UNIT 19 INTERNET OF THINGS

Assignment 2

Learning Aim B & C

Develop a design for an Internet of Things system or device to solve a problem & Carry out the prototyping of an integrated Internet of Things system or device to solve a problem

Oliver Collins-Cope
2102775@rutc.ac.uk

Contents

Introduction

For this assignment, I will delve into the aspects of a home security system, specifically an alarm, designed to detect and alert homeowners of any intrusion. The advantages of this kind of system are multifold, with some of the most notable being detection of break-ins and a sense of security for the occupants of the home. The downside, however, primarily revolves around the initial installation and ongoing maintenance costs. That being said, once these financial aspects are taken care of and the IoT device is regularly maintained, it stands to provide significant benefits, enhancing the safety of the home environment.

Problem definition statement

The problem in this scenario is the issue of having an alarm that can be used to detect whenever a door or someone has set off a motion alarm that can then alert the homeowner covertly, such as through a mobile notification. The intended audience of this would be the any homeowners looking to secure their property from malicious thieves.

The constraints of this project vary depending on the perspective you take, such as a lack of technical ability not knowing how to utilise these different aspects of the technology, like the motion sensor or camera. Another example of a constraint of this would be the cost to create and make all of these pieces of technology, or to purchase all of these components.

The benefits of using a motion detection system means that it will create a safer environment within the home for the homeowner, and it creates a self-sustaining alarm system that will constantly notify the homeowner if something happens within the home, like unauthorised access.

The nature of user interactivity here will be based in mobile applications and access to alerts/camera through this application. Due to this access, through the mobile application, the user will be able to gain access to their home and view it through the camera, while also being aware of any changes that might happen through the motion detection.

Some accessibility considerations of this application might be audible alerts that describe what can be seen on the camera, such as “a hooded figure moving across the room”, or audio alerts describing the time that the alert was made. Additionally, another accessibility feature that could help might be text-based options for the video feed, i.e., describing what is going on through the use of AI, or a microphone in the camera.

Purpose requirements

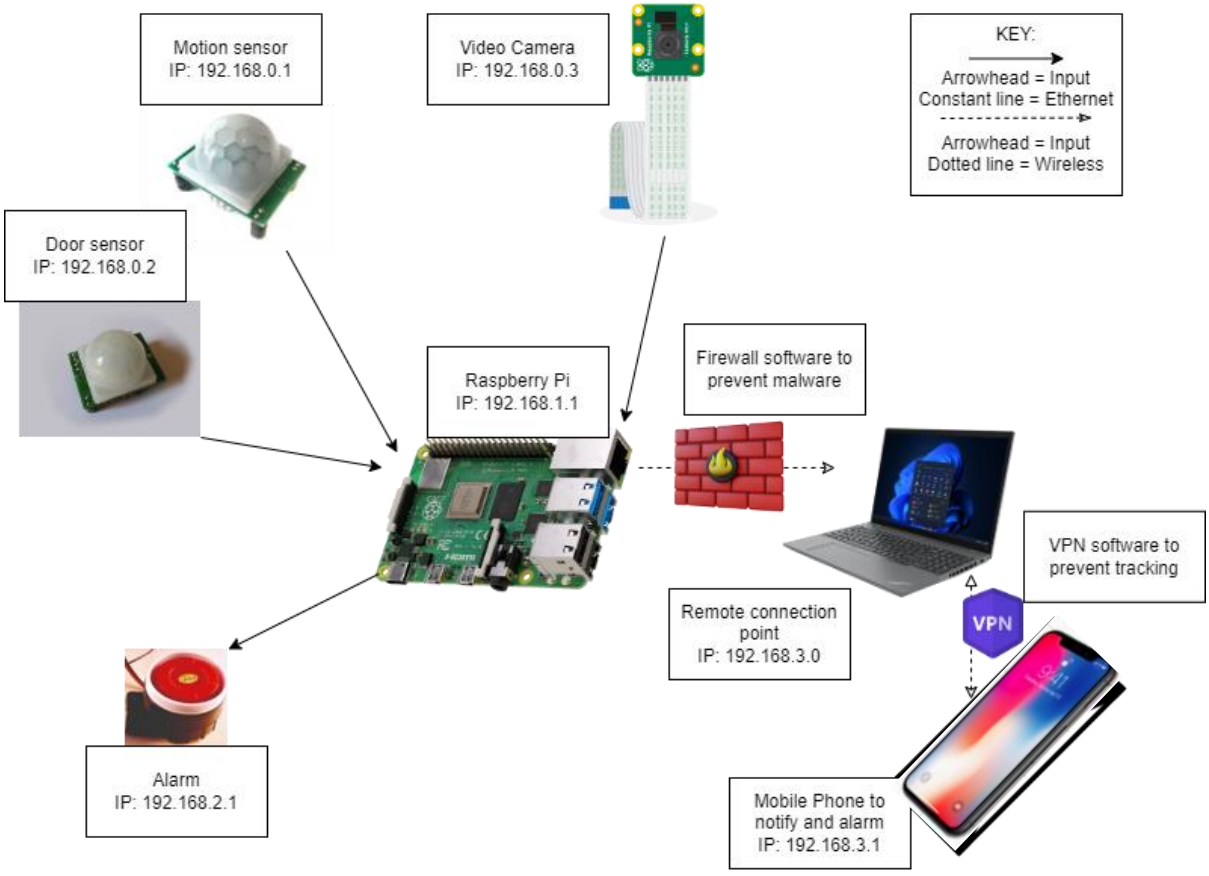
The purpose of the IoT system is to address the alarm system. The system should be able of detecting any movement within a room using a camera connected to a Raspberry Pi or a similar microcomputer. Once movement is detected, the system must send an alert to a mobile device. When the creation of this system is made in packet tracer, it will likely use a home network as a placeholder for the raspberry pi.

Several parts are needed to be able to complete this. Firstly, the system should provide a detection ability. This can be achieved by using cameras capable of differentiating between different types of movement, such as distinguishing a person from a pet, to prevent false alarms.

Next, the system should ensure real-time alert notifications. This means there is a need for consistent connectivity. Continuing, the system should be user-friendly and offer easy customisation of alarm settings, including setting up the app to receive alerts. The system should also provide an interface for system status monitoring and alarm management.

Lastly, the system should be designed considering scalability. As houses expand, the system should allow for an easy integration of additional cameras and motion sensors and be adaptable to new technologies and standards in the IoT ecosystem.

Diagrammatic illustrations and written annotations



The design of the IoT system involves an optimised functional system. The system's central element is a Raspberry Pi, acting as the microcontroller (which will be replaced by the home network in packet tracer when creating the actual IoT system as a raspberry pi cannot be used there), interfacing with all components.

The system incorporates a camera, providing the necessary input. Upon sensing motion, these motion detector sends a signal to the Raspberry Pi (again, this will be replaced by the home network in packet tracer in order to make this functional). The sensor's sensitivity parameters can be changed to prevent false alarms.

The Raspberry Pi (otherwise known as the home network in packet tracer, as there is no way to get a raspberry pi in packet tracer), once triggered, sends a notification. This alert is sent to a mobile device through Wi-Fi. Wi-Fi has been selected as the method of sending the notification due to its availability and ease of integration with the Raspberry Pi (which will be replaced with the home network in packet tracer). It provides the system with internet connectivity, allowing the sending of notifications.

