CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

DEPARTMENT OF COMPUTER SCIENCE

4th YEAR PROJECT EXPO 2019

Architecture Factory – May 8th – 17:00 to 19:00

Student Name: Andrew Kenneally	**Supervisor:** Gerard MacSweeney

Project Title: Operating System for Irish Primary and Secondary School Students

Research Question: Is there an operating system which meets the needs of our public education system?

Project Abstract:

This Operating System provides in-depth logging, comprehensive parental controls, firewall rules to block illicit and adult content, close to bleeding edge software to protect from modern vulnerabilities, easy access to educational resources, an easy to use child friendly interface and an adult administrator login which allows for thorough monitoring and tweaking of each individual system. I plan to research the software, the market, the security and the various methods of distribution and present it as a research report. I will then develop a virtual machine to analyse the real world usage and uses of such a system and complete the report with my findings.

The workstations will gather and send all the information required across a LAN /WAN to a physical machine accessed by a domain manager. This physical machine will not necessarily need to run the same OS as the workstations, but will be able to access the logs, diagnostics or remote terminal of any given workstation or classroom. Any data collected can then be further used to inform on a course of action regarding the OS or the hardware using it. For example; This data could be used to work on possible improvements and to examine any areas of inefficiency, malfunction or exploits. I intend to achieve this design using a plethora of open source technologies.

Technologies used:
Manjaro Linux, Python, Bash Shell, SSH, Qt Display Manager, Atom, C Programming Language, Xorg, Git, Kerberos, Gitlab, Dropbox

Student Name: Sean Mullane	**Supervisor:** Paul Rothwell
Project Title: Social Networking Website for Diets	
Research Question: Can we set up a social networking website for assisting people who want to diet and improve fitness?	
Project Abstract: The aim of this project is to provide a website that allows users who have no prior knowledge about health and fitness to organise their efforts to lose weight in a manner that is healthy, easy and efficient. It provides a user with a customised meal and exercise plan that is suited to them and a platform to message other users of the website looking for diet tips and/or motivation. The website uses the users' favourite foods in order to create a specialised, but editable, meal plan that is not only healthy but also incorporates those favourite foods. As well as this the website will also suggest exercise plans for the user to complete depending on the details they have entered and allow them to alter these. The meal and exercise plan will work together through calorie counting by informing the user of how many calories they have consumed and burned each day and whether or not they have exceeded their calorie intake for that day.	
Technologies used: React, JavaScript, Node.js, MySQL	

Student Name: Calvin Riordan	**Supervisor:** Mary Davin
Project Title: First Steps	
Research Question: Can we use gamification to make exercise fun for kids?	
Project Abstract: Exercise can be a tedious and sometimes overwhelming activity for some kids. To make exercise more enjoyable I have decided to create a fitness app for kids. The app tracks their footsteps and converts them into an in-app currency which is spent on a game built into the app.	
Technologies used: Android Studio , Firebase , Google Maps	

Student Name: Eoin Healy	**Supervisor:** Mary Davin
Project Title: An analysis of Anti-virus software limitations & the application of Incident Response techniques.	
Research Question: How can improving security reduce the likelihood of a user's endpoint being breached?	

Project Abstract:

In recent years cyber-crime has been on the rise and is becoming a bigger and bigger problem. A lot of companies are relying heavily on antivirus software as a way of protecting their systems.

When you consider how common breaches, hacks and cyber-crime is in today's world, it's crucial that companies take a layered approach towards security to help mitigate damages if a breach does occur.

The purpose of the project is to highlight the limitations of traditional antivirus software and how easy these limitations can be exploited by malware authors. How would a layered approach to security reduce the probability of a breach?

A layered approach would involve the following three defences;

1. Antivirus software.
2. Endpoint Detection and Response solution.
3. Incident response plan.

This approach can increase the speed and efficiency of handling a breach. The improved response to a breach can lessen the financial and reputational damage to the company.

Technologies used:
Ollydbg, IDA Pro, Kali Linux, Windows, Kaspersky, Cylance Optics, Volatility, Virus Total

Student Name: Stephen O'Callaghan	**Supervisor:** Mary Davin
Project Title: Comparison and evaluation of mobile security protection vendors	
Research Question: Can the use of a mobile security protection guide reduce the impact of malware on modern day android mobile devices?	
Project Abstract: This project involves the creation of a guide that provides users with information regarding modern mobile cyber threats. It also provides solutions for these various threats. The threats addressed in the guide include Phising, Data leakage, Out-dated anti-virus software, Cryptojacking, Ransomware, Banking malware and Wi-Fi/Bluetooth interference.The guide addresses four categories of users, namely Social, Work, Online banking and E-commerce users. The guide compares five mobile security vendors. The vendors used for comparison are McAfee, Kaspersky, Sophos, Symantec and Trend-micro. Each vendor is compared under their Feature sets, Pricing and Language support in the guide. The guide provides a suitable vendor selection for each individual user based on their requirements for their mobile devices. A questionnaire is used to gather data about users' requirements. An evaluation is carried out and a suitable vendor is selected to suit the user's mobile security requirements.	
Technologies used: McAfee, Kaspersky, Sophos, Symantec, Trend-Micro.	

Student Name: Andrejs Hrjascevskis	**Supervisor:** Cliona Mcguane
Project Title: SAM - Shopping Assistant Manager	
Research Question: Can be used progressive web application by customers for managing and reminding of shopping dates of discount vouchers.	

Project Abstract:

Stores have different marketing approaches. For example, for every €50 spent, Dunnes Stores gives the buyer a €10 voucher for the next purchase, to be used within 10 days from the day after the day of purchase. In addition, a cumulative bonus is provided in the form of 1% for each Euro spent. After a certain time, a booklet with discount vouchers comes to the buyer's address.

For the customer, it can be a challenge to keep track of these discounts. For the businesses, it costs money to print the vouchers. Moreover, many of these vouchers end up in the trash, which is bad for the environment.

This project proposes a solution to these difficulties – a mobile app which keeps track of loyalty cards and associated vouchers in digital format. This app is specified to following tasks

helps speed up notification and the provision of additional bonuses
track days before the end of bonuses and vouchers
check the price of the goods
exclude the loss of the aforementioned vouchers and bonus checks
conserve of natural resources by transferring process to digital environment

Technologies used:
FileZilla, HTML5, SVG, LocalStorage 5, JSscanning, EcmaScript 6, Base 64 image generator, PWA, 200 OK!, FireBase, GitHub, CSS 3, Hostinger, VS Code, Lighthouse audit, jQuery.

Student Name: Jack Power	**Supervisor:** Seamus Lankford
Project Title: Vulnerability Recommendation for Unsecured Systems	
Research Question: How can unsecured machines on a network be discovered efficiently, and how can known vulnerabilities be exposed and mitigated.	

Project Abstract:

Unpatched systems on a network can leave a whole organization vulnerable to an array of vulnerabilities. Allowing threat actors to attack a network in numerous ways, through malware campaigns and phishing scans to name a few.

Client data is an integral part of a business, keeping this data secure is of paramount importance. Knowing what vulnerabilities are on your systems and how these vulnerabilities can be taken advantage of is important, not just for security professionals to be aware of, but for everyone throughout an organization.

The purpose of this project is to create an easy-to-use system for vulnerability discovery and mitigation. This will be done with the use of 3 scripts:

1) Shell script to automate the NMAP process to gather data on machines on a network
2) A python script to input the NMAP file and parse the output to a CSV.
3) A python script to match system information with a back-end database of known vulnerabilities.

Technologies used:
VMware vCloud, Python, Bash, Kali Linux, NMAP

Student Name: Bryan Byrne	**Supervisor:** John O'Brien, Diarmuid Grimes
Project Title: Improving Awareness of Social Engineering Attacks Within Industry	
Research Question: Is it possible to raise awareness and reduce the amount of social engineering attacks within a company/organisation with the use of an online tool?	

Project Abstract:

Social engineering is the art of manipulating people into giving up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick them into giving out sensitive information such as user credentials, bank information. Oftentimes they use this information to gain access to a computer and secretly install malicious software.

The main aim for this project is to create an online assessment tool which is easily accessible to users to undergo an evaluation of their company/organisation and find weaknesses that could be exploited by social engineers.

The resulting application, Social Engineering Security Assessment Tool (SESAT) is the online tool hosted on a WordPress website. Users navigate to our live site and take part in our assessment. During this assessment users answer a variety of questions under the following headings:

- Infrastructure Security
- Application Security
- Operation Security
- People Security

Once the assessment is taken by the user he/she will receive their results via email in under 60 seconds. The users receive their results along with security tips, and potential solutions to the weaknesses found in their organisation. Results are also given in the form of visual aids. Users' results are unique and based specifically on the answers they have chosen throughout the assessment.

As well as that, this website will consist of information regarding specific aspects around social engineering. This information includes the best social engineering & pen-testing tools on the market, social engineering attack vectors and a regularly updated section on the most common attacks. From the information provided online, users will become more aware of this niche area within cybersecurity, thus enabling them to protect themselves and improve their systems.

Technologies used:
WordPress, HTML, FormidableForms, MS Project & XAMPP

Student Name: Liam Chambers	**Supervisor:** Byron Treacy
Project Title: S.M.A.R.T Dairy	
Research Question: Can we improve the accuracy of data recording on dairy farms, and reduce the time it requires, using mobile/IOT devices?	

Project Abstract:

There are over 570 million farms worldwide, and with the advent of IOT devices data is fast becoming an essential part of the agricultural industry. Already for farmers, this means animal details must be recorded regularly and accurately. A time-consuming task that is prone to error.

