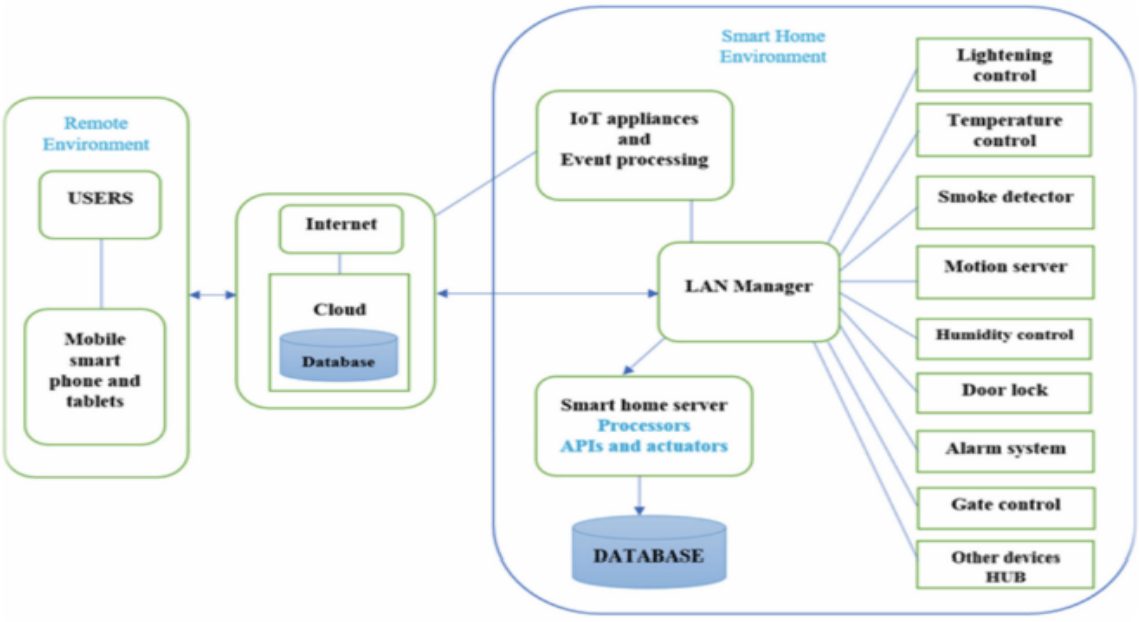


Figure II-2:Building an IoT-based architecture model for smart homes [11]

II.6 Overview of Simulation Tools

In this section, we will present the simulation tool utilized, offering a detailed explanation of its functionality. Subsequently, we will discuss the requirements of our smart home system.

II.7 Cisco Packet Tracer Overview

Cisco Packet Tracer is a comprehensive networking simulation software tool for teaching and learning how to create network topologies and imitate modern computer networks. The tool offers a unique combination of realistic simulation and visualization experiences, assessment and activity authoring capabilities, and multi-user collaboration and competition opportunities. Its innovative features help students and teachers collaborate, solve problems, and learn networking concepts in an engaging and dynamic social environment [12].

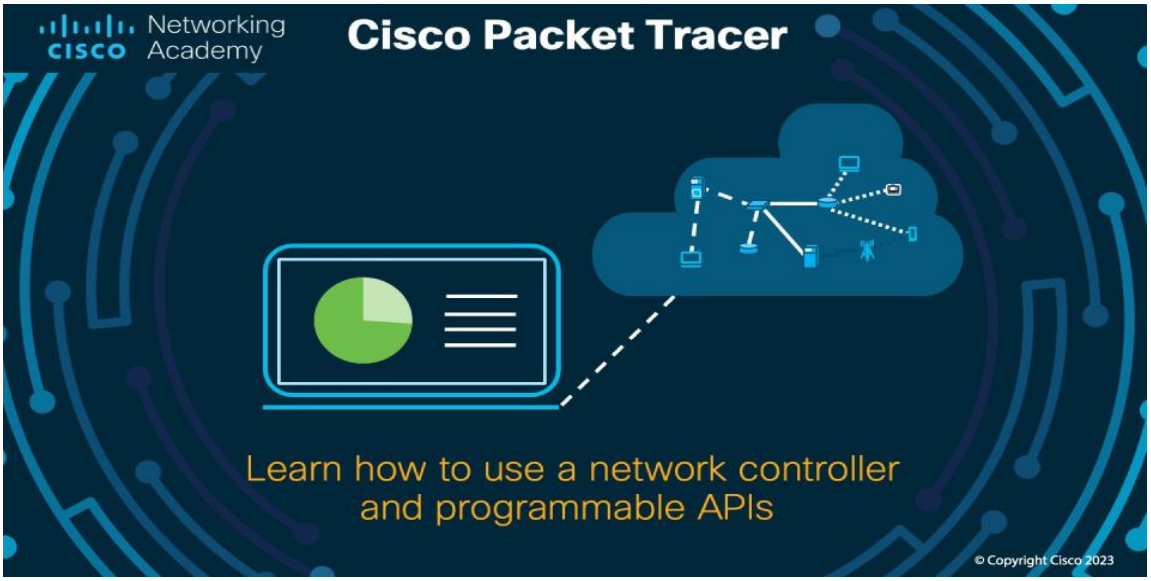


Figure II-3:Cisco Packet Tracer Interface

II.7.1 Packet Tracer Workspaces

There are two types of workspaces, each serving a specific purpose in network design and simulation [13]:

The logical workspace enables users to design and build logical network topologies. Various networking devices can be selected, dragged, and placed within this workspace to simulate their interconnections and functionality.

- **Physical Workspace**

The physical workspace allows users to create a network as it would appear in the real world. It provides a geographical representation where networking devices can be positioned at different locations, such as different parts of a city, to simulate physical deployment and connectivity.

II.7.2 Packet tracer Mode

There are two types of modes available, each designed to support different aspects of network

learning and simulation [13]:

- **Real-time Mode**

In this mode, devices within the network operate exactly as real-world devices would. Their behavior and appearance closely resemble actual physical equipment, providing users with a realistic experience of network operations.

- **Simulation Mode**

This mode offers users greater control over network activities by allowing them to manage and observe the timing of data transmission and network events. It is particularly useful for educational purposes, as students can slow down or pause processes to better understand how networks operate and to practice troubleshooting network failures.

II.8 Cisco Packet Tracer and the Internet of Things

The latest version of Cisco Packet Tracer introduces several new features that enhance the simulation of Internet of Things (IoT) environments. These features include the addition of smart devices, sensors, actuators, and microcontrollers. Among the smart devices now available in Packet Tracer are smart windows, smart fans, smart lights, and alarm sirens. Additionally, a variety of sensors—such as water level sensors, temperature sensors, humidity sensors, and carbon dioxide sensors are also included.

The IoT devices in Cisco Packet Tracer can be utilized to design and simulate a wide range of IoT applications, including smart homes, smart industries, and smart cities. One of the key advantages of using Cisco Packet Tracer is that users can interact with the simulated devices in much the same way they would with real-world devices. Moreover, with its multiuser functionality, multiple users can collaborate to build virtual networks across a real network infrastructure.

In addition to classical network devices such as routers and switches available in the previous versions, Packet Tracer 8.2 Components Box now contains a wide variety of Smart Things and components [14]:

II.8.1 Smart Things

Are physical objects that can connect to the Registration Server or Home Gateway through a network interface. They are separated into 4 subcategories: Home, Smart City, Industrial, and Power Grid.

Figure II-4:Smart things in packet tracer

II.8.2 Components

Are physical objects that connect to microcontroller (MCU-PT) or single boarded computers (SBC-PT). They typically does not have a network interface and rely on the MCU-PT or SBC-PT for network access. These are simple devices that only communicate through their analog or digital slots.[14]

There are three subcategories for Components:

- **Boards**: microcontrollers (MCU-PT), single boarded computers (SBC-PT), and a special device called Thing which are used to create self-contained physical objects like coffee makers or smoke alarms.
- **Actuators**: these components manipulate the Environment, themselves, or the area around them.
- **Sensors:** these components sense the Environment (photo detectors, temperature sensor), the area around them (RFID, metal sensor), or interactions (potentiometer, push button).

MQTT protocol and applications have been added in Packet Tracer since version 7.1 to improve communications between IoT devices.

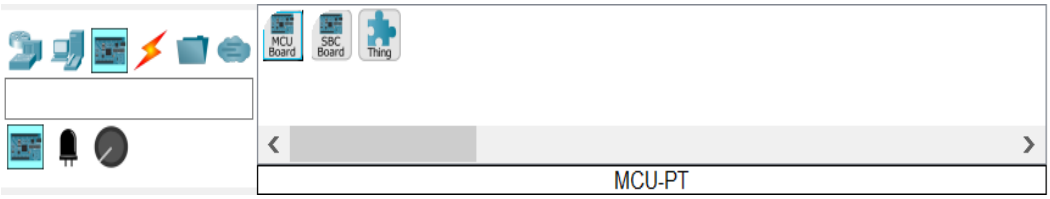


Figure II-5: Components in packet tracer

II.9 The Environment

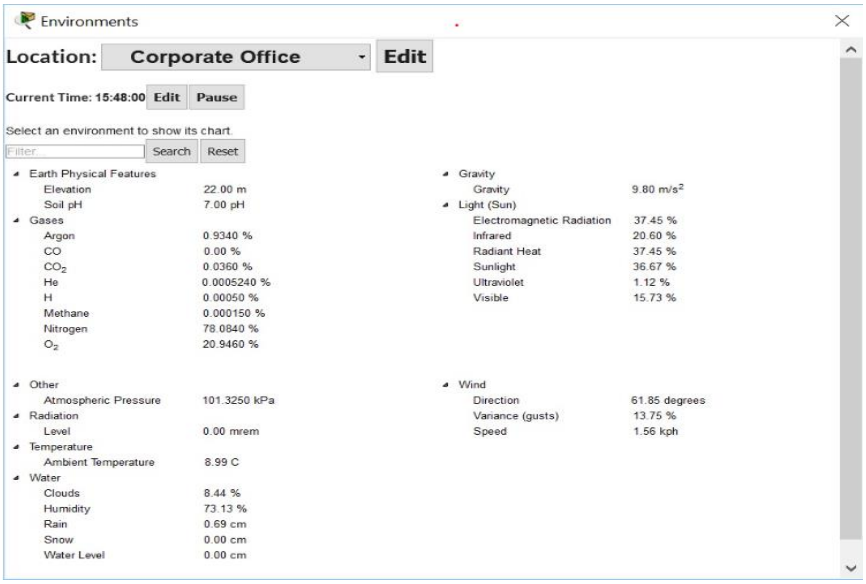
The intercity, city, buildings, wiring closets, and generic containers all have an environment. There are a couple dozen default environments, such as temperature, rain, water level, wind speed, and snow. When no devices are affecting the environment, their values are looped on a 24-hour cycle. For example, the sun will come up at 6am and set at 6pm. The ambient temperature will peak at 25°C at noon. This cycle is set on the intercity level and its ambient temperature range will

propagate all the way down to the main wiring closet automatically. If a heater is added to the Corporate Office and turned on, the temperature inside the Corporate Office will increase along with all the containers within it. Note however, the heater does not heat up the parent container, Home City, it will only heat up the child containers. When the heater is turned off, the Corporate Office will eventually converge to the parent container's ambient temperature, Home City, based on its transference value. Different containers may have different levels of insulation and thus different transference values the transference values determine the rate that the child container converges with the parent container and works the same way for all environment types.

Many devices or Things affect or respond to the environment in some way. A Fire Sprinkler will raise the water level and humidity in a container. An old car will increase various gases and ambient temperature when turned on. A smoke detector can be used to trigger an alarm when the smoke in environment increases to a certain point. A full range of devices and things that respond and affect the environment is listed below [15].

II.9.10 Environment Dialog

The Environment Dialog allows as to view and edit the environment inside the physical



. Figure II-6:The Environment Dialog [15]

To open the environment dialog, press the Environment button on the Logical or Realtime toolbars.

Location: The physical location of the container. You can change the location by selecting the drop-down or simply navigate Physical View.

Time: The current time. The environment time is decoupled from the network simulation time. This is a modelling limitation; typically, the environment time moves much faster than the network time. On large networks, a modern computer may struggle to keep up with 2x real time for the network simulation, while the default environment time is at 30x by default.

Environment Values Tree: At a glance view of environments that are set to show. You can filter the values to show only the environments you are interested in:

- **Chart**: To view a chart of the environment, click on an environment name from the Environment Values Tree.

- **Name**: The name of the current environment. Only one chart can be shown at a time.
- **Data Ranges:** There are two ways to change the data range. The first is to use the Zoom levels, which ranges from 1 minute to 1 day. The second is to use the handle bars on the compressed chart view below the main chart. It is also possible to scrub the chart timeline by selecting and dragging the highlighted area on the compressed chart.

- **Series**: Depending on the level, you may have four or five series: current, keyframe value, transference rate, things rate, and parent. Current refers to the current environment value. Transference rate is the rate of change contribution to the current environment. Keyframe value is the keyframes contribution to the current environment. Things rate is the total rate of change to the current environment from Things that affect the environment in the workspace container. If not in the Intercity,parent is the current value of the parent container.

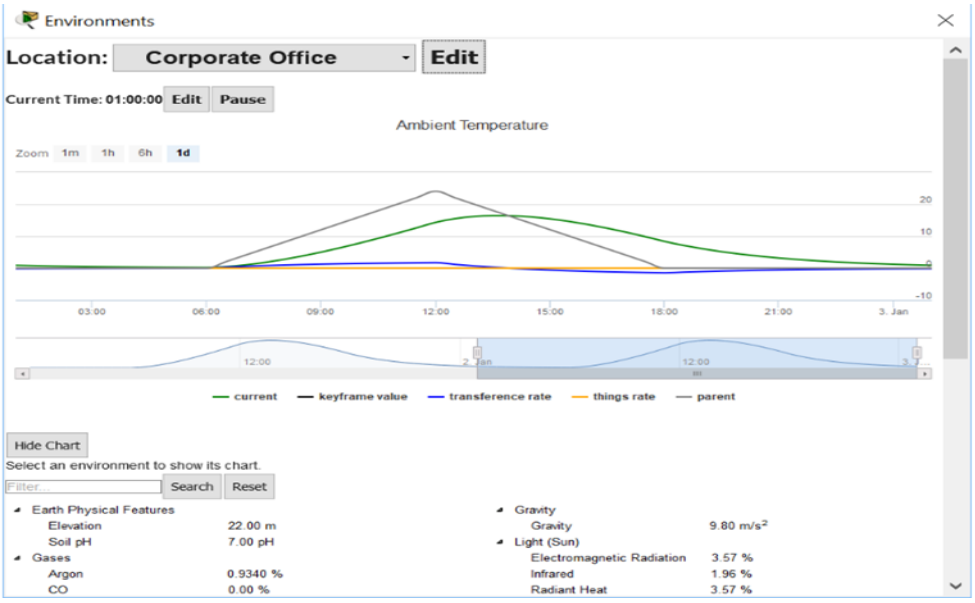


Figure II-7::Chart of the environnement[15]

II.10 Environment Dialog Edit Mode

To enter edit mode, click on the Edit button next to the location or environment values header. In Edit mode, you can change the timescale and create keyframes to manipulate how the environment should behave over a 24-hour cycle [15].

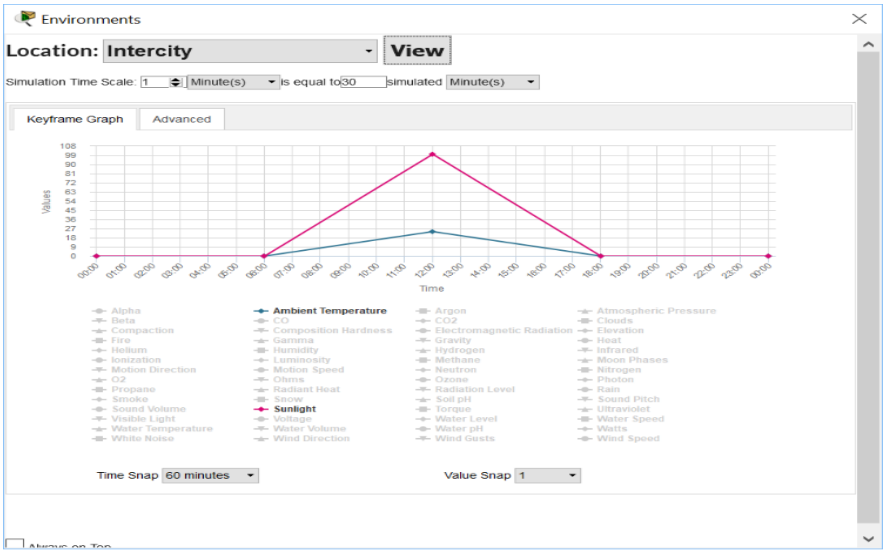


Figure II-8:Environment Dialog Edit Mode

– **Environment Dialog Edit Mode : Timescale**

The timescale determines how fast the simulation should evaluate time. Selecting 1 second is equal to 30 simulated minutes means that in one second of real time, 30 minutes would have passed in our simulation, two seconds would be an hour, and so on.

The simulation evaluates the environment based on the timescale settings and interpolates in between. A rule of thumb is to set your timescale to the smallest value between keyframes. For example, if your smallest keyframe spacing is 15 minutes, your timescale should be 1 second in real time is equal to 15 simulated minutes.

Recall that the environment time is decoupled from the network simulation time. This is a modelling limitation; typically, the environment time moves much faster than the network time. On large networks, a modern computer may struggle to keep up with 2x Realtime for the network simulation, while the default environment time is at 30x [15].

– **Environment Dialog Edit Mode : Keyframe Graph**

Keyframes is one way to affect the environment. Transference to the parent and Things on the workspace also affects the current environment value.

The graph is set to a 24 hour cycle from 00:00:00 to 23:59:59. During simulation, this keyframe

graph will continuously loop.

These are the ways that the environment keyframe graph can be manipulated [15]:

Show and Hide an Environment: In the legend, click on an environment name. Faded environment names are not shown on the graph, to show them, click on the name. To hide, click on the name again.

Add an Environment Keyframe: Double-click anywhere on the line series of the Environment you want to change.

Remove an Environment Keyframe: Double-click on the point you want to remove

Edit an Environment Keyframe Value: Mouse-over the point and change the Value in the tooltip. Press the Enter key to set the value.

Higher or Lower Bounds: Drag a point off the graph either to the top or to the bottom to extend the y-axis of the graph.

Time Snap: By default, the time axis snaps at every 60 minutes. This can be changed to 15 or 30 minute intervals. Finer controls can be made using the Advanced tab.

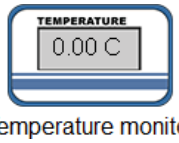
Value Snap: By default, the values axis snaps at every 1 step. The range of values are from 0.001 to 100. Finer controls can be made using the Advanced tab.

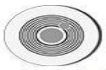
II.10.2 Things That Affect and Respond to the Environment

Things can also affect or respond to the environment. The size of the physical container matters. If a heater is added at the city level, it will barely affect the city versus putting the container inside a building or a small room. All the rates of change specified below applies to a container that is 100000 cm3 in size.

Below is a table of things available in Packet Tracer 8.2 and their behaviors with respect to the Environment [15]:

Table II-1:Things effected in packet tracer environment [15]

Thing	Icon	Environment B e h a v i o r
Door		Affects Argon, Carbon Monoxide, Carbon Dioxide, Hydrogen, Helium, Methane, Nitrogen, O2, Ozone, Propane, and Smoke. When the door is opened, those gases will decrease to a maximum of 2% in total change.
Home Speaker, Speaker	 	Affects sound volume at 65 dB. Affects sound pitch at 20 CPS to 60 CPS. Affects white noise at 20%.
Carbon Dioxide Detector		Detects carbon dioxide.
Fan		Affects wind speed, humidity, and ambient temperature.
Lawn Sprinkler, Floor Sprinkler		Affects water level at a rate of 0.1 cm per second. Affects humidity at a rate of 5% per hour.
Light		Affects Visible Light with a maximum output of 20%.
Temperature Monitor		Detects Ambient Temperature.

Wind Turbine	 Wind turbine	Detects Wind Speed to generate electricity.
Window	 Window	Affects Argon, Carbon Monoxide, Carbon Dioxide, Hydrogen, Helium, Methane, Nitrogen, O2, Ozone, Propane, and Smoke. When the door is opened, those gases will decrease to a maximum of 1% in total change.
AC, Air Cooler	 AC  air cooler	Affects Humidity at a rate of -2% per hour. Affects Ambient Temperature at a rate of -10°C per hour.
Smoke Detector, Smoke Sensor	 Smoke detector  Smoke sensor	Detects Smoke.

II.11 Smart Home Required Equipment

A smart home requires essential equipment to ensure proper automation and control. These include sensors, actuators, communication modules, control units, and smart devices, all working together to provide comfort, safety, and efficiency. In this section, we will explore the most important equipment needed to create a smart home system, such as sensors, actuators, communication modules, control units, and smart home appliances.

II.11.1 Garage

The garage door is equipped with an RFID reader that verifies the validity of access cards presented by individuals seeking entry. Additionally, it includes a smoke detector that detects smoke emitted by the old car, triggering the door to open automatically.

II.11.2 Front yard

This part contains the door of the house equipped with an RFID reader which allows

checking the validity of the cards of the person wishing to enter the house. Furthermore, the entrance is equipped with a webcam that captures images of any object approaching the door. The Front yard is divided into sections:

Water Monitoring: This section includes lawn sprinklers for water distribution and a water level sensor for measuring the quantity of water.

Light Control: This section features a streetlight that automatically activates when ambient light levels fall below a certain threshold. Streetlight

Web camera &motion detector: The camera is monitoring and recording the entrance to the door when detection a movement by the motion detector.

II.11.3 Kitchen

The kitchen design is divided into two sections: automatic fire control and wind control.

- **Auto fire monitoring:** this section is almost the same as the one in the; also, a siren is needed to make an alert in case there is a fire. It also includes a fire sensor connected to a microcontroller, which in turn is linked to a fire sprinkler system used to control the opening and closing of the kitchen windows.

II.11.4 The Bad Room

Automatic Temperature Monitoring: This section comprises an air conditioner (AC) and a temperature sensor, which measures and outputs the ambient temperature in degrees Celsius. The sensor's readings are influenced by the surrounding environmental conditions.

Room Lighting Control: This section operates on battery power, with the batteries being recharged using solar energy.