This system design reflects a balance of functionality, and user-friendly operations. The choice of components aligns with the requirement to use off-the-shelf hardware, simplifying the assembly process. The visual diagram accompanying this details the connections and communication flow within this IoT system.

Communication infrastructure

Understanding Sensors in the IoT Systems

A key component of an IoT system is its sensors. These devices are tasked with the important role of collecting data from the surrounding environment. These sensors make sure to capture all the data, and in this instance that means video feed and motion detection. Following data collection, raw data is digitised and made understandable. This conversion facilitates real-time data interpretation and interaction by the system, therefore making it efficient.

Wired and Wireless Communications in IoT

IoT systems heavily rely on both wired and wireless communication channels. Wired connections like Ethernet provide high-speed data capabilities, which are crucial for specific applications within IoT. On the other hand, wireless technologies including Wi-Fi and Bluetooth Low Energy (BLE), introduce flexibility in setup and deployment. In addition, unique identification systems using RFID and QR codes further enhance the performance of IoT applications.

Actuators in IoT Systems

The actions in an IoT system are primarily driven by actuators, effectively serving as the "muscles" of the system. Based on instructions received from the control system, actuators initiate physical movements or changes by controlling various devices, motors, and servos. This way, the digital data and commands in the system are transformed into concrete actions, sealing the loop within the IoT system.

Device Domain in IoT Systems

The device domain within an IoT system is what allows communication between its components within a given scope like a Personal Area Network (PAN). Essentially, the device domain is responsible for creating an interconnection between multiple devices, such as sensors and actuators, enabling data sharing environment.

Network Domain in IoT

Linking Machine-to-Machine (M2M) gateways with M2M applications is the primary role of the network domain within an IoT system. It uses Wide Area Networks (WAN) or Wireless Local Area Networks (WLAN) to ensure connectivity and data sharing between system components, no matter their geographic locations.

Application Domain in IoT Systems

The application domain forms the intermediary layer within an IoT system. This is where data captured by sensors gets processed and is made available to business logic layers. The application domain is tasked with making sense of the data and providing actionable insights that deliver value to the end-user or customer. The application domain, in essence, turns raw data into comprehensible and useful information for informed decision-making and automatic responses.

Feedback

This is the feedback I received for the design that I showed to others:

1. This is my design, how would you rate it on a scale of 1-10 based on quality?

5 Responses

ID ↑	Name	Responses
1	Dylan Bangar	9
2	Tamas Tokics	10
3	Ahmed Ahmed	9
4	Luka Radosavljevic	8
5	anonymous	10

This questions included a screenshot of the design and shows how it is highly evaluated the design is just based on the initial idea.

2. What is the reasoning for your answer?

5 Responses

ID ↑	Name	Responses
1	Dylan Bangar	Its very detail and includes IP addresses for each device.
2	Tamas Tokics	The picture explains evrything in detail
3	Ahmed Ahmed	It looks unique
4	Luka Radosavljevic	Looks good
5	anonymous	It's a good design that includes most things.

This response further encourages the idea that people who responded thought that the design was high quality, as it “includes most things”, “explains everything in detail”, and more.

3. Is the design secure in terms of safety from cyberattacks?

5 Responses

ID ↑	Name	Responses
1	Dylan Bangar	Yes
2	Tamas Tokics	Yes
3	Ahmed Ahmed	Yes
4	Luka Radosavljevic	Yes
5	anonymous	Yes

This question ensures that the system is secured from potential vulnerabilities, meaning that the design is safe to implement.

4. How would you improve the design?

5 Responses

ID ↑	Name	Responses
1	Dylan Bangar	Improving design can be a subjective matter as it depends on the specific context, purpose, and target audience
2	Tamas Tokics	Maybe add firewall/vpn between the cameras and the main system
3	Ahmed Ahmed	Add alerts going to every device
4	Luka Radosavljevic	N/A
5	anonymous	Add a door into the design and mention a notification for the alarm.

This shows potential improvements for the design that I will implement below, the idea of adding in an additional firewall and a door/application is definitely an attractive idea.

5. When I make this into an actual IoT system, what should I adjust for that?

5 Responses

ID ↑	Name	Responses
1	Dylan Bangar	Improving design can be a subjective matter as it depends on the specific context, purpose, and target audience
2	Tamas Tokics	Just configure the system correctly woth the vpn
3	Ahmed Ahmed	Nothing
4	Luka Radosavljevic	Nothing
5	anonymous	Add a password.

This was another question aimed at improving the system and shows options that I could take to make sure that the system works well.

6. Finally, are there any components missing from the IoT system design?

5 Responses

ID ↑	Name	Responses
1	Dylan Bangar	While the specific components of an IoT system design can vary depending on the application and requirements, here are a few components that are commonly essential in an IoT system: Sensors and Actuators: IoT systems rely on sensors to collect data from the physical environment and actuators to control or interact with physical devices. These components enable the system to sense and respond to the surrounding conditions.
2	Tamas Tokics	N/A
3	Ahmed Ahmed	None
4	Luka Radosavljevic	Not that i can see
5	anonymous	A door and an app.

There are both actuators and sensors in this, however I will ensure that there is a door and mentions of an application for the notification.

Justifying alternative ideas and preferred solution

The primary focus of our IoT system is to address the alarm system requirements. The system must be able to detect any movement within a room, with the assistance of a camera interfaced with a Raspberry Pi or a similar microcomputer (in the actual system, it will likely be the home network/home gateway as the microcomputer). Upon sensing movement, it's important for the system to deliver an alert to a mobile device promptly.

There are several components needed to realise this solution. The foremost requirement is for the system to possess a detection capability. By utilising cameras, capable of differentiating between different types of movement - such as a human from a pet - the system can effectively prevent false alarms.

Moreover, ensuring real-time alert notifications is a key requirement. This means a system with constant connectivity. Furthermore, the system should be simple, offering straightforward customisation of alarm settings, including the configuration of the app to receive alerts. A system status monitoring and alarm management interface should be provided, enhancing the user experience.

Beyond the current implementation, some improvements could be considered. Firstly, introducing a door would enhance the designs security and accuracy capabilities.