This project proposes an interactive, easy-to-use mobile application for capturing data using a camera/wireless sensor technology. The application will be designed to be intuitive, using proven UI/UX principles, and display meaningful metrics of the recorded data. The ICBF private cloud will be used for remotely storing data, with offline storage used until a data connection becomes available to the device. As data will be easier to record, it will result in more farmers recording events.

On completion, the farmer should benefit from using this app in both time-saved, and the visualisation of data for future decision-making. For ICBF, it should increase the accuracy of data in their database.

Technologies used:
Angular JS, Oracle DB, HTML, CSS, Ionic Framework

Student Name: Emily O'Connell	**Supervisor:** Mary Davin
Project Title: Solving Problems in Cyber Security	
Research Question: Where are the immediate, tactical and long term future pathways for cyber security?	

Project Abstract:

There are two primary problems the cyber security industry face today, the problem of human error in an organisation and the time taken to respond to a cyber security incident. My project has been broken down into two sections.

Section One: Over 40% of cyber security incidents reported are caused by employees in the workplace. To help overcome this, I have written an E-Book which highlights the basics of cyber security. The E-Book has been written for three different user groups, an everyday user, an employee and a manager.

Section Two: The longer it takes to respond to an incident the greater the risk to the company. By researching problem solving techniques such as Biomimicry & TRIZ, I have developed an application using an automation tool called Tines which helps reduce the amount of time it takes to respond to an incident.

Technologies used:
Tines, SPLUNK, Google Docs

Student Name: David Kiely	**Supervisor:** Colin Manning
Project Title: Emotion Recognition with Artificial Intelligence	
Research Question: Can human emotion be identified through image classification?	
Project Abstract: Our emotions play a large role in how we interact with technology. We might choose to consume media based on our current mood or even want to get in contact with certain people depending on how we are feeling. If a person's mood can be recognised by recognizing their facial expression, it opens a new door of possibilities for enhancing our growing relationship with technology. The project is an interactive application that uses machine learning to identify emotion on a user's facial expression in real time through the front facing camera of their device.	
Technologies used: Python, TensorFlow, Keras, OpenCV, NumPy	

Student Name: Sinead Coughlan	**Supervisor:** Arthur Tobin
Project Title: Project Management software for College students	
Research Question: How do I complete a project in the most time and cost efficient way?	

Project Abstract:

Efficient project management is a very import factor to consider when successfully carrying out a project at any scale. A good project manager should be able to negotiate achievable deadlines and objectives between Clients, Developers and Shareholders.

A highly popular topic at the moment is how to successfully complete a project with the most effective tools available on the market. Project management is important because it ensures the correct expectations are set around what has to be delivered, by when, and for how much.

From studying Software Development at college, I have had to rely heavily on project management applications in order to keep track of the work that I have to complete.
I have found myself using a range of software applications in order to keep track of my work load. This can cause confusion and will be hard to manage if you do not have an efficient project management system. I have decided to create a project management application to address these issues. By having all your required applications within the same software, you can reduce the time spent clicking between the different sites and essentially manage your project from the one place.

Technologies used:
JavaFX, SQL, CSS, FXML

Student Name: Keith Walsh	**Supervisor:** Mary Davin
Project Title: Common Vulnerability & Exposure Feed	
Research Question: Can we adopt a more proactive approach to CVEs with the use of a live feed?	

Project Abstract:

The objective of this project is to create functional software which will provide a Security Operations Centre (SOC) with a live feed updating them on CVE releases as they become available.

This feed will enable users to view CVE releases in real-time while also permitting them to escalate particular CVEs for action, or to acknowledge any CVEs which are not pertinent.

As a result of using this feed, a SOC Team/Support Engineer can improve how exposures and vulnerabilities are addressed and resolved.

As cybercrime is having such a serious impact on companies and organizations globally, having a proactive approach to how security events are handled is essential.

Technologies used:
phpMyAdmin, CVE Mitre, cURL, CVE Circl, PHP, Bootstrap, PostgreSQL, Javascript.

Student Name: Paul Murphy	**Supervisor:** Dr John Creagh
Project Title: Community Alert App	
Research Question: Can an Android App be used to allow members of the public to report any community issues to local authorities, such as faulty street lights, litter, and road damage?	

Project Abstract:

Community Alert App is a mobile application that attempts to empower members of the public by giving them the ability to make a difference within their local community. It will allow the public to report any issues to local authorities, such as faulty street lights, litter, road damage etc.

The project will consist of an Android application as well as an AngularJS based web application for administration purposes, while making use of Google's Firebase to implement a real time database.

A user of the mobile application can quickly create a report by using their smartphone to take a photo, add a short description and a location before submitting their report to a database. An administrator can then access all reported issues and send the information via email to the relevant local authority or local councillor depending on where the issue is located.

Technologies used:
Java, Android Studio, Android, AngularJS, Firebase, Google Maps,.

Student Name: Jodie Bermingham	**Supervisor:** Mary Davin
Project Title: Containerisation on Single Board Computers with Micro-Services	
Research Question: Can micro-services be hosted on containers and migrate if a specific event were to occur?	

Project Abstract:

Containerisation is considered an alternative to hypervisor-based virtualization. The main aspect of containerisation is the layer to which it sits in a typical virtual architecture. The layer is situated on top of the operating system. This allows the containers to function with the underlying hardware and software regardless of what it may be.

This project's aim is to place container technology on a Single Board Computer. Single board computers are computers which are built on a single circuit board, but have the same functionality as a normal sized computer. Once the container is placed on the single board computer, a micro-service is designed and placed in the container. Upon the triggering of an event, the container hosting the micro-service is stopped. Once stopped, the container is migrated to a second Raspberry Pi where the micro-service is resumed to its normal function.

This project demonstrates how micro-services and containers can be used in any size production environment. Micro-services are hugely beneficial to application developers. Placing these applications within containers gives the added benefit of them running regardless of the underlying architecture. The migration aspect prevents downtime if an event were to occur where the application could go offline

Technologies used:
Raspberry Pi, Docker, Kubernetes, Raspbian, MySQL, SFTP

Student Name: Tony O'Keeffe	**Supervisor:** Diarmuid Grimes
Project Title: F.O.S.U (Fast Operating System Upgrade)	
Research Question: How do you upgrade multiple operating systems fast and efficiently?	
Project Abstract: An operating system is software that supports a computers basic functions, such as scheduling tasks and controlling your peripherals. After time this software becomes outdated and may be more vulnerable to viruses and other malicious software. To ensure their devices run smoothly and safely for users, corporations must keep their machine up to date. This project is a demonstration of how to effectively upgrade a computers operating system from one version to another. This can be used on a small or large corporate scale just as well. Once the machine is upgraded, a power-shell script is run to re-add the machine back to the company's domain and install any necessary network printers all in one go. This makes the upgrade faster and more efficient.	
Technologies used: Microsoft Deployment Toolkit, Power-Shell, VMware ESXi, Windows Server, Windows 7 & 10	

Student Name: Shane Carroll	**Supervisor:** Jinghua Ye
Project Title: Library Seat Monitoring System	
Research Question: To provide students with a study area at a reasonable time.To be able to monitor the students time in the library to benefit their study period.	

Project Abstract:

Being seated for long a duration is proven to be a factor of risk to human health. As a result, back and spinal injuries can develop due to compromised posture. About 80% of adults experience low back pain at some point in their lifetime due to this.

The overall goal of this project is to improve and monitor the students seating while studying in the library. This can be achieved through the development of a timing system. To improve the current library model, we explored seat monitoring systems and smart monitoring system. To expand both the library and user experience, a web-based model is built to allow users to track and book seats in the library.

The development of this project was carried out on a single board computer, with an Ultrasonic sensor attached, the purpose of this sensor is to detect an occupant of this area. Once the user is detected the system will indicate the study area is engaged. Using the latest web technologies, a web-based application was built to create a user-friendly interface for interaction with the library system. The use of different coloured indicators is to determine the status of the study area.
The Library Seat Monitoring System concept proves that such device has multiple applications. This system can provide an external access through the internet, this allows users to plan their studies and can ensure that they have a seat prior to entering the library. The various lights will represent the status of a seating area, which will allow for easier viewing of vacant seat through production of a green light. This monitoring system will also recommend the optimal seating time for users and advise study breaks.

Technologies used:
SQLite, Nodejs, Python, HTML, CSS, JavaScript

Student Name: Kian Buckley Maher	**Supervisor:** Mary Davin
Project Title: Modifying Suricata Rules Using Matching Algorithms	
Research Question: Is it possible to improve security detection rules using matching algorithms?	

Project Abstract:

The aim of this project is to help reduce the levels of false positive security incidents that a security analyst is expected to handle in a single day, by improving the accuracy of intrusion detection rules. These rules can quickly become inaccurate due to how quickly exploits, attacks, and malware events evolve.

Using the program, an analyst can compare a packet capture of malicious traffic to the intrusion detection rule that would have triggered for it. The program will first extract the detection signatures from the intrusion detection rule. The extracted signatures will then be compared with the packet capture using a matching algorithm. This comparison will return a value between 0 – 100% for each of the detection signatures seen in the rule, creating visibility into the areas of these rules that are causing issues and allowing for improvements to be made.

When successful, this program will help to improve the overall accuracy of intrusion detection rules. This will lead to a decrease in the level of false positive events seen in day to day activity in a security operations center.

Technologies used:
Python, Suricata, Fuzzy Wuzzy Matching Algorithm, Kali Linux, Wireshark

Student Name: Andrew Remo	**Supervisor:** Mary Davin
Project Title: Monitoring and evaluating network statistics in a Software-Defined Network	
Research Question: How can network delays be monitored and evaluated?	

