



INSTITUTE *of*
TECHNOLOGY

CARLOW

Institiúid Teicneolaíochta Cheatharlach

Secure SCADA/IoT System to track live data

Research Report

Student: Neil Kane

Student Number: C00242418

Supervisor: James Egan

Abstract

The purpose of this project is to create a secure SCADA system to monitor live data from IoT devices and sensors. A front end web application will be implemented to monitor the readings from the sensors. It will also log the data from the sensors. The sensors will be connected using a Raspberry Pi, which will send the data. The system will have full control over the sensors for monitoring and controlling. SCADA systems are used in many industries and this project could be used for a range of monitoring.

Table of Contents

Abstract.....	1
Table of Contents.....	2
1. Introduction.....	3
1.1 Description.....	3
1.2 Deliverables.....	3
1.3 Technologies.....	3
1.4 Purpose.....	3
2. Overview.....	4
2.1 SCADA(Supervisory control and data acquisition).....	4
2.1.1 SCADA Testbed.....	4
2.1.2 HMI-Human Machine Interface.....	5
2.1.3 PLC-Programmable Logic Controller.....	5
2.1.4 ICS.....	5
2.1.5 SCADA,HMIs and PLCs working together.....	5
2.2 IoT – Internet of Things.....	6
2.2.1 IIoT - Industrial Internet of Things.....	7
2.3 Python.....	9
2.3 SunFounder Sensor Kit.....	10
2.4 Raspberry Pi.....	11
3. Potential Projects.....	12
3.1 Weather Station.....	12
3.2 Home Automation.....	12
3.3 Energy Saving on Campus or Home use.....	13
3.4 Camera.....	14
3.5 Combining Projects.....	15
4. Security.....	15
4. Glossary.....	20
5. Figures.....	21
6. References.....	22

1. Introduction

Creation of a secure SCADA/IOT system to track live data and log the readings.

1.1 Description

Supervisory control and data acquisition (SCADA) is a control system using a GUI application for supervision of machines, sensors and processes. An example being a dashboard that links to a windfarm to view how much energy is being produced and to control aspects of the windfarm. These systems are very beneficial but have security concerns.

1.2 Deliverables

- Secure implementation of Web Front End that connects to IOT sensors via Raspberry PI
- Dashboard that monitors live readings of IOT sensors
- Logging of data about the sensors
- Control of IOT Sensors
- Full security risk analysis and mitigation

1.3 Technologies

- Raspberry PI
- SunFounder Sensors
- Python
- Gitlab

1.4 Purpose

The main purpose of this Research Report is to document all research found regarding SCADA systems, IOT, reading data from sensors, Programming Languages like Python, Raspberry Pi and security. I will detail all my findings and this will help me decide on what approach to take when creating my project. My goal for the research report is to be able to use it as a tool for myself throughout the implementation stage of my project. I also want anyone who reads this to get an understanding of what I am trying to do and to understand the different systems used to monitor and control, and how they work. I will also research similar projects as to try create a project that has not been done before, or make mine unique. I will discuss the programme languages I will use, as well as any other software, devices or systems.

2. Overview

This project is going to contain features from SCADA, IOT and similar systems that are used in conjunction. I will research the systems and describe how they work. I can then make a decision based on the findings of what system will suit best for the purpose of my project.

2.1 SCADA(Supervisory control and data acquisition)

SCADA is a computer-based system for gathering and analysing real-time data to monitor and control hardware and equipment that deals with critical and sensitive materials or events.

The term SCADA came along in the 1970s to describe technological advances that allowed operation personnel to track digital information(data) from certain hardware and equipment. They were originally intended for site operators to quickly diagnose the system. The early features included real-time HMIs, Alarming, Control interface, and simple data historians. When these systems were starting, they managed to do exactly what was required of them, but over time as systems got bigger and more complex, certain issues would arise. The main concern, is the system up to date with what you are tracking and more importantly security. SCADA systems work best when used in an intended manner and not tweaked to serve another purpose. These systems were not designed to create data for engineers, accountants, marketers, or executives. They are and should be used by a group of dedicated people to monitor equipment who can react if there is a failure or discrepancy with the hardware. Although there have been many attempts to cross-platform this data into the hands of the executives or accountants, it has never been fully successful. This is when we see IOT-based remote monitoring platforms grow.¹

2.1.1 SCADA Testbed

When SCADA systems were being designed and implemented, security was not much of a priority. Even if they were made secure, the high level of attacks and cyber threats in recent years would still outmatch the security. As SCADA systems had a high cost to implement and the importance of what they were monitoring, there was never a good time to perform safe cyber-attack experiments, that would give researchers and engineers the data they needed to improve on security. This is where we see the importance of testbeds to perform any data logging and information that we can gather to properly secure a SCADA system. Previously most testbed environments that were developed, were not portable and hard to replicate. In recent times, there has been more progress regarding testbeds for SCADA systems, with researchers and developers, seeing the importance and the need to upgrade SCADA security.²

2.1.2 HMI-Human Machine Interface

HMI is a user interface or dashboard that allows the user to connect to the machine or system. The term can be associated with any screen but is most commonly associated within the context of an industrial process. HMIs are used for many things within an industrial setting like visually displaying data, monitor machine inputs and outputs and track production time. The same way we can control our heating in our house to check or change the temperature, a floor operator could use a HMI to check the temperature of an industrial water tank. HMIs come in different forms from a tablet to a monitor or a build in screen into machinery. However we see these HMIs doesn't really matter as they all serve the same purpose, to provide data into mechanical performance and progress. ³

2.1.3 PLC-Programmable Logic Controller

A Programmable logic controller is a computer with a microprocessor that has no keyboard, mouse or monitor. It receives information from connected input devices and sensors, processes the received data, and triggers required outputs as per its pre-programmed parameters. It is a form of computer device designed for use in industrial control systems. Based on its inputs and outputs, a PLC can monitor and record runtime data like operating temperature, machine productivity automatic start and stop processes and more. This means PLCs are robust and flexible manufacturing process control solutions that are adaptable to most applications. PLC hardware components include CPU, Memory, Power Supply and I/O. ^{4 5}

2.1.4 ICS

ICS describes types of control systems including devices, systems networks and controls used to operate or automate industrial processes. Within different industries, ICS functions differently built to manage tasks efficiently. There are different types of ICSs, two of the most common are SCADA and DCS(Distributed Control System).⁶

2.1.5 SCADA,HMIs and PLCs working together

SCADA,HMIs and PLCs working together

Most of the systems I have researched and described are all some shape or form of a system that allows the user to control and monitor different types of systems. This includes reading data, monitoring information and controlling different machines. The more I researched these systems, I realised that most of these systems are integrated. SCADA systems are a type of ICSs. HMIs are an important part of SCADA systems. When we talk about these different systems and devices, there is a few things to note.