Additionally, in the interest of securing data integrity, a firewall between the camera and the Raspberry Pi (though in the real system this will actually be the home gateway/ home network and the raspberry pi is just for the design) should be installed. This digital firewall

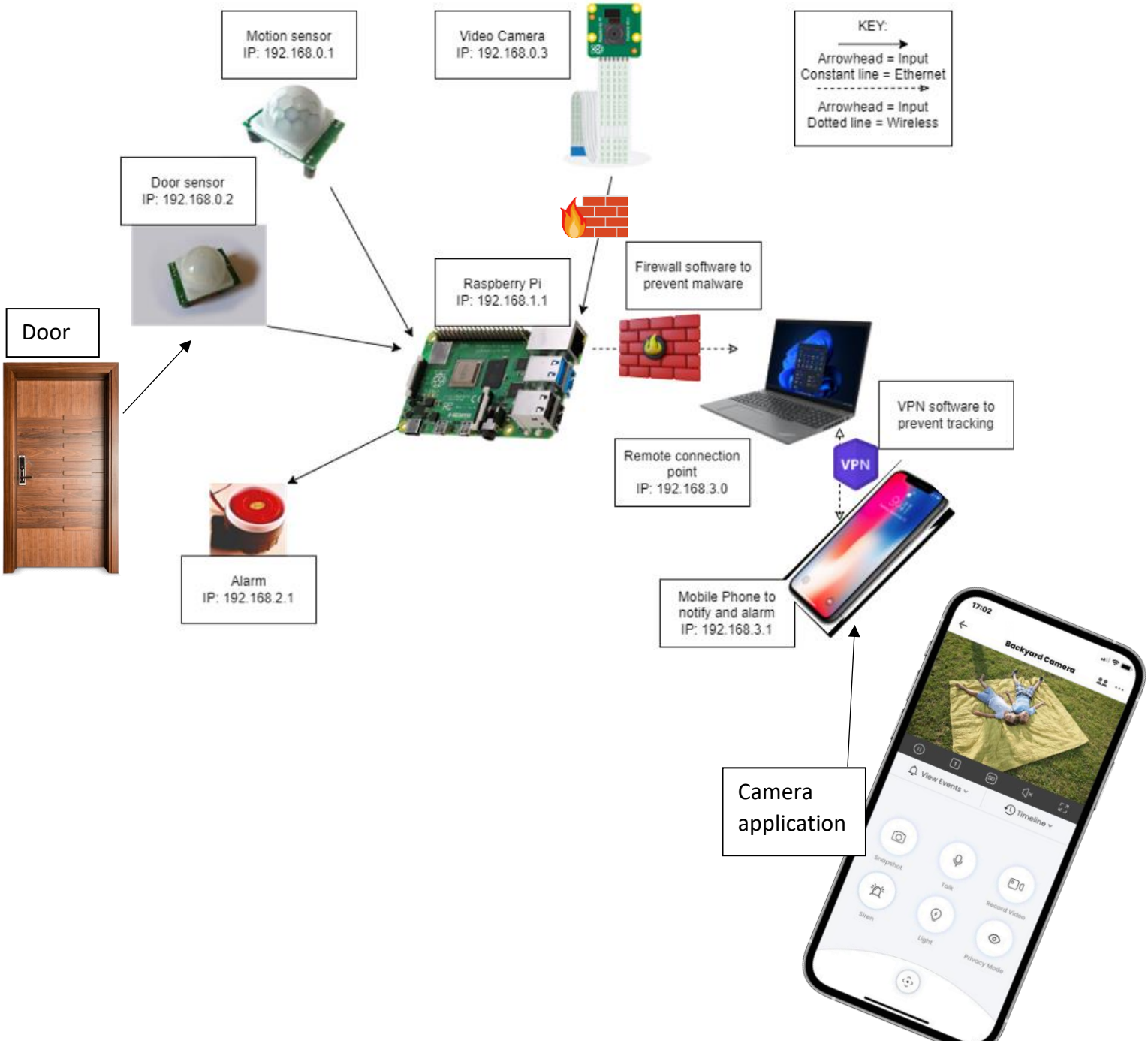
would monitor and control the network traffic, securing the system from potential cybersecurity threats.

Lastly, for a better user experience, the implementation of an application for phone notifications should be included. An app could provide real-time updates, user-friendly customisation of alarm settings, a clear interface for system status monitoring, and effective alarm management.

In conclusion, the design of the system should consider scalability, facilitating easy integration of additional cameras and motion sensors as the house expands. It's also essential for the system to remain adaptable to new technologies and standards in the ever-evolving IoT ecosystem.

Improvements on design

Following the previous sections, to improve the *design*, I will be adding a door, a new firewall, and mentions of an application on the design. This can be seen below.



Final design review

At the heart of our IoT system is the Raspberry Pi (which will eventually become the home gateway/network), which is a hub that efficiently manages multiple connections. Five key connections are in the design, with a mix of both incoming and outgoing connections that ensure the system's functionality.

Firstly, incoming connections delivering data to the Raspberry Pi (which will be replaced by the home network/gateway in the actual system) include a door sensor, a motion sensor, and a video camera. Each of these components contributes to the system's capacity to accurately detect intrusions. The door sensor and motion sensor provide discrete, targeted detection capabilities, whereas the video camera gives a view of the monitored space.

Importantly, the connection from the video camera to the Raspberry Pi (which will again be replaced by the home gateway) is secured by a firewall. This barrier plays a significant role in the system by monitoring and controlling data traffic, ensuring the protection of data, and maintaining the overall security of the system.

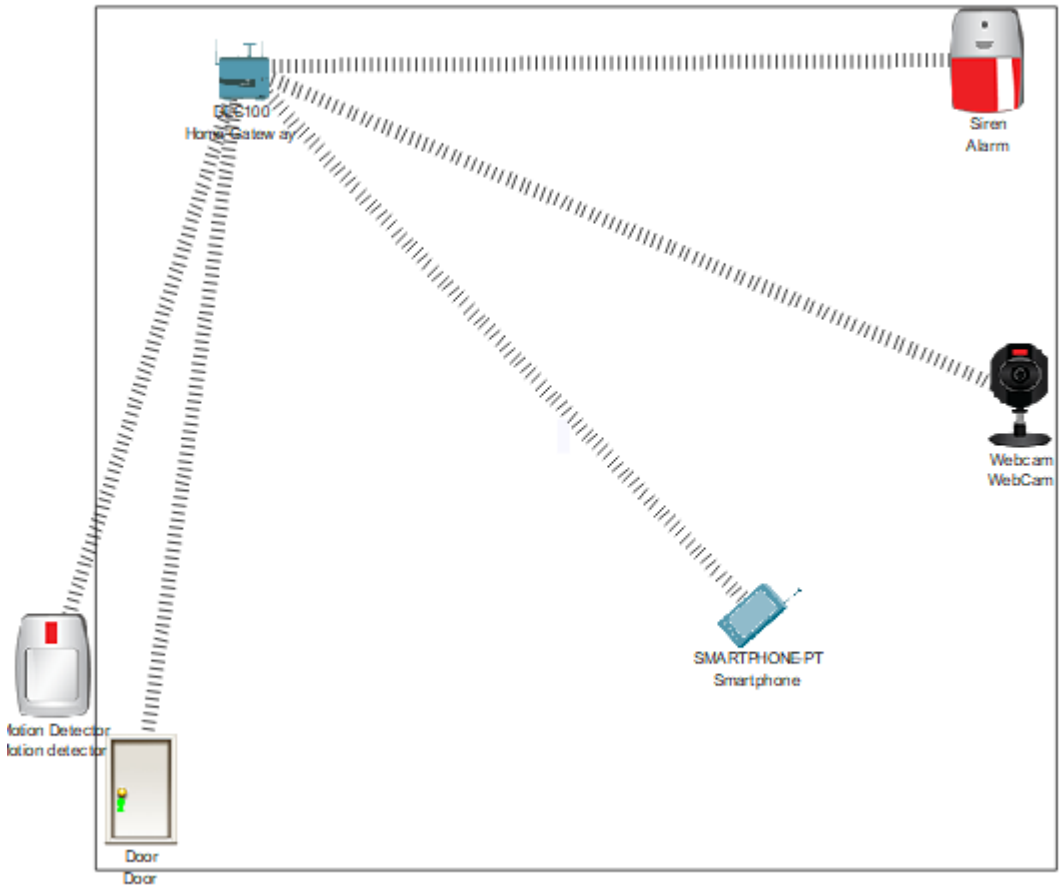
On the other end, outgoing connections from the Raspberry Pi (otherwise known as the home network/gateway in the actual system as this is the only way to make it function) include an alarm and a device capable of sending alerts to a mobile app. The alarm serves to notify the local environment of a potential intrusion, while the mobile app alerts provide the user with immediate updates, regardless of their location.