Rain monitoring: This component detects the presence of rain and responds by closing the window and activating the LED indicator.

II.11.5 Living room

This section includes a :

Trip sensor: that detects movement in the event of an intrusion through the window.

Temperature Monitoring: The temperature of the living room is measured, and the fan is activated accordingly.

Solar panal: The solar panels generate electricity that charges the battery, which in turn powers the light and fan

In addition, there is a TV screen that is connected to the cloud.

II.12 Conclusion

This chapter has examined the concept of smart homes, detailing their functionalities, structural components, and the pivotal role of the Internet of Things (IoT) in enhancing their operational efficiency. Particular emphasis was placed on the contribution of IoT technologies to resource conservation within smart home environments. Additionally, the methodologies utilized in the simulation process were reviewed, and the principal components of the proposed smart home system were systematically identified. Building upon this theoretical framework, the subsequent chapter will focus on the practical implementation of the smart home model through simulation in Cisco Packet Tracer. This implementation aims to assess the design's effectiveness and evaluate the system's performance within a controlled virtual environment.

III Chapter Three

simulate a smart home using cisco packet tracer

III.1 Introduction

This chapter presents a smart home simulation developed using Cisco Packet Tracer, showcasing the integration of IoT devices to automate and monitor household functions. The simulation includes key components such as environmental sensors, smart lighting, security systems, and remote control mechanisms, all interconnected through a network infrastructure. Each component's functionality is thoroughly described, and its operation is demonstrated within the simulated environment. Additionally, the controllability and responsiveness of the system are verified to ensure reliability and efficiency.

By leveraging this simulation, the chapter provides valuable insights into the design, configuration, and management of IoT-enabled smart homes, highlighting both the benefits and challenges of such systems. The findings contribute to a deeper understanding of IoT applications in home automation, serving as a foundation for future research and real-world implementations.

III.2 Practical plan

Our project of a smart home system is deployed in six structured phases using Cisco Packet Tracer. First, the network backbone is established: a central switch connects to individual gateways for each zone (front yard, living room, bedroom, kitchen, garage), a cable modem for internet access, and an ISP router linked to critical servers (DHCP for IP allocation, DNS for domain management, and IoT for device coordination).

Second, zone-specific devices are deployed: the **front yard** integrates motion-activated cameras, RFID door locks, and weather-responsive sprinklers; the **living room** installs rain sensors, solar- powered fans, and smart windows that close during rain/wind The **bedroom** connects RFID-secured doors, solar-paneled lamps, and thermostat-controlled HVAC; **the kitchen** embeds fire detection systems with sprinklers, wind-override windows, and a smartphone-controlled coffee maker; and the **garage** implements smoke-triggered emergency protocols for its RFID door

Third, automation rules are programmed per gateway: rain sensors activate living room lamps, kitchen fire alarms override windows during smoke events, and garage emergencies prioritize door opening over RFID locks.

Fourth, cross-zone integration is configured: front yard motion alerts trigger garage recordings, kitchen fires activate whole-home alarms, and solar panels prioritize energy distribution.

Fifth, remote access is enabled via a smartphone app that interfaces with the IoT server, allowing users to monitor cameras, adjust thermostats, or trigger sprinklers.

Finally, rigorous testing validates scenarios like simultaneous rain and fire events, RFID conflicts, and network stress, while solutions like sensor confirmation delays and MQTT protocols address latency and false alarms. This phased approach ensures modular scalability, real-world reliability, and seamless user control.

III.3 Project scenario

IoT Smart Home Network Setup In the following steps we will present the major functionalities of creating and preparing the environment.**:**

Step 1: Initiate the project.

Step 2: Open the. pkt (Packet Tracer) file and save it under a desired name.

Step3: Add the necessary components to the workspace.

Step4: Establish wireless connections among all devices in the workspace.

Step5: Configure each device and set up the Internet Service Provider (ISP) router.

Step6: Integrate the Home Gateway into the network.

Step7: Connect all smart devices to the wireless network

Step8: Add and connect the end user device to the network.

Step 9: Terminate the setup process.

III.4 Technical Requirements

In order to perform this work, we need the following requirement:

Cisco Packet Tracer (PT) version 8.2 or above: Open-source software by Cisco Systems developers to create a virtual network topology before building it in the real world, PT does not require a big amount of RAM since it is a simulator, not an emulator. In addition, version 8.2 contains new important features for IoT.

III.5 Implementation of smart home sections

The smart home system was developed using Cisco Packet Tracer 8.2.2, structured across two workspaces: the logical workspace for configuring network infrastructure (subnets, DHCP/DNS servers) and IoT automation rules, and the physical workspace for spatially organizing devices into functional zones (kitchen, bedroom, etc.). The logical design established network connectivity and programmed device interactions, while the physical layout mapped hardware placements to simulate real-world environments.

Figure III-1**:**Logical workspace Cisco Packet Tracer interface.

The figure presents the logical workspace where network devices are strategically positioned throughout a residential space. Blue connection lines indicate network cabling paths connecting

various devices. Cloud clusters represent device groupings in different home areas such as the living room, bedrooms, kitchen, and garage.

Network switches are positioned at junction points to facilitate connectivity between different zones. The blue lines show the primary network backbone, while dashed gray lines appear to represent wireless connections between devices.

This logical representation demonstrates how the network topology maps to the physical home environment, showing both wired and wireless connectivity paths.

Upon switching to the physical workspace, the intercity view appears, which is a visual representation of the house's geographical location. This broader perspective shows the property's position within the larger urban context, highlighting its relationship to surrounding infrastructure and services. The intercity view helps establish important connectivity considerations like proximity to ISP access points, local network infrastructure, and potential signal interference sources. as illustrated in the following figure.

Figure III-2**:** intercity view

After identifying the geographical location, access to the smart house becomes possible. I'll now focus on the home as illustrated in the following figure.

Figure III-3: physical workspace

This interface provides a detailed visualization of the smart home's physical layout within the simulation workspace, emphasizing how devices are interconnected and linked to the internet. The house structure is mapped with precision, showing the placement of IoT devices (e.g., sensors, cameras, and smart appliances) in their respective zones, such as the kitchen, living room, and garage. Purple circles overlay each area to represent localized Wi-Fi network coverage, ensuring seamless connectivity for devices within specific regions of the home for instance, robust coverage in high-activity zones like the living room and kitchen and optimized signals in peripheral areas like the garage. A distinct green

circle denotes the cellular tower's coverage range, extending beyond the home's boundaries to illustrate how remote access and cloud-based services are enabled for users via cellular networks. This layered representation clarifies the interplay between indoor wireless networks and external cellular infrastructure, ensuring reliable internet access for both local automation and external connectivity. The design highlights the balance between localized device communication and broader internet integration, essential for a fully functional smart home ecosystem.

Having established the logical workspace for network topology design and the physical workspace for device placement, the next critical phase involves network configuration within the logical environment. This step defines how devices communicate across zones, assigning IP addresses, configuring subnets, and setting up DHCP/DNS servers to ensure seamless connectivity.

III.6 Network Layout

The implementation begins with establishing the network backbone, the foundational infrastructure that interconnects all components of the smart home system. This backbone comprises a central switch linking zone-specific gateways (e.g., kitchen, garage) to a gateway router, which interfaces with an ISP modem for internet connectivity. The router acts as the bridge between the home network and the Internet Provider Cloud, assigning a public IP address to enable external access. To ensure logical separation

The figure illustrates the project network topology implemented in the IoT simulator chosen (Cisco Packet Tracer).

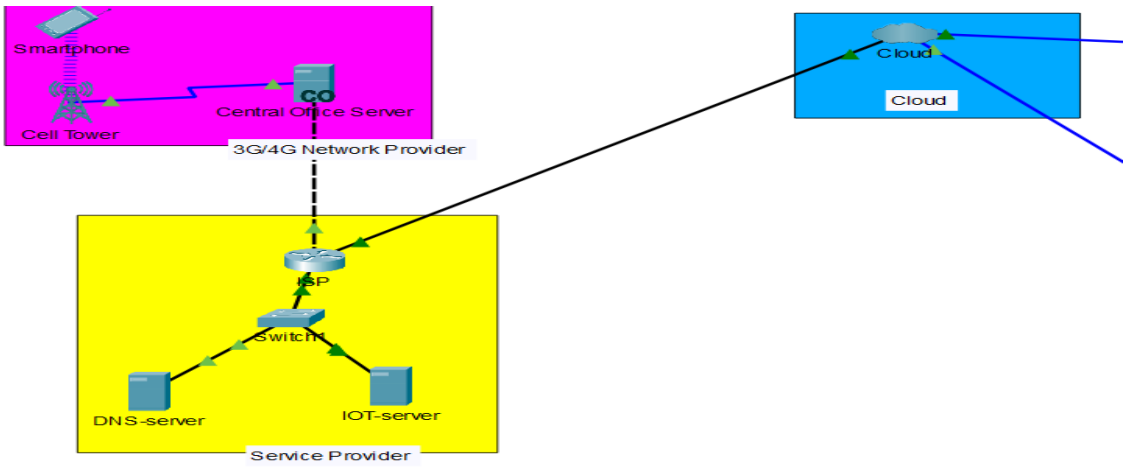


Figure III-4 the project network topology

III.6.1 Addresses of the system

Table 3 below shows all devices' IP addresses that they will get after configuration.

Section	Device	Interface	IP address
Service Provider	**ISP Router**	GigabitEthernet 0/0	209.165.201.225
		GigabitEthernet 0/1	10.0.0.1
		GigabitEthernet 0/2	209.165.200.225
	DNS server	Fastethernet 0/2	10.0.0.254
	IOT server	Fastethernet 0/3	10.0.0.253
3G /4G Provider	**Central office Server**	Backbone	Dynamic 209.165.201.230
		Cell tower	172.16.1.1
	3G/4G clients	3G/4G Cell	Dynamic 172.16.1.100
Smart home	**Home Gateway 0**	LAN	192.168.25.1
		Internet	Dynamic209.165.200.230/24
	Home Gateway2	LAN	192.168.25.1
		Internet	Dynamic209.165.200.231/24
	Home Gateway3	LAN	192.168.25.1
		Internet	Dynamic209.165.200.232/24
	Home Gateway 4	LAN	192.168.25.1
		Internet	Dynamic209.165.200.233/24

	Wireless Router0	LAN	192.168.25.1
		Internet	Dynamic209.165.200.24/

Table III-1: devices' IP addresses

III.7 Internet connection configuration

This section covers the basic steps to set up internet access in the smart home network, including configuring the ISP router and connecting all devices to ensure proper communication and remote control.

III.7.1 Internet provider

To ensure internet connectivity across all departments, a cloud device was configured to act as a cable router. This device facilitates communication from Coax Port 7 to Eth Port 6 , in addition to the cable line that connects to the COX87 TV unit, as shown in the figure that displays the configuration tab of the cloud.

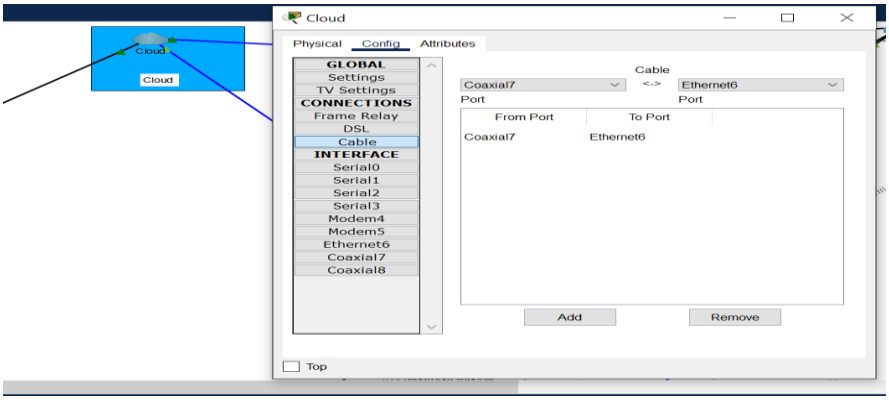


Figure III-5: Cloud Connection and Internet Provider Setting.

Figure III-5 shows the configuration interface for establishing the connection between the smart home and the internet service provider (ISP).

The configuration window displays the "Cloud" component settings, which represent the internet or WAN connection to the external network. In this specific setup, we can see the connection is being configured to use a cable internet service. The interface is showing how the physical connection is established between two different technologies. the ISP's coaxial cable infrastructure (Coaxial7) is connected to the home network's Ethernet interface (Ethernet6). This represents the demarcation point

where the service provider's network meets the customer's equipment.

This connection allows Router R1 in the ISP section to automatically assign a WAN IP address to your home network via DHCP. This is the first crucial step in establishing internet connectivity, as it creates the gateway through which all external traffic will flow.

III.7.2 Service provider

– **ISP Router Settings:**

The router connects to the Central Office Server (3G/4G Provider) via the GigabitEthernet 0/0 port, interfaces with the Service Provider through the GigabitEthernet 0/1 port, and links to the WAN via the GigabitEthernet 0/2 port. The following commands are entered into the Command Line Interface (CLI) tab of the ISP router to configure these connections:

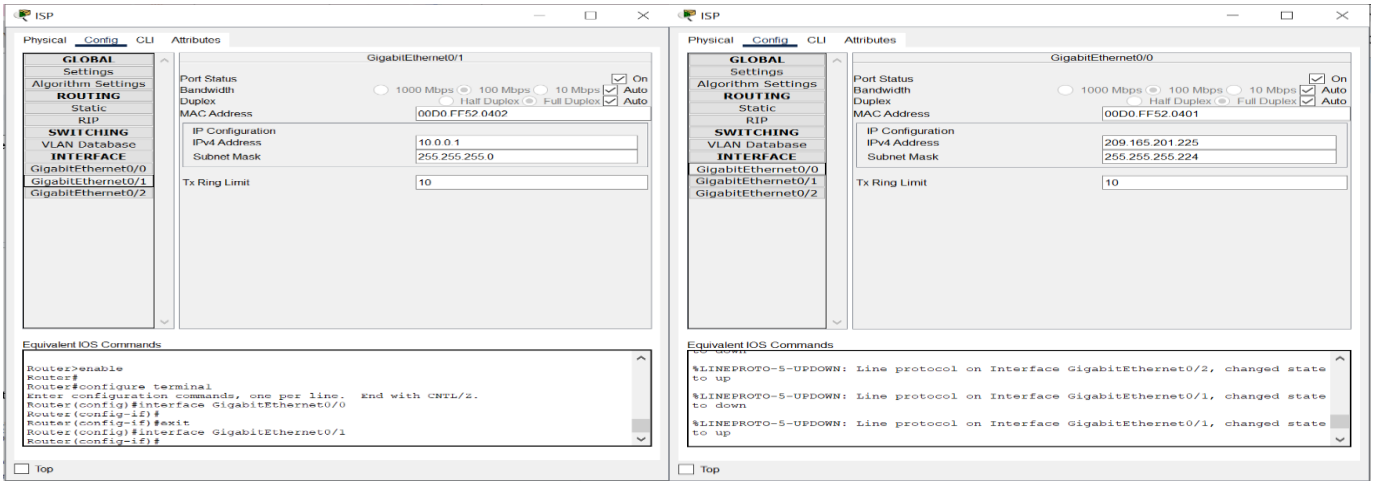


Figure III-6: ISP interface configuration

This figure the initial setup and device connectivity procedures, the next essential step is configuring the DHCP service to enable automatic IP address assignment within the network. This ensures efficient and dynamic distribution of network settings, such as IP addresses, default gateways, and DNS servers, to connected devices. The configuration is performed on the ISP router, where specific IP ranges are reserved and multiple DHCP pools are defined to serve different network segments.

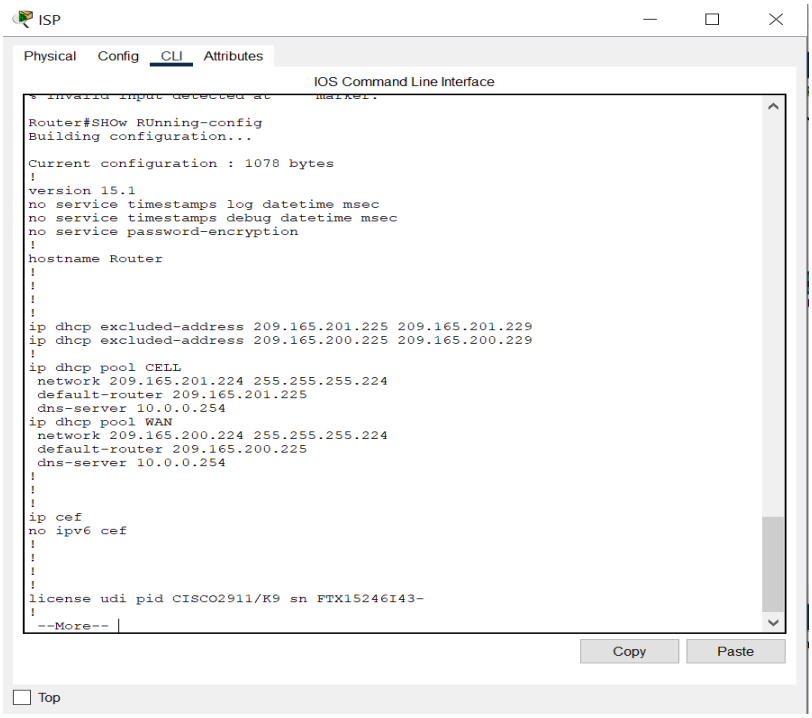


Figure III-7: DHCP configuration

– **Switch Settings**

The settings are configured automatically and are specifically intended to facilitate the connection of home gateways to the network.

– **DNS Settings**

The server is physically connected to the network through its FastEthernet0 interface, which serves as the primary port for data transmission. To ensure stable and predictable communication, the server is configured with a static IPv4 address of 10.0.0.254, paired with a subnet mask of 255.255.255.0. This subnet mask designates the local network segment (10.0.0.0/24), allowing the server to communicate directly with devices within the same subnet. The default gateway is set to 10.0.0.1, enabling the server to route traffic to external networks or the broader internet via the designated gateway device .

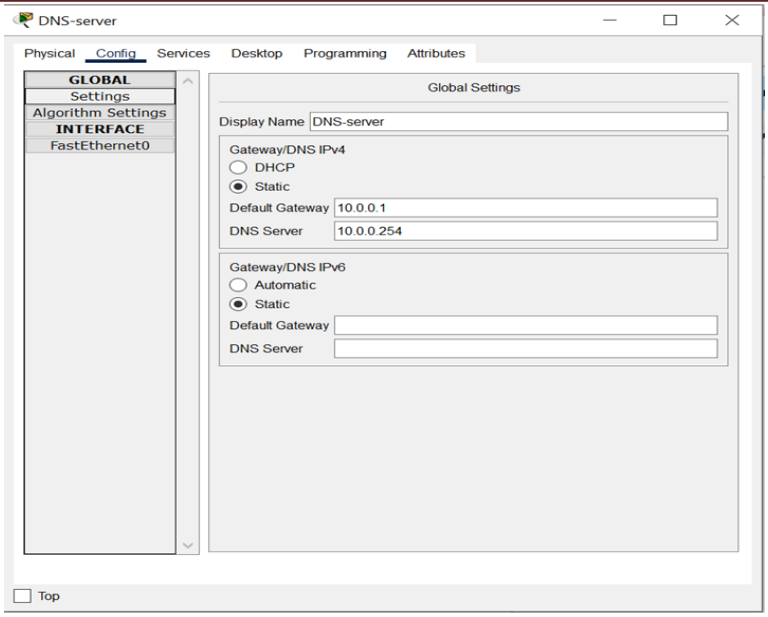


Figure III-8: DNS configuration

This figure configuration, the port status is rigorously verified to confirm that the physical and logical connections are active and error-free. This step ensures that the FastEthernet0 interface is operational, with proper link status and no packet loss or collisions. Once validated, the interface is explicitly enabled to activate its functionality within the network infrastructure, as illustrated in the figure, which provides a visual reference for the setup process.

To activate critical network services, the DNS server is enabled via the Services tab in the server's configuration interface. By navigating to the DNS section and switching the service to "On," the server gains the ability to resolve domain names to IP addresses, a foundational requirement for networked applications and user accessibility. This configuration step finalizes the server's role as a central component for both local communication and broader network operations, ensuring seamless integration into the smart home ecosystem.

III.7.3 IoT server Settings

- **Network configuration**

The FastEthernet0 interface is connected to the network and configured with a subnet mask of 255.255.255.0. The default gateway is set to 10.0.0.1, and the interface is assigned the IP address 10.0.0.253. Once the configuration is complete, the port status is checked and the interface is enabled, as demonstrated in Figure (A). Subsequently, under the same tab, we navigate to the Settings section to input the DNS server and default gateway IP addresses.

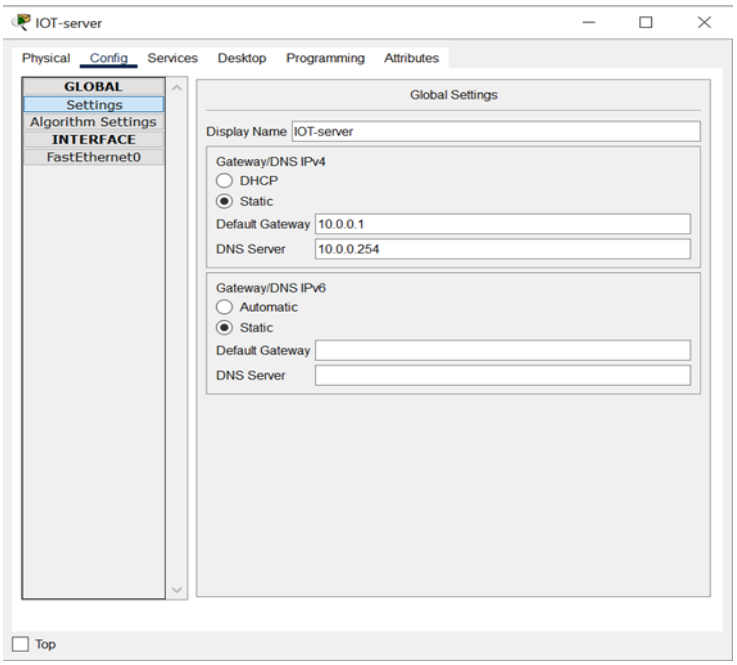


Figure III-9: Iot server configuration

After configuring the server as an IoT server, you must enable the IoT service from the "Services" tab. Once the service is enabled, a user account is created by opening a web browser from the server's desktop and accessing it via its IP address: 10.0.0.253. Since there is no existing account, we click "Register Now" to register a new user. In this setup, the chosen username is "admin," as shown in Figure III-10.