A PLC is a piece of hardware, something physical. While SCADA is software, that operates on a computer system. It is sometimes compared to an Operating System like Windows. Another key thing about SCADA and PLCs are that SCADA is

designed to control the whole system, monitoring all devices and collecting data from all inputs. On the other hand, PLC focuses on one element of the system. The two best work together as PLCs are part of the system that SCADA oversees.. The PLC need SCADA to control their function but SCADA relies on data from the PLC to properly monitor. The two communicate to create the best and safest system. If a PLC collects data that a piece of equipment is running too fast for example, the PLC will transmit the data back to the SCADA software. SCADA will analyse this and determine if an adjustment is needed to the system. If so the SCADA will send the changes back through the PLC to make this change happen.⁷

2.2 IoT – Internet of Things

The Internet of Things refers to a set of “things” or devices connected together through the internet that can share data without human interaction. It is looked at as one big network, connecting everything. There are billions of devices connected and passing data back and forth. These “things” are physical devices usually fitted with sensors, processing ability, and software. The IoT is at an all-time height of importance, as industries and technology grows, the IoT is expanding. With more devices than ever before connected, we are starting to rely more and more on the Internet and the IoT. In our own homes, we can see IoT system in play, from our phones to laptops and now with smart homes, the list is growing.

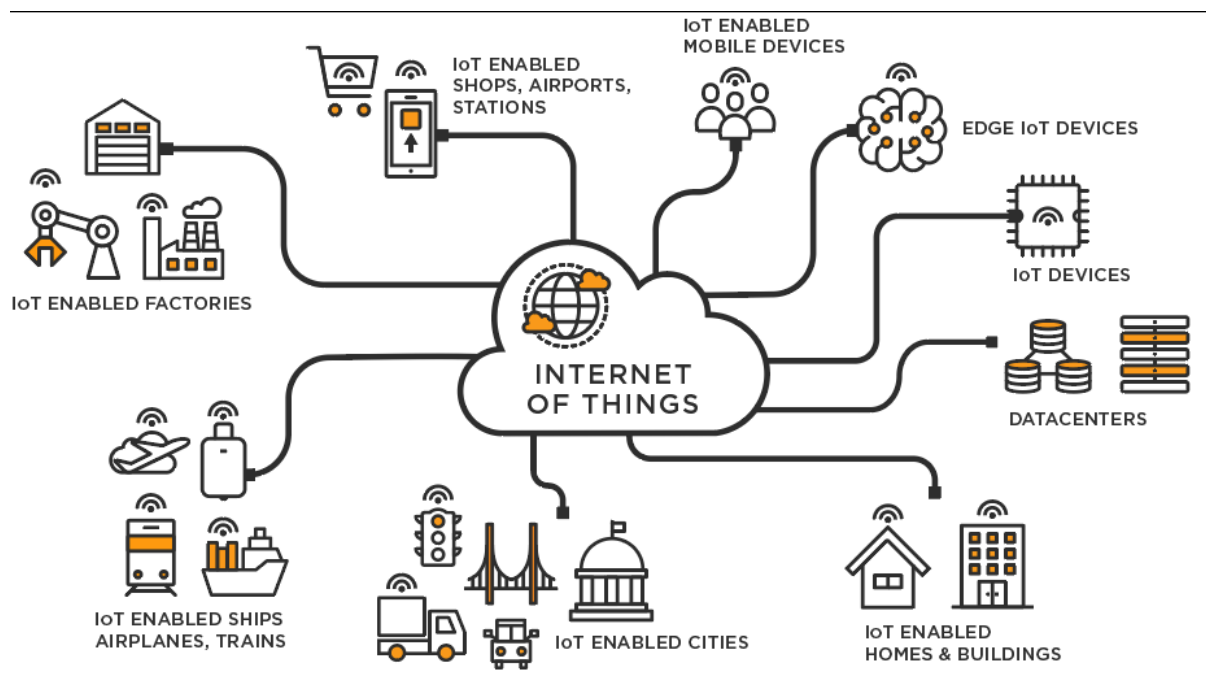


Figure 1-Internet Of Things

There are many examples of IoT devices and/or systems, from smart watches to hospital equipment. The devices can gather, save and transfer data. Any smart device is categorized as an IOT, watches, phones, refrigerators. All these devices are fitted with many different sensors and are connected to the internet. We can gather much data from these devices and monitor and save information. As the IOT is growing all the time and at a drastically high rate, it is estimated there are 46 billion

devices. Industries also rely on these IoT devices, which are now being called IIoT.
89

IOT describes objects that are embedded with sensors, processing ability and software that are connected and exchange data with other devices and systems over the internet or other communication devices. Most IOT based remote monitoring platforms offer a variety of integration tools that use modern protocols such as MQTT(MQ Telemetry Transport), which is a lightweight open messaging protocol. These type of protocol's allow getting data directly to the point of need, meaning getting equipment data directly into tools. These tools include accounting software and business intelligence dashboards and ERP systems. This is the big difference between IOT and SCADA systems, that many people believe IOT systems are the way to go as they allow the data to be giving directly to the different groups.

The figure below shows just how much can be connected within a Smart Home, which is connected and part of the Internet of Things



Figure 2-Smart Home

2.2.1 IIoT - Industrial Internet of Things

IIOT refers to the extension and use of the internet of things in industrial sectors and applications. It is often referred to as a sub category of IOT. The IIOT encompasses industrial applications, including robotics, medical devices and software defined

production processes. As different industries grow and change, everybody wants quicker and more reliable ways to perform any task or job. IIOT is now at the forefront for this, it allows the industry to develop systems for monitoring, gather and analyse data at a greater rate than humans and in real time. IIOT can be beneficial in many ways within industries, an example being saving time and money by finding problems and errors quicker. In a manufacturing environment, IIOT can be used for quality control, traceability and even efficiency. As I have stated IIOT is like an extension of IOT, so it has many of the same principles, but maybe on a bigger scale. It still uses smart devices connected together through the internet. This system then collects, exchanges and analyses data. Many industries are starting to use IIOT, an example of one of these is the automotive industry. The IIOT devices are used in the manufacturing process, where industrial robots are used and IIOT helps to maintain the systems and find problems before they cause disruptions to the production line. Agriculture is another industry that has taken advantage of IIOT, using sensors to gather data and a range of things from moisture to soil nutrients.