Project Abstract:

Software-Defined Networking (SDN) is redefining the way datacentre networks are built and managed. SDN is a concept of a logically centralised controller which manages a network of programmable switches. As a result, obtaining a complete overview of the network topology can significantly simplify the operation of new network services.

This project builds upon the existing SDN design but focuses on developing an application that can identify latency's or any abnormal behaviour across arbitrary paths in a network and to work in conjunction with the SDN controller to provision forwarding rules into the switches. The data collected from the switches is processed by the application and displays the latencies through a dashboard to assist network administrators with identifying network bottlenecks.

Technologies used:
OpenFlow, Pox, VMWare Workstation 15, Mininet, Python

Student Name: Owen Leen	**Supervisor:** Olivia Brickley
Project Title: Using Virtualisation to Process System Data for Analysis	
Research Question: Can virtualisation be utilised to allow users to tailor software more effectively?	

Project Abstract:

This project provides users with a virtual environment with which they can test and analyse software before implementing it in a real-life environment. The core architecture of this system is composed of a host computer to interact with the virtual operating system, the virtual environment that is used to test and analyse software uploaded by the user, and a network share directory that acts as a network bridge between the two destinations.

On the virtual environment, the user is provided access with a suite of tools with which they can attempt to examine their software in a number of ways, such as file management tools, Network statistics, system performance displays and software execution utilities. Depending on the scenario, the user can mould the virtual environment to mimic a physical device to act as a testbed before implementation of the software deployment.

All information gathered is executed using the tools on the virtual environment and is sent to the network share directory, which is linked to the host device. This information can be extracted and examined in an external environment for easier access and interpretation. Users can then use this information to tailor their own software to fit their own needs and achieve the best possible outcome for it.

Technologies used:
Virtualisation, Network share directory, Networking, Programming, Linux OS, Windows OS, Bash, various open-source Linux applications and tools.

Student Name: Adam Martin	**Supervisor:** Gerard McSweeney
Project Title: EternalBlue And Deployment Methods	
Research Question:	
Project Abstract: This project is an investigation into the damaging effect and prolific nature of Ransomware, this is done in tandem with an analysis of the two most infamous samples that have been found to date: ”WannaCry” and ”NotPetya”. The cultural along with the financial impact are what provided the motivation for this project along with the level of skill and complexity that will need to be displayed. As one if not both of these examples were state sponsored the question must be asked, at what point is the line of criminality passed. This was the first instance where the entire world had taken notice of the real threat presented by cybercrime. This research will be conducted in order to find attainable solution to these issues, utilizing yara rules and a range of malware analysis techniques. The end product will intertwine all of these into the Malscan platform to provide threat mitigation and prevention. While every effort is made to secure the data of private enterprise and that of the home user, the same effort is made on the part of threat actors to exfiltrate this information	
Technologies used: IDA Pro, PeStudio, FileAlyzer, OllyDebug, FakeNet, HexEdit, Cuckoo, MetaSploit, YaraGen, ProcMon, SandBoxie, ProcessHacker, VmwareFusion, ProcessHacker	

Student Name: Geoff O Rourke	**Supervisor:** Mary Davin
Project Title: Increase in cyber-attacks due to the increasing number of IoT devices.	
Research Question: With the large number of IoT devices coming online, how can we combat the threat of them being hacked and exploited?	

Project Abstract:

The aim of this project is to create an informative guide on securing consumer-grade IoT (Internet of Things) devices. This guide will aid user's using "smart" IoT devices and show the user how to secure them correctly. It will also give novice user's important information about IoT devices, the growing IoT landscape and how these products can aid their day-to-day lives.

Over the last few years, millions of these IoT devices have come online. The consumer-based markets have seen a surge in popularity, making everyday household items "smart" and internet enabled.

Issues have arisen though because of a potential knowledge gap of some users in relation to securing their device(s) on both setup and maintenance correctly.

This leads to hackers and other cyber-criminals seeing the growing IoT market's as 'low-hanging fruit' and now are targeting consumer IoT device's with malicious intent.

Technologies used:
Kali, Raspberry Pi, Shodan, Metasploit, Debain, Hydra, WireShark

Student Name: Joseph Evangelista	**Supervisor:** Gerard Macsweeney
Project Title: Malware Analysis with Machine Learning AI	
Research Question: Can we tell if a file has a malicious content and can we predict a pattern of the type of content being sent to organizations?	

Project Abstract:

This is a tool set put together using open source software's to analyze a file to see if the content has a malicious activity in an autonomous fashion.

In this application a file will be sent to a cloud storage. The file will be put into a que system. A dispatcher will then send the file to its designated analyzer. The data will then be stored in logs and metrics. When the analyzer detects a malicious malware in the file, it will then send a SNS alert to the user. This will give a warning to the user not to open the file they have receive.

Once that is done. The results of the file will then be send to a machine learning model to be analyzed and give us a prediction of the occurrence of the activity and help us predict the type of malware being send to the organization to potentially protect our environment in case this malicious activity does affect the organizations environment.

Technologies used:
VMware Work station, Linux, Python, Terraform, SSH, AWS, YARA-Rules

Student Name: Allen Simbul	**Supervisor:** John Creagh
Project Title: Infectious Disease Forecasting	
Research Question: Can Twitter Data help in tracking the spread of infectious diseases?	

Project Abstract:

The outbreak of infectious disease like Ebola, Zika and Mers has become a major issue worldwide if left uncontrolled. In the past, an example of an uncontrolled disease can be seen in the outbreak of Spanish Flu in 1918. Within months the disease ravished the population infecting over a third of the worlds population and killed between 50 and 100 million which is absolutely staggering as it killed more people in World War 1 in 1918. The origins of the disease are still unknown and worse still the disease was never treated, there was no great cure or vaccine made, neither was there a plan to stifle the spread of the disease as it was already too late at the time. In fact, the disease has never disappeared, and many medical scientists fear its return in a more evolved form. Though the evidence of this is still unconfirmed one thing is clear without a system to track and forecast infectious diseases like Spanish Flu and Ebola it will result in numerous infections and then deaths.

The main use case of this system is to use machine learning to create an early warning system in the form of disease forecasting and to visualize the data to see how large or small the disease has spread. To accomplish the objectives of this project Twitter Data will be used as Training and Test data in a machine learning algorithm called Naive Bayes, a predictive model. As there are over 500 million tweets a day, this project will also research the validity of Social Media data in tracking diseases, finding their origins and prevent further spread.

Technologies used:
Twitter, Tweepy, Python, Naive Bayes, Vue.js

Student Name: Sinead Hegarty	**Supervisor:** Gerard MacSweeney
Project Title: Word Road	
Research Question: Interactive Gamification-based Mobile App for Speech Therapist Sessions	

Project Abstract:

Speech therapy is the science that specializes in the evaluation, diagnosis, and treatment of communication disorders. It includes word-finding issues, social communication difficulties and structural language impairments.

On the other hand, gamification is the term used for the application of game-design elements and game principles in non-game contexts.In this project we want to create a mobile app allowing speech therapists to introduce interactive gamification-based activities during their sessions with children.

The goals of the project are as follows:
1. Survey of the current speech therapy techniques applied for improving the speech of children.
2. Compare and contrast the gamification-based approaches available for existing mobile apps.
3. Survey of different algorithms/libraries for speech recognition.
4. Create an app that put all pieces together:
5. It must propose a set of activities following a gamification-based approach.
6. The activities must give support to an underlying speech therapy methodology.
7. The app must be able to interact with the child, collecting some sound inputs and running some speech recognition algorithms in the background, so as to provide reports/feedback.

Technologies used:
Android, Java, Github, Android Studio

Student Name: Cathal Kenneally	**Supervisor:** Dr John Creagh
Project Title: FireMap: Predicting the intensity of wildfires using machine learning	
Research Question: Is it possible to use Machine Learning to predict the intensity of wildfires?	

Project Abstract:

Since 1976, the global mean temperature has risen by more than half a degree (Celsius) and this could indicate that the drought conditions and wildfires caused by the heat-waves and high temperatures during the summer of 2018 will become a more frequent occurrence. The number of wildfires hitting Europe in the summer of 2018 has been 43% higher than the average number of wildfires for the last 10 years. The 2018 wildfire season in California was the most destructive and deadly wildfire season on record in the region with the largest amount of burned acreage recorded in a wildfire season in California. Every wildfire season a number of people are killed or injured because of these devastating wildfires.

FireMap is a web app that uses wildfire data gathered from NASA that can predict the intensity of a potential wildfire in a location using Machine Learning. It can also predict a potential intensity of a wildfire at the users current location which can give the user an indication of the likelihood of a wildfire occurring in their area.

Technologies used:
Node.JS, Express.JS, JavaScript, HTML, CSS, Bootstrap, Mapbox API, IBM Watson Machine Learning API, NASA MODIS c6 Active Fire Data

Student Name: Dominik Bahrynowski	**Supervisor:** Sean McSweeney
Project Title: Web based multiplayer game	
Research Question: Suitability of web development technologies to make a game.	

Project Abstract:

The aim of this work is to make a web based game. Browser games have been highly popular since the beginning of the internet, and since then, the power of computers and the connectivity on the internet has increased dramatically. With this increase, programming technologies and paradigms have also improved significantly and there are now far more tools to accomplish almost any conceivable task. In this work numerous different technologies have been used to create a browser based strategy game, these include languages such as JS, SQL, HTML5 and CSS as well as various libraries and environments such as Node, D3, JQuery and Express.