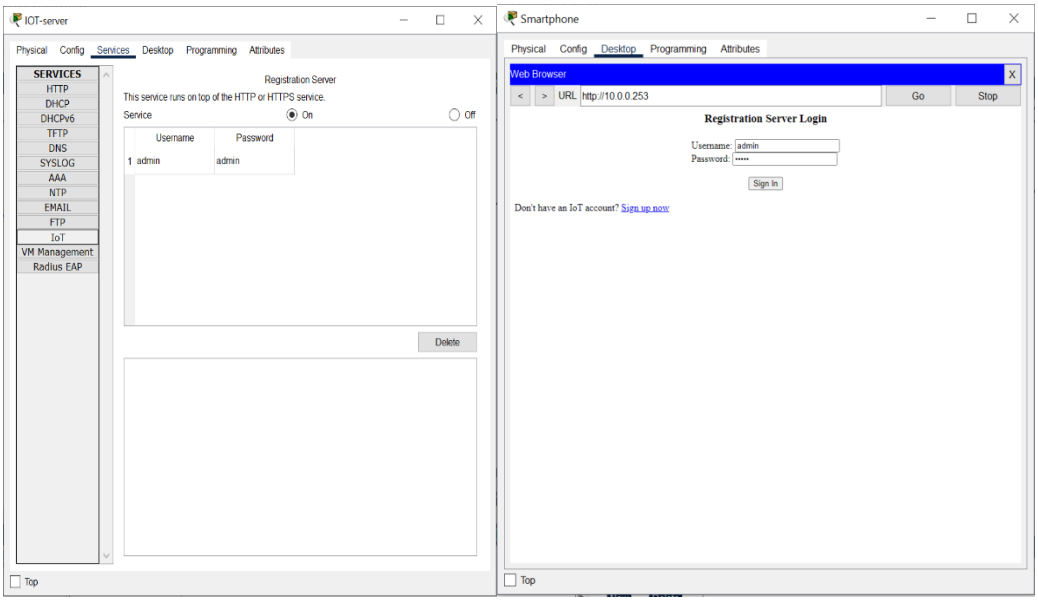


Figure III-10: IoT service configuration

III.7.4 3G/4G provider network

– **Cell Tower**

The cell tower enables wireless 3G/4G connectivity between mobile devices and the IoT server, transmitting encrypted data via cellular networks. It ensures comprehensive property-wide coverage, linking mobile users to the smart home system even during local Wi-Fi outages. The tower routes requests through the provider's core network to the IoT server for authentication and response handling. This integration supports real-time remote control and redundancy, maintaining uninterrupted access. Cellular infrastructure thus creates a resilient, secure bridge between mobile interfaces and IoT ecosystems.

Here We can only change the provider's name so that any 3G/4G client can connect with the provider by typing the appropriate name. The name chosen was ptcellular.

– **Central Office (CO) Server**

Act as the backbone of telecom networks, aggregating and routing data/voice traffic between providers and subscribers. Configuration focuses on network interfaces,

QoS prioritization, security protocols, and redundancy to ensure seamless, high-performance service delivery.It is equipped with two interfaces: a backbone interface that connects the provider to the WAN and a coaxial interface that links the server to the cell tower.

Backbone Interface: This interface is connected to the Internet Service Provider (ISP) and will automatically obtain a dynamic IP address once the DHCP protocol is enabled, as illustrated in the Figure *III-11*.

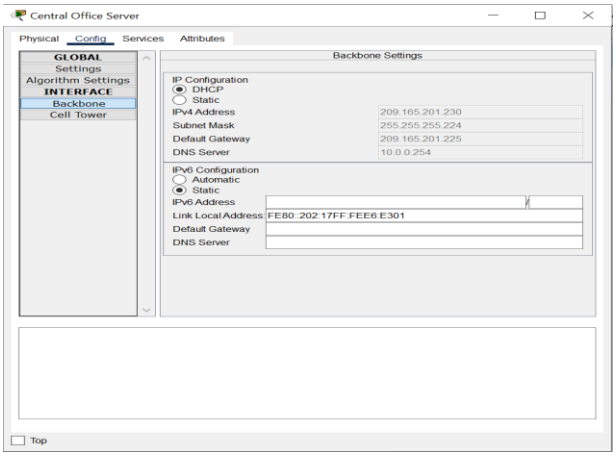


Figure III-11:Backbone interface DHCP enabling.

Backbone Interface: This interface is connected to the Internet Service Provider (ISP) and will automatically obtain a dynamic IP address once the DHCP protocol is enabled, as illustrated in the Figure *III-12*.

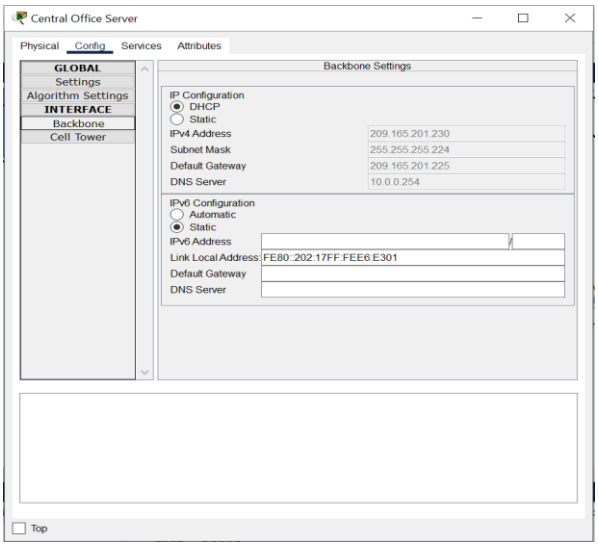


Figure III-12:Backbone interface configuration.

Cell tower interface: This interface manages wireless communication with user devices via 3G/4G. protocols, assigning static IPs. IT connects the CO server to cell towers via protocols (e.g., S1/N2) for data/control traffic.as illustrated in the figure.

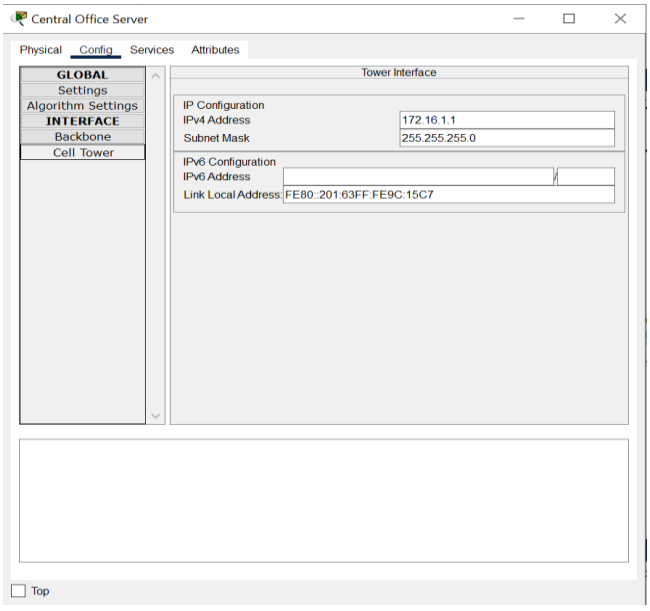


Figure III-13Cell tower interface configuration.

– **Modem**

Once the Ethernet cable and coaxial cable are connected, the modem operates automatically without need for extra configuration.

– **3G/4G Client**

When the smartphone is added to the simulation workspace, it initiates a connection to the cellular tower using 3G/4G protocols, leveraging the tower's coverage to register itself on the cellular network. The tower's integrated DHCP server dynamically assigns the smartphone a public IP address, enabling it to establish a secure communication channel with the IoT server via encrypted HTTPS or MQTT protocols. Once authenticated by the IoT server through pre-configured credentials or token-based authorization, the smartphone gains access to the server's dashboard or API, which acts as a centralized interface for managing connected devices (e.g., lights, sensors, cameras). Users can then send commands (e.g., "unlock garage door" or "adjust thermostat") through the smartphone's interface, which are routed via the cellular network to the IoT server. The server processes these requests, validates permissions, and relays instructions to the target devices, ensuring real-time control and monitoring. This end-to-end connectivity demonstrates the seamless integration of mobile devices into the smart home ecosystem, even when operating outside local Wi-Fi boundaries

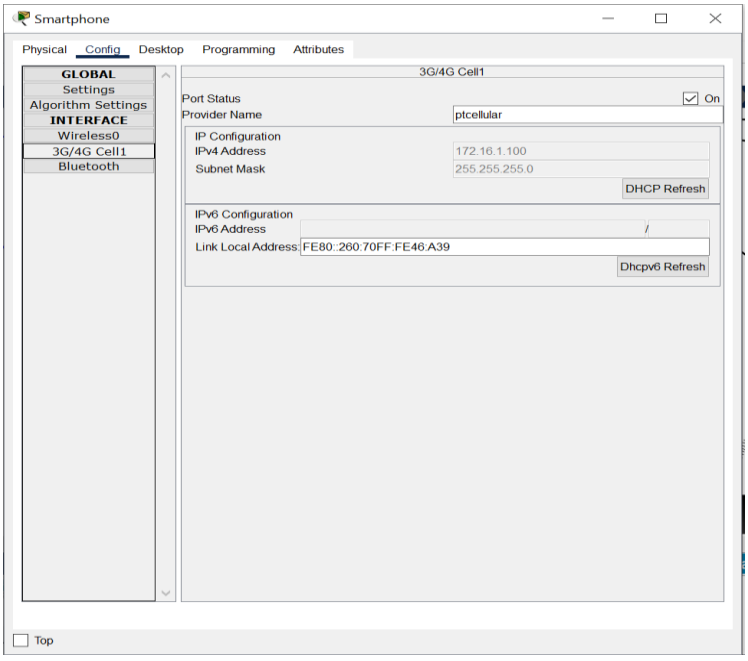


Figure III-14:3G/4G cell configuration

III.8 Home

As already described in section 2.8 of chapter 2, our home consists of 5 parts: front yard, garage, living room, bedroom, and kitchen. Figure shows the topology of our home design created using packet tracer software, and the way these devices are connected will be explained in the coming subsections.

III.8.1 Home Gateway setting

We deployed four Home Gateways, each equipped with three interfaces: an Internet interface, a LAN (Local Area Network) interface, and a wireless interface.

- **Internet interface**

This interface serves as the connection between the home network and the internet through the modem. As it is linked to the Internet Service Provider (ISP), selecting DHCP from the Internet The Settings tab enables each Home Gateway interface to automatically obtain a dynamic IP address from an available pool. The default gateway is set to 209.165.200.225, and the DNS server is 10.0.0.254, as illustrated in the coming figures.

- **LAN Interfaces**

In this project, the household appliances are equipped with wireless interfaces, and the home network operates as a Wireless Local Area Network (WLAN).

- **Wireless Interface**

Through the Wireless Interface Configuration tab, a Service Set Identifier (SSID) and a custom password (12345678) can be defined to facilitate the simulation process. This configuration was applied to all Home Gateways, each assigned a unique SSID.As illustrated in the figures. **Home gateway 0**

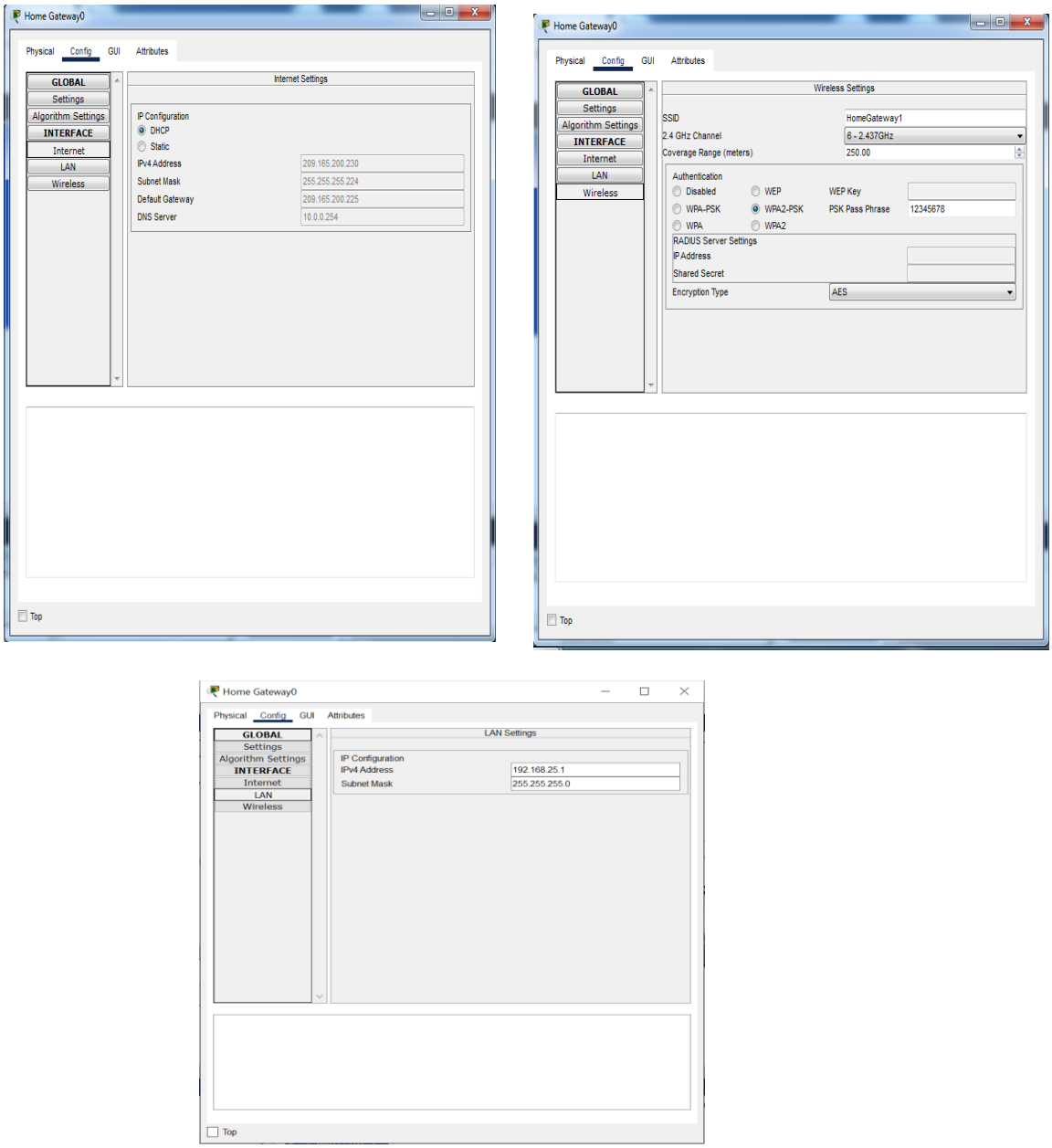


Figure III-15:Home gateway 0 interfaces

After configuring the primary gateway, the same settings (IP addressing) are replicated across the four other gateways.

III.8.2 Home Router setting

Similar to home gateways, the home router is deployed with three primary interfaces: an Internet-facing interface, a LAN interface, and six wireless interfaces (e.g., wireless 2.4G, wireless 5G(1), wireless 5G(2), wireless Guest 2.4G, wireless Guest 5G(1), and wireless Guest 5G(2)) to accommodate diverse connectivity standards and IoT devices seamlessly.

Wireless Interface (2.4G)

The 2.4 GHz wireless band was used to configure the home router, with the "Wireless Interface Configuration" tab enabling the setup of a Service Set Identifier (SSID) and a custom password (12345678) to streamline the simulation process.A unique SSID was assigned to distinguish the network and ensure secure connectivity, as shown in the accompanying figure, which illustrates the bandwidth and encryption settings (WPA2-PSK).

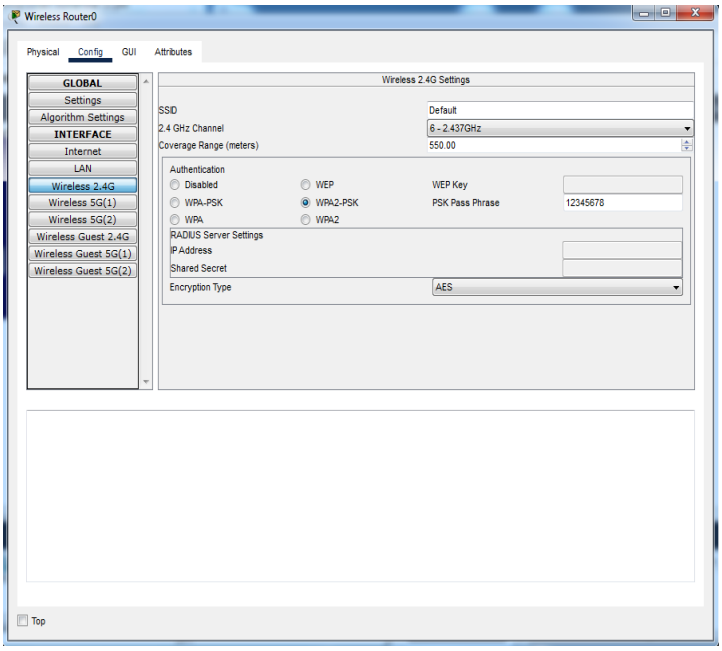


Figure III-16:Home router wireless interface configuration

III.9 IoT Devices Configuration:

III.9.1 Wireless interface

By default, IoT devices in Cisco Packet Tracer have an Ethernet NIC, which needs a cable to connect to the home gateway, so we need to change the NIC for all devices to allow them to connect via a wireless interface.

To install a wireless network card:

1. Open the device’s advanced settings (refer to the figure).
2. Navigate to the Input/ Output Configuration tab.
3. Each device supports up to two network cards. For the network adapter, select PT-IOTNM-1W.

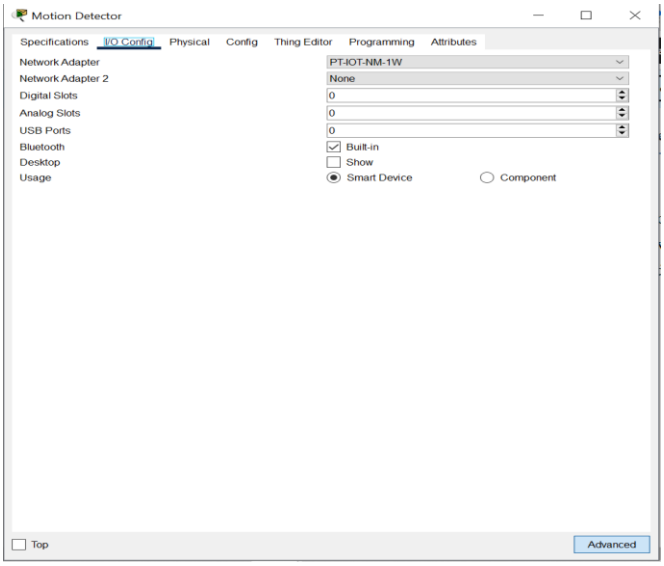


Figure III-17:I/O Config TAB of Motion detector .

III.9.2 Connecting devices to the Internet

Once we type “HomeGateway” in the SSID field in the wireless0 interface from the config TAB, the interface connects to the home gateway as illustrated in figure 3.17. We have said before that our home gateway works as a DHCP server.

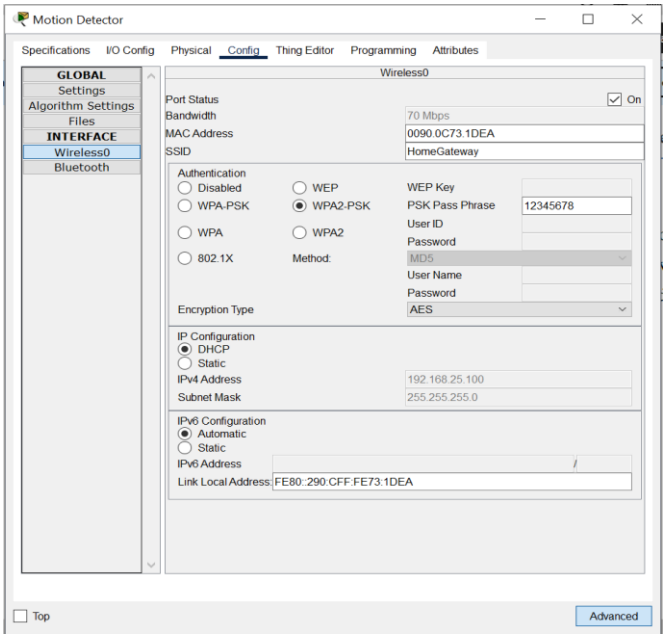


Figure III-18:wireless0 interface config TAB.

In the same way as home router Once we type “Default” in the SSID field in the wireless0 interface from the config TAB, the interface connects to the home gateway as Once each device is

assigned a unique IP address and DNS configuration, it becomes connected to the Internet, as illustrated in the figure.

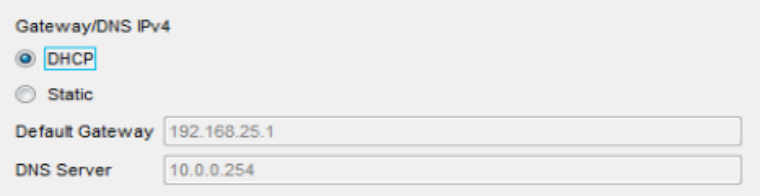


Figure III-19:Devices' default gateway and DNS server addresses

– **Registration server**

To allow your smartphone to access and control all connected home devices, it is necessary to register each device with an Internet of Things (IoT) server. This process involves entering the server address, username, and password. Navigate to the REMOTE SERVER tab for each individual device, and input the required credentials: server address, username, and password, as needed and then press “connect” .Figure illustrated in the figure below.