Figure 3-IoT Applications

Some of the benefits in using IIOT system are cost saving in a range of fields. Organisations can use real time data to see when a machine needs a service. It can also pinpoint easier where an issue is coming from, instead of human interaction, trying to figure it out. Another major reason is data gathering allowing for data to be shared with your client or customer.

This then brings us to the concerns of IIOT, much like everything in the IT sector, the main concern is security.

Like its counterpart IoT, the IIoT is as secure or unsecure, as we make them. One company could have the same machinery, sensors and devices but one could be a security risk, while the other was safely and securely installed. In 2014 many

technology companies came together to form the Industrial Internet Consortium(IIC). The group was initially set up to further the development of technology and to accelerate the IIoT to more companies and industries. A big focus was security, even creating a security working group.¹⁰

2.3 Python

Python is a high-level programming language and was first released in 1991 by Guido van Rossum who started working on it in the late 80's. It is considered one of the more popular languages, and is a general purpose language, meaning it can be used in a variety of development. One of the main features contributing to the success of Python is the ease of use, compared to other programming languages. It is highly recommended for beginners as a starting off point as the code is more readable.¹¹

“Python is now also the language of amateurs, and I mean that in the best possible way.” —Guido van Rossum.¹²

With the ease of readability it also keeps the cost down on program maintenance. Python also encourages code re-use and sharing code across all platforms freely.¹³ The use of libraries also make it very desirable, for many projects, there will be a library to get you started so it's not always a case of starting with an empty canvas. We also see the popularity of Python based on Stackoverflow's annual survey from 2020. We see that python has 44.1% beating out the like of Java and C, C++ and C#.

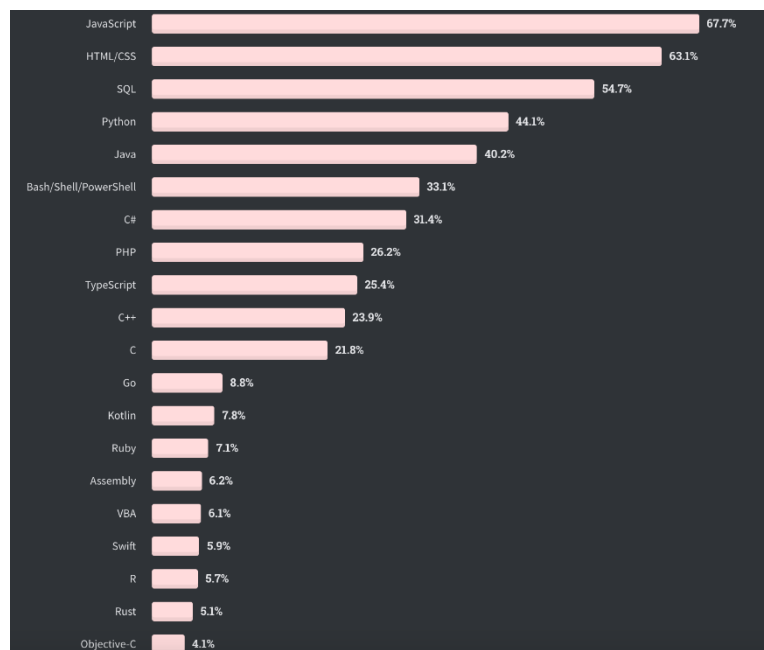


Figure 4-StackOverFlow 2020 Survey

As my project will be based around a raspberry pi, I looked at a wide range of forums and other projects online.¹⁴ The most widely used seemed to be python and python

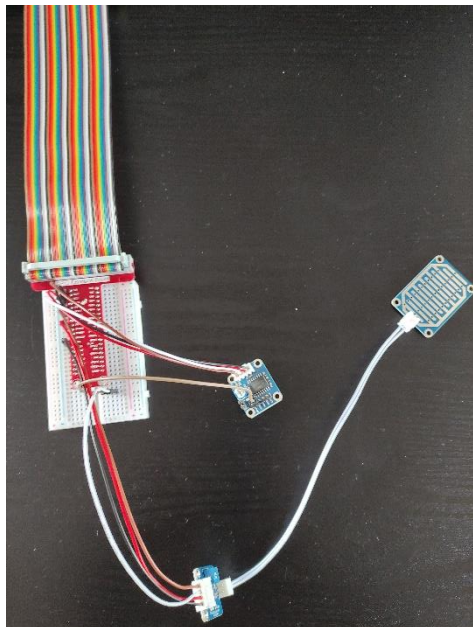
is fully functional and operational on raspberry pi from out of the box. I will also be using a range of sensors with the GPIO, which python has a range of extensions specifically for this. As I have never used python before I liked the idea of learning a new programming language for my final year project.

Flask is a web-framework written in Python. This provides a user with libraries and tools to develop web applications.¹⁵ Flask is considered a microframework which is designed to keep things simple and scalable. Flask is a popular web framework which means it's up to date and there are plenty of interesting projects to guide me for ideas.¹⁶

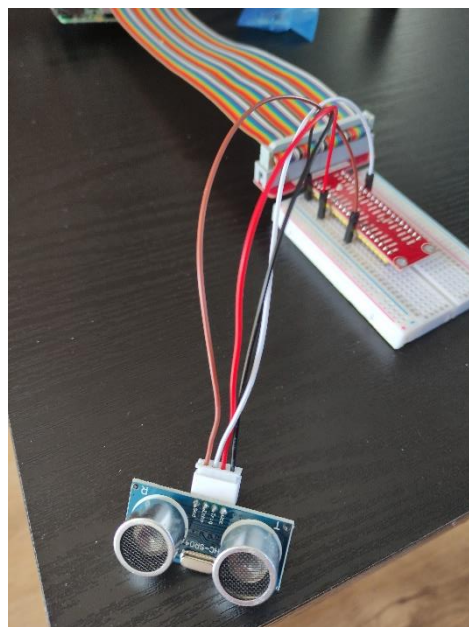
2.3 SunFounder Sensor Kit

The sensor Kit includes 37 sensor modules. It is marketed as a learning kit for use with a Raspberry Pi. It can be used as a way to teach or learn about programming and very useful in creating a wide range of projects. With so many different sensors, the kit has many functions and can be used in many ways to create a new project or to familiarise yourself with programming and controlling, turning on and off these sensors. Some of the sensors included are temperature sensor, sound sensor, gas sensor and a whole other range of sensors that can be implemented in unique ways to create a project or to learn.¹⁷ As part of the research I have worked with and implemented some of these sensors to familiarise myself with them. I followed the instructions provided to get comfortable connecting the sensors with specific cables to the breadboard. The photos below, that I took show the type of connection that is needed to wire and connect the sensors.