The game uses the board game RISK as a sort of inspiration, but it expands on its concept greatly. The technical functionality of the game includes features such as scalable multiplayer, embedded database, dynamic map generation, turn based system, microservice based server structure and other things. The developed game captures the complexity of RISK well and includes new user experience features such as an economy based on population, culture and religion mechanics, a more advanced combat system and a reworked turn system. The program I have created is also flexible, and thus allows for easy expansion or change of the playable map, which is generated by a JSON file using D3. It utilises web socket and a restful API for facilitating of data exchange between the clients and the server.

Technologies used:
HTML, CSS, JavaScript, Jquery, Node, SQLite, D3

Student Name: Yevgeniy Lapko	**Supervisor:** Dr. Ruairi O'Reilly
Project Title: Cyberthreat Related Text Detection in Natural Language	
Research Question: Is it possible to detect text related to cyberthreat domain in natural language text articles?	

Project Abstract:

A tremendous amount of information is circulating on the web continuously. Studying and separating this information into different domains using manual analysis can become a problem. Important parts are often neglected or omitted completely. Using computational power these problems can be reduced and the accuracy of results can be improved.

Cyberthreat Text Detection(CTD) is a system, that was designed to analyse and evaluate text for the presence of text relating to a particular field. This system was developed within the scope of a cyber threat domain. Project pipeline consists of multiple parts: data gathering, machine learning data analysis model and intermediate infrastructure.

The purpose of CTD is to create an application which will use the efficiency of machine learning to evaluate large amounts of information. Natural language classifier is used to calculate the probability of text being related to a cyber threat domain. The classifier is built using data received from NewsAPI and applying Naïve Bayes theorem to analyse between separate pieces of text.

Technologies used:
NodeJS, React, NewsAPI, MongoDB

Student Name: Aaron Sheehan	**Supervisor:** Noreen Gubbins, Diarmuid Grimes and John O'Brien
Project Title: The Modern Honeypot	
Research Question: Is It possible to create an easy to use honeypot?	

Project Abstract:

A honeypot is a network security tool used to entice and entrap hackers by faking a system that they would want to attack, and this is similar in concept to a mouse trap. The basic premise of a Honeypot is to trap hackers before they can hack your actual system. IT in recent years has become even more prevalent and the technology landscape is ever changing. The news recently has been filled with hacking reports in just January 2019 alone there have been more than 1.76 billion records leaked. This project involves creating a honeypot that is simple to use and set up. Part of this project includes the investigation in to the currently available honeypots in the market. This research is then used in order to determine the best way to achieve the project goal.

This project involves creating two virtual machines in vmware workstation an attacker and a victim (honeypot). A honeypot is then created using Python on the victim machine in order to fake port (23). This is then used to lure the attacker into the honeypot. The attacker machine is then used to scan for any open ports on the victim machine (like a hacker would). The attacker will see that port 23 is open and then try to connect to it. The victim machine (honeypot) will then get a notification that the hacker is trapped in the honeypot along with the IP address of the attacker machine. This information can then be used in order to blacklist the IP address and help prevent further hacking attempts.

Technologies used:

Student Name: Brendan Harrington	**Supervisor:** Arthur Tobin
Project Title: Using a vSphere environment to analyze the performance metrics of storage solutions	
Research Question: How would you accurately and consistently determine the performance metrics of various storage solutions	
Project Abstract: Storage has become a crucial part of many organizations profitability and requires careful consideration before implementing. Each storage solution provides wildly varying performance metrics based on a range of factors. For this project, a vSphere environment will be deployed as the production environment. At the center of this environment, various storage solutions will be implemented so rigorous performance tests can be ran against each storage solution. The performance metrics generated by these tests will be consolidated into a readable format where users have a statistical view of performance metrics. Due to hardware limitations, this project had to be scaled back to a single storage solution appliance. Instead we will be examining alternative factors that influence a storage solutions performance including wired/wireless and SSD/HDD devices. The methodology used for this project can be replicated and expanded upon, should the reader want to analyze how their storage solutions perform.	
Technologies used: VMware Workstation & vSphere, Linux, FreeBSD and Networking	

Student Name: Adrian Davidson	**Supervisor:** Paul Rothwell
Project Title: Exploration into the use of Open CV alongside Python to create a hand gesture recognition application	
Research Question: Is it possible to interact with the computer's Operating System using hand gestures?	

Project Abstract:

The modern user of information communications technology (ICT) will interact with this technology in some form at least once a day, often to great benefits. However, the people who don't benefit from this rise in technology are people who suffer with various disabilities, unfortunately these users are often left unable to use technology to its fullest simply because they are unable to use a computer via the conventional interaction mechanisms such as a keyboard and mouse. My proposed project aims to aid such users. It will allow the user to interact with their computer and have the freedom to explore technology on their own terms.

With this application, the user can interact with the computer using hand gestures. The user simply faces the camera and holds up their hand to control the mouse. The system will detect the users hand and track its movement to effect the mouse movement. The mouse's left click and right click functions can be performed with the use of two simple hand gestures. To facilitate convenient text input, the application provides an onscreen keyboard with bold font specifically designed for easy button presses using mouse clicks.

The application uses Open CV, a computer vision library which easily integrates with python. Open CV handles the computer vision behind the scenes and python allows full use of the computer vision library through its Application programming interface (API).

Technologies used:
Open CV, Python, Spyder IDE, GitHub, Trello

Student Name: Evan Day	**Supervisor:** David Murphy, John O'Brien
Project Title: Automated CI/CD Creation Platform	
Research Question: Can we create a platform for CI/CD encapsulating all the necessary tools for enterprise grade software delivery?	

Project Abstract:

Continuous integration/continuous delivery (CI/CD) is an important aspect of the software development life cycle which enables the automation of manual steps throughout the development process. This automation minimises the time and cost associated with testing, reduces the time it takes to identify problems and accelerates the quality and delivery of production-ready code.

In this work, we explore why the state of automation is not enough in today's world. We investigate what has already been done and how we can drive this area forward. We take an in depth look at containerisation versus virtualisation and explore why Kubernetes has become such a major force in the open source world. Following this, we establish guidelines for a prototype implementation. With these guidelines, we deliver on a collection of four independent services that work together in order to deliver an application that automates the delivery of the core tools required.

Utilising technologies around orchestration and containerisation, we encapsulate the infrastructure provisioning and tool deployment into a singular offering. This offering enables the creation of a CI/CD infrastructure platform in a matter of minutes. As a result, we simplify the infrastructure provisioning process, we improve the quality of life for developers and enable the faster release of software by the enterprise.

Technologies used:
Terraform, Docker, Kubernetes, Concourse CI, jFrog Artifactory, Sonarqube, Nginx Ingress, Minio

Student Name: Angelika Jedrusiak	**Supervisor:** Deirdre Dunlea
Project Title: Paw Buddy - Dog Tracking Application	
Research Question: Can we use real-time geolocation tracking to monitor and learn about our domestic animal's activity and safety?	
Project Abstract: Dogs are considered a human being's best friend. Biggest fear of dog owners is to lose their beloved companion. Unfortunately, the number of lost pets is still high, and it has been found that 10 million dogs are lost or stolen in the U.S. every year and only 22% are reunited with their families. Ireland is considered a Puppy Farm Capital of Europe. It has been found that a large number of animals bred forcefully are from owners stolen animals. Official figures show that there are 73 registered puppy farms in the Republic of Ireland, and they are producing at least 30, 000 dogs a year. The goal of my project is to develop a tracking application. This application can track where the dog is currently located with the use of Google Maps. Owner can set geolocation to mark safe zone for their dog. If the pet leaves the secure area the owner gets a warning notification. As soon as the dog leave the geofence they receive a sound notification in order to stop their actions. The dog will have knowledge of the sound and its meaning prior to its used in this application.	
Technologies used: Android Studio, Java, Google Maps, XML	

Student Name: Martin Bluszcz	**Supervisor:** Deirdre Dunlea
Project Title: Food classification and recognition application	
Research Question: Food classification and recognition application using machine learning algorithms.	
Project Abstract: Machine Learning is the art and science of enabling machines to learn things which are not explicitly programmed. The intention of this project is to develop an Android application, which uses a machine learning algorithm in order to recognize and classify objects in the camera view of the mobile device. Undeniably, nutrition is one of the valuable aspects of life. Unfortunately, people don't have time to prepare healthy meals or don't know how to do it. Taking advantage of technology utilizing machine learning algorithms, the aim of this project is to create a food-classification application, which based on information provided by algorithm and user preferences will generate lists of recipes and methods needed to prepare a given recipe.	
Technologies used: Tensorflow, Android Studio, Firebase, FoodAPI	

Student Name: Micheal Lucey	**Supervisor:** Gerarsd
Project Title: Internetworked microcomputers for small data centre environmental monitoring.	
Research Question: Can a cluster of Raspberry PI microcomputers equipped a sensehat be used to assist small data center administrators cuts costs by acting as a cost effective environmental monitoring solution.	
Project Abstract: This project aims to provide a cost effective alternative for small data center administers to monitor their data center environments without having to buy and install expensive proprietary equipment. To achieve this, I used a the raspberry pi computer platform equipped with sensehat modules, a number of python scripts, and free to use online services such as google firebase, and Initial state. When installed onto the network, and global configs setup logs are automatically generated on each PI from the sensor data. Once log files are created they moved over to a main master PI that uploads the files to google firebase where they are then stored. Files can then be accessed by using an Admin script that allows the users to Download log files, view folders, and view files. For a live view of environmental data I used a separate logging program that streams the barometric pressure, temperature, and humidity to a service called initial state which can be access via browser.	
Technologies used: Python, Pycharm IDE, Raspbian, Raspberry pi 2, , firebase, Initial state	

Student Name: Hugh Cawley	**Supervisor:** Arthur Tobin
Project Title: Developing A Headless E-commerce CMS Application	
Research Question: Can a headless CMS enhance how traditional ecommerce cms systems operate?	