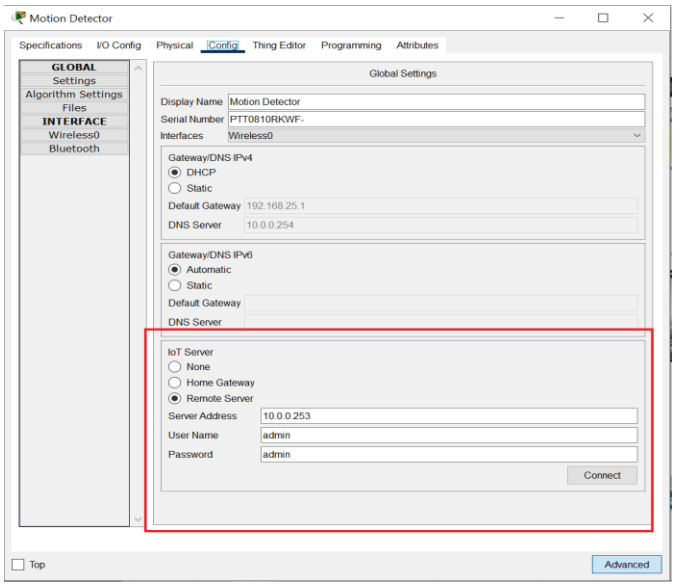


Figure III-20:Authentication of devices in iot server

Authentication process for each field device connecting to the IoT server. Remote home monitoring via mobile phone becomes possible after successfully registering the devices on the server. This can be achieved either through the browser at **"safa.com"** or via the IoT Monitor application. Through these platforms, users can view the status of all registered devices, as illustrated in the following figure.

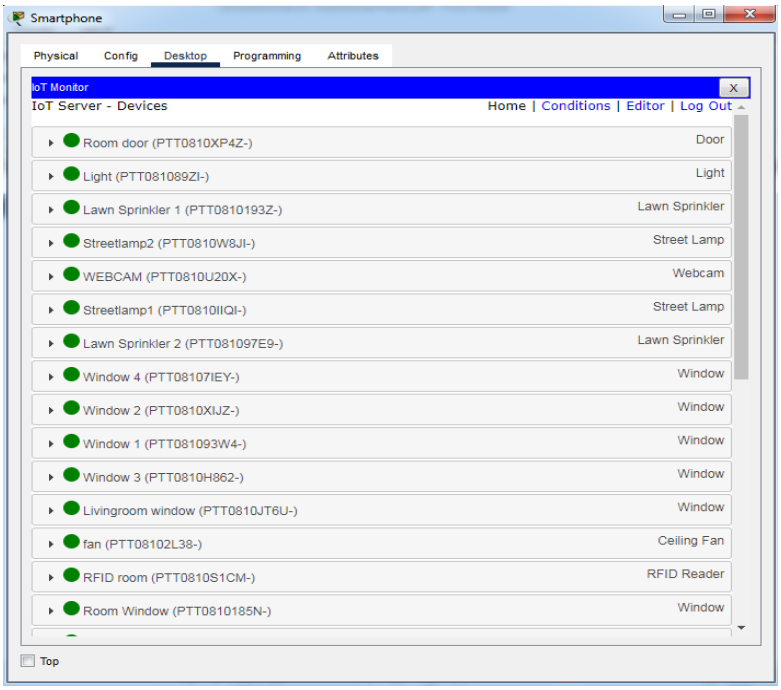


Figure III-21: overview of IoT devices registered on the IoT server.

This TAB (shown in figure) allows the owner to supervise some devices, whether they are working or not, and see some devices that provide useful information. From this TAB also, the owner can interact with devices directly, if the device has the property of direct use.

III.10 Interaction between Devices:

III.11 The Garage:

For the system shown in Figure, the RFID (garage security), smart garage, street lamps, and smoke detector can be registered in the IoT server. To manage garage security via RFID, specific conditions must be configured in the IoT server. Authorized RFID card (ID 100) must be registered in the server, with access permissions configured based on these IDs.

The garage can also be opened by the smoke detector triggered by the exhaust smoke of the authorized vehicle. Additionally, this section includes two streetlights for improved external illumination.

Figure III-22 illustrates the physical layout of devices positioned around the garage door.

This figure inside the garage cluster

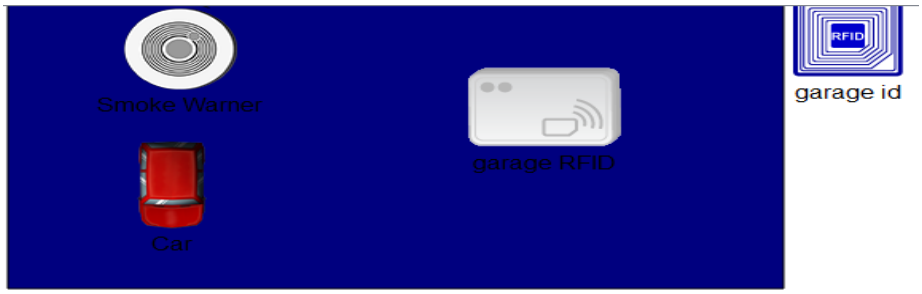


Figure III-23:Distribution of devices around the garage door area within an internal cluster.

III.11.1 Implementation:

The devices, including a smoke detector, card reader, garage door opener, and RFID reader, were installed in the designated area and connected via a wireless network. To ensure secure access to the garage using RFID technology, specific conditions must be configured on the IoT server, allowing only a single authorized card to operate the garage door. The adjacent figure illustrates the RFID card activation process.

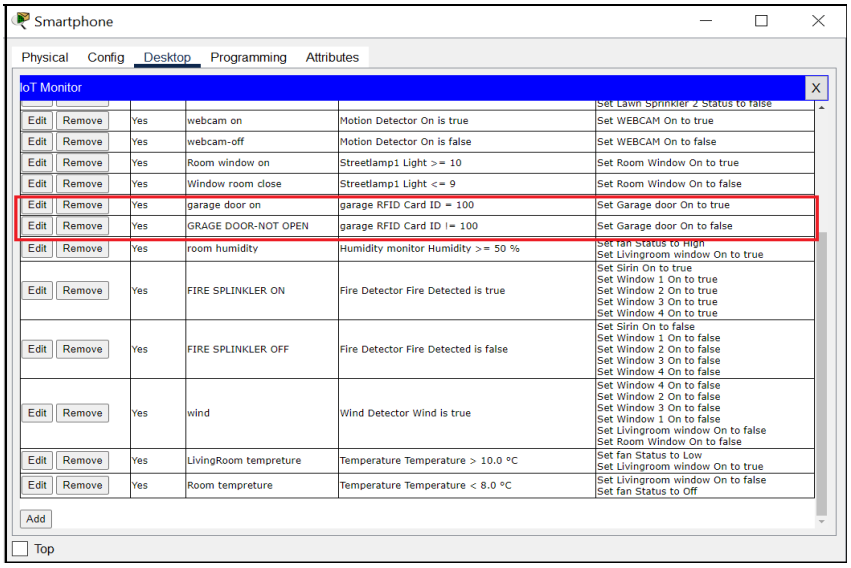


Figure III-24:The rule governing garage door operation

III.11.2 Garage Security Algorithm

1. **RFID Detection:** Reader activates when a card is within proximity.

2. **ID Validation:** Checks if card ID is authorized (e.g., ID 100).

3. **Signal to Server:** Sends "Valid" signal if authorized; "Invalid" if not.

4. **Door Action:** Server opens garage on "Valid"; remains closed on "Invalid".

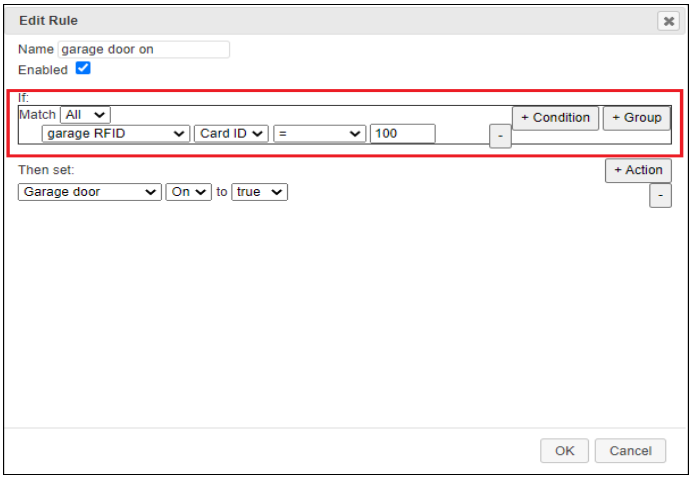


Figure III-25:Procedure for Activating the Garage Door via RFID Reader

In this Figure *III-25*the garage door access control rule is a system that was configured to verify the ID card number presented at the entry point. Specifically, ID card number 100 was designated as an authorized user within the access control list. When this particular card is scanned, the system recognizes it as valid and grants access.

Consequently, the system automatically transmits an 'open' command, represented as a Boolean value of true, to the door mechanism. This signal prompts the mechanism to unlock or open the garage door, thereby enabling authorized entry.

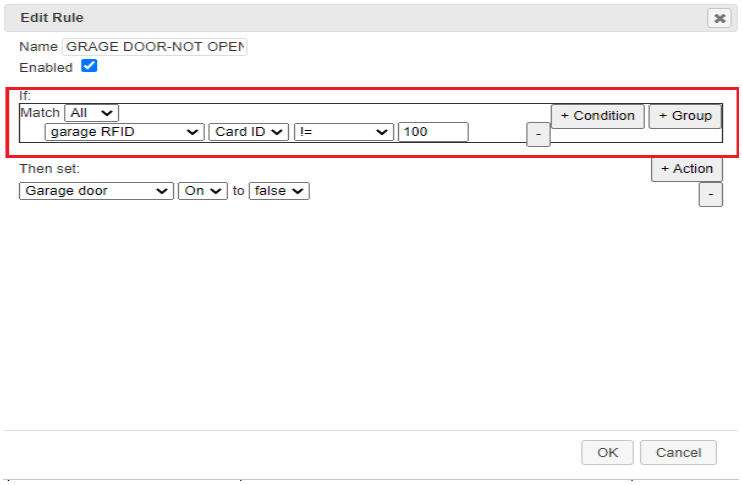


Figure III-26:Procedure for Closing the Garage Door via RFID Authentication

In this aspect of the access control rule, any ID card number other than 100 is classified as unauthorized. This means that when a person attempts to access the garage using an ID card not explicitly listed as authorized (not card number 100), the system does not recognize the card as valid. As a result, the system generates and sends a command with a Boolean value of false to the door mechanism. This 'false' signal indicates that access should be denied. Consequently, the door remains locked or closed, effectively preventing entry. This approach ensures that only individuals with authorized credentials can operate the garage door, reinforcing the security of the access control system.

III.11.3 Testing the rules of the garage door

When the authorized RFID card is brought close to the reader, the system identifies the card's unique code. If the code is valid, a signal is sent to activate the garage door mechanism, causing the door to

open automatically. This process provides a secure and convenient method for access control. The following figure visually demonstrates how the garage door responds upon detecting the RFID card.

The garage, by default, is closed as shown in Figure *III-27*:

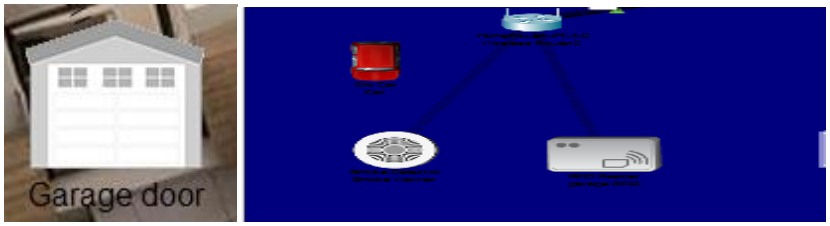


Figure III-27:The garage door is in a closed position

After check the Id card , it turns green as illustrated in figure and opens the garage.

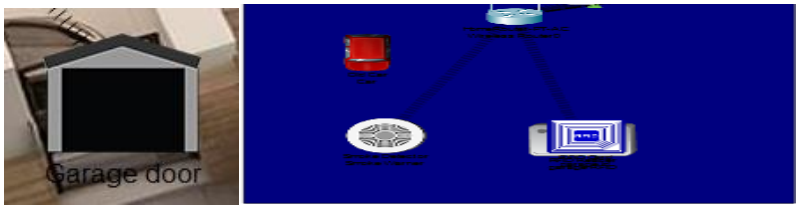


Figure III-28:Garage door status post ID card verification.

III.11.4 Smoke Detection Algorithm

1. **Smoke Monitoring:** Detector measures smoke density (e.g., ppm).

2. **Threshold Check:** If smoke > 0.01 ppm, trigger "Emergency Alarm".

3. **Emergency Action:** Server opens garage (overrides security) and alerts users.

4. **Normal State:** If smoke ≤ 0.01 ppm, garage operates via RFID security.

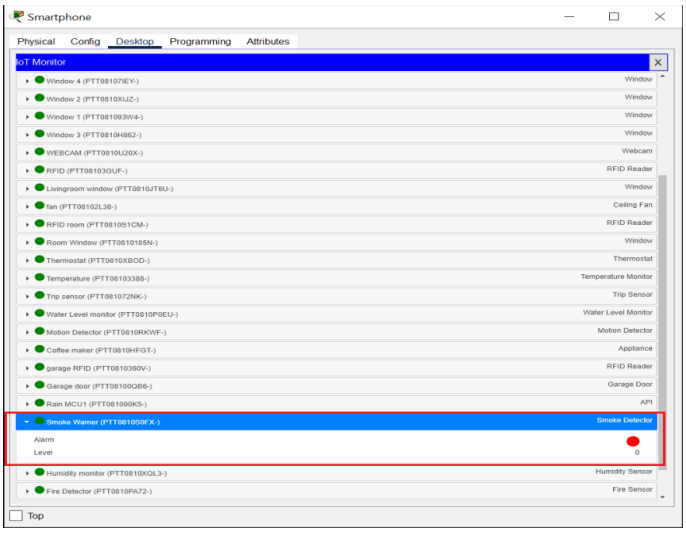


Figure III-29:Visualization of the smoke detector via the smartphone IoT monitoring application.

The smartphone's IoT Monitor interface displays connected devices, including the strategically placed smoke detector (PTT08106SFX) in the garage, which specifically monitors for emissions from the older vehicle. This critical safety component provides early warning of potential smoke buildup or engine combustion issues from vintage vehicles that may produce more exhaust particulates or experience fuel system leaks. The zero reading on the "Level" indicator confirms normal conditions, while the red alarm indicator shows the system is properly armed.

Scenario 1: if there is a smoke inside the garage

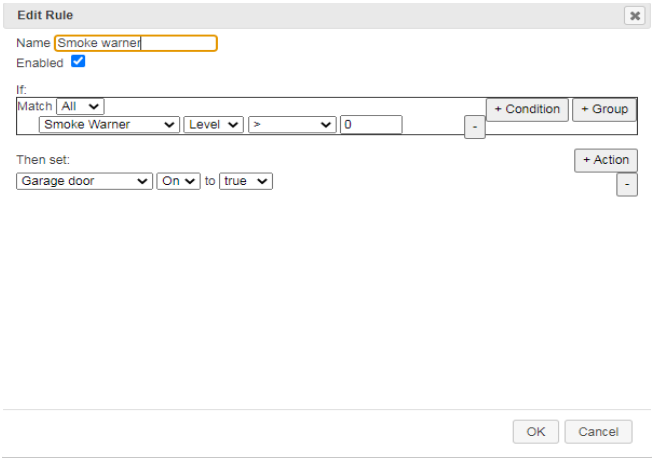


Figure III-30:Procedure for Activating the Garage Door via Smoke Detection

This rule represents an automated safety response integrated within a smart home system. It utilizes a smoke detector, referred to as "Smoke Warner," which continuously monitors the surrounding environment for any indication of smoke. When the sensor detects a smoke level greater than zero potentially resulting from exhaust emissions produced by an old vehicle, the system is programmed to automatically trigger a predefined action: opening the garage door by setting its operational state to "On" (true). The primary objective of this response is to enhance safety by enabling ventilation, thereby reducing the concentration of potentially harmful gases and allowing fresh air to circulate.

Scenario 2: If there is no smoke

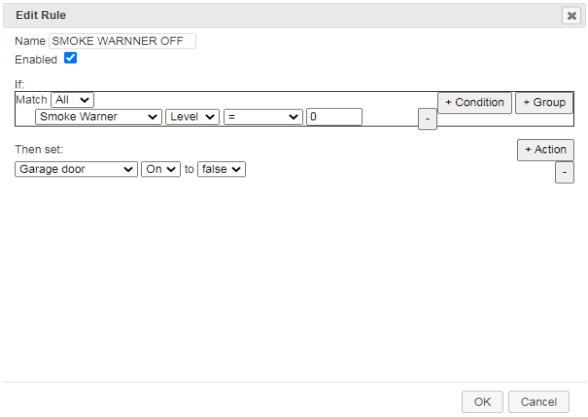


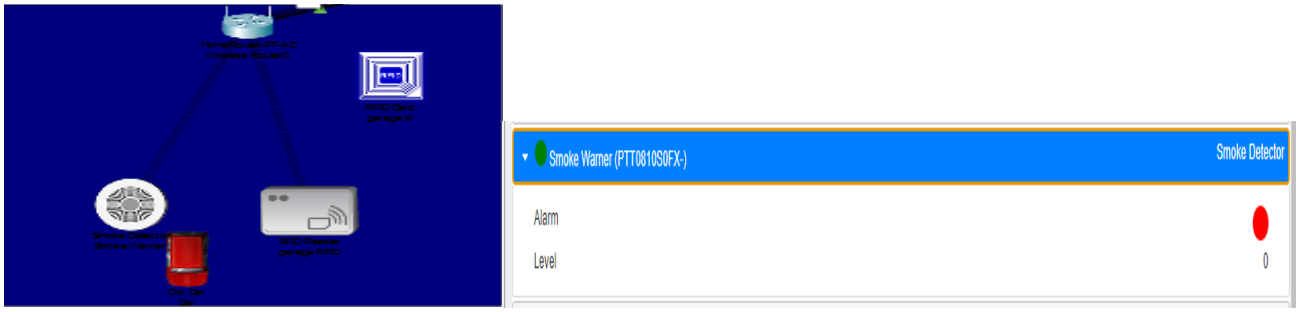
Figure III-31:Procedure for Securing the Garage Door via Smoke Detector Activation

In this Figure *III-31* When the sensor detects a smoke level equal to zero, indicating the absence of any emissions from an old vehicle’s exhaust, the system is programmed to automatically activate a predefined action: closing the garage door by setting the stop state to 'Off' (false). The main goal of this response is to enhance the safety of the garage against theft or damage.

III.11.5 Test and result of the smoke detector

By pressing the Alt button installed in the old car, a wireless signal is transmitted to initiate two simultaneous actions. First, the car's engine is activated. Second, the garage door receives a signal to open automatically, ensuring smooth and synchronized access.

Scenario 1: When there is no smoke inside the garage



The door by default close

Figure III-32:Structural state of the garage door in the absence of smoke.

Scenario 2: When there is smoke inside the garage

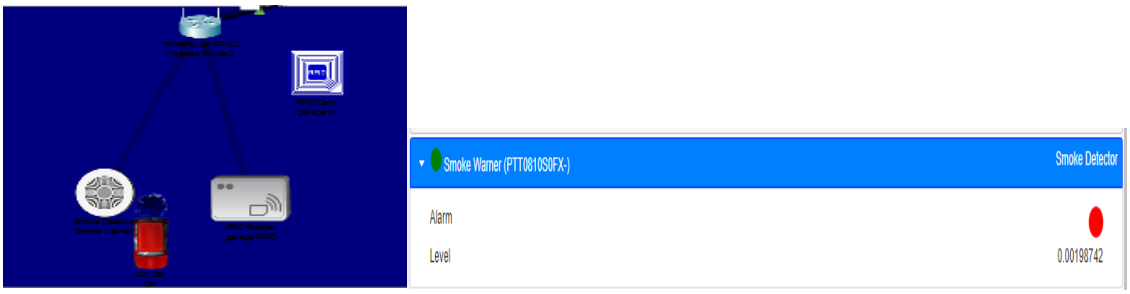


Figure III-33:Structural state of the garage door in the presence of smoke.

III.11.6 Street lamps

Street lamps are simulated as IoT devices that monitor and control lighting via network protocols (e.g., MQTT/CoAP). Their configurations include sensor thresholds (e.g., light intensity) were configured to respond to ambient sunlight levels.

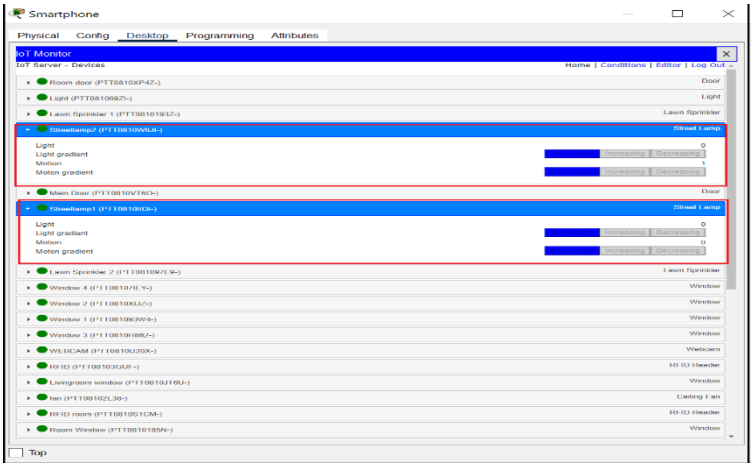


Figure III-34:Street lamp management via the IoT-enabled control interface

The smartphone interface displays the IoT with expanded controls for two street lamps (Streetlamp1 and Streetlamp2) that enhance the smart home's exterior system. These intelligent lighting fixtures incorporate both illumination and motion detection capabilities, as shown by their configuration panels with adjustable light and motion gradient settings.

The street lamp interface reveals sophisticated control modes through the "Increasing," "Decreasing," and implicit "No Change" states for both light and motion parameters. These adaptive settings allow the lamps to respond dynamically to environmental conditions rather than operating in simple on/off states.

The light gradient controls enable automatic brightness adjustment, with "Increasing" mode gradually intensifying illumination as ambient light fades, while "Decreasing" mode dims lights to conserve energy when natural light is sufficient. Similarly, the motion gradient settings determine sensitivity levels - "Increasing" mode gradually heightens motion detection sensitivity during nighttime hours, while "Decreasing" reduces it during high-traffic periods to prevent false alarms.When neither option is selected (effectively "No Change" mode), the system maintains constant settings.