Rain Sensor



Ultrasonic Range Sensor



Intelligent Sensor

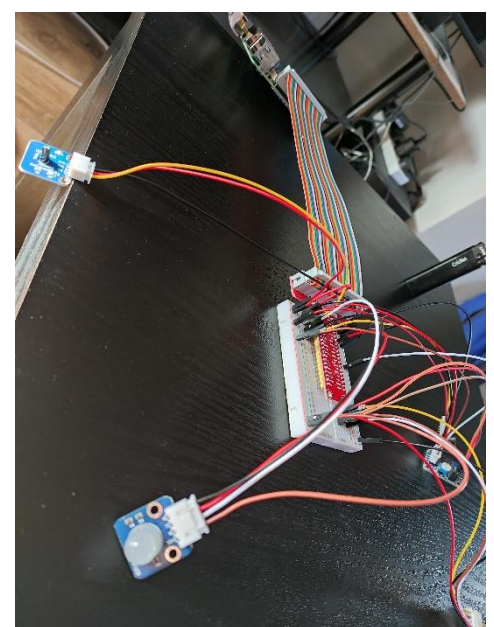
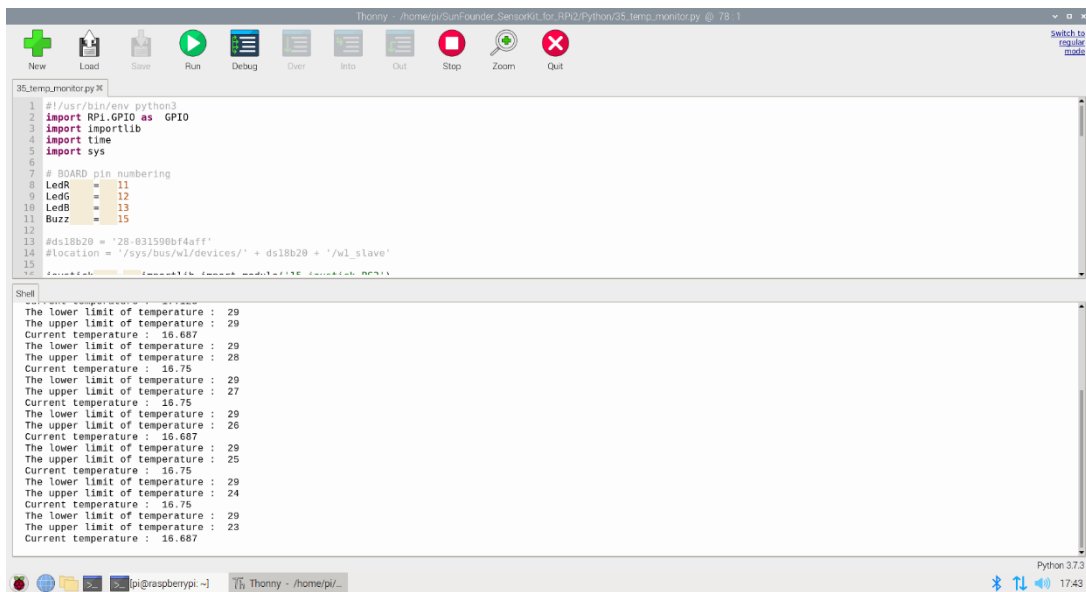


Figure 5-My Connection Photos

The Image below shows the output from running the intelligent sensor setup



```
1 #!/usr/bin/env python3
2 import RPi.GPIO as GPIO
3 import importlib
4 import time
5 import sys
6
7 # BOARD pin numbering
8 LedR = 11
9 LedG = 12
10 LedB = 13
11 Buzz = 15
12
13 #ds18b20 = '28-031590b4aff'
14 #location = '/sys/bus/w1/devices/' + ds18b20 + '/w1_slave'
15
16 # Import the module
17 importlib.import_module('186_SensorKit')
```

```
-----
The lower limit of temperature : 29
The upper limit of temperature : 29
Current temperature : 16.687
The lower limit of temperature : 29
The upper limit of temperature : 28
Current temperature : 16.75
The lower limit of temperature : 29
The upper limit of temperature : 27
Current temperature : 16.75
The lower limit of temperature : 29
The upper limit of temperature : 26
Current temperature : 16.687
The lower limit of temperature : 29
The upper limit of temperature : 25
Current temperature : 16.75
The lower limit of temperature : 29
The upper limit of temperature : 24
Current temperature : 16.75
The lower limit of temperature : 29
The upper limit of temperature : 23
Current temperature : 16.687
-----
```

Figure 6-Output From Intelligent Sensor Lesson

As we see from the above images, there is a wide range of cable and connections needed. These can be as simple as a 2 pin connector from the sensor to 2 cables into the breadboard and be as complex as the Intelligent sensor image. This demonstrates the need to understand the connection and how the sensors and cables can work together.

2.4 Raspberry Pi

The Raspberry Pi is a low cost credit card sized computer that can plug into a monitor or TV. It uses a system on a chip, which has the CPU and GPU in a single integrated circuit, with RAM and USB ports soldered onto the board. It uses a mouse and keyboard. It is a great device for learning and experimenting. We can learn and use programming languages like Python. The Raspberry Pi was initially designed for an inexpensive computer for teaching programming, but users soon realised the power of the Raspberry Pi for projects regarding a huge range of things.