Finally, an important element of our design is the connection representing the door monitored by the door sensor. This inclusion shows the focus on securing key entry points, as well as making sure that our system can effectively monitor and alert users of any unusual door activity.

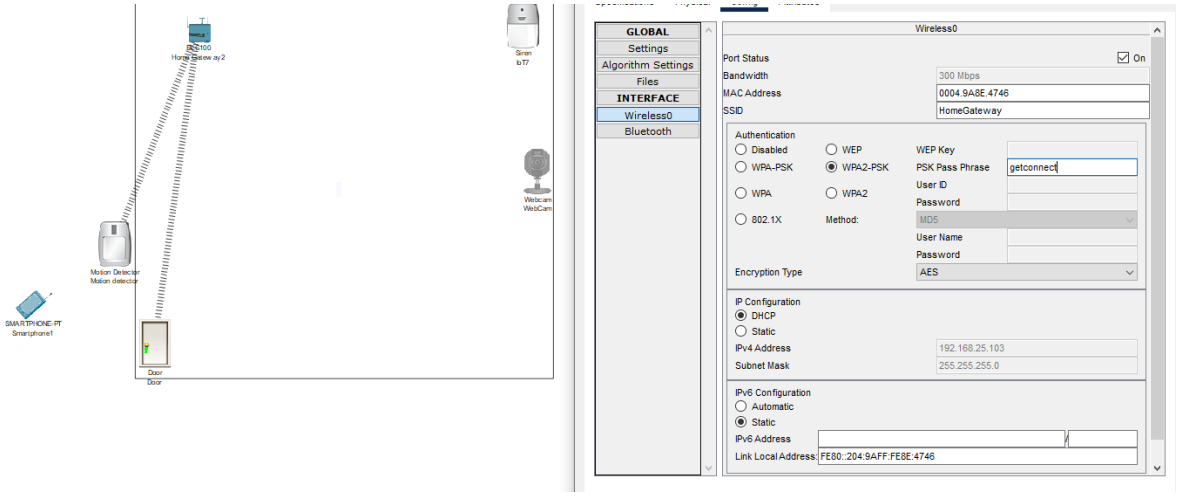
This design reviews a system that effectively includes various IoT technologies to provide a, secure, and user-friendly home security solution. It has been structured for ease of use and adaptability, with the Raspberry Pi's at its core (in the packet tracer system this will be the home gateway to make it actually functional). The design also acknowledges the need for system security, particularly through the inclusion of the firewall. Ultimately, this design aims to provide a reliable and secure IoT-based alarm system.

Creating the system

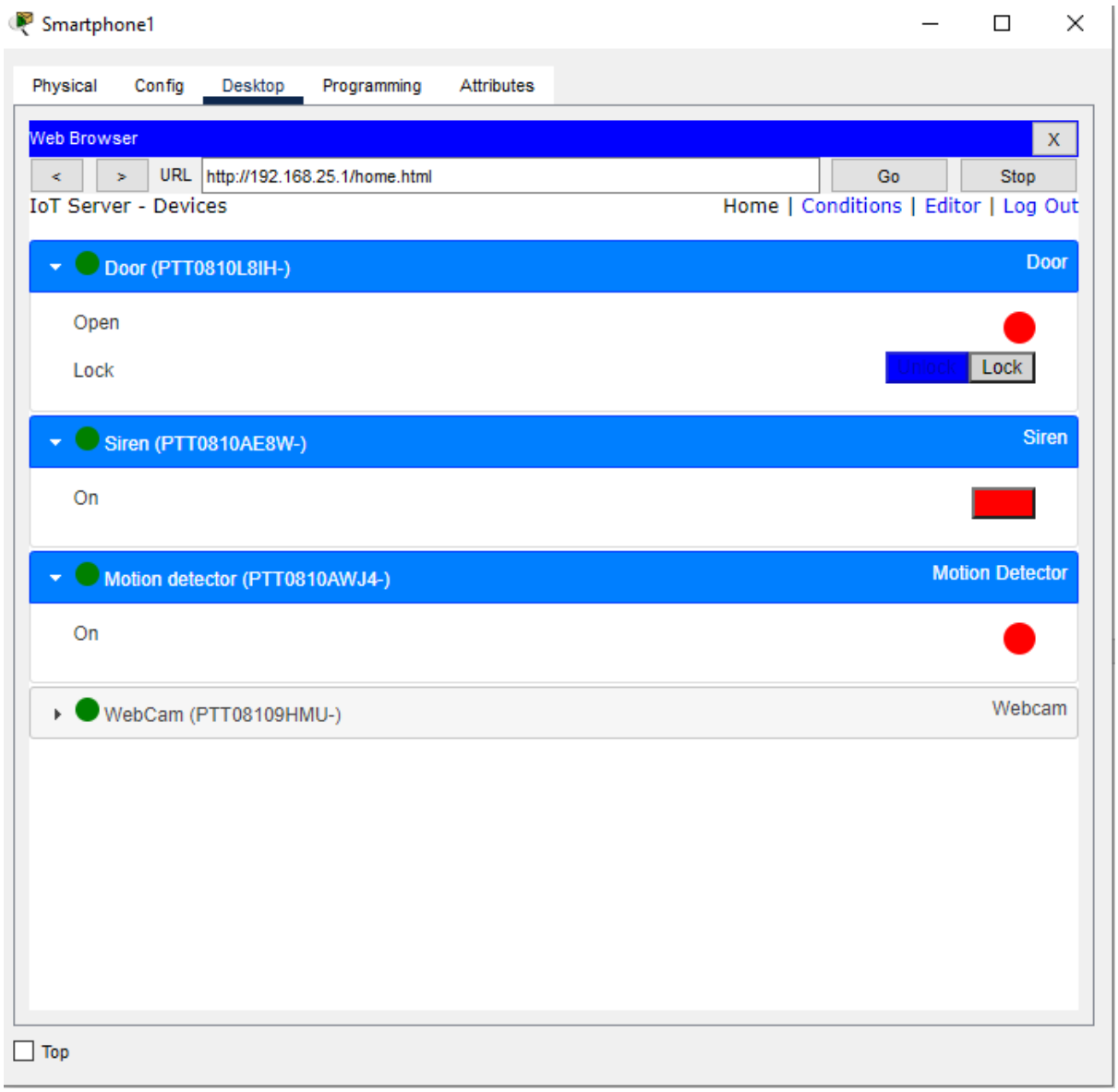
Below you can see the screenshots depicting how the system was created using packet tracer.