-Sunlight curve

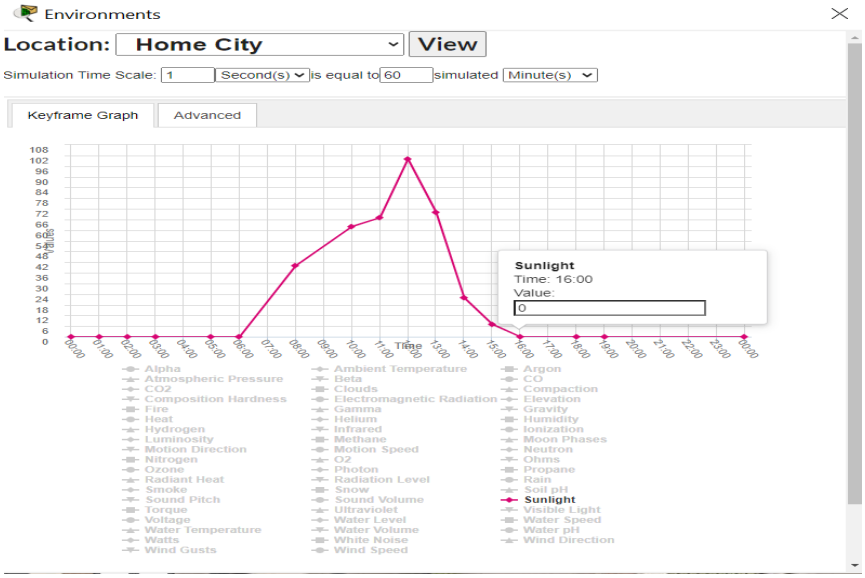


Figure III-35:Sunlight incidence curve over time

This curve represents the variation in sunlight intensity throughout the day and can be used to automatically control the operation of street lamps. In the early morning hours, from 6:00 AM to 8:00 AM, the sunlight level is very low, which means the street lamps should be on to provide the necessary lighting. From 8:00 AM to 12:00 PM, the light intensity gradually increases, so the lamps can be dimmed or turned off gradually. At midday (around 12:00 PM), the sunlight reaches its peak, and the lamps should be completely turned off. Then, from 1:00 PM to 5:00 PM, the sunlight starts to decrease gradually, which requires the lamps to be turned on again step by step. After 5:00 PM until night, the sunlight becomes very low once more, so the lamps should be fully turned on. This control process is done using a light sensor that reads the sunlight intensity and automatically determines when the lamps should be switched on or off, depending on the natural light throughout the day.

III.11.7 Testing street lamps with the environment

We will evaluate different scenarios at different times: 6 AM, 9 AM, 16PM, and 19 PM

– **Lamp street in 6 AM**

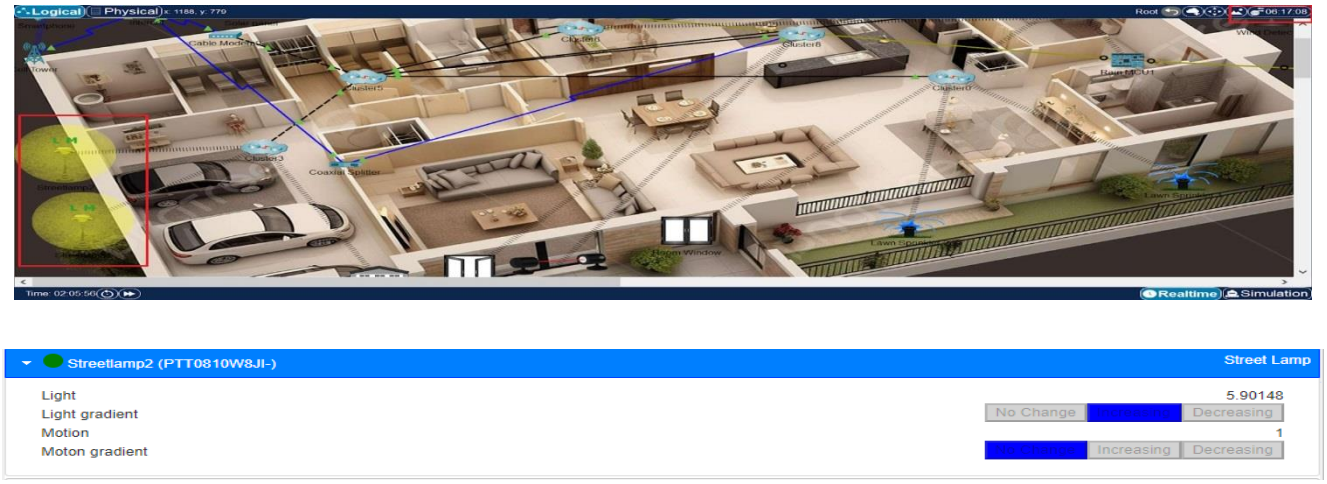


Figure III-36:Status of the street lamps during nighttime conditions

The street lamps employ an adaptive dimming algorithm, where illumination intensity inversely correlates with ambient sunlight levels (as per historical luminosity curves). As sunlight increases, the system dynamically reduces lamp brightness via calibrated, time-synchronized protocols (e.g., MQTT/CoAP), ensuring seamless transitions that align with environmental conditions while optimizing energy efficiency and adhering to predefined safety thresholds.

– **At 9AM**

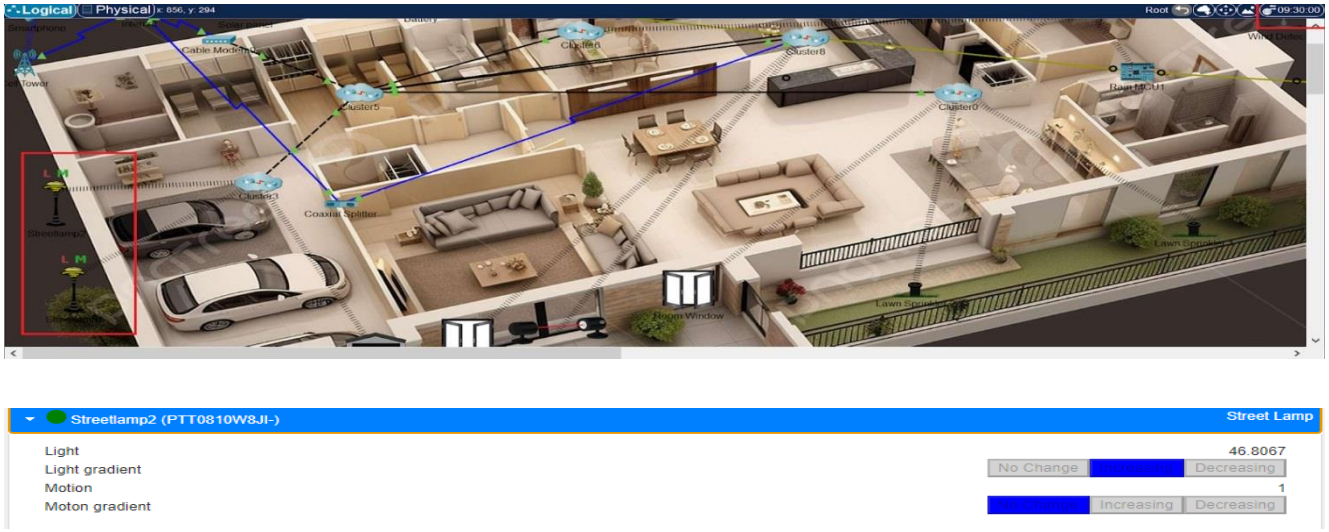


Figure III-37:Status of the street lamps at 9:00 AM

The street lamps are programmatically deactivated at 09:00 (9 AM) following a predefined schedule integrated into the IoT server, synchronized with real-time sunlight sensor data confirming sufficient ambient light levels (e.g., ≥ 200 lux). This ensures energy conservation during daylight hours while maintaining compatibility with dynamic environmental conditionsAnd the smartphone detected decreasing at 16 PM

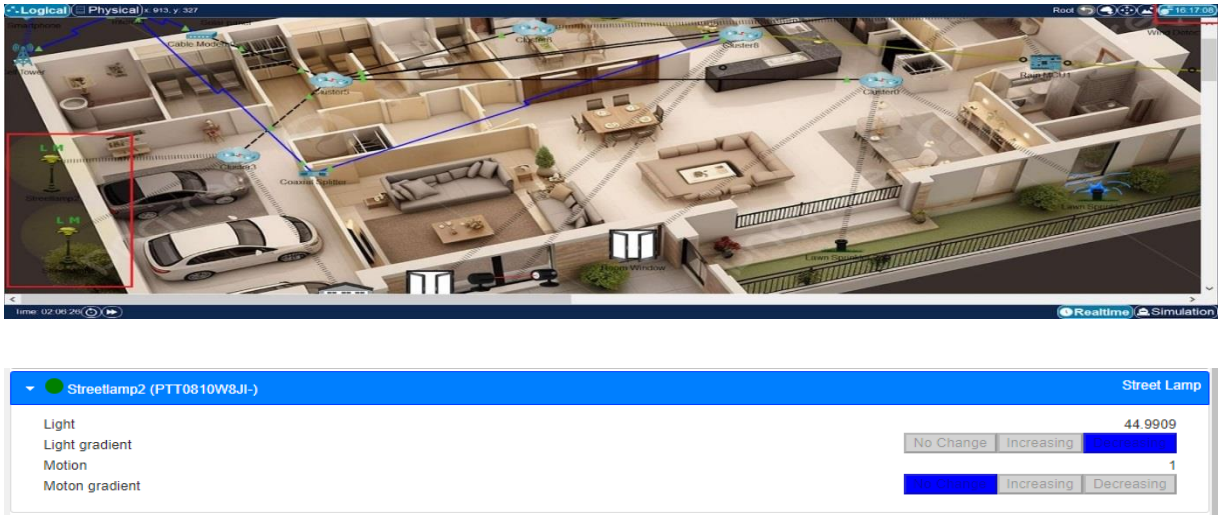


Figure III-38:: Street lamp status on16 PM

The street lamps activate at 16:00 (4 PM) at full intensity (90%) and initiate a gradual dimming protocol, reducing brightness incrementally until midnight (24:00/12 AM) to align with energy optimization strategies and reduced nighttime activity.

-19 PM

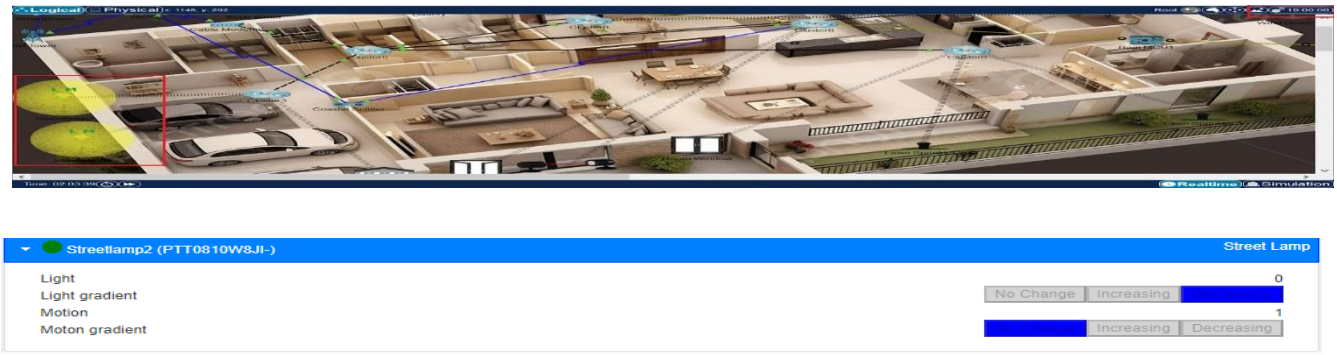


Figure III-39:status of the street lamps at 19 PM

The street lamps are autonomously activated when ambient sunlight levels diminish to 0% (full darkness), as detected by calibrated light intensity sensors, ensuring illumination aligns precisely with environmental conditions.

III.12 The kitchen:

The kitchen is equipped with an alarm system, a fire sprinkler, a fire detector, a coffee machine, and four windows. Outside, there is a wind detector.

In the event of a fire, the fire detector identifies the hazard and triggers three actions: activating the sprinkler system, sounding the alarm, and automatically opening the kitchen windows to vent smoke. However, if the wind detector (located outside) senses strong gusts, it overrides the window-opening mechanism to prevent fire spread, closing the windows immediately. Meanwhile, the coffee machine can be operated remotely via a smart device or manually by pressing a dedicated button labeled Alt.The figure illustrate the kitchen cluster

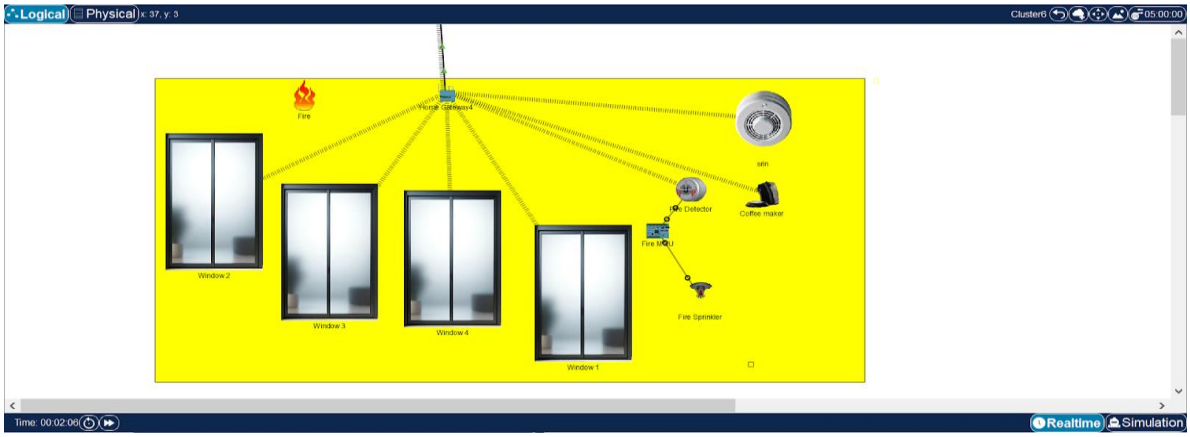


Figure III-40:Kitchen design within the cluster area

III.12.1 Implementation:

The windows, siren, fire detector, coffee machine, and wind sensor were wirelessly integrated into the network infrastructure.

III.12.2 Fire system

The fire detection unit and sprinkler system are connected to the microcontroller unit (MCU) via a dedicated Internet of Things (IoT) cable, with port D0 linked to the fire detector's D0 terminal and port D1 connected to the D0 terminal of the sprinkler system. The control unit was programmed using JavaScript instructions, as illustrated in Figure *III-41*to activate the sprinkler system in the event of fire detection. The accompanying figure presents the operational logic, detailing the corresponding actions and conditions for system activation.

Steps to programming the MCU:

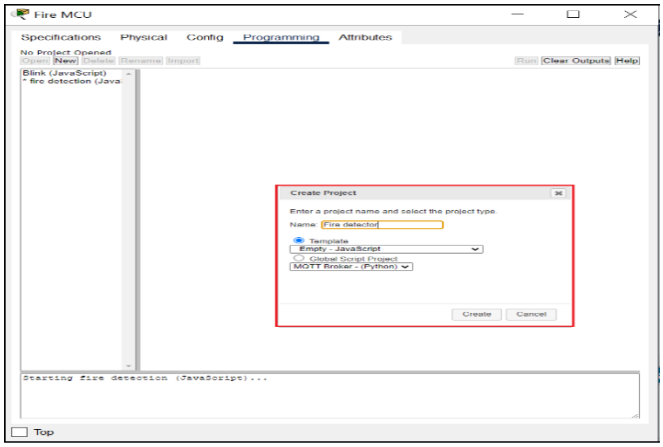


Figure III-41:Application Programming Interface

Create a new project named "Fire detector" with two available programming options using a JavaScript template or implementing a Python-based MQTT Broker global script.

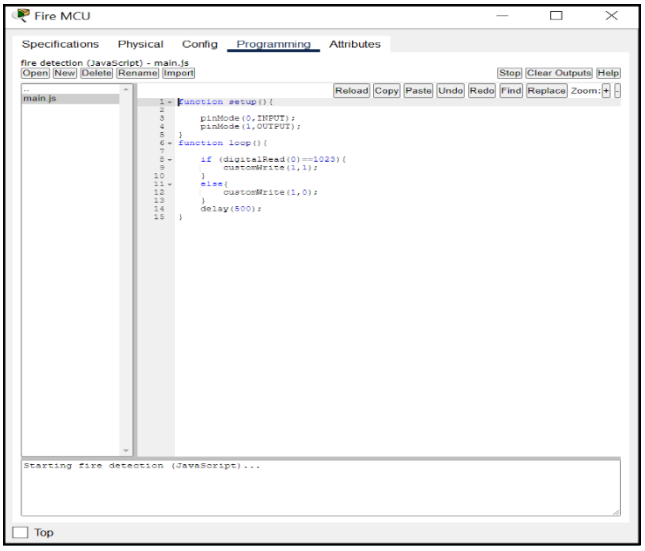


Figure III-42:Fire MCU programming

This program is designed to control the activation of water sprinklers based on input signals from a fire sensor connected to a control unit. Port 0 is configured as an input to receive signals from the fire sensor, while Port 1 functions as an output to trigger the sprinkler system. When a maximum signal value (1023) is detected on Port 0, Port 1 is activated to initiate the sprinkler. If any other value is read, the output is deactivated. This operation is executed at 500 millisecond intervals, ensuring a continuous and automatic response in accordance with the fire sensor's status.

– **The rules**

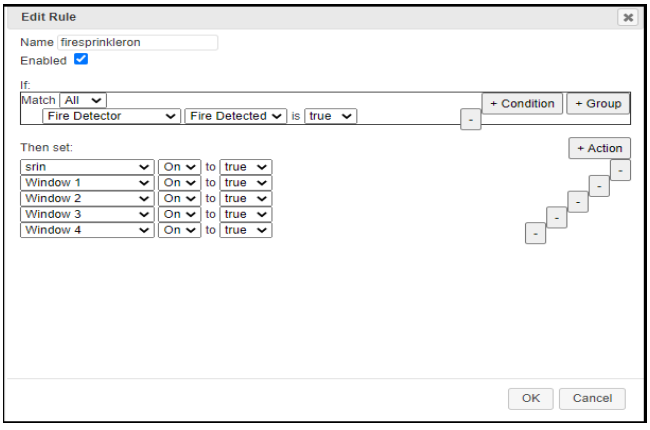


Figure III-43:System Actions Triggered by Fire sprinkler Activation

This form specifies the requirements for activating the sprinkler and alarm systems in the event of a fire in the kitchen. When the fire detector signals a fire (True), all four windows open and the siren is activated (true).

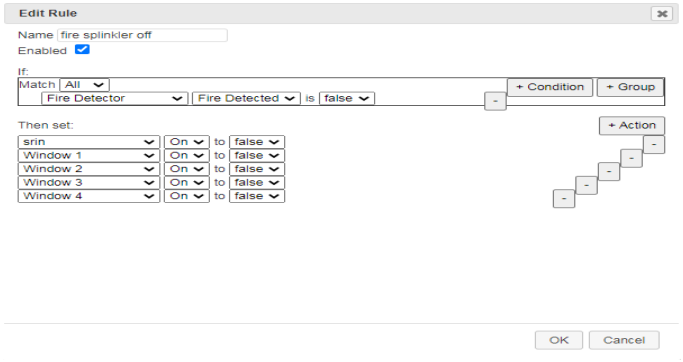


Figure III-44:System Actions Triggered by Fire sprinkler Deactivation

This form outlines the requirements for shutting down the sprinkler and alarm systems when no fire is detected in the kitchen. If the fire detector indicates no fire (false), all four windows are closed and the alarm siren is turned off (false).

III.12.3 Testing The Fire System:

Scenario 1 :

When a fire source is placed in front of the fire sensor, both the fire sprinkler system and the alarm siren are activated. Additionally, these systems can be monitored and controlled remotely. The following figure.

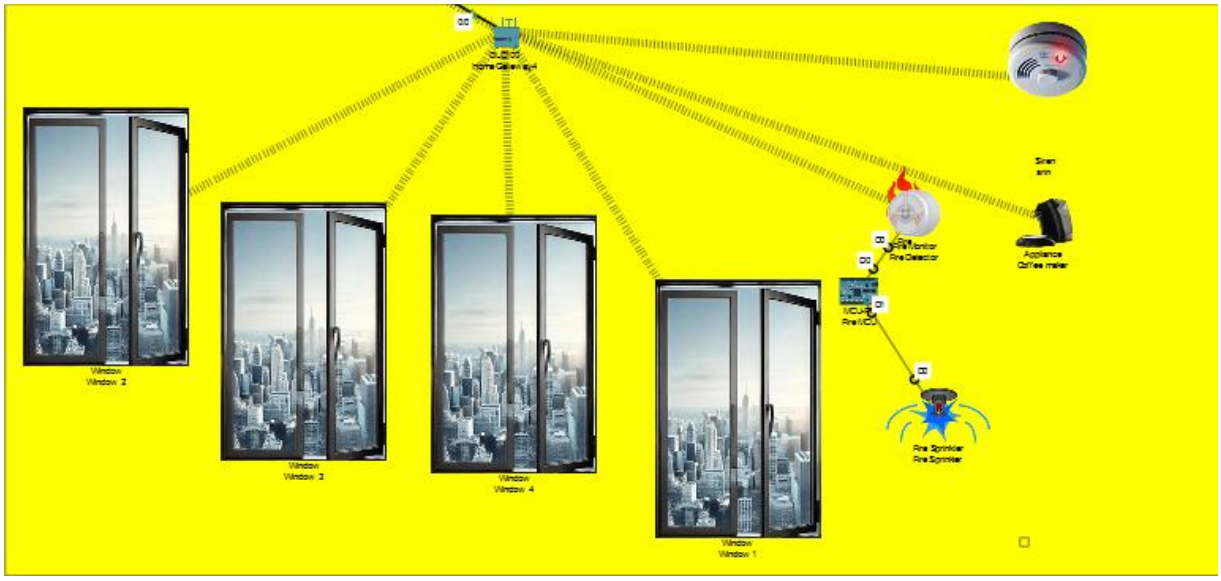


Figure III-45:Kitchen environment during fire exposure in the logical space

Figure III-46:Kitchen environment during fire exposure in the Physical space

Scenario 2:

When the fire source in front of the fire sensor is eliminated, the fire sprinkler system and siren are automatically deactivated. Furthermore, these systems support remote monitoring and control, as illustrated in the figure below.

Figure III-47: Kitchen environment under normal conditions within the physical space.