There are many advantages and disadvantages to this device, like everything. Some advantages are the size, its open source and a low cost machine. A few disadvantages are low processor and unable to perform complex multitasking. The Raspberry Pi is as secure as the user makes it. As the Pi will not always be online for some users, security would not be an issue, but if we wanted to connect the Pi to IOT device, we have to make sure we secure the device.¹⁸

Raspberry Pi3 Premium Kit comes with micro-SD card has NOOB software pre-loaded. If we want to choose an OS, we can do this by connecting to the internet before we turn it on. If we turn on the Raspberry Pi without connecting to the internet, Raspbian OS is installed

The Operating Systems available for Raspberry Pi are :

- Raspbian
- Pidora
- OpenElec
- RaspBMC
- RISC OS
- Arch
- Linux

3. Potential Projects

All my recommendations for proposed projects all fall under similar ideas regarding the data collecting and monitoring. All of my research on SCADA and IOT, will come into play in some way with any of the researched project ideas. A weather station will have a SCADA like system. Home Automation will be a mixture of the mentions systems, (IoT, SCADA). Energy saving project will also still have these two incorporated with different devices to gather the information, which will still be monitored and needs to be secure. As all the mentioned projects use a variety of devices and will be connected to the internet, we need to secure the system.

3.1 Weather Station

Using a Raspberry Pi to create a weather station reading control system. Using a variety of sensors from the sunfounder sensor kit, I will take readings from the sensors. The readings and data will be sent/linked to either an IoT service or to a webpage acting as a SCADA system. There are many libraries and tools that can be installed on the Pi to help with things like the data of certain sensors or input data. One way is the send live readings to a CSV file. We can then import the CSV file into our program and display the data. I would also use the DHT and python library. The DHT library is for humidity and heat sensors, while the python library is used for nearly all the implementation. The data sent back from the sensors, will be fed to the user in graphs, plain text and any other format to make it easy to read but also look like a monitoring station.

3.2 Home Automation

With the constant growing and evolving world of technology. There may be none more evolving than the Internet of Things. This is a system we are all connected to in some way and adding to it every day. We are now seeing more Home Automation, with the development of many household items, now coming with sensors and devices connecting them to the IOT. An idea for a project is to develop a smart home/home automation system to control and monitor devices used around the home. I will create a web based system to monitor and control any device that will be

incorporated into the system. I can use sensors for temperature, cameras smart lights and more. The main concern will be to securely implement this as there will be lots of devices connected to a home network, opening it up for attackers. All devices will have to be secured, as well as the web based controller, which will monitor all devices.

3.3 Energy Saving on Campus or Home use

Upon researching many options to create a system that I can monitor, control and read in data, an exciting one was about energy sustainability. Once again this sees an IoT platform with wireless receivers used to monitor the energy usage. If this project was successful the idea could be done at a home, office, hospital etc. to try to improve on the energy efficiency for a wide range of people and areas. My proposed idea is to test this in the college, I could test a new building and test an older part of the building and compare the both. This data could show where energy might be being wasted or where areas can improve. As a University or College hosts 1000's of people on campus, the energy usage will be extremely high. A project like this might highlight just how much is being used and show us the growing need for smart campuses.

Energy usage in any building the size of a college or university is always going to be extremely high. This is not going to change when we take not account the huge numbers of people that a college serves. The amount of equipment used in colleges, are also extremely high. If we just looked at the computers that are on a campus alone. Then there is also heating, air-con and lights to consider. The amount of energy consumed is always going to be high, but this doesn't mean it can't be improved on. If we could monitor the energy of a campus and either try to lower it once we seen the data or even improve on it by implementing new technologies to help us bring it down altogether. There are many ways this can be done like the standard ways, new windows and insulation etc., but what if this is out of budget or we already have insulation.

One proposed way is to create a system to try monitor the levels of energy used in varies areas of the campus. This will help pinpoint where more energy is being used or even wasted. There is obviously going to be massive discrepancies in different buildings as the sizes of the buildings differ, the footfall and equipment will be different in each building. The time of year and weather will also show different results. The main goal should be to find out how much electricity is being used in a particular building or room and see if we can improve on it. This project could be used in a home either.

An example in a home would be a temperature sensor, which can recommend if it hits a certain temperature to turn on or off the heating. I could connect an alarm, lcd screen and the temperature monitor to a raspberry pi. The lcd screen would display the temperature at all times. If the standard room temperature is 20-22 degrees

Celsius we could have a sound/alarm sensor beep when the temperature drops to low or goes to high. The data would also be fed back to us.

For my project I looked into designing an Internet of Things(IoT) platform incorporated with wireless devices to gather information and data on energy being used in various parts of the campus. A web based system will be designed which will allow me to monitor and control the system. An example of the devices used for this are SONOFF products. SONOFF is a company that sells a wide range of home automation devices, from home security to smart lights and smart plugs. They also have a great range of Wi-Fi enabled devices to monitor energy consumption like the Sonoff POW R2 below.



Figure 7-Sonoff Energy Monitor

An example of a test I could run is to just let a device monitor the energy used in the network lab for a week. I will then have the data sent to my web based controller. The following week I could use the same device and control what gets turned off when, and be more conscious of what energy is being used in that week. When the information is back from the 2 weeks, we have a baseline to start comparing data. On the web based controller we can chart the differences and see the high points for each week to find out what might be causing it.

The MQTT is a simple messaging protocol used to deliver messages between devices. It is useful solution from IoT applications. It allows us to send commands to control outputs and read data from sensors.¹⁹ Here we can use the Raspberry Pi as a gateway for accessing the data from the sensors.

3.4 Camera

I also looked into the camera feature to be used with the raspberry pi. This fits the security team as a camera can be used in a variety of ways. I looked up projects using recording features and connecting to a doorbell. I also investigated facial recognition projects and having the camera recognise an inputted user. We train the

Pi to recognise a user by inputting a range of photos at different angles to help verify a user.²⁰ To install the camera we just connect the ribbon cable of the camera into the slot on the Pi. Once this is connected we run through a few commands like update and upgrade. The libcamera²¹ library is then up to date and ready for your camera to take photos and videos. If we want to use it for anything beyond this we can install the necessary libraries or programmes.

3.5 Combining Projects

After researching different idea and themes, I realised I could create a project that incorporated aspects from many areas of my researched projects. Rather than just monitoring energy usage, or just a weather station, I could create a system that allows us to monitor and give us control over a combination of systems. I will still use the sensors to act as a mini weather station and send the data back to the web application. I will use a temperature sensor to read the temperature in a home and could add an lcd screen to display the temperature, while also reading in the data. I will have control of this to maybe display the humidity also. I will also use Wi-Fi enabled devices to read the energy usage in a home. This could still be used in the college also, as I think that would give more important readings. This device should be able to act as 3 of these projects as I choose. I will do this in a control centre, with each having its own page with different information and data. The LCD screen might also be able to display the energy usage at intervals, e.g. daily or weekly readings.