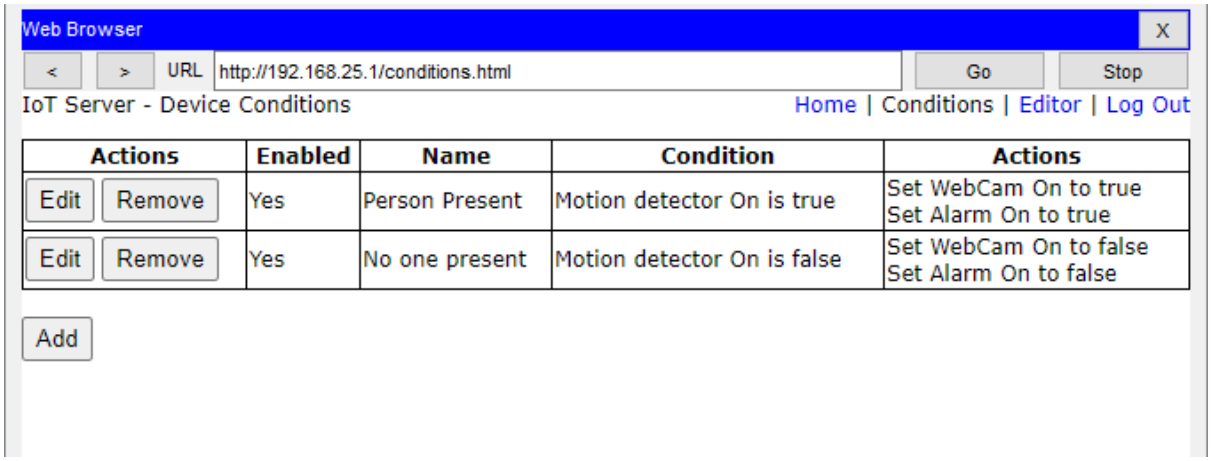
This is the initial configuration that will be optimised and improved in the future. It shows how all of the previously mentioned aspects of the system are being used, with a difference of the router being the connection rather than the raspberry pi.



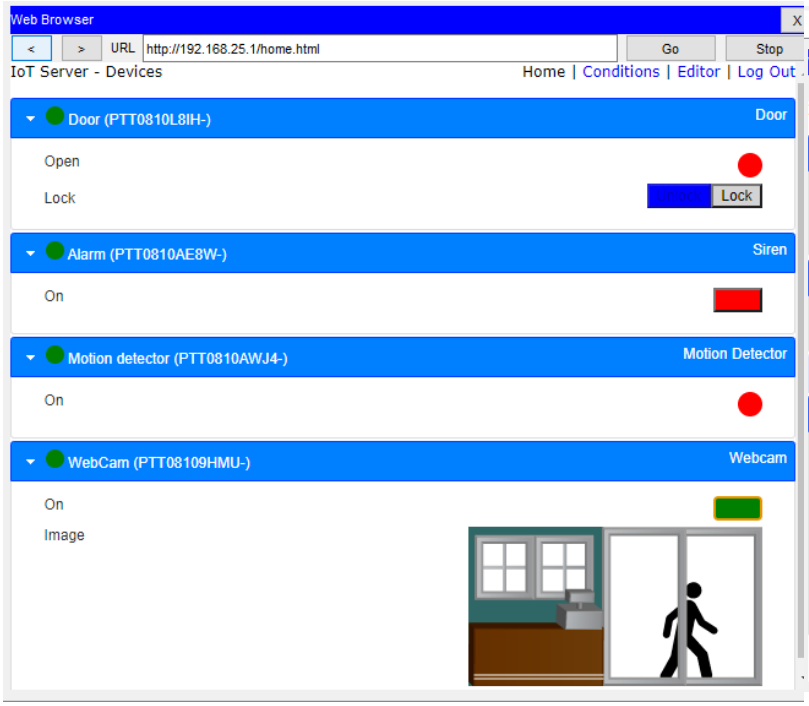
This screenshot shows the process of the first image being set up, including the implementation of the password that was mentioned in the feedback. All of the connected devices had to go through this procedure.

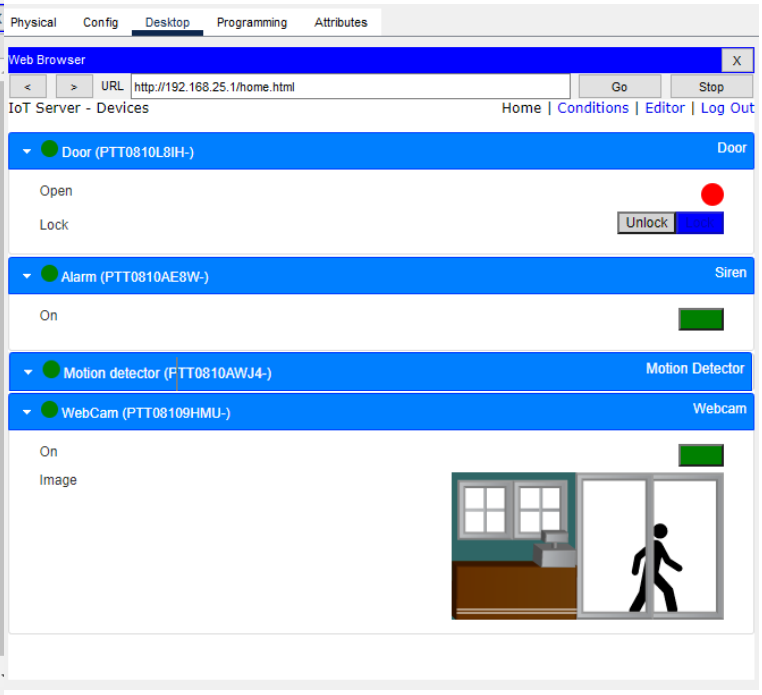


This screenshot shows how all of the devices were connected to the network, and how the mobile device was used to view these features using the internet explorer on the device.



This screenshot shows the networks conditions and statements, where "**If**" the motion detector is on, the WebCam and Alarm turn on, and vice versa for then the motion detector is off.