Project Abstract:

For this project, the aim is to create an e-commerce Headless Content Management System. The most popular e-commerce CMS's in use today are traditional, with their frontend templates linked to backend code & database. Using a Headless CMS, we separate the data from the template using an API. The project will be built on the MEAN (MongoDB, Express, Angular, Node) stack. A number of technologies and skills are explored in this project, encompassing numerous areas associated with computer science, such as: Database Management, API Building, Web Application Development using Angular 7, as well as Design & Usability.

For the design the project I chose to follow the MVC (Model, View, Controller) pattern. Administrators manage data through the use of the content management application, and this data will be presented to the customers browsing the web store. The application is easy-to-use for all end-users, providing a similar web experience to other Content Management Systems, while utilising the benefits of operating with a Headless CMS.

Technologies used:
MongoDB, Express, NodeJS, Angular 7, Java Web Tokens, Bootstrap, SASS, Github

Student Name: Michael O'Connell	**Supervisor:** Byron Treacy
Project Title: Sentiment Analysis in Help Desk Software Systems	
Research Question: Can we use Sentiment Analysis to improve help desk software and customer support teams?	
Project Abstract: Customer support teams often employ help desk applications to aid in the efficient execution of customer service. Customer service is vital to the public image of a company. It is therefore extremely important for companies to quickly and accurately identify, categorise and solve customer issues. Sentiment Analysis, also known as opinion mining is an area of computer science and artificial intelligence. It is the process of analysing natural language in user-generated text to categorise emotional sentiment. This project seeks to automate the sentiment analysis to produce a categorisation based on a spectral scale ranging from positive to negative. Sentiment analysis makes use of natural language processing, artificial intelligence and machine learning. The sentiment analysis will be made available via a web service which receives text and returns a score that indicates sentiment.	
Technologies used: Tensorflow (ML), Uber Ludwig (ML), Flask (Web Server), Google Colab (Cloud ML Environment), VueJS (Front-End Framework), SCSS (CSS Preprocessor), Docker (Virtualization), Firebase (Application Development Platform).	

Student Name: Diarmuid Kelly	**Supervisor:** Dr. Sean McSweeney & Dr. Paul Davern
Project Title: Distributed Artificial Neural Network Risk Minimization using Federated Learning	
Research Question: How can multiple data sources be modelled for continued use across applications without the underlying data security being compromised?	

Project Abstract:

Machine Learning has made significant improvements over the last few years, these improvements can be primarily attributed to 3 major factors: The increase in compute resources available, improved access to big data, and better algorithm design. As in the beginning of traditional computing much of the work was achieved by mainframe or centralised servers. The transition towards powerful compute resources being edge based or even fully embedded followed a natural progression from central to decentralised. Machine Learning is following a similar trend. Formerly only large industrial or research laboratories had access to the computational and data volume requirements to run Machine Learning algorithms. Today, mobile or smart devices are capable of both training and inferring using Machine Learning models. This edge based learning enables otherwise unreachable data to be actively used in updating model accuracy. There is however requirements and responsibilities to the underlying data integrity and compute resources. These requirements may be in the form of data sensitivity, latency/bandwidth connectivity, or heterogeneous computational resources available across devices in a shared learning environment.

Federated Learning is a subfield of Machine Learning, aiming to access users data for use in training models collaboratively. Federated Learning works where each user in a learning pool receives a globally trained model, applying their local updates based on their data to adjust the global model. This is done by sending weight adjustments to other users on the network. This approach has the potential to minimise bandwidth and protect the underlying data using a Differentially Private technique whilst making use of the valuable information to be learned from the data. A major advantage of Federated Learning is the ability for idle or seldom used devices on the network to actively improve their models. This project investigates the value of rich data, the importance of data security in Machine Learning, and proposes a deployment architecture for a Federated Learning system.

Technologies used:
Python, TensorFlow, Flask, Docker, gCloud, AWS, NumPy, RabbitMQ, Unity3D

Student Name: James McCarthy	**Supervisor:** Dr. Sean McSweeney & Dr. Olivia Brickley
Project Title: Securing an Industrial Wi-Fi Network	
Research Question: How to secure an industrial Wi-Fi network while providing ease of access to the industrial components for authorised personnel	

Project Abstract:

In recent years, Pharmaceutical companies have become more focused on developing products on a smaller scale and in a more flexible environment. In order to achieve this, process equipment such as mixing vessels and filtration systems are now mobile i.e. on wheels and can reside in numerous locations during the various stages of production. The challenge that this poses for Automation and Control System engineers is connecting equipment to servers and controllers regardless of the current location of this equipment. The advancement of the Industrial Internet of Things also known as "Industrie 4.0" has resulted in the availability of large amounts of real-time and analytical data which provides the challenge of how to access and interpret this data in a highly secure, and mobile way.

This project implements an Industrial Wi-Fi Network, for use by the engineers at Rockwell Automation. The main motivation for this project is to provide the engineers the means to carry out their work in a wireless manner. Using a wireless network will allow for greater efficiency and ease of access to their working infrastructure. As this infrastructure may contain sensitive information, it became apparent that the network would need to be secured, which is one of the primary objectives of this project. This network will need to prevent unauthorized access and encrypt wireless traffic to keep the data being transported across the network secured. It is also critical that this network operates efficiently in terms of strong coverage in each of the desired areas and a high throughput provided to the users of the network.

Technologies used:
Kali, Ubuntu, VMware, FreeRADIUS, Cisco, Rockwell Automation, Allen Bradley, Solarwinds

Student Name: Artiom Sumigora	**Supervisor:** Seamus Lankford
Project Title: DynamiCrypt	
Research Question: Dynamically encrypt data, an alternative to public key cryptosystems.	

Project Abstract:

In today's world information is mostly sent in an encrypted form over the public internet. Traditionally when a client connects to a server the public keys are shared and the same set of public/private key pairs are used for the session and potentially for future sessions, depending on how the system is setup. Provided that industry standard encryption is used it would take the attacker longer than the lifetime of the earth to crack the key using common cracking techniques, making the system secure. The problem arises if the attacker managed to get the key in some other fashion other than brute force it could be possible to decrypt potentially sensitive information that was captured over the network.

This thesis explores an alternative method of generating keys safely over the public network without using public key cryptography schemes such as RSA. This thesis also further increases security by changing encryption keys during the session. In order to achieve this a type of neural network called a tree parity machine will be used.

This thesis provides a software solution that is capable of handling synchronisation using multiple tree parity machines to exchange encrypted data between multiple hosts. An API will be provided that will allow other any web server to use dynamic encryption. A NodeJs App will also be provided to demonstrate the use of the API in a messaging type environment.

Technologies used:
C++, Pistache, Boost, Boost Asio, Crypto++, Chrono, NodeJs, ExpressJs, EJS, Python, Bash, g++, git, Netbeans 8.2, Webstorm, Arch Linux with kernel 5.0.7-arch1-1-ARCH.

Student Name: Patrick O'Shea	**Supervisor:** John Creagh
Project Title: Augmented reality in industrial maintenance	
Research Question: How can augmented reality be used to help engineers solves problems more quickly?	
Project Abstract: Engineers in the role of industrial maintenance, often run inspections or repairs on machines. Most of the time the engineer could be faced with an error code, that would describe what the problem they're facing and how to they remedy the problem. This means that they would need to refer to a manual or a database of error codes. This can take a bit of time to look up and find the error code that they are looking for. This project hopes to find a faster solution by using augmented reality to speed up the process. For this project we will use the logic board PNOZMuliti created by Pilz. This can be used to simulate the functions of machines or systems. Then can display an error code based on any problem that machine is having. Since we do not have access to augmented reality glasses, we can use our mobile phones to simulate this. We will use OCR technology to read the error code, check a database of error codes to find a solution and display that solution in augmented reality.	
Technologies used: Android, android studio, wikitude, anyline, firebase, oneplus 6t android device, Pilz PNOZMulti logic board training system. PNOZMulti configurator	

Student Name: Michael Slattery	**Supervisor:** John Creagh
Project Title: Translate Irish Sign Language (ISL) using a Mobile Application	
Research Question: Can a mobile application be used to translate Irish Sign Language to English	

Project Abstract:

Irish Sign Language (ISL) is the first or preferred language of approximately 5,000 people and at least another 40,000 can communicate using ISL in Ireland. ISL makes use of a persons hands, head, facial expressions and body movement. ISL is a language itself with its own unique signs in different areas.

It can be difficult to learn a new language and this is why having a mobile application that can translate ISL from hand signs to English words on the screen could be helpful to a number of people. Using TensorFlow and Core ML to learn off different ISL words should allow for an app that will be able to display sentences to a user.

Upon completion this application should benefit both people who want to learn ISL and people who simply want to understand what a person who is using ISL is saying.

Technologies used:
Swift, XCode, Core ML, Python, TensorFlow, Git

Student Name: Billy Lyons	**Supervisor:** Irene Foley
Project Title: RFID-based Lecture Attendance System	
Research Question: Can student attendance in Cork Institute of Technology be improved by implementing an RFID-based Attendance System?	

Project Abstract:

Lecture Attendance can be a problem in many colleges and can result in students failing their courses, if it is not monitored efficiently. This RFID-based Lecture Attendance System aims at improving each students attendance in CIT, by introducing a system where the student must scan their student card, as a clock-in method, at the beginning of their timetabled class.

An Arduino UNO device can be plugged into the lecturers computer and the lecturer can run the Attendance Scan by simply clicking on a Desktop icon. Once a student scans their card, this information is sent to a MySQL database, containing the Card ID number and the time of the scan.