UPDATE

The Energy monitor did not work out, as the product I wanted to purchase to use was not compatible with a DIY mode, they had their own interface. Initially from what I was reading this could be done, but it was a different product from the same company.

I have now began work on a facial recognition security Pi.

4. Security

This security section is broken down into two section, the first is the research of what I may use to implement on the Pi. The second acts as a reference or guide of common attacks some of which I will implement.

The raspberry pi has some basic security concerns from out of the box, like the generic user name and password on all pi's are the same. This leads to issues as if we do not change these it's easier for a user to gain access through SSH. If someone had physical access to your device this is the credentials they would try as they are the generic credentials.

The raspberry pi does not come with a firewall, but we can install UFW on the pi, which stands for Uncomplicated Firewall. This allows us to create a type of IP tables,

allowing certain IP addresses access and denying others. We can allow an IP address access using certain protocols and deny them against others.

Fail2Ban is another security feature that can be installed on the Pi. This helps us fight against brute force attacks, which are extremely common on the Pi. If a wrong password is typed in a set number of times the IP address is banned for a set amount of time. We can adjust the amount of tries and the duration of the ban.

SSH is also a security concerns with the Pi, once again because the generic credentials. If we changed these, there is till more we can do. We can change the default port for SSH, as an attacker will initially try Port 22.

We can also set up SSH authentication, which uses a public and private key to sign in. This takes away the need to use our password to gain access although we can still use a passphrase for an extra layer of security. An attacker could not brute force the password as they need the key.

Although I will not implement all security listed below, these should always be considered of areas of concern. I included this as a guide for people to learn from and maybe become more aware of the large list of potential attacks. Some of these include a quick mitigation, while others are just to make you aware of them.

Wired and wireless scanning and mapping attacks

There are several types of attacks that are used to target wireless networks. One of these attacks is Packet Sniffing, this captures the packets as they travel through the wireless network. A lot of this data is sent in plaintext, making it easy for an attacker to target and gain access to sensitive information like passwords. We should make sure this data is encrypted, although an attacker could still gain access it would be much harder when the data is encrypted. To help prevent these attacks we should always be scanning and monitoring the network.²²

Another attack we see used on wireless networks is a Man in the Middle Attack(MITM). This type of attack is used on many systems and involves an attacker gaining access to your data by intercepting it in transit or tricking you to send it them directly, without your knowledge of this happening. An attacker can alter the data you receive back from your request. They could have installed malware and once again you unknowingly go along and potential have malware attacking your network or device. A simple thing like typing in the URL instead of clicking links, has the potential to avoid this type of attack. We can also try use HTTPS websites, as they are designed to avoid these type of attacks.²³

An attacker can also cause major disruption using a WIFI jammer. This could include flooding the access point with unauthenticated frames. This cause the network to crash and become unusable by anyone. Although this might not be used specifically for stealing data. In can cause major issues and a company could lose huge

amounts of money. It could also be used as a distraction for another attack. We can use Intrusion Detection Systems(IDS) to help prevent this jamming.²⁴

Other potential attacks include Wardriving, Warshipping and MAC spoofing.²⁵

Protocol Attacks

Protocol attacks are intended to target network resources like servers and firewalls. They use up the processing power of these devices. Under the title of Protocol attacks, there are a variation of attacks that fall under this category. These attacks include SMURF attacks and SYN attacks, although there are many more. The similarity with these attacks are they all need many attackers(zombies) to perform. These are also very similar to a brute force attack.²⁶

A SMURF attack is a type of Denial of Service(DoS) which uses ping traffic to flood the network. It can also exploit vulnerabilities within the Internet Protocol(IP) and Internet Control Message Protocol(ICMP).²⁷ To help prevent this attack we can block directed broadcast traffic coming into the network. We can also configure routers and hosts to ignore and not respond to ICMP echo requests.²⁸

SYN attacks also known as SYN flooding and TCP SYN attack also falls under the DoS. An attacker uses the IP/TCP protocols to repeatedly send SYN requests which in time floods the system making it become unresponsive. As the SYN requests are sent by an attacker, the server is waiting for acknowledgment(ACK), but the attacker will not respond. This causes the server to keep the SYN requests in a queue which continues to build as more requests come in eventually causing it to crash. We can defend against this by installing an Intrusion Prevention System(IPS) which will detect traffic pattern. We can also tweak the TCP stacks which might not prevent it but will limit the damage. We can reduce the time until a stack frees its memory which was allocated to a connection.²⁹

Other Protocol attacks include Authentication server attack, ICMP attack and CGI request attacks

Eavesdropping attacks (loss of confidentiality)

An eavesdropping attack also referred to as a snooping or sniffing attack, is when information is stolen as it is transmitted over a network by a number of devices like a computer or smartphone. A common example of this type of attack is the Man in the Middle Attack. Although this fell into the category of wireless attacks it is also a eavesdropping attack, as with other types of attacks they fall under different categories or are just known by several names.³⁰

Mitigation = Some of the tools we can use to prevent an ease eavesdropping attacks are similar to other attacks, as they fall under similar categories. A big line of defence is encryption, emails, networks and communications should all be encrypted. If data is stolen, an attacker would not have the key to decrypt it. We can also monitor the network for strange activity using an IDS.³¹

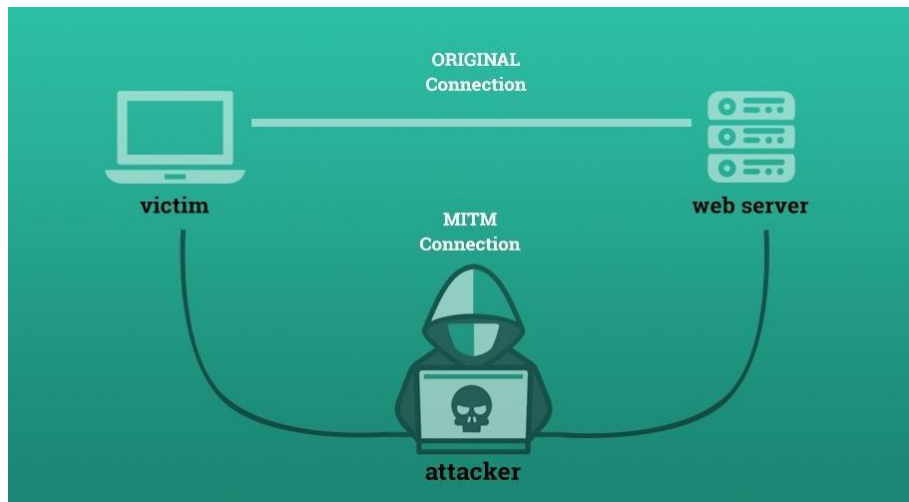


Figure 8-Man In The Middle Attack

Cryptographic algorithm and key management attacks

Cryptography has been used for a long time now and is a must regarding security and the importance of key management cannot be underestimated. When there is any new form of security, in time there will be an attacker trying to take advantage of it. We have seen the importance of cryptography and encryption and now attacks are targeting this. If an attacker steals data and they do not have a key or the decryption method, it is worthless to them. This is why we are seeing an uptake in this type of attack as it would be huge for attackers to have access to the keys.³²