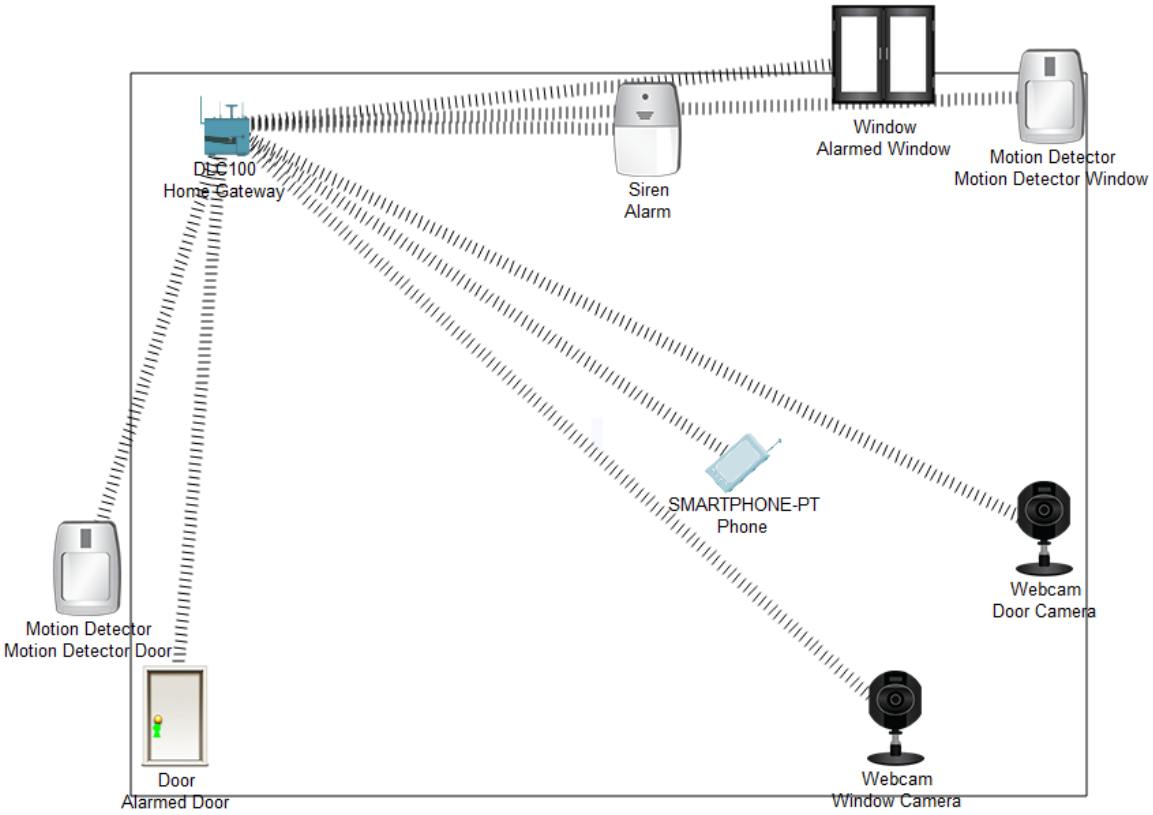




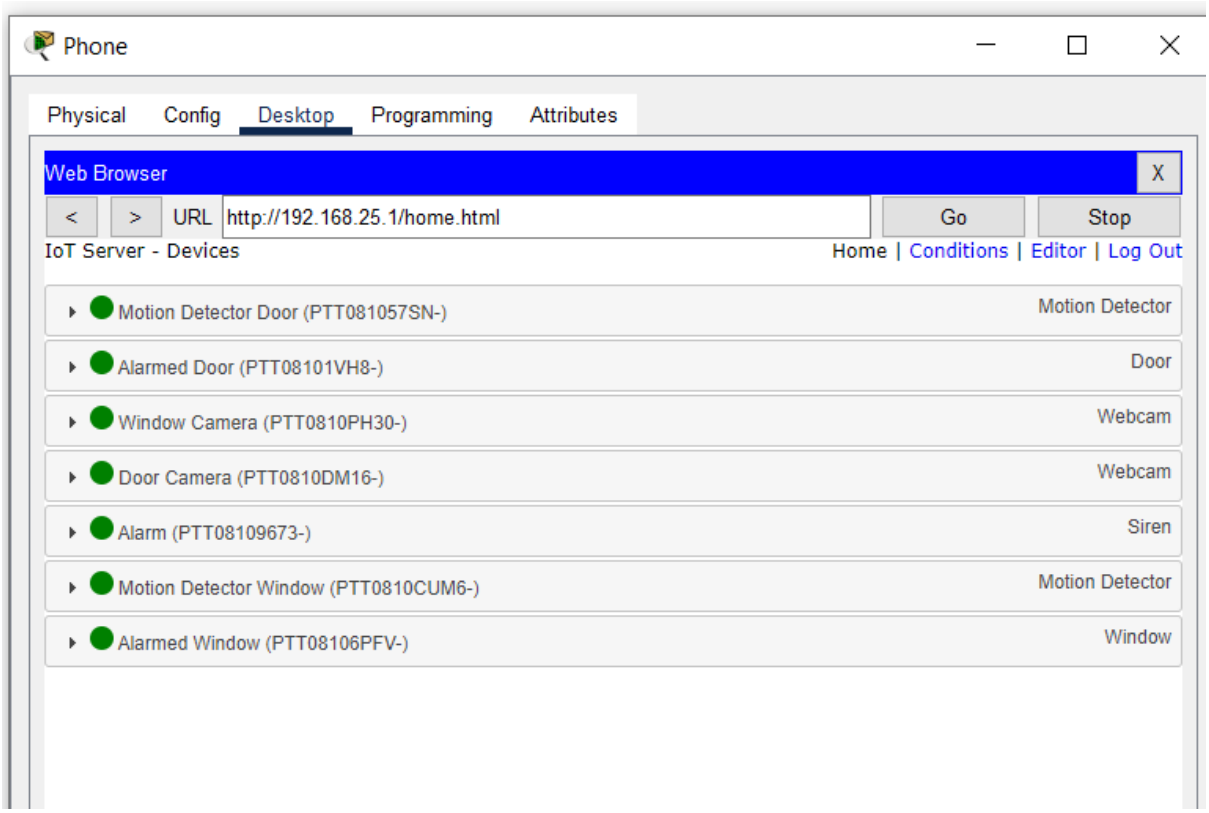
Finally, these screenshots show how the system is all turned on when the door is locked/unlocked and the motion detector it triggered.

Optimisation

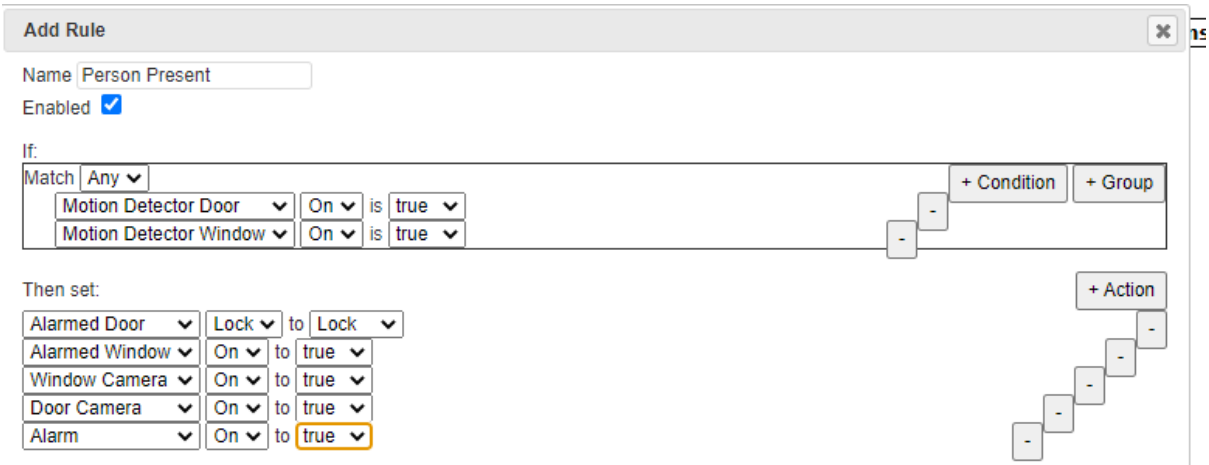
In the process of optimising our IoT system, crucial changes were incorporated to enhance its functionality. The key enhancements included the addition of a window, an accompanying motion detector, and a webcam focused on this new point of entry. These additions brought fresh security, effectively reinforcing the system's performance. In the optimised design, clear names have been assigned to each IoT device, as seen in the first screenshot, offering a clear differentiation and enhanced understanding of the system's operations.