A website has been set up for the lecturer to view this information. From here, they have the ability to view any particular class that they wish, by choosing the class group, month, date and time. They also have the option to change a students attendance in cases where the student has forgotten their card, or for other reasons.

Technologies used:
HTML, CSS, PHP, MySQL, Apache, RFID, XAMPP, Python, JavaScript, Arduino UNO

Student Name: Patrick Kent Dacoliat	**Supervisor:** Dr. Donna O'Shea

Project Title: Student Record and Verification System Using Blockchain Technology

Research Question: Can we develop a system that uses blockchain technology for storing academic records of students?
What type of a blockchain network implementation is most appropriate for an academic institution?
How can we evaluate that blockchain technology provides us with the security required to reassure that tampering of academic records is nearly impossible?

Project Abstract:

A diploma mill is an entity that provides illegitimate academic degrees and diplomas for a fee. In 2018, the Irish Times reported the existence of a diploma mill based in Dublin called Isles International which offers Irish qualifications online usually to foreign students. Due to the fact that fraudulent credentials and degrees can now be easily acquired using these diploma mills, academic institutions are encouraged to thoroughly verify the authenticity of the academic records provided by the students. In an academic institution such as the Cork Institute of Technology, the process of verifying the academic records of the students is handled in a tedious and human-error prone manner. The current process includes manually checking, using the human bare eyes, any indication on the student's certificate or diploma that might suggest its illegitimacy. A set of guidelines is being followed by the person verifying the authenticity of the academic records but it is still inevitable that an error might occur. The time being consumed by this process is also one of the factors why it is deemed inefficient and not recommended. Apart from academic institutions, employers also suffer from the fact that a system to verify the authenticity of these academic records is non-existent. Such a system can help the employers speed up the employment process by reducing the time it takes to verify the academic records of the applicants.

The aim of this project is to develop a system that academic institutions and companies can use to verify the authenticity of the academic records of the students. This will be achieved by developing a web application with an underlying implementation of a blockchain network. The system aims to leverage the characteristics of blockchain such as transparency and immutability to provide a secure way of storing academic records. The blockchain network will be owned by one academic institution in which they will be allowed to store the academic records of their students. Their students will be a participant in the network but will only be allowed to view their own records. Other entities such as other academic institutions and companies that wants to verify a student's records will be invited to network. They will be given permission to view the academic records stored in the blockchain. The project aims to speed up the process of verifying the authenticity of the academic records and to showcase how blockchain can help solve current problems in the academic sector.

Technologies used:
Hyperledger Fabric, Hyperledger Composer, Node.js, Express.js, Bootstrap, JQuery, EJS, Docker, Gulp, Git

Student Name: Daniel Perkins	**Supervisor:** Olivia Brickley
Project Title: SMTP Deep Packet Inspection & Automated Threat Reporting	
Research Question: Can a network security solution be created and implemented for free in a virtual SME environment?	

Project Abstract:
The implementation of a security solution for a small to medium sized business is not as simple as it sounds. Licence fees for premium grade products like Falcon crowdstrike, Microsoft Enterprise Client Access, 365 and Palo Alto can be in the thousands. The purpose of this project was to prove the concept of a free utility running in a virtualized and small scale SME's internal network where files could be extracted from TCP/IP packets, specifically those using the simple mail transfer protocol and determine whether they are a threat the work environment through different techniques. The goal is for a skilled employee such as an analyst to be notified when a suspicious file is detected and to automatically receive relevant information on such files so that he or she can perform an investigation without having to monitor end user activity directly. Automation is a crucial part of this project. The target market for such a project would be small to medium sized businesses, startup companies, non profit companies etc. The fact that they can't afford high end security solutions means it is likely they haven't got the budget for a full security team either. A free utility to bring the ideas above to life is entirely possible but the more automated it is, the less human intervention needed. This will allow for it to fit into an organisation with a low financial turnover.

I created an application from scratch using the Python programming language that integrates with network minor which is a free network forensic packet inspector. For back end file scanning and processing, I decided to make use of one of the many free online sandbox solutions that also offer their service through a Python compatible API. I chose VirusTotal as it is the most recognised and likely to have a larger amount of known malware on file.

The simple and high-level procedure of this solution is as follows. Full packet captures are captured live and continuously. These are then filtered again so that only TCP frames using the SMTP protocol on port 25 are recognised by the application. Files will then be pulled out and stored in a remote quarantine storage area and a range of operations performed on each one as it arrives to determine a level of threat to the network. The information gathered is then logged to a logfile and forwarded to security personnel for further investigation. This application is able to run continuously without user intervention. The application sits on a server within the virtual organisation between two routers (one router for servers and one for workstations) so it can see all traffic traversing the network.

The result of this project is that all files extracted from SMTP packets are saved to a quarantine area, scanned by virus total and logged. Files marked as a threat are processed automatically and the files SHA256 hash, name, detection timestamp, compression, first 16 bytes in hex and the JSON sandbox threat report and presented to a security analyst in the form of and email.

Technologies used:
VMware Workstation, Python & Visual studio, VirusTotal Sandbox & API, Openfiler SAN, Freesco routers, Zentyal Domain Controller, Windows Server, Ubuntu Server, Network Minor

Student Name: Ieva Rutkovska	**Supervisor:** Byron Traecy
Project Title: An in-depth research and analysis on information-stealing malware	
Research Question: A famous proverb says that: " Prevention is better than a cure ", so how can we avoid on becoming a victim of this threat?	

Project Abstract:

In early 2019, banking trojans also known as bankers have been the most dominating type of malware appearing in several malspam campaigns world-wide. Bankers are increasingly versatile piece of malware that are used by malicious actors for distributing secondary payloads, crypto-currency mining and harvesting various type of data such as banking credentials, passwords, emails, login information and so much more.

The aim of this project is to research the information stealing malware and have a better understanding on how this malware operates.

Before conducting the analysis, a sample will be acquired from Virus Total. Analysis will begin with static analysis, followed by dynamic, code and lastly memory analysis. Upon completion of the analysis, a YARA rule will be written and submitted to Virus Total for a retro hunt to test rules accuracy.

Human curiosity, error and lack of knowledge is still the key aspect on how this type of malware can be introduced to your system by opening attachments in your email, clicking on links you receive in an email that appears to be from your bank and other ways.

Technologies used:
Virus Total + including retro hunt, PeStudio (static analysis), Cuckoo Sandbox (automated malware analysis system), IDA (static code), Olly dgb (dynamic code), Volatility (memory analysis), YARA (signature based, pattern matching rule)

Student Name: Sean McCarthy	**Supervisor:** Pat McCarthy
Project Title: Automating Mobile Testing Processes for Software Engineering Teams.	
Research Question: Is the effort of creating an automation solution for a core testing process worth the time and bandwidth it takes.	

Project Abstract:

Automation is the idea of making a process faster than its manual counterpart. This is the general idea behind software test automation and also the idea behind this project. Many companies utilise software automation in order to test all aspects of their products, from general functionality to localisation.

This project wanted to look at a neglected area of a case studies testing cycle and see if implementing automation can increase the time and bandwidth available to testers by decreasing the time it takes for the testing process to be complete. Along with this, it will be seen if implementing the automation on a simple but important test process is worth the time, effort and bandwidth it takes.

The project was also aimed to follow core principles that are used when developing software: usability, performance and scalability. The final results of the project demonstrate these qualities well with different features that allow for a dynamic testing process.

Technologies used:
C#, Visual studio, Selenium WebDriver, WPF, XML

Student Name: Darragh Murphy	**Supervisor:** Deirdre Dunlea
Project Title: One Stop Defence	
Research Question: Cyber-threats are increasing, Is there a need for a central location that helps limit their effect?	

Project Abstract:

The Internet has given us a wealth of information, possibly too much. For example, If you have an issue with your phone not connecting to your bluetooth speaker, how many different sites are there explaining how to fix the issue? Thousands if not hundreds of thousands all with different methods, tips, tricks and technical jargon. Now imagine that you fall victim to a serious cyber attack? You will be overwhelmed with a vast amount of information and with nothing guaranteed to work.

But if there was one central point for the information you need, then there is no need to open 10 different tabs/websites trying all the different methods hoping one of them will work. On one single page you get:
- The definition of the cyber attack your facing
- The symptoms of said attack
- How to defend against it
- What to do when you're a victim of such an attack

The website will also educate users how to defend devices such as smartphones, PC's, Amazon echo dots, security cameras and other devices prone to attacks or those that are typically vulnerable. Along with this a "bible" or "10 commandments" of best cyber-security practices will be available, e.g. how to pick a strong password, how to avoid potentially malicious sites or files and how to protect you information and privacy. This allows all users, no matter their skill level, to understand and gain a thorough knowledge of the problems presented. This type of website would enable someone to quickly and easily fix their internet connected device. I intend to achieve this by researching the most common issues facing internet users and using wordpress (and it's many plugins) to design a website that is easy to use and appealing to look at. I will host the website locally using xampp and when the need arises use a web hosting service that would allow anyone to access the site on their internet connected devices.

I believe this project will benefit many different people as it will be designed to be as efficient as possible in regards to providing necessary information and usability. Whether the person using the website is an experienced IT technician or somebody who only got their first internet connected device the day before, my aim is to ensure they are able to get the help they need from one website rather than various different ones. A crucial aspect of making a good website for users is not just it's usability but also the overall user experience, if the site is not pleasant to look at no matter how valuable the information is on the site if it's users can't easily read and see it then I failed the proper implementation of this project. I intend to do this by presenting the information in both an eye catching way through a proper color scheme but also an organised presentation of the information.