Spoofing and masquerading (authentication attacks)

Masquerading is when an attacker claims to be somebody they are not to gain valuable data and information. This could be as simple as an emailing claiming to be from a certain company to taking over someone's identity with actual authentication and using the victims credentials to gather information. This is used to trick someone into giving out information. An attacker could pretend to be a co-worker, who the victim would trust and might share information with freely.³³

Denial of service and jamming

Denial of Service(DoS) attacks are known as some of the most common and easy to perform attacks on IoT systems. As stated above the purpose of these attacks is to drain resources from the system and cause a disruption to it. This stops the systems performing the basic functions it was intended to do and can also make it totally unusable. Jamming is a form of DoS attack, where the user sends signals which can interrupt the system or network. Under the banner of DoS, we also have Flooding and collision attacks also known as timed flooding. As we could potentially have multiple devices within our IoT system, it is allowing for more targets to attack.³⁴

Access control attacks (privilege escalation)

Privilege Escalation is a way for an attacker to gain unauthorized access to a system without the proper security clearance. If an attacker penetrates a system in a certain way, and they realise they do not have access to certain data or information, they can then try privilege escalation which may grant them more access. This can also occur when an organisation does not have adequate privilege rights to the correct users. If we leave user with full privileges when they shouldn't have them or do not need them, this can lead to this type of attack.³⁵

Other common access control attacks include Buffer/Stack Overflow, Access Aggregation Attacks, Password attacks and Social engineering attacks.³⁶

As we see with all the above attacks, there is lots of overlap within the attacks and the type of attacks they fall under. Most of the attacks mentioned are often seen as common attacks on an IoT network. Although they can all be used on many systems. There is so many methods of attack for someone to take advantage off, we have to make sure we have at a minimum, done our best to defend against the most common and well known attacks. As there is always a new vulnerability to exploit or way to attack a system, we have to have the basics covered and be prepared to upgrade and be ready to defend against any of these potential new threats.

4. Glossary

SCADA – Supervisory Control and Data Acquisition

IOT – Internet of Things

GUI – Graphic User Interface

HMI – Human Machine Interface

PLC – Programmable Logic Controller

CPU – Central Processing Unit

I/O – Input/Output

ICS – Industrial Control System

DCS – Distributed Control System

IIOT – Industrial Internet of Things

MQTT – MQ(Message Queue) Telemetry Transport

IIC – Industrial Internet Consortium

GPU – Graphics Processing Unit

RAM – Random Access Memory

USB – Universal Serial Bus

OS – Operating System

CSV - Comma Separated Values

DHT – Digital Humidity Temperature

LCD – Liquid Crystal Display

SSH – Secure Shell

UFW – Uncomplicated Firewall

MITM – Man in the Middle

HTTPS – Hypertext Transfer Protocol Secure

MAC – Media Access Control

SYN – Synchronize

DoS – Denial of Service

IP – Internet Protocol

ICMP – Internet Control Message Protocol

TCP – Transmission Control Protocol

ACK – Acknowledge

CGI – Common Gateway Interface

5. Figures

Figure 1-Internet Of Things	6
www.tibco.com/reference-center/what-is-the-internet-of-things-iot .	
Figure 2-Smart Home.....	7
www.hindawi.com/journals/js/2018/6464036/fig1/ .	
Figure 3-IoT Applications	8
www.researchgate.net/figure/Applications-of-the-Internet-of-Things-in-various-sectors-such-as-smart-city-e-health_fig1_329969562	
Figure 4-StackOverFlow 2020 Survey.....	9
https://insights.stackoverflow.com/survey/2020	
Figure 5-My Connection Photos.....	10
Figure 6-Output From Intelligent Sensor Lesson	11
Figure 7-Sonoff Energy Monitor	14
Media-Amazon.com , 2022, m.media-amazon.com/images/I/51QXDh-q6jL._AC_SY450_.jpg	
Figure 8-Man In The Middle Attack	18
www.infiniteedge.com.au/blog/cyber-attack-14-eavesdropping	

6. References

-
- ¹ Archer, C. (n.d.). *What's the difference between SCADA and IoT?* [online] blog.wellaware.us. Available at: <https://blog.wellaware.us/blog/difference-between-scada-and-iot-scada-vs-iot> [Accessed 26 Nov. 2021].
- ² Alves, T., Das, R., Werth, A. and Morris, T. (2018). *Elsevier Enhanced Reader*. [online] reader.elsevier.com. Available at: <https://reader.elsevier.com/reader/sd/pii/S0167404818304905?token=5502CEB74E99653C3B4D81230C9CC9C22C522444442330C39AB23BB82B8FF4881C8E15E77F63C92149B657B0CED2432B&originRegion=eu-west-1&originCreation=20211126191216> [Accessed 26 Nov. 2021].
- ³ Inductive Automation. (2018). *What is HMI?* [online] Available at: <https://www.inductiveautomation.com/resources/article/what-is-hmi>.
- ⁴ Mobile Automation. (2017). *Mobile Automation*. [online] Available at: <https://www.mobileautomation.com.au/plc-industrial-application/>.
- ⁵ Automate. (n.d.). *What's a PLC (Programmable Logic Controller)?* [online] Available at: <https://www.automate.org/editorials/what-s-a-plc-programmable-logic-controller>.
- ⁶ Trendmicro.com. (2019). *Industrial Control System - Definition - Trend Micro USA*. [online] Available at: <https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system>
- ⁷ High Tide. (2019). *Programmable Logic Controller in SCADA system | High Tide Technologies*. [online] Available at: <https://htt.io/the-role-of-programmable-logic-controllers-in-a-scada-system/>.
- ⁸ Softwaretestinghelp.com. (2019). *18 Most Popular IoT Devices in 2019 (Only Noteworthy IoT Products)*. [online] Available at: <https://www.softwaretestinghelp.com/iot-devices/>.
- ⁹ G, N. (2019). *How Many IoT Devices Are There In 2020? More Than Ever!* [online] Tech Jury. Available at: <https://techjury.net/blog/how-many-iot-devices-are-there/#gref>.
- ¹⁰ from, D. (2019). *What is industrial internet of things (IIoT)? - Definition from WhatIs.com*. [online] IoT Agenda. Available at: <https://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT>.
- ¹¹ "Python vs Java: What's the Difference?" *BMC Blogs*, www.bmc.com/blogs/python-vs-java/.