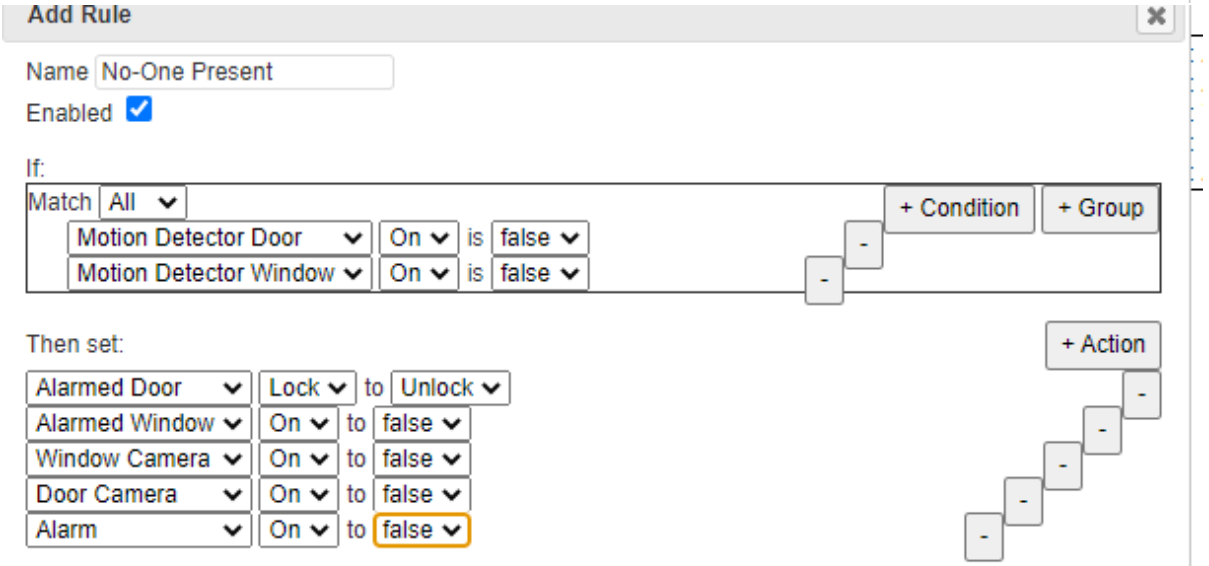


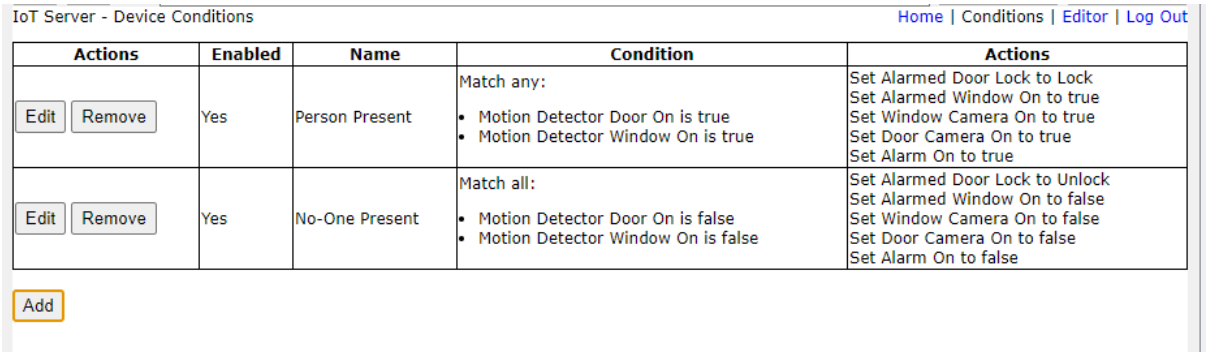
Screenshot 1 depicting more accurate classification and new devices.



This is the internet page showing all the connected devices to the network and their online status.