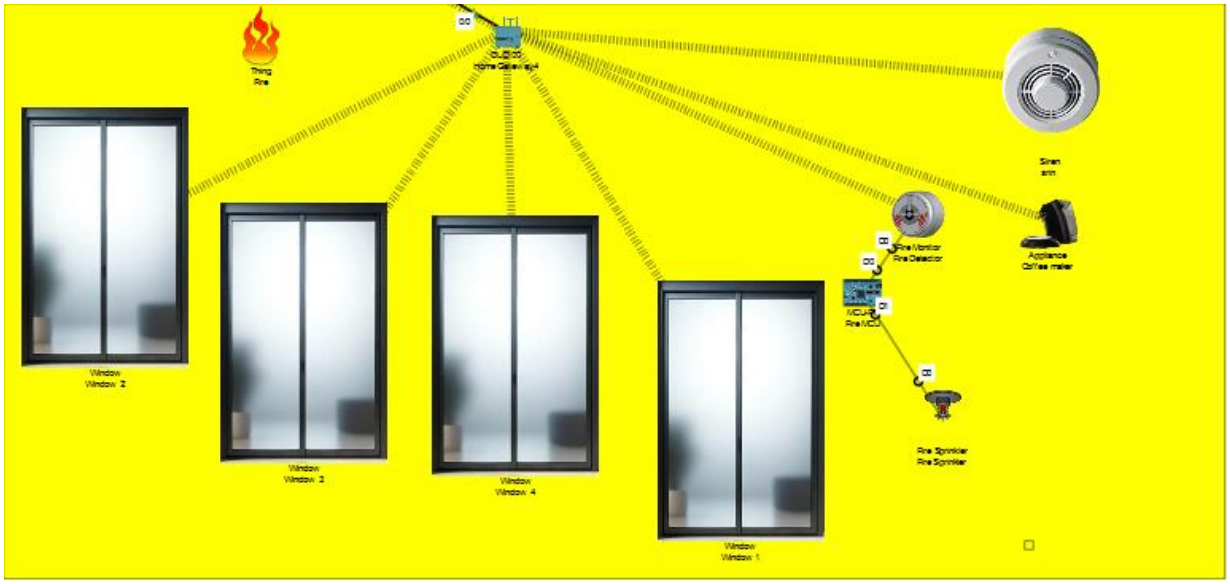


Figure III-48:Kitchen environment under normal conditions within the logical space

III.12.4 Wind Detector

The window actuation mechanism is engineered to close automatically upon detecting elevated wind speeds, as governed by the operational thresholds and logic defined in Figure (A). This conditional response is directly contingent on real-time environmental data transmitted by a wind sensor mounted externally on the smart home's exterior. The sensor's readings are processed by the central control system, which executes the predefined protocol to override any conflicting commands fire-

triggered window openings and ensures immediate closure when wind velocities exceed permissible limits. Figure *III-49* delineates the operational rules embedded within the IoT server's logic, defining conditional actions.

Figure III-49:Procedure for closing windows when wind is detected.

This outlines the operational requirements for the wind detector. When the wind detector registers the presence of wind (true), all windows in the house are required to be closed (false).

The graph in Figure *III-50* displays real-time fluctuations in wind gust intensity across the smart home system's external environment.

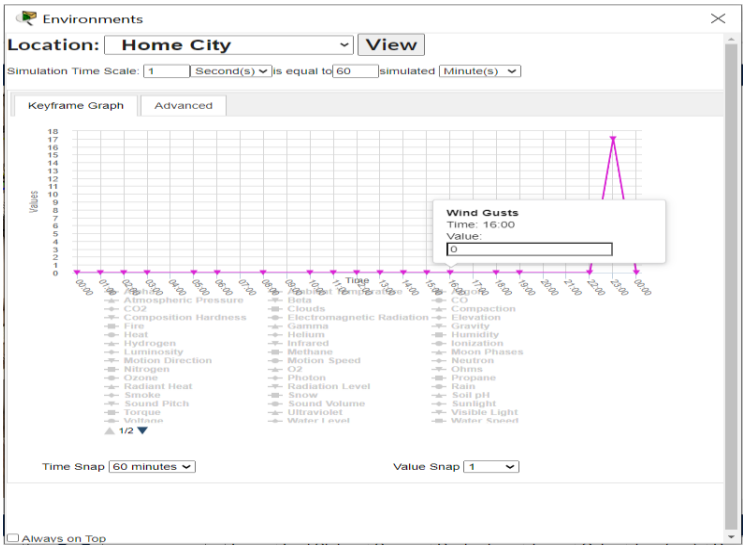


Figure III-50::Wind Gusts variation curve with time

The Environments configuration window displays the wind gust simulation for Home City, with a time compression ratio of 1:60 (1 second equals 60 simulated minutes). The keyframe graph reveals elevated wind speeds from 1:00 AM through most of the day, followed by a period of calm extending until 22:00 PM, after which wind activity resumes between 22:00 PM and midnight.

III.12.5 Testing the wind detector

Scenario 1: the wind detector during the day

Figure III-51:Wind detector status

Scenario2: the wind detector at 22 pm

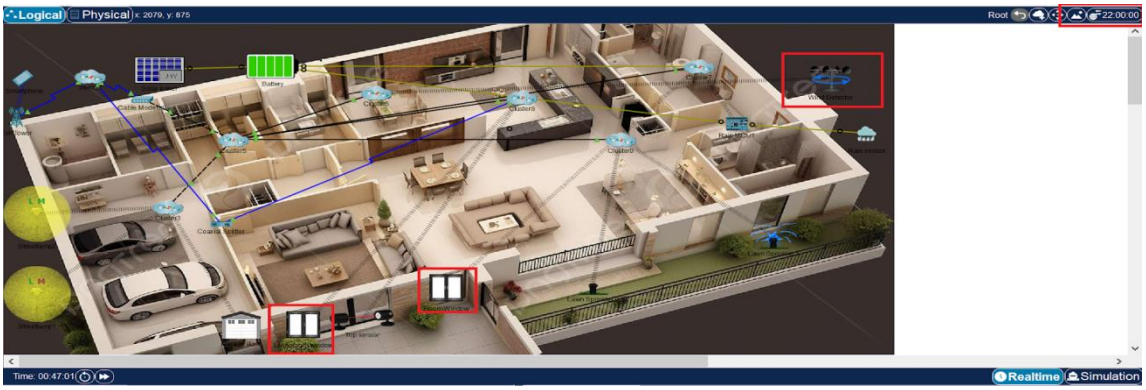


Figure III-52:Status of window at 22: The kitchen windows

The windows automatically close in response to the presence of wind in the environment.

Figure III-53:Evaluation of the kitchen windows' condition within the cluster under wind influence.

III.12.6 Coffee machine

Packet Tracer has another IoT device, which is a coffee machine; it can be registered in the server. When we access the IoT server account, we can turn it on to prepare a coffee, as shown in Figure *III-54*

The coffee maker is an example of a simple appliance; it can, for sure, be manually turned ON and OFF. Then, like the others, a click on the red rectangle will turn it green and start the appliance to make coffee; a red led will appear in the bottom-left of the appliance if it is ON

Scenario 1: enabling the coffee machine

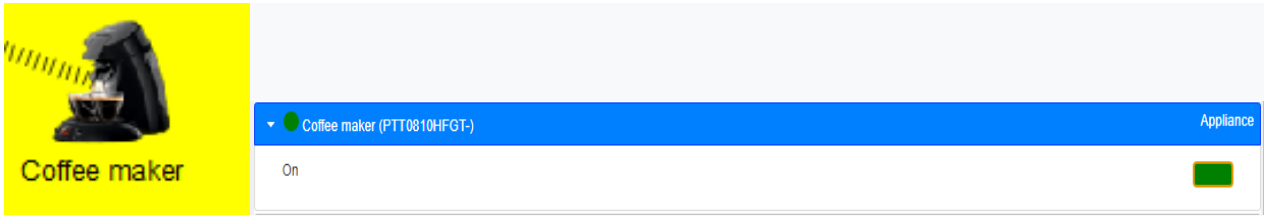


Figure III-54:The coffee machine is enabling.

The coffee machine is manually activated by pressing the "Alt" button.

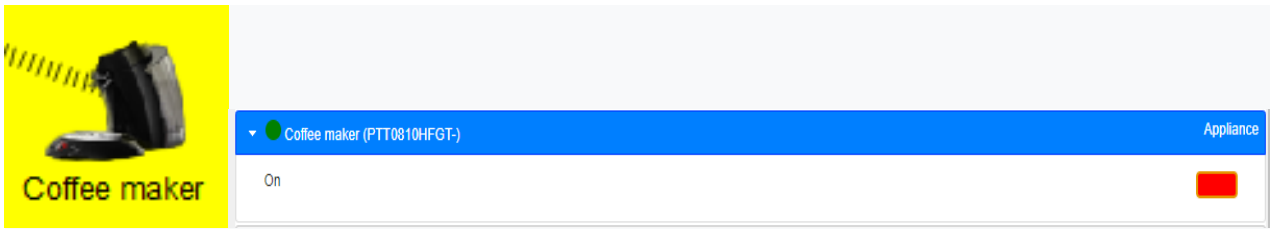


Figure III-55:The coffee machine closed

III.13 The BedRoom

Now we move to the bedroom, which has been designed with several smart features aimed at enhancing both comfort and security. The room includes a lamp powered by a battery, allowing it to function independently of the main power supply, a useful feature during power outages or for energy efficiency. Additionally, the bedroom is equipped with both an air conditioner and a heater, which can be controlled through a thermostat with specific temperature settings or operated via remote access. This allows residents to manually adjust the room temperature to their preferred comfort level as needed, rather than relying on automatic temperature regulation.For security and controlled access, the room features a door equipped with an RFID-based access control system. A card reader installed near the door reads RFID tags and determines whether access should be granted or denied. In this setup, two RFID cards are used for demonstration purposes: the first card is registered under the name Safa and is authorized to open the door, allowing entry. The second card, registered under the name Amira, is unauthorized, and thus access is denied when it is presented.

Figure III-56:Room layout in physical space.

III.13.1 Implementation

III.13.2 The room door

A door lock, an RFID reader, and RFID cards are all connected to a central gateway. When a user scans their RFID card, the reader identifies them, and if the card is authorized, the gateway sends commands to unlock the door and turn on the light.

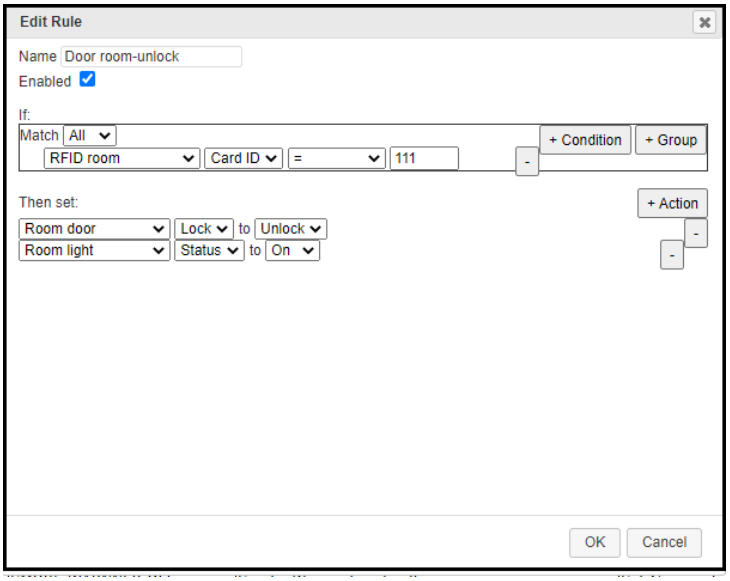


Figure III-57:Room RFID card parameter settings.

This rule is designed to automatically unlock the room door and control the lighting upon detection of a specific RFID card. It verifies whether the room's RFID reader has scanned a card with the ID 111, which corresponds to Safa's card. If this condition is satisfied, the system executes two predefined actions: first, it unlocks the room door, and second, it turns on the room light to provide immediate illumination upon entry. This creates a seamless and convenient access experience where both entry and lighting are automatically managed when the authorized RFID card is detected.

We also applied the opposite rule at the room door to prevent stranger access. This security rule activates when an unauthorized RFID card is detected by the room's reader. If any card other than Safa's authorized card (ID 111) is scanned, the system automatically ensures the door remains locked and keeps the room light off, preventing unauthorized access and maintaining security.

III.13.3 Testing the door

Scenario 1: Authorized Person

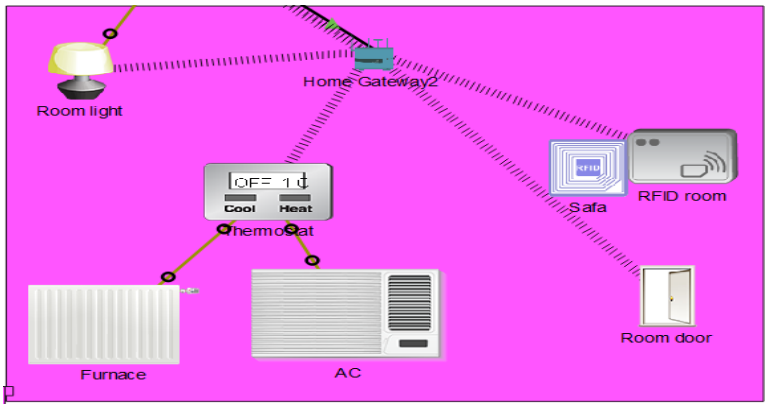


Figure III-58:Status of the room door upon proximity of the door-opening card.

The room door unlocks and opens automatically when an authorized individual, such as Safa, presents their assigned RFID card (ID: 111). Upon successful verification by the encrypted database, the door mechanism activates, and simultaneously, the room lights turn on to ensure immediate visibility and convenience. This dual-action system—combining secure access with ambient lighting—ensures both safety and comfort

Scenario 2: unauthorized person

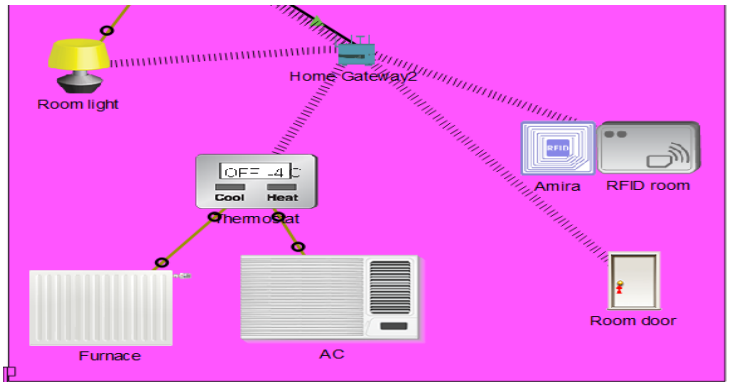


Figure III-59:Condition of the room door when an unauthorized card is used.

The room door remains locked and the lights stay off unless an unauthorized RFID card (any ID other than "111") is scanned. In this scenario, the system triggers a security protocol: the door refuses access, and the lights flash red as an alert, signaling an invalid credential

III.13.4 HVAC system

It is also equipped with a comprehensive HVAC system consisting of a programmable thermostat, air conditioning unit, and furnace to maintain optimal temperature and air quality throughout the sleeping area.

The thermostat displays the current room temperature, allowing residents to monitor the ambient conditions and manually decide whether to activate the heating or cooling system based on their comfort preferences.

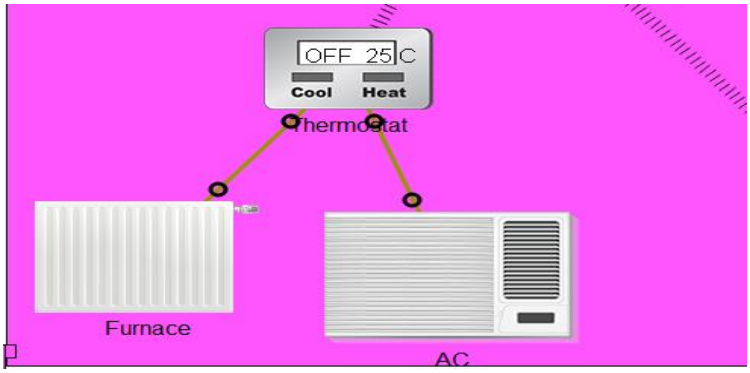


Figure III-60:HVAC system.

The figure shows the integrated HVAC system features a central smart thermostat that coordinates the furnace and air conditioning (AC) unit to maintain optimal comfort in the bedroom. The thermostat displays real-time temperature readings in Celsius (°C) and system status. Users can remotely switch between heating (furnace) and cooling (AC) modes via a smartphone, adjusting setpoints or overriding automated settings.

The thermostat in Iot monitor

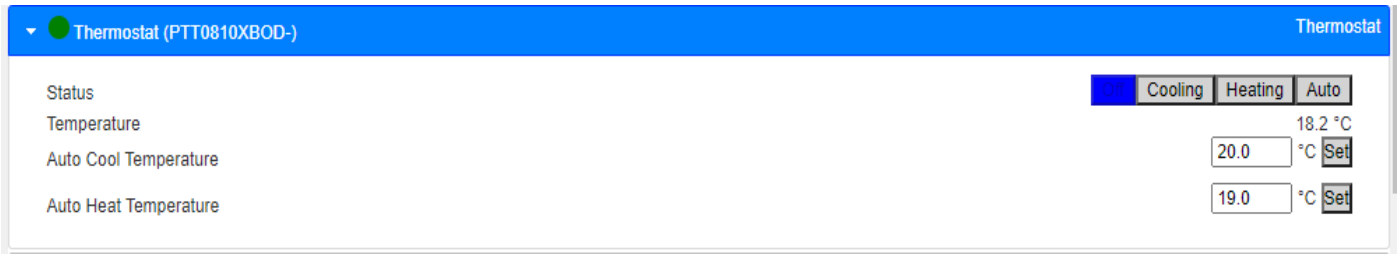


Figure III-61:Temperature data through the IoT server

The thermostat allows users to easily switch between Cooling, Heating, and Auto modes using the clearly labeled buttons.

III.13.5 Rain Guard Auto Close System

A simple system of rain detection and alert mechanism using a microcontroller (Rain MCU1). It is connected to a rain sensor that detects the presence of rain and sends a signal to the microcontroller. Upon receiving this signal, the microcontroller activates a rain alert indicator, such as an LED, to notify users of rainfall conditions.

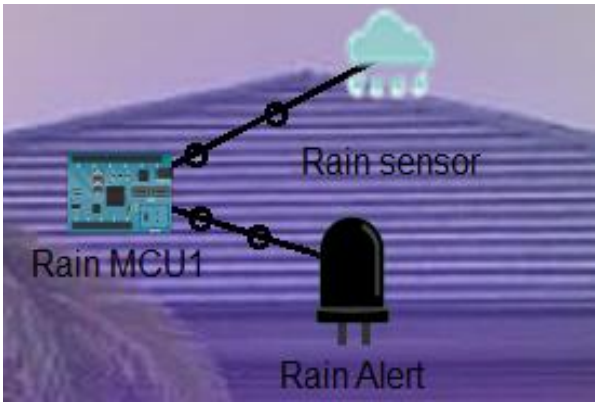


Figure III-62:Rain Guard Auto Close System

The system can be extended to include an automatic window-closing mechanism, which triggers the windows to close automatically when rain is detected, protecting the interior from water damage.

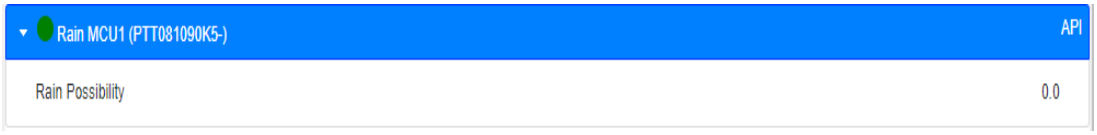


Figure III-63**:**Rain level monitoring via the IoT server

– **The rule in Iot server**

the room window automatically closes when rain is detected.It checks the rain possibility from Rain MCU1. the window automatically close

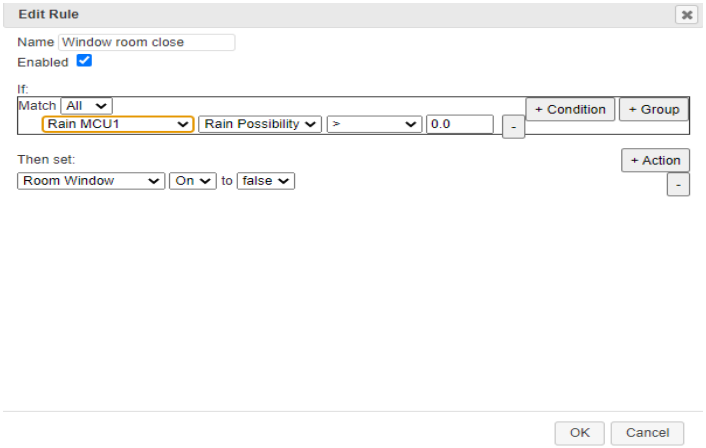


Figure III-64:Rain MCU Control Settings

The diagram below illustrates the rain environment that affected

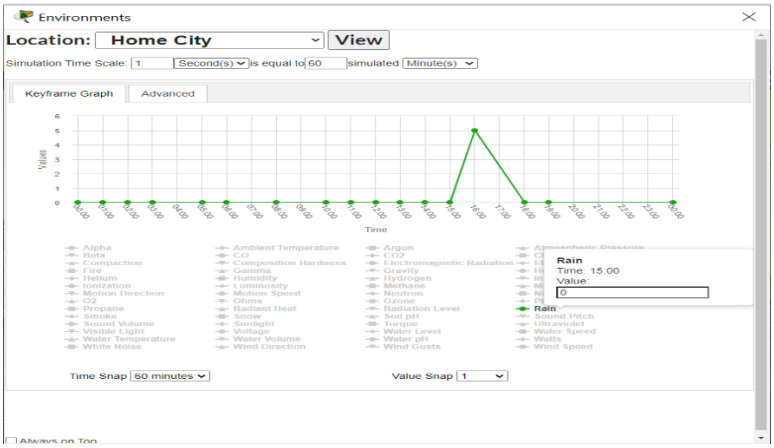


Figure III-65:Rain data configuration in the environment.