-
- ¹² “The Mind at Work: Guido van Rossum on How Python Makes Thinking in Code Easier.” *Blog.dropbox.com*, blog.dropbox.com/topics/work-culture/-the-mind-at-work--guido-van-rossum-on-how-python-makes-thinking.
- ¹³ Python.org. “What Is Python? Executive Summary.” *Python.org*, Python.org, 2019, www.python.org/doc/essays/blurb/.
- ¹⁴ “What Is the Best to Program Raspberry Pi: Java or Python?” *Quora*, www.quora.com/What-is-the-best-to-program-Raspberry-Pi-Java-or-Python.
- ¹⁵ “Introduction to Flask — Python for You and Me 0.4.Alpha1 Documentation.” *Pymbook.readthedocs.io*, pymbook.readthedocs.io/en/latest/flask.html.
- ¹⁶ “What Is Flask Python - Python Tutorial.” *Pythonbasics.org*, pythonbasics.org/what-is-flask-python/.
- ¹⁷ docs.sunfounder.com. (n.d.). *Download the Code — SunFounder SunFounder_SensorKit_for_RPi2 documentation*. [online] Available at: https://docs.sunfounder.com/projects/sensorkit-v2-pi/en/latest/download_the_code.html [Accessed 26 Nov. 2021].
- ¹⁸ ie.rs-online.com. (n.d.). *RS Pi 3B+ Kit | DesignSpark Raspberry Pi 3B+ Premium Kit with PSU, NOOBs & Case | RS Components*. [online] Available at: <https://ie.rs-online.com/web/p/raspberry-pi/1747510> [Accessed 26 Nov. 2021].
- ¹⁹ Santos, R. (2019). *What is MQTT and How It Works | Random Nerd Tutorials*. [online] Random Nerd Tutorials. Available at: <https://randomnerdtutorials.com/what-is-mqtt-and-how-it-works/>.
- ²⁰ October 2020, Caroline Dunn 18. “How to Train Your Raspberry Pi for Facial Recognition.” *Tom’s Hardware*, www.tomshardware.com/how-to/raspberry-pi-facial-recognition.
- ²¹ “Raspberry Pi Documentation - Camera.” *Www.raspberrypi.com*, www.raspberrypi.com/documentation/accessories/camera.html#libcamera-and-libcamera-apps.
- ²² “Greycampus.” *Greycampus.com*, 2013, www.greycampus.com/blog/information-security/what-is-a-sniffing-attack-and-how-can-you-defend-it.
- ²³ Irwin, Luke. “How to Defend against Man-In-The-Middle Attacks.” *IT Governance Blog En*, 17 Feb. 2020, www.itgovernance.eu/blog/en/how-to-defend-against-man-in-the-

middle-attacks.

²⁴ Dorus, R., and P. Vinoth. "Mitigation of Jamming Attacks in Wireless Networks." *IEEE Xplore*, 1 Mar. 2013, ieeexplore.ieee.org/document/6528486.

²⁵ "Most Common Wireless Network Attacks - WebTitan." *WebTitan*, 24 Sept. 2019, www.webtitan.com/blog/most-common-wireless-network-attacks/.

²⁶ Rewaskar, Sushant. *Protocol Attacks*.

²⁷ "What Is a Smurf Attack? Smurf DDoS Attack." *Fortinet*, www.fortinet.com/resources/cyberglossary/smurf-attack.

²⁸ "What Is a Smurf Attack?" *Usa.kaspersky.com*, 13 Jan. 2021, usa.kaspersky.com/resource-center/definitions/what-is-a-smurf-attack.

²⁹ "What Is a TCP SYN Flood | DDoS Attack Glossary | Imperva." *Learning Center*, www.imperva.com/learn/ddos/syn-flood/.

³⁰ Frankenfield, Jake. "What Is an Eavesdropping Attack?" *Investopedia*, www.investopedia.com/terms/e/eavesdropping-attack.asp#:~:text=An%20eavesdropping%20attack%2C%20also%20known.

³¹ "How to Prevent Network Eavesdropping Attacks." *SearchSecurity*, www.techtarget.com/searchsecurity/answer/How-to-prevent-network-sniffing-and-eavesdropping.

³² Stubbs, Rob. "Cryptographic Key Management - the Risks and Mitigation." *Cryptomathic.com*, 2018, www.cryptomathic.com/news-events/blog/cryptographic-key-management-the-risks-and-mitigations.

³³ "Masquerade Attack – Everything You Need to Know in 2021." *Jigsaw Academy*, www.jigsawacademy.com/blogs/cyber-security/masquerade-attack/.

³⁴ "Denial-of-Service Attack - an Overview | ScienceDirect Topics." *Www.sciencedirect.com*, [www.sciencedirect.com/topics/engineering/denial-of-service-attack#:~:text=1%20Denial%20of%20Service%20\(DoS\)%20Attacks&text=For%20any%20wireless%20network%2C%20for](http://www.sciencedirect.com/topics/engineering/denial-of-service-attack#:~:text=1%20Denial%20of%20Service%20(DoS)%20Attacks&text=For%20any%20wireless%20network%2C%20for).

³⁵ Cynet. "Understanding Privilege Escalation and 5 Common Attack Techniques." *Cynet*,

2020, www.cynet.com/network-attacks/privilege-escalation/.

³⁶ "Common Access Control Attacks and How to Fend Them Off." *House of IT*, 31 Aug. 2020, houseofit.ph/blog/common-access-control-attacks-and-how-to-fend-them-off.