Technologies used:
Wordpress, Xampp, CSS, HTML

Student Name: Colm Ryan	**Supervisor:** Byron Treacy
Project Title: Using Gamification To Create Mobile Apps For Use In Speech And Language Therapy	
Research Question: Is it possible to create a mobile app, incorporating gamification techniques, to assist Speech Therapists working with children to improve their language skills?	
Project Abstract: This project seeks to apply Gamification techniques in a mobile application for use in the domain of Speech and Language Therapy (SLT). The project's main elements are therefore Gamification, Mobile technologies and SLT. The goal of the project is to create a mobile app to improve the current tools available to Speech Therapists working with children. SLT is the science that specialises in assisting and treating social communication difficulties in adults and children. It involves cognitive and expressive language problems as well as pronunciation difficulties. Gamification is the term used for the application of game design elements and game principles in nongame contexts. It is a well-known fact that children learn through play. Speech therapy sessions include a lot of repetitive activities where the therapists need to keep a child interested for an effective time span. Gamification is used to incorporate the play and 'attention-keeping' elements into the educational context.	
Technologies used: Android Studio, Android, Java, MongoDB, MongoDB Atlas, Git, GitHub	

Student Name: Shane P Twohig	**Supervisor:** Mary Davin
Project Title: Evaluating Security Monitoring tools for use within Security Operations Centres	
Research Question: Can a guide be produced which makes the process of selecting tools for a Security Operations Centre, an easier one?	

Project Abstract:

The project aimed to to explore the concept of Managed Detection & Response (MDR) and the tools which may be used in its provision.

A Guide to Security Operation Centre (SOC) Tools was created through extensive testing and comparison of a range of the most popular Tools and Platforms employed by SOCs worldwide today.

These tools were tested and compared on several levels, including cost, complexity of use, range of functionality, etc. From this testing, a series of recommendations are made on the applicability of a specific tool to a particular type of SOC.

The overall goal of the Project was to both explain the concept and benefits of MDR and to make the process of selecting tools, when establishing a new or adapting an existing SOC, an easier one.

Technologies used:
Suricata, Network Miner, Snort, OleTools, Wireshark, Bro, Carbon Black, Splunk, Palo Alto, SumoLogic, Symantec Endpoint Protection

Student Name: Jeremiah O Donovan	**Supervisor:** Diarmuid Grimes & John O'Brien
Project Title: Why Companies should be investing in Automation	
Research Question: Can automated testing greatly reduce manual testing?	

Project Abstract:

The aim of this project is to create an automation test suite that software developers or software quality analysts can use in a company.

The test suite allows Software Developers and Software Quality Analysts (SQA) to automatically test new software code to see if it's stable for release.

The SQA will code a series of manual tests that can be then run automatically at any time against software developers code to ensure its implementation won't create an unstable build.

These automated tests can be run against new and pre-existing code to ensure stable releases of software updates.

If the code passes all tests in can be merged into the final release build.

This project is to show why companies should be looking to invest in test-automation in the near future.

Technologies used:
Ranorex, Katalon Studio, TestComplete, Selenium, Windows, C#

Student Name: Dominik Skarbon	**Supervisor:** Vincent Ryan

Project Title: Distributed Denial of Service attacks in Cloud Computing and Software-Defined Networking

Research Question: Why are Distributed Denial of Service attacks so prevalent in cloud computing, and will Software-Defined networking serve as a means of eradicating this threat or will it become its next victim?

Project Abstract:

Since the beginning of the Internet, cyber-threats have plagued users and organisations. The level and sophistication of attacks have increased dramatically in recent years. Distributed Denial of Service (DDoS) is one such attack which has been used extensively both against physical networks and, more recently, against cloud-based networks, which inherited multiple vulnerabilities from its precursor the on-premise architecture while adding some of its own. The emergence of Software-Defined Networking (SDN), has created a new plane for an attacker to target.

This research paper covers the taxonomy of these attacks in the Cloud and SDN environments. The paper examines attack methods, impact characterisation, and collateral damage to non-targets. The main focus of the theoretical aspect of this project is to provide a comprehensive illustration of all factors involved in the execution, impact and defence against DDoS attacks in both technologies, while the implementation aspect focuses mainly on SDN. Its open-source ideology facilitated access to a wide range of technologies that enabled practical research in this area, were experiments in a realistic virtual network have reflected the behaviour of real-world scenarios. An offensive approach involving various attack methods allowed the identification of the most effective means of executing these attacks and the identification of potential vulnerabilities in SDN networks.

The implementation involved directing various DDoS attacks against several different topologies in an SDN environment, and an examination of the results from these attacks allowed for the identification of the topologies that were most and least resistant to this form of attack.

Technologies used:
Python, Bash, Mininet, ONOS, Floodlight, Kali, Hping3, Wireshark

Student Name: Wei Liu	**Supervisor:** John O'Brien
Project Title: Local Service Hub	
Research Question: How can we improve our everyday life through the use of content management system?	
Project Abstract: This project is to facilitate the connection of service consumers with service producers on an online platform, for example Music student with music tutor. This is local use only depends on which area the audience is in. There are multiple categories of choices including, 'Courses', 'Tutors' , 'Repairs'. Additional categories can be dynamically added to the list at any time. The objective is the empowering of end-users to find appropriate information, thereby enabling them to make informed decisions on the services provided by sellers. There will be front-end web app and an android app associated with this project for the user interface interaction and secure back-end Web APIs. All the important information will be stored on database. The web app and android application will display only public information which is required for visitors to view. Access to personal information will require authorization through API micro-service endpoint.	
Technologies used: MDB Framework, C#, Java, Cloudinary, SQL, Visual Studio, ASP.NET Web API, Android studio, Google Maps, Entity Framework, Git, Azure web server, React.js, OkHttp3	

Student Name: Kamil Markiewicz	**Supervisor:** Dr Laura Climent
Project Title: Scanner Analytics System for Snap-On	
Research Question: Automation of the testing process at Snap-On Diagnostics and enabling data analytics.	
Project Abstract: Snap-On Diagnostics creates scanner devices that help mechanics diagnose vehicle issues by communicating with the car's on-board computer. Any new hardware or software for these scanners needs to be tested before being deployed to the public. Currently the testers at Snap-On go through the functions being tested while writing down on paper what they did and what results they got. This process is slow and error-prone due to the large amount of manual work required to write down all the information and enter it into an excel spreadsheet. This project aims to automate the scanner device testing process at Snap-On Diagnostics, by using the log files generated by the scanner devices during testing. Valuable information can be extracted programmatically to remove unnecessary manual work as well as enable analysis on the data. The project uses a C# desktop application to collect the log files from the scanner devices into an MSSQL database while an ASP.NET website will enable data analysis on the data contained in the database.	
Technologies used: C#, MSSQL, ASP.NET	

Student Name: Rebecca McCarthy	**Supervisor:** Jing Hua Ye
Project Title: Employee Scheduler: Comparison between SAT and CSP	
Research Question: Can we find the best method for solving a work scheduling problem?	

Project Abstract:

Manually creating work schedules for employees, through Microsoft Excel or on paper, can be time-consuming, error-prone and labouring for the administrator. Within companies, there are many different constraints that affect how employee schedules are set-up, such as, an employee working only one shift at a time, varied shift rotations, and the number of employees needed per shift. These constraints must be satisfied to create agreeable work schedules.

This problem of generating a feasible schedule for employees within a company can be identified as a problem in Constraint Satisfaction Problem and Boolean Satisfiability Problem. For this project, we compare the time taken for a solution to be provided against the number of constraints added to the problem. Once a model has been created for the scheduling problem, an appropriate algorithm is applied to the issue and used in generating a feasible scheduling solution based on the constraints applied. The resulting schedule would give the employee a 7-day timetable. Each employee who is assigned to work a shift will be listed along with the number of employees required. During a 7-day period, an employee is to work 2-day shifts, followed by 2-night shifts and 3 days off for rest after being on nights. These are only a few constraints of many and can grow into more complex areas such as job allocation, depending on the profession.

A successful outcome will be based on the schedule created. This should provide us with a schedule that doesn't have an employee working two shifts at once, the required number of employees assigned to a shift, and varied shift rotations. The result of this application will benefit both the employee and the administrator, reducing time, error and labour. After both CSP and SAT are tested, we will be able to compare the results and see what approach would most suitable.

Technologies used:
C++, Python, Gecode, PySAT, VMware Workstation, Ubuntu

Student Name: Kieran Healy	**Supervisor:** Dr. Ruairi O'Reilly
Project Title: How to refactor a monolithic application into a microservice application	
Research Question: Comparing a monolithic architecture against a microservice architecture	

Project Abstract:

This project aims to refactor a crowd funding web application using the Microservice design pattern and the other using the Monolithic design pattern and compare their response times and their scalability. Using a Microservice design pattern in an application can lead to numerous advantages, the main advantage being scaling as Microservices when scaled do not lead to redundant deployments. However if the Microservice design pattern is not followed correctly and or the Monolithic application is not correctly broken down into its application layers then the Microservice application will suffer from disadvantages when compared with the Monolithic application.

The applications will allow a unregistered user to register, allow a user to upload a project, allow a user to pledge money to a project (as long as the project was not uploaded by the user and if the project has not met its funding target yet), allow a user to logout, a user can view a list of their projects, unregistered users can view all the projects. Both applications are also localised meaning that it is is simple to add support for another language.

Technologies used:
Spring Boot, Thymeleaf, SQL, JPA

Student Name: Chun Hin Lam	**Supervisor:** Colin Manning
Project Title: Machine Learning in Viral Music Prediction	
Research Question: Can machine learning be used to predict a song's popularity by identifying the patterns between the elements of previous songs and their popularity?	