The Environments configuration window displays the rain simulation for Home City, with a time compression ratio of 1:60 (1 second equals 60 simulated minutes). The keyframe graph reveals rain from 15:00 AM through most of the day to 17:00, followed by a period of calm the rest of the day

III.13.6 Testing Rain Guard Auto Close System

Scenario 1: There is no rain

The automated system operates on a simple rain-dependent logic: when no rain is detected, the LED indicator remains off, and the window stays open to allow natural

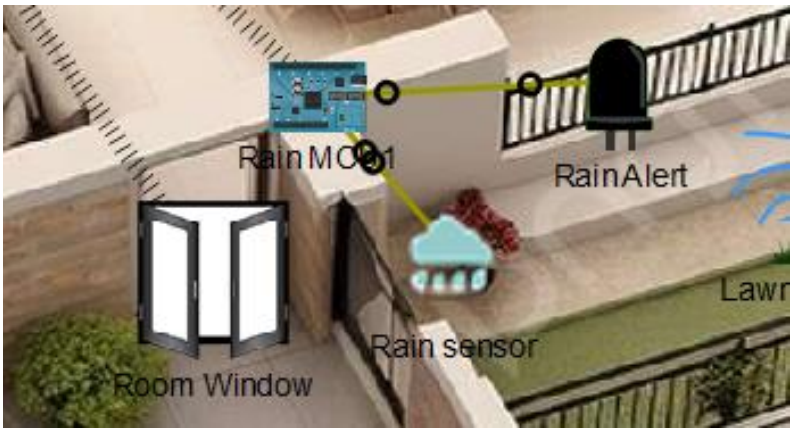


Figure III-66:Status of the window and rain alert system during rainfall.

Scenario 2: There is rain

Conversely, if rain is sensed by environmental detectors, the LED instantly illuminates (signaling precipitation), and motorized mechanisms trigger the window to close, preventing water ingress. This binary design ensures energy efficiency during dry conditions while prioritizing protection against moisture damage during rainfall.

Figure III-67:Condition of the window and rain alert in the absence of rainfall.

III.14 Front yard

The IoT-managed front yard features two smart sprinklers equipped with water level detectors that activate irrigation only when soil moisture drops below predefined thresholds, conserving water while maintaining lawn health. Motion detectors, linked to web cameras, trigger real-time video recording and alerts to a smartphone app when movement is detected, enhancing security. Simultaneously, the RFID-controlled main door grants access exclusively to authorized users , ensuring seamless entry.

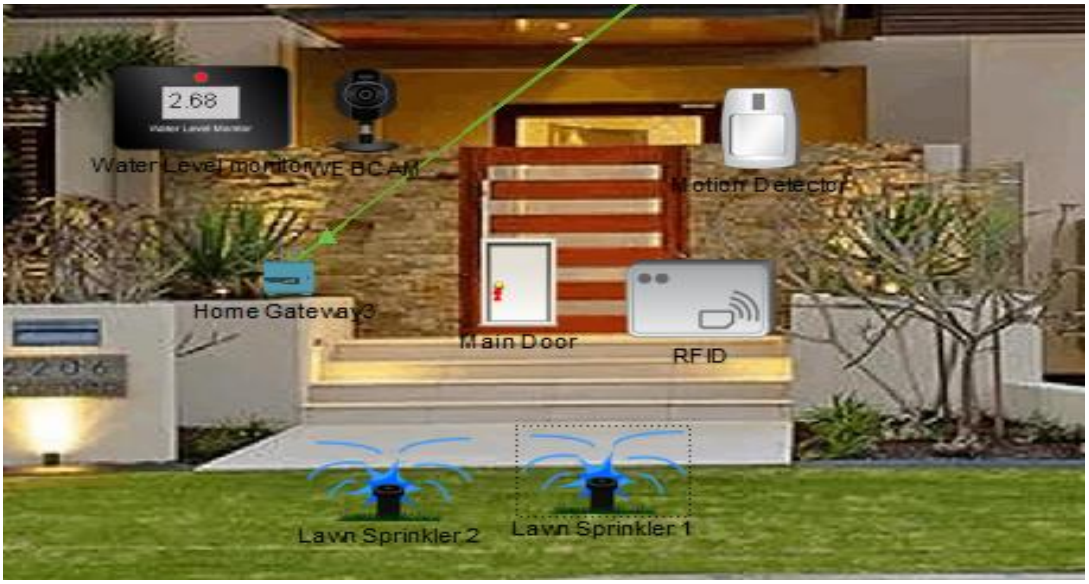


Figure III-68:front yard in physical space

III.14.1 Implementation

We will classify it into two systems

III.14.2 Security System

RFID Main Door Access: The main door unlocks automatically via an RFID reader, granting entry only to authorized users. Failed attempts trigger alerts.

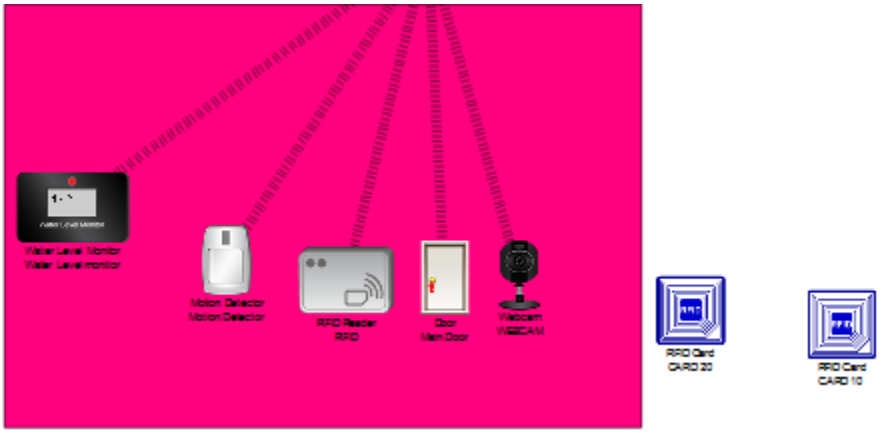


Figure III-69:front yard in logical space.

The RFID-controlled main door grants access exclusively to authorized users, such as CARD 10. When the authorized card is scanned, the door unlocks automatically, allowing entry (such garage door and the bedroom). Conversely, unauthorized cards, like CARD20 trigger an instant security alert denying access The system logs all attempts, pairing timestamps with card IDs for auditing, and employs encryption to prevent tampering or cloning. This ensures secure, seamless access for approved individuals while actively deterring unauthorized entry through automated alerts and strict verification protocols.

Motion Detection & Surveillance: Motion sensors trigger webcams to record and send real-time alerts to a smartphone, deterring unauthorized activity. When the motion detector senses movement in the monitored area, it instantly triggers the connected web camera to activate and begin recording. The camera streams real-time footage to a secure IoT server while simultaneously sending an alert to the user's smartphone.

Scenario 1 : When the motion detector on

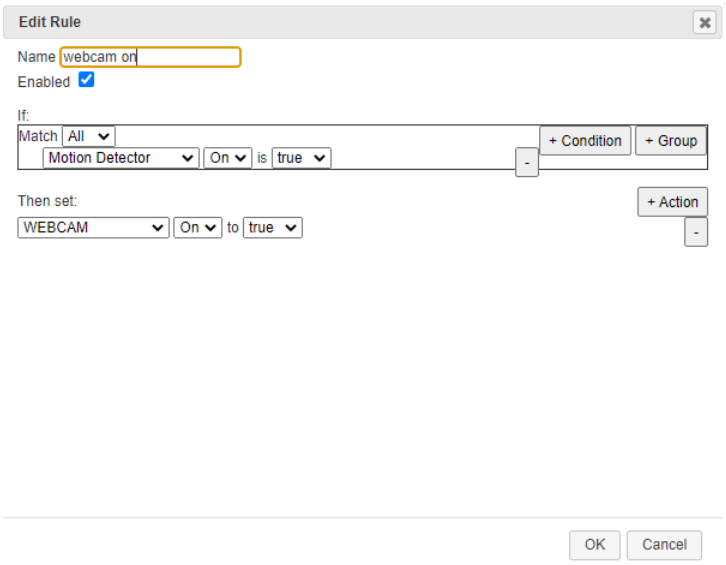


Figure III-70:Webcam Operation Triggered by Motion Detection(on).

This configuration creates an intelligent security response where motion detection automatically triggers webcam recording or monitoring. This type of rule-based automation is common in smart home security systems, allowing for immediate visual documentation when unauthorized movement is detected.

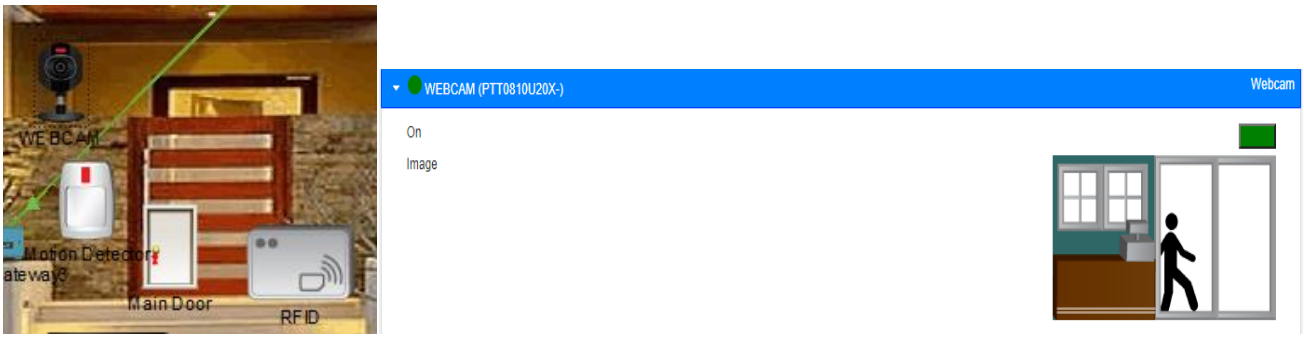


Figure III-71:Webcam When the motion detector on.

When motion is detected in the physical space, the webcam system automatically activates and provides visual monitoring, creating a comprehensive security response that combines multiple detection methods for enhanced home protection.

Scenario 2: When the motion detector off

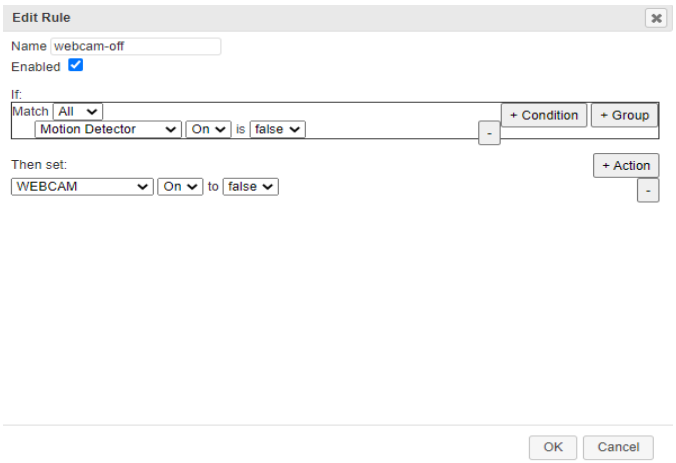


Figure III-72:Webcam Operation Triggered by Motion Detection(off).

the rule configuration interface for "webcam-off" settings. The rule is set to turn the webcam "off" when the motion detector state is "false," creating an automated system that deactivates the webcam when no motion is present, conserving resources and maintaining privacy when the area is unoccupied.

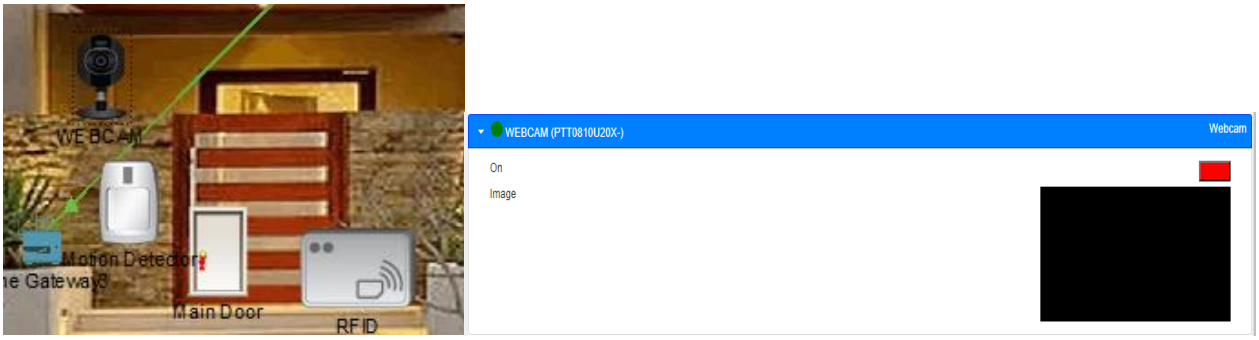


Figure III-73:Webcam When the motion detector off.

The smart home security setup has the webcam interface displaying a black screen, indicating the system is in standby mode. But no motion is currently detected, so the webcam remains inactive.

III.14.3 Irrigation System

The automated irrigation system consists of two lawn sprinklers and a water level detector to optimize lawn hydration. Soil moisture sensors embedded in the ground

continuously monitor moisture levels; when they detect dry conditions, the system checks the water level detector to confirm sufficient supply. This ensures precise, sustainable lawn care while eliminating manual intervention and waste.

This system utilizes environmental sensors to assess soil moisture conditions and coordinates multiple sprinkler zones to maintain optimal lawn health while conserving water resources

Scenario 1: Activate the sprinklers

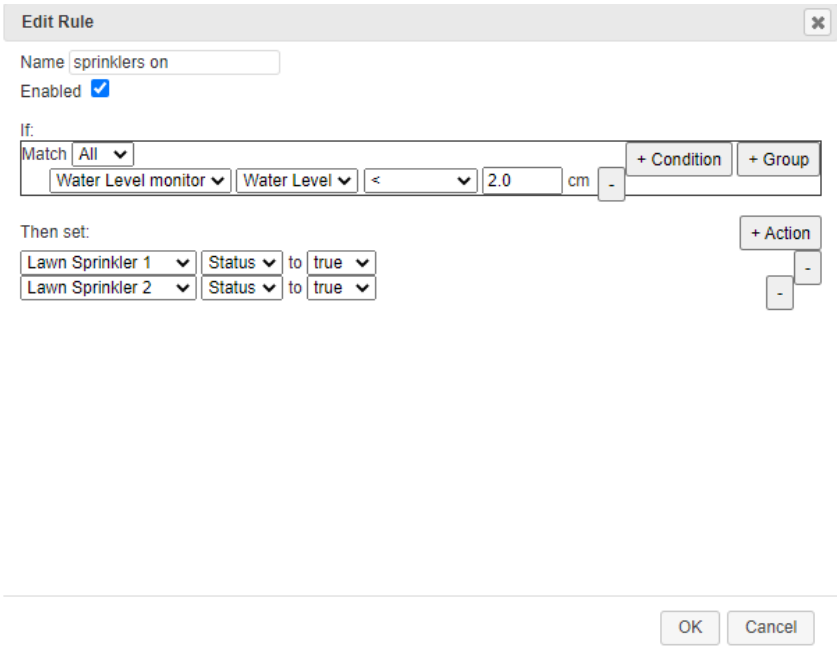


Figure III-74:Water Sprinkler Activation Settings.

The Figure III-74 shows the rule setup for automated sprinkler activation based on water level monitoring. The rule named "sprinklers on" is enabled and configured to trigger when the water level monitor detects levels below 2.0 cm. When this condition is met, both Lawn Sprinkler 1 and Lawn Sprinkler 2 automatically activate (status set to "true"), ensuring immediate irrigation response to prevent lawn dehydration.

Figure III-75:status of water sprinklers at values less than 2 cm.

The physical implementation displays the water level monitor reading in cm, which falls below the 2.0 cm threshold established in the automation rule. This triggers the connected lawn sprinklers to activate, as evidenced by the blue network connections between the monitoring device and sprinkler units. The system demonstrates real-time responsiveness, with the sprinklers engaging automatically when soil moisture drops to critical levels, maintaining optimal growing conditions without manual intervention while preventing water waste through precise threshold-based control.

Scenario 2: Deactivate the sprinklers

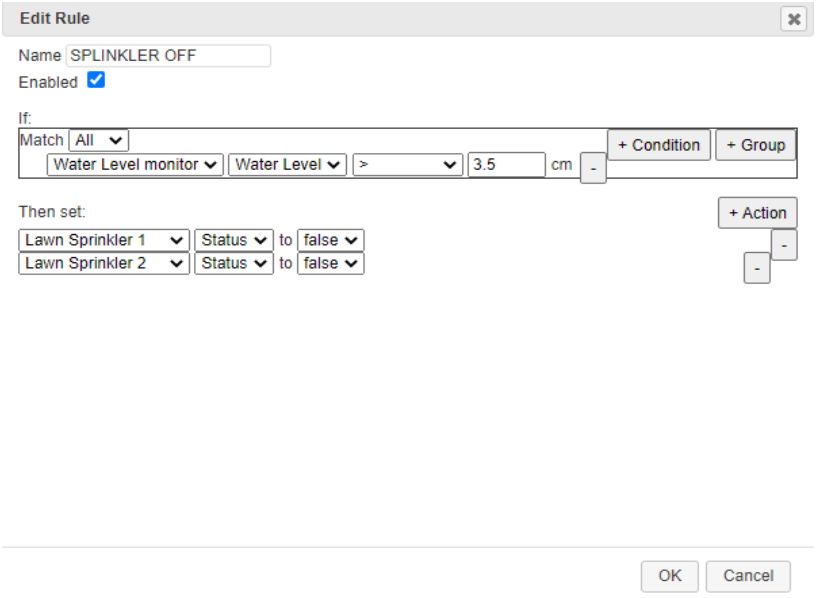


Figure III-76:Water Sprinkler Deactivation Settings

The "SPLINKLER OFF" rule configuration establishes the upper boundary for irrigation control, set at 3.5 cm water level. When the monitor detects moisture levels above this threshold (as shown by the 4.24 cm reading), both Lawn Sprinkler 1 and Lawn Sprinkler 2 automatically deactivate (status set to "false").

Figure III-77:Condition of water sprinklers when values surpass 2 cm.

The *Figure III-77* shows The water level monitor now displays 4.24 cm, indicating significantly improved soil moisture levels. This reading exceeds the upper threshold established in the system's conservation protocols, demonstrating that the previous irrigation cycle successfully restored adequate soil hydration. The elevated moisture reading triggers the system to prepare for sprinkler deactivation to prevent watering.

This dual-threshold system creates an intelligent hysteresis loop - sprinklers activate below 2.0 cm and deactivate above 3.5 cm - preventing rapid cycling and ensuring efficient water usage while maintaining optimal lawn conditions. The 1.5 cm operational band between activation and deactivation thresholds provides stable system behavior and prevents unnecessary water waste.

III.15 The Living Room

The smart living room system integrates IoT devices to automate comfort, security, and energy efficiency. At its core, temperature and humidity sensors monitor environmental conditions. When the living room temperature rises beyond a set threshold, a solar-powered fan connected directly to a rechargeable battery activates to cool the space. while a separate bedroom light (also battery-powered) can be triggered by other conditions like humidity or user schedules. Energy sustainability is ensured by a solar panel that charges the battery, reducing reliance on the grid. For security, motorized windows open automatically during sunny weather to ventilate the room but snap shut if a trip sensor detects an

intrusion, simultaneously activating a siren. The TV connects to the internet via a coaxial splitter, which splits the cable signal to enable both traditional TV viewing and cloud connectivity. This setup allows the TV to stream alerts or data to the cloud without interfering with other devices. Crucially, security protocols override environmental controls; for example, closing windows during a breach even if temperatures remain high. This cohesive system harmonizes renewable energy, adaptive automation, and real-time cloud connectivity, delivering a responsive, eco-friendly living space that prioritizes safety and comfort.

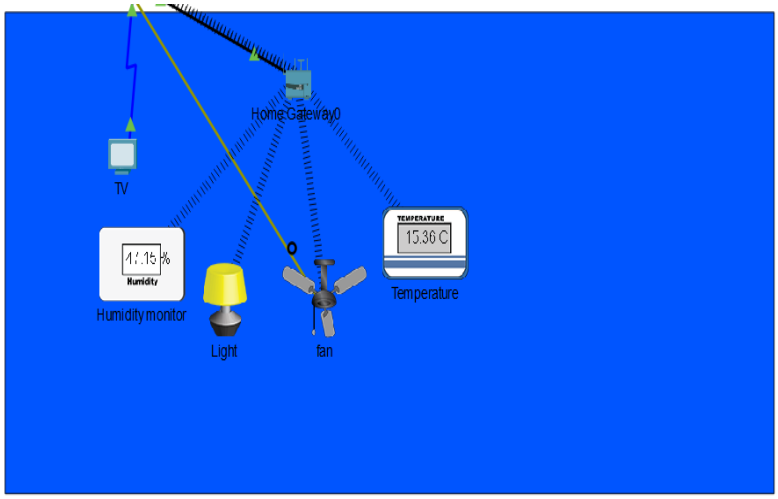


Figure III-78:Living room design

III.15.1 Implementation

Here's a concise breakdown the smart living room into systems, focusing on their unique roles and connections

III.15.2 Environmental Control System

The solar panel in the system operates by detecting sunlight through its photovoltaic cells, which convert solar energy into electrical power. The amount of energy generated depends on environmental factors like sunlight intensity, with real-time metrics (watts) displayed for monitoring. This power is then regulated by a charge controller, which ensures safe and optimal transfer to the battery by adjusting voltage and current to prevent overcharging. The battery stores this energy, enabling it to power devices like the fan and bedroom lights even when sunlight is unavailable. By dynamically adapting to sunlight conditions and prioritizing efficient energy storage.

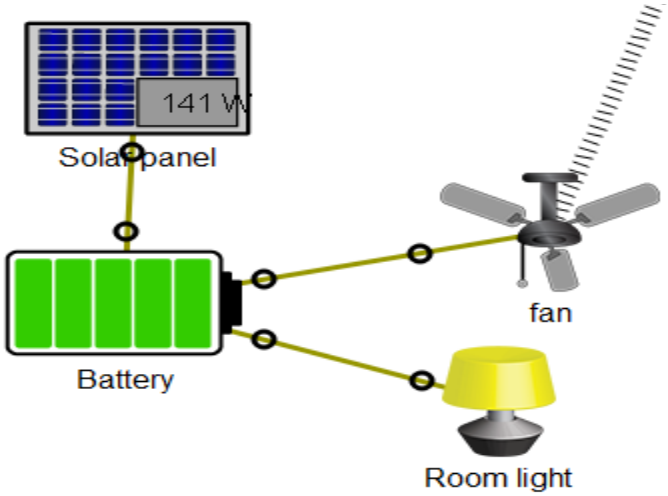


Figure III-79:Control System.