IoT Server - Device Conditions

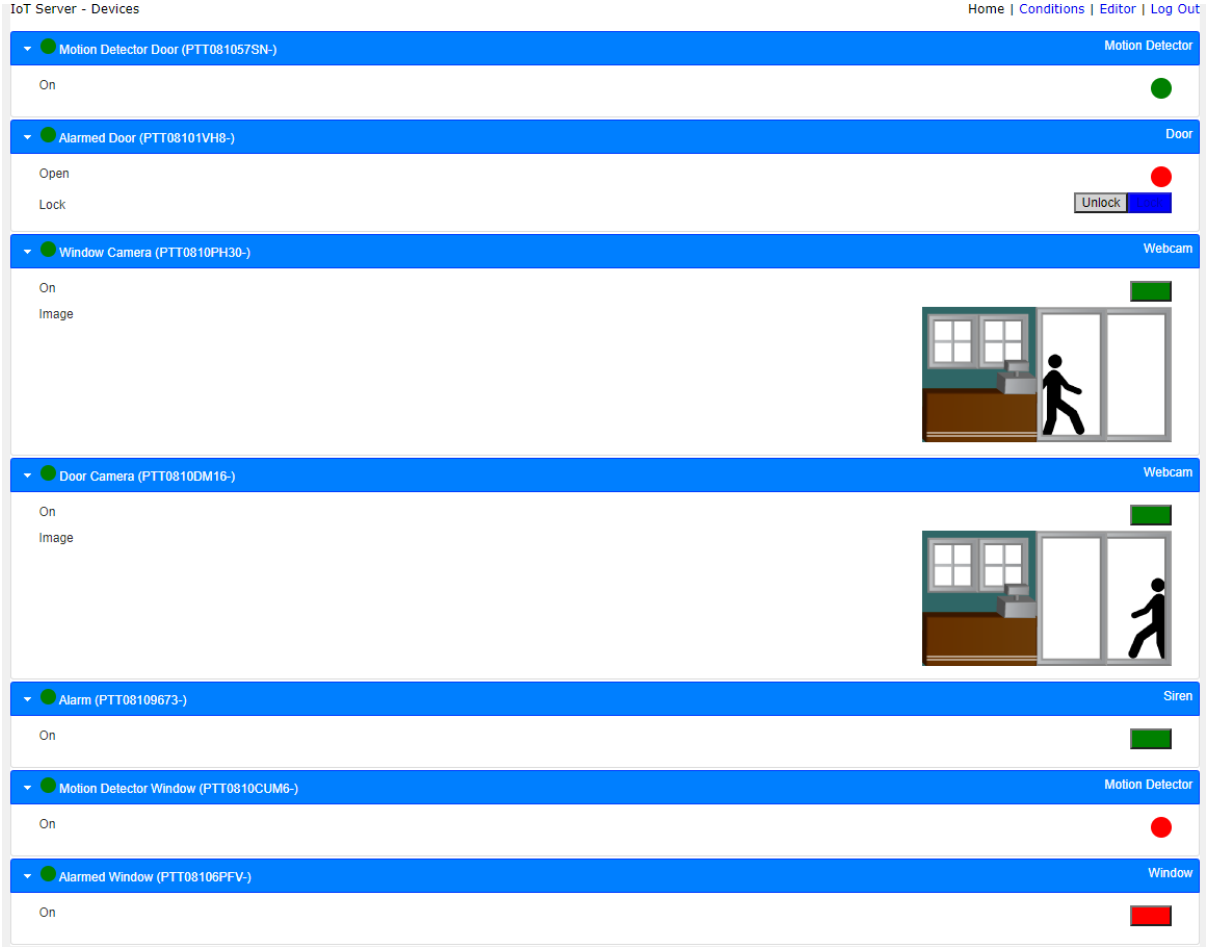
Home | Conditions | Editor | Log Out

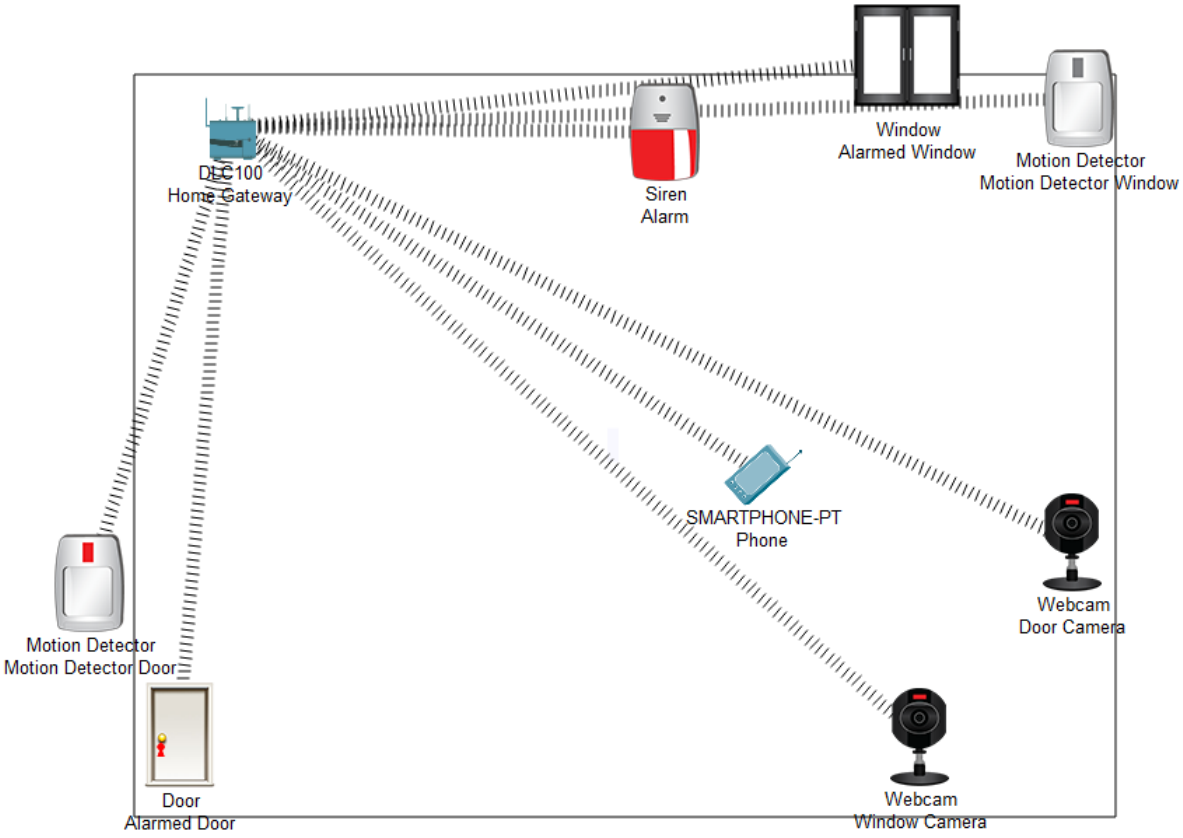
Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Person Present	Match any: • Motion Detector Door On is true • Motion Detector Window On is true	Set Alarmed Door Lock to Lock Set Alarmed Window On to true Set Window Camera On to true Set Door Camera On to true Set Alarm On to true
Edit Remove	Yes	No-One Present	Match all: • Motion Detector Door On is false • Motion Detector Window On is false	Set Alarmed Door Lock to Unlock Set Alarmed Window On to false Set Window Camera On to false Set Door Camera On to false Set Alarm On to false

Add

Further developments were made with the response of the system when the motion detectors are triggered. With the optimised system, an alarm procedure activates upon detection of motion at either of the two motion detectors. However, the alarm will only be deactivated once both detectors are turned off, thus providing an additional layer of security and certainty. This aspect of operation is shown in the screenshot above.

Moreover, in the event of the motion detectors being triggered, the response of the system is multifaceted. Not only are the webcam and the alarm activated, but the door automatically locks and the window self-shuts, adding an extra level of security. This protective measure ensures a response to any perceived threat, ensuring the maximum safety and security for the users. This response mechanism is also shown in the screenshot.





In conclusion, the optimisation of our IoT system reflects an advancement in my efforts to provide a flexible security solution. The enhanced features and the response mechanisms ensure that the system is prepared to handle potential security concerns while keeping user convenience at its core.

Evaluation

The system has demonstrated clear **strengths** in its adaptability. This is evident through the optimisation process where the system has been expanded to accommodate additional security features like a window and an additional motion detector. Each modification has been implemented with a **specific purpose**, for instance ensuring the system remains vigilant even if one of the motion detectors is off. **The system's responsiveness is another strength**. The multifaceted response, activating not only an alarm and a webcam but also locking the door and closing the window, highlights its **effective approach** to providing security.

One potential **weakness** that may arise could be the complexity of the system with the increasing number of sensors and actuators. This **complexity** could potentially lead to difficulties in setup, maintenance, and troubleshooting for the user. Another **potential weakness** could be the system's dependence on a **reliable power supply** and **internet connectivity**. Any interruptions to these could potentially disable the security system, leaving the area vulnerable. For example, in the event of a power outage, the Raspberry

Pi/Home gateway, sensors, and actuators would not function, therefore compromising the security. Similarly, any disruptions in internet connectivity could **prevent** real-time notifications from reaching the user's mobile device, delaying the necessary response. This **highlights** the need for a backup power solution and a more resilient communication setup to ensure uninterrupted operation.

Aligning the system with the client's requirements has been a crucial part of this journey. The **optimised design** shows the commitment towards ensuring the solution **fits the needs and preferences of the client**. **Feedback** from others has been **considered**, as seen in the inclusion of **additional features** such as the **window** and a **new motion detector**.

Careful planning, timely execution, and effective responses to feedback have been the cornerstone of the success. However, there is always room for refinement, learning and adaptation will be continue to happen.

In terms of the **improved system's evaluation**, the **optimised solution** does stand out as being **more effective**. It offers a **better security network**, incorporating **additional points of entry**, and **enforcing safety** measures promptly. The **successful integration** of extra security features, while maintaining a user-friendly interface and seamless operation, shows the system's progress.

In **conclusion**, the **development** and **optimisation** of this **IoT-based security system** has been a success. It **meets** the **client's requirements and provides an effective solution** for the specified problem. This is not the end, but rather a part of the process to improve IoT systems constantly.