This configuration enables off-grid operation for essential components, reducing dependency on municipal power and lowering energy costs. The battery acts as both a storage medium during peak solar generation and a power source during low-light conditions, ensuring continuous operation of the fan and lighting systems.

III.15.3 Temperature and humidity

A temperature monitor is a subsystem that measures thermal conditions in its surroundings using sensors to detect and read ambient temperature in a living room. The temperature sensor continuously reads the living room's ambient conditions. A temperature monitor is a dedicated subsystem designed to ensure optimal thermal comfort in a living space by continuously tracking ambient conditions. Using precision sensors and digital thermometers, it measures real-time temperature data within the room and converts raw electrical signals into readable values (e.g., degrees Celsius). This data is processed by a microcontroller, enabling dynamic responses such as activating a fan or adjusting ventilation.

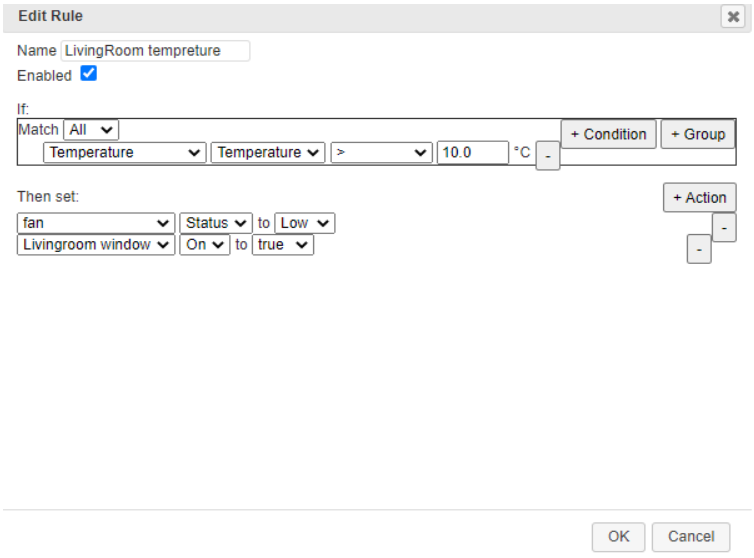


Figure III-80:Temperature-Based Control Rule for the Living Room Using IoT Server.

when the temperature sensor detects readings exceeding 10.0°C, triggering a dual-action cooling strategy. When the temperature threshold is breached, the system simultaneously sets the fan status to "Low" speed operation and opens the living room window by changing its status to "true." This creates a natural ventilation system that combines mechanical air circulation with fresh air intake to effectively reduce indoor temperature. The coordinated approach maximizes cooling efficiency while minimizing energy consumption by utilizing both forced air movement and natural airflow.

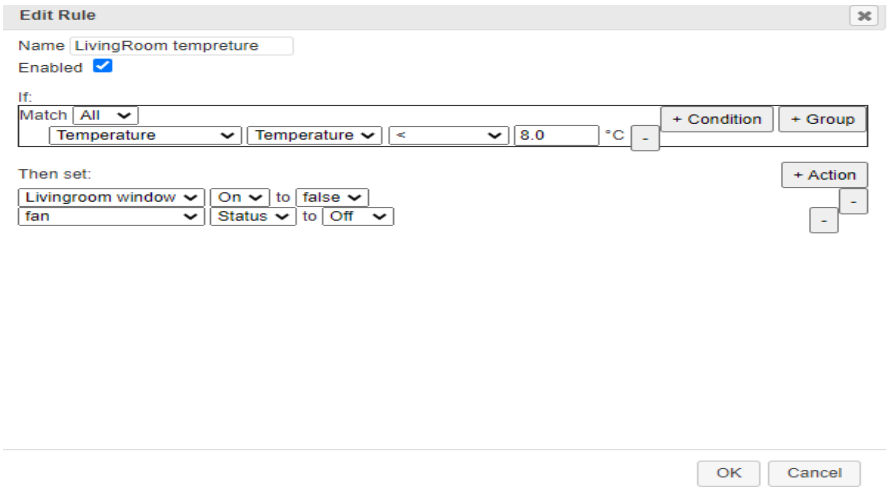


Figure III-81:Automatic Deactivation of Fan and Window Below 8°C in Living Room

This automation rule establishes a temperature-based deactivation protocol for the living room's climate control system. The rule triggers when the ambient temperature drops below 8.0°C, indicating that cooling is no longer necessary and the room has reached a comfortable temperature level.

When the temperature threshold is met, the system automatically closes the living room window (setting status to "false") and turns off the fan completely (setting status to "Off"). This coordinated shutdown prevents over-cooling and conserves energy by eliminating unnecessary air circulation when ambient conditions no longer require active cooling intervention.

III.15.4 Testing these rules

Scenario 1: When temperature below 8°

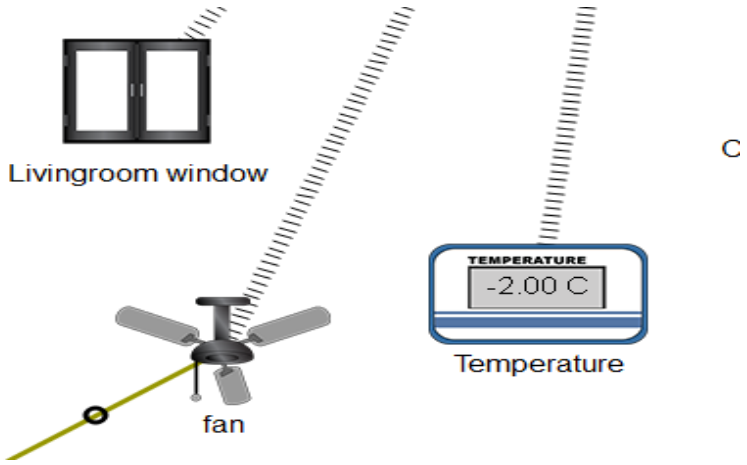


Figure III-82:Living Room Devices Response to Low Temperature Reading (-2°C).

When ambient temperature drops below 8°C, the system automatically closes the window and deactivates the fan to conserve heat and reduce energy consumption.

Scenario 1: When temperature above 10°

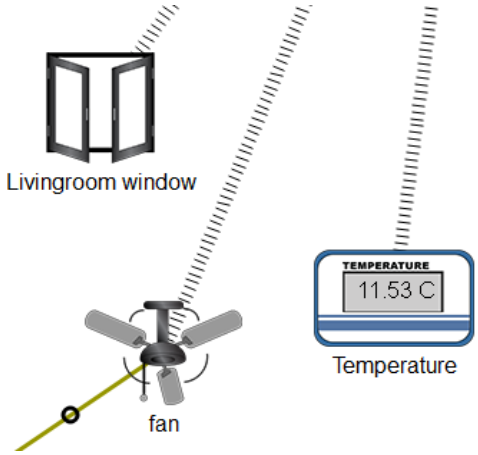


Figure III-83:Living Room Devices Response to Low Temperature Reading (11°C).

When the ambient temperature rises above 10°C, the system activates an automated response to improve thermal comfort: the motorized window opens to allow fresh airflow, while the fan operates at a low speed to gently circulate air. This dual-action approach ensures efficient cooling without excessive energy use, maintaining a balanced indoor environment.

III.15.5 Humidity monitor

The humidity control system uses sensors (e.g., a hygrometer) to monitor moisture levels in the living room. When humidity exceeds 50%, the system triggers two actions:

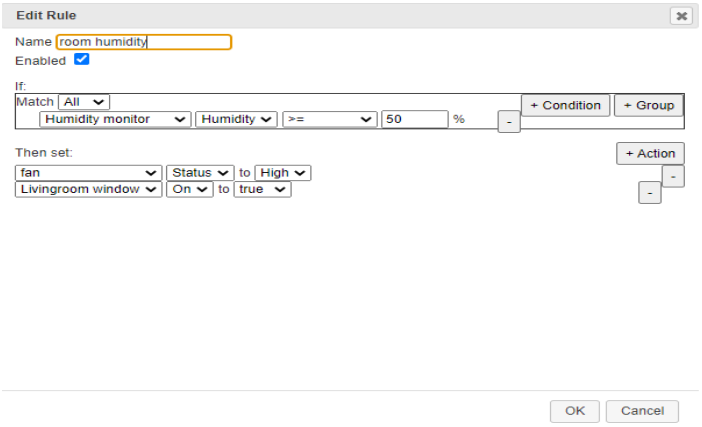


Figure III-84:Activation Rule for the Humidity Monitor.

The automation rule shown is designed to maintain optimal indoor air quality by managing humidity levels in the living room. The rule is configured with a 50% humidity threshold, which serves as the trigger point for activating ventilation systems. When the humidity monitor detects levels at or above 50%, the system automatically responds by setting the fan to high speed and opening the living room window to increase air circulation and reduce moisture buildup. This type of automated humidity control is essential for preventing condensation, mold growth, and maintaining comfortable living conditions.

III.15.6 Testing the humidity system

Scenario 1: High Humidity Alert

Figure III-85:System High Humidity Scenario (56.66%).

We see the automation rule in action. The humidity monitor displays 56.66%, which has exceeded the 50% threshold set in the rule. As a result, the system has automatically activated both response mechanisms: the ceiling fan is running at high speed, and the living room window has been opened. This demonstrates the rule working as intended, with the ventilation systems actively working to reduce the elevated humidity level.

Scenario 2: Normal Humidity Levels

Figure III-86:System– High Humidity Scenario (37.66%)

the system in its resting state after the humidity has been successfully reduced. The humidity monitor now reads 37.98%, which is well below the 50% trigger threshold. Consequently, both the fan and window have returned to their normal states - the fan is no longer running at high speed and the living room window has been closed.

III.15.7 Security System

A trip sensor is installed at the living room window to detect unauthorized entry. The sensor employs a laser emitter and receiver pair positioned across the window frame. When an intruder crosses the laser beam, the interruption triggers an immediate security response Alert Activation: A loud siren is activated to deter the intruder and alert occupants.

Figure III-87:Activation Rule for the Trip Sonar System.

The automation rule displayed is a basic security system configuration designed to provide immediate alert notification when unauthorized entry or movement is detected. The rule is named "trip sensor" and functions as a simple but effective intrusion detection system. When the trip sensor detects movement or is triggered (status changes to "true"), the system automatically activates the siren by turning it "On" to provide an audible alarm.

III.15.8 Testing the trip sensor

Scenario 1: Normal Security State

Figure III-88:*The* Normal state.

We observe the security system in its normal, inactive state. The trip sensor appears dormant with no detection activity indicated, and the siren remains in standby mode . Both devices are connected and operational, with signal lines indicating they are communicating with the home automation system, but no security event has occurred. This represents the typical resting state

Scenario 2: Security Breach Detected

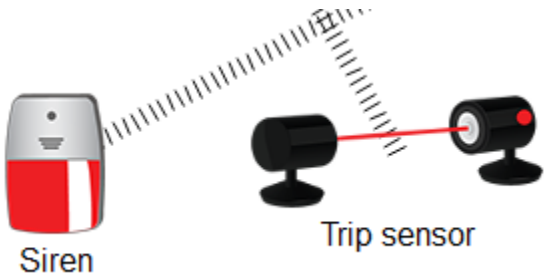


Figure III-89:Status of intrusion detection

The *Figure III-89* demonstrates the security rule in active response mode. The trip sensor has been triggered, likely by detecting movement or an intrusion attempt, as indicated by the red warning signals

emanating from the sensor. Consequently, the automation rule has immediately activated the siren, which is now displaying in red color to show it is actively sounding an alarm. This scenario shows the complete security response cycle, from initial detection by the trip sensor to the immediate activation of the audible warning system, providing the homeowner and potentially deterring intruders with the loud alarm notification.

III.15.9 TV systems

The system receives the TV signal from the cloud (representing the cable provider's headend), which then feeds into a coaxial splitter. The splitter divides the signal to serve two endpoints - a cable modem and a TV set.

III.15.10 Key Components

- **Coaxial Splitter:** The central component that takes one input signal and distributes it to multiple outputs while maintaining signal integrity.
- **Cable Modem:** Extracts internet data from the cable signal
- **TV:** Receives broadcast channels directly through the coax connection
- **Cloud Integration:** Enables access to streaming platforms (Netflix, YouTube) or cloud-based smart home controls (e.g., voice assistants via the TV).

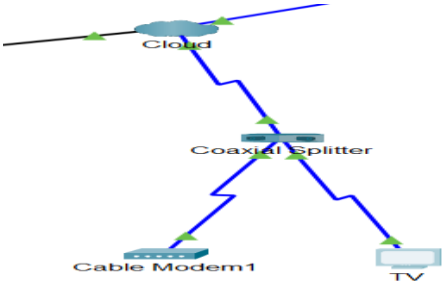


Figure III-90::Tv system

III.15.10 System Characteristics

This setup supports both internet and traditional cable TV service over the same coaxial infrastructure. The TV receives allavailable channels simultaneously through the cable signal, with channel selection happening at the TV tuner level.

III.15.11 Configure TV setting In The Cloud

The TV Settings section specifically allows users to upload and configure television content through image files, as evidenced by the file browser showing multiple image files from the user's local system.

This setup enables administrators to configure TV hardware (via serial/coaxial ports) while leveraging cloud-based tools for global settings distribution.

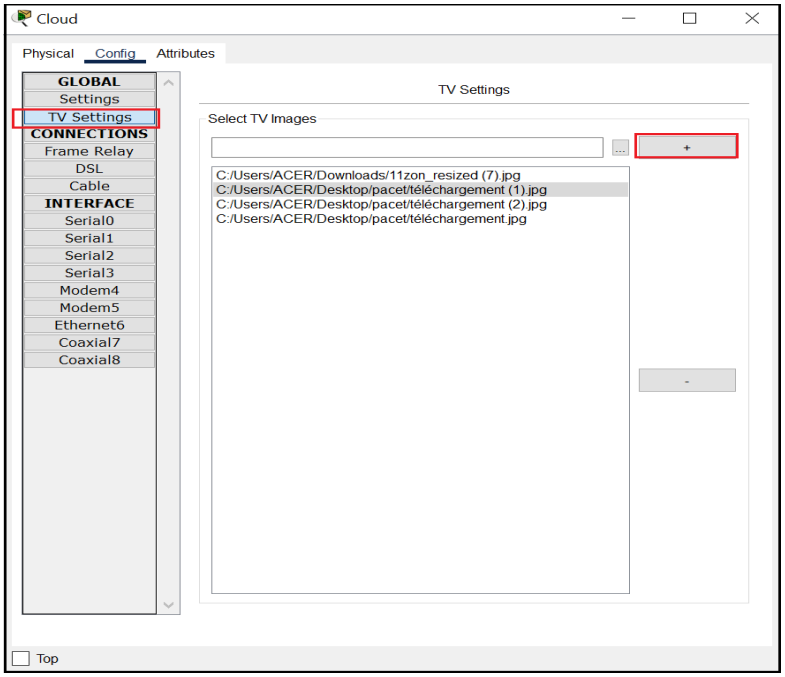


Figure III-91:Tv setting

To configure TV settings in this cloud simulation interface, follow these steps:

1. Enter the cloud device: First, double-click on the "Cloud" icon in network topology. This opens the cloud device's configuration window, which represents your service provider or internet gateway in the simulation.

2. Navigate to the Configuration Tab: Once the cloud device window opens, you'll see several tabs at the top. Click on the "Config" tab to access the configuration options for this network device.

3. Access TV Settings: In the left sidebar menu, you'll see a list of configuration categories. Under the "GLOBAL" section, locate and click on "TV Settings" (highlighted in red in the interface). This opens the television service configuration panel.

4. Configure TV Content: In the TV Settings panel, you'll see a "Select TV Images" section. Here we can: Browse for image files by clicking the "+" button (highlighted in red)Select TV content images from your computer's file system

5. Apply Settings: After selecting the TV images and configuring the settings, the simulation will use these images to represent television content being transmitted through the network topology to connected TV devices.

III.15.12 Testing the Tv

The TV device's physical interface after clicking on the TV in the network simulation. The interface demonstrates how the television content configured in the cloud is now being displayed on the TV screen.

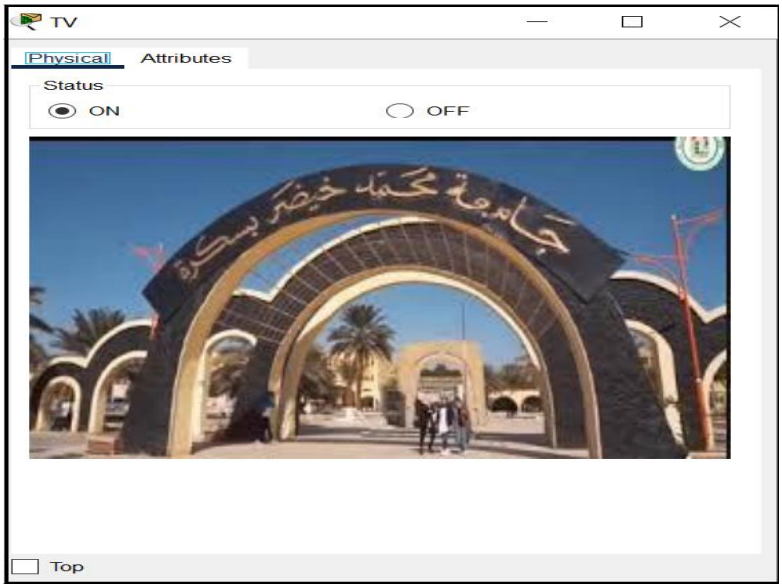


Figure III-92:Display images in the tv screen

III.16 Conclusion

The implementation of the IoT-based smart home system across functional zones (garage, kitchen, front yard, living room, and bedroom) successfully demonstrated the integration of automation, safety, and remote accessibility within a unified network framework. By leveraging decentralized zone-specific gateways and centralized servers, the system achieved seamless communication between IoT devices, prioritized emergency protocols (e.g., fire suppression, intrusion alerts), and enabled real-time control via 3G/4G-enabled smartphones. Rigorous testing validated the network's reliability, responsiveness, and adherence to security standards, while the modular architecture ensured scalability for future expansions. This practical exercise underscored the viability of IoT technologies in enhancing residential efficiency, safety, and convenience, providing a foundational blueprint for real-world smart home deployments.

General Conclusion

In conclusion, the adoption of Internet of Things (IoT) technologies within the domain of smart homes represents a foundational step toward the realization of intelligent and sustainable living environments. The seamless integration of smart devices, advanced communication infrastructures, and cloud computing platforms has facilitated the development of sophisticated functionalities that significantly enhance user comfort, security, and energy efficiency. Furthermore, the capacity of these systems to learn from and adapt to residents' behavioral patterns while responding dynamically to evolving needs underscores their critical role in elevating the overall quality of life.

As technological innovation continues to accelerate and IoT solutions become increasingly pervasive, smart homes are poised to evolve beyond their traditional roles. They are expected to become dynamic nodes within broader digital ecosystems, actively contributing to environmental sustainability and fostering intelligent, context-aware interactions between humans and their surroundings. Within this context, the current project establishes a robust technical and conceptual foundation upon which further innovations can be developed, in alignment with the requirements of the digital era and the vision of a more interconnected and intelligent society.

❖ Benefits

- **Enhanced Comfort and Convenience**: Automation and remote control of household functions lead to improved daily living experiences.
- **Increased Energy Efficiency**: Smart energy management systems help reduce consumption and utility costs.
- **Improved Security**: Real-time surveillance, access control, and alert systems contribute to a safer home environment.
- **Adaptive Personalization**: The system can learn user preferences and routines, tailoring its behavior accordingly.
- **Remote Accessibility**: Users can monitor and control home functions from anywhere, enhancing flexibility and responsiveness.

❖ Future Scope

- **Scalability Enhancements**: Expand the system to support a greater variety and number of IoT devices and sensors.
- **AI Integration**: Incorporate artificial intelligence and machine learning to enable autonomous decision-making and adaptive behavior.
- **Interoperability Improvements**: Facilitate seamless integration with diverse third-party platforms and home automation ecosystems.
- **Privacy and Security**: Develop more robust security mechanisms to safeguard user data and maintain trust in connected environments.
- **Sustainability Expansion**: Integrate renewable energy sources and optimize energy consumption through intelligent management strategies.
- **Cross-Domain Applications**: Extend the system's architecture to support broader domains such as smart cities, eldercare, and assisted living.

Bibliography

[1] Recommendation ITU-T Y.2060, "Overview of the Internet of things," *SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS,* 2006.

[2] D. THERA, "INTERNET OF THINGS SIMULATION USING CISCO PACKET TRACER," İzmir Institute of Technology, İzmir, 2020.

[3] M. Rouse, "Internet of things iot," *IOT Agenda,* 2019.

[4] G. S. G. B. H. David Hanes, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, Cisco Systems,, 2017.

[5] L. Abdeldjalil, "An Internet of Things Based Smart Home System For Toxic Gas Detection," 2020.

[6] R. v. Kranenburg, Introduction to the Internet of Things, 2013.

[7] D. THERA, "INTERNET OF THINGS SIMULATION USING CISCO PACKET TRACER," İZMİR, 2020.

[8] E. C. E.-Y. F. Marie Chan, "Smart homes - Current features and future perspective," vol. 64, no. 90-7, 2009.

[9] A. V. K. H. P. T. Odamboy Djumanazarov, "An Overview of IoT-Based Architecture Model for Smart Home Systems," Urgench Branch of Tashkent University of Information Technologies named after Muhammad, Uzbekistan, 2022.

[10] M. Domb, "Smart Home Systems Based on Internet of Things," in *IoT and Smart Home Automation ,* 2018.

[11] Y. Ismail, Internet of Things (IoT) for Automated and Smart Applications, IntechOpen, 2019.

[12] "Getting Started with Cisco Packet Tracer," 2019.[Online]. Available: https://www.netacad.com/cisco-packet-tracer.

[13] S. R. Javid, "Role of Packet Tracer in learning Computer Networks," International Journal of Advanced Research in Computer and Communication Engineering ,2022.

[14] "Packet Tracer 8.2 - IoT devices configuration," 12 SEP 2023. [Online]. Available: https://www.packettracernetwork.com/internet-of-things/pt7-iot-devices-configuration.html.

[15] "environment,"2020. [Online]. Available: https://tutorials.ptnetacad.net/help/default/environment.html.