Project Abstract:

The music industry is an enormous industry, estimated every year there are about 360 million songs produced by music producers around the globe. Out of these 360 million songs, only 1000 songs make it to billboard global charts. The questions are “what element of a song driven its popularity?”, and “is there any pattern in all previous successful songs?”.

The objective of this research project is to predict the popularity of a newly written song by using machine learning. In order to achieve this, the Million Song Dataset will be used as a training and testing set, this dataset contains songs’ information such as actress rating, song genre, song loudness, song timbre, song tempo, etc. These data will then be analysed by the machine learning model, which will find the common patterns in all previous popular songs. These patterns can also be known as the formula for a successful song. Using this formula, the popularity of a newly written song can be predicted before it releases.

The machine learning model is based on three areas: data cleaning, the impact of a feature on song rating, and the type of machine learning algorithms and their accuracy. For data cleaning, any unused data fields will be removed to reduce the size of the dataset which will improve the performance as less processing is required. To find the impact of a feature on song rating, data visualisation will be used to visualise the correlation between features and the song rating. Based on the correlation, the proportion of the impact on song rating in each feature can be identified. The last area is to implement different types of machine learning algorithms and find the most suitable algorithm with the highest accuracy.

Technologies used:
Python, R, Postgres, RPostgresSQL, ggplot2, h5py, rhdf5, PGadmin, scikit-learn.

Student Name: William Coomey	**Supervisor:** Deirdre Dunlea
Project Title: Detecting Network Anomalies on Distributed Control Systems	
Research Question: Can an automated system to detect network anomalies increase reliability in a Distributed Control System	
Project Abstract: Distributed Control Systems are a vital part of modern manufacturing processes. These systems contain numerous devices, such that they cannot all feasibly be monitored by humans. If a device in the system were to fail unnoticed, it could have catastrophic consequences up to and including the loss of millions of euro in lost product. The goal of this project is to create a system that monitors the network for failed or malfunctioning devices, so the people responsible for the devices on the network can be alerted to the issue and rectify the situation.	
Technologies used: Java, WinPcap, Wireshark, nmap, jNetPcap, Eclipse	

Student Name: Robert O Callaghan	**Supervisor:** Gerard MacSweeney
Project Title: Comparative Analysis of Latency in Software Defined Networks	
Research Question: Does the configuration of a network have an effect on the latency of that network?	

Project Abstract:

As networks get larger, moving from LAN to WAN, the need for businesses and organisations to make communications between multiple sites as efficient as possible is paramount. The make-up of a network is evolving also where hardware is shrinking in size and, in the respect of this project, disappearing.

Software-Defined Networking (SDN) is providing a cheaper platform for organisations. Changing a network from a physical platform to a software-defined platform is cost related (some articles quote up to a 40% saving on the network), so we should have the attitude to make the communications on that network as efficient as possible. Latency can become an issue for an organisation deploying an SDN. This can be avoided by deploying high-level architecture on the outskirts, but this may add to costs on the initial configuration and deployment of the new Software-Defined setup. This may prove difficult to provide for an SME.

This project will explore latency differences in different configurations of SDNs. In order to achieve this, software will be needed to simulate these differences. Latency is an effect on the speed of delivery of packets over a network connection. There are several factors that can lead to high levels of latency. This, of course, resulting in slower delivery of packets and poorer performance.

Through a certain technique (the Precision Time Protocol), the latency between Software-Defined devices will be measurable and results can be garnered. This will be done on a set of Virtual Machines. This will also be compared to known research and studies that may already exist to confirm findings.

Those who can potentially benefit from this project are SMEs who are attempting to change over to an SDN. Also as latency is a universal issue that may even appear to a more sophisticated network, it may also be relevant to larger setups.

If this project is successful, it will provide a better blue print to setting up and SD-WAN in a more specific configuration. I hope to achieve a definitive result that can be compared to research and studies that have already been carried out and presented.

Technologies used:
Mininet, Dummynet (Network Emulator), xQuartz, Python, VMware Workstation

60

Student Name: Alex O Regan	**Supervisor:** Donna O' Shea

Project Title: An Artificially-Intelligent, Self-Learning Image-Sharing Platform

Research Question: Implement a deep-neural network using transfer-learning for classifying the contents of images.

Utilize the neural network in the back-end of a web-based image-sharing platform, and gather descriptive data about images collected.

Periodically reconstruct training data-sets for the neural network using images uploaded on the platform.

Project Abstract:

Deep Neural Networks(DNN's) are a highly-powerful, but computationally-expensive means of providing machines with human-like intelligence in specific tasks. One such use for Deep Neural Networks is in the field of computer vision (CV), where, after extensive training, an image recognition system can determine the contents of images with over 90% accuracy. However, these models can only achieve these levels of performance after being trained on datasets that are comprised of millions of example images, and this training process can often take weeks of constant computation on powerful machines. While online resources exist to supply this many images, there is very little variety in their shape and format, which can lead to models under-performing when introduced to more diverse examples.

This project hopes to solve the issue of sourcing more diverse datasets by offering an image-sharing online platform to the public. Images uploaded by users will be passed to an image-recognition model that will generate descriptive keywords for the content. The user can then determine if the tags are accurate, and can specify their own additional keywords. Periodically, the platform will gather images for popular tags, and create new training datasets, allowing the model to improve and adapt itself to the data it's most-often presented with.

One major challenge that this project faces is the initial cost of training the first image-recognition model, since potentially hundreds of thousands of images are required to create a viable neural network. To overcome this, a series of state-of-the-art techniques are used, such as the concept of "transfer learning", where a portion of a pre-trained, open-source neural network is adapted to function on a new dataset, essentially "transferring" it's previously-learned knowledge. This reduces the size of data necessary for training by orders of magnitude.

Technologies used:
Keras ML Framework, Flask Web Server, MySQL, gRPC, Docker/Docker-compose, Python, HTML/JS/CSS

Student Name: Jack Hickey	**Supervisor:** Ruairí O'Reilly
Project Title: Blockchain: automated insurance risk analysis and data validation	
Research Question: Can blockchain be utilised to improve risk analysis within the insurance industry?	

Project Abstract:

Blockchain has made headlines for its use as a cryptocurrency, most notably with Bitcoin; however, academics and industry alike are researching its other potentials in diverse sectors.

This project proposes the use of smart contracts and blockchains' immutability of records to perform risk analysis of potential policyholders in a more efficient, cost-effective, and secure manner than conventional insurance models.

Blockchain-based risk analysis can automate these tasks as well as use the immutability of the blockchain to get more valuable data. The proposed solution uses Hyperledger Fabric, a permissioned blockchain network. The application allows policyholders to retain ownership of their data and claims. As the policyholder changes insurers, policyholders carry their data with them to new insurers, allowing for the smart risk analysis to make more accurate assumptions. As time proceeds, insurers are thus enabled to make smarter offers based on this assessment. Hyperledger Fabric allows policyholders to retain privacy with regards to their data, and for insurers to offer contracts using the blockchain network that are only visible between the policyholder and the insurer.

The project ultimately determines that smart contracts can indeed automate and increase the efficiency of how risk analysis is performed for the insurance industry. The adoption of blockchain technology within the insurance industry will revolutionise the way we do insurance.

Technologies used:
Hyperledger Fabric and Composer, ReactJS, JavaScript and REST

Student Name: Alan McCarthy	**Supervisor:** Colin Manning
Project Title: Investigating Ransomware	
Research Question: An investigation into ransomware, its growing number of attacks on business's and a deep dive analysis on how exactly these are performed	

Project Abstract:

This project investigated the inner workings of ransomware. Specific ransomware samples were analysed in detail using static and dynamic analysis and the results were documented. Malware samples were identified and classified. The Jigsaw ransomware family was analysed in depth. Yara rules were written that could be used to detect this ransomware. Yara rules are sets of unique identifiers of a malicious sample that can identify it and distinguish it from other malware. Yara rules can be used with historical virus databases, such a VirusTotal, to conduct retro-hunts. This can identify early occurrences of the malware and its variants.

They can be used to help cluster in the identifying and classifying of malicious threats and can also be used in a process that is known as malware hunting. This is a service that allows you to hook onto the stream of files submitted to VirusTotal and get notified whenever one of them matches a certain rule written in the YARA language. Yara rules are written using a set of unique identifiers from the malicious sample.

Technologies used:
VirtualBox, PEStudio, PEiD, Process Hacker, File Alyzer, VirusTotal, DnSpy, Atom

Student Name: Jack Walsh	**Supervisor:** Deirdre Dunlea
Project Title: Hunting for malware using Indicators Of Compromise.	
Research Question: Can open-source intelligence and freeware be used to build comprehensive Indicators Of Compromise ?	

Project Abstract:

This thesis aims to examine the possibility of using Indicators Of Compromise to investigate potential cyber-attacks/breaches. These indicators look at the behavior of the malware on the Endpoint as opposed to traffic detected by an IDS or a firewall.

I aim to conduct a cyber-attack on a simulated environment, investigate the attack using open-source/freeware tools and develop IOCs for 5 strains of malware.

The attack process is based on the 'kill chain' (originally derived from a military term) which defines how an attacker gathers information on a target, how they use that information to create a payload specific to their target, and finally how they exploit and exfiltrate information such as personal information, passwords, etc., from their target.

The defense process is where the IOCs come into play as they compartmentalize the different approaches used by attackers to exploit a system. After something has been flagged investigation begins, google and other online services are utilized to gather info on the possible threat, and indicator is developed based on the intelligence and then tested. This is a cyclical process, meaning, threat intelligence is added to the IOC after each hunt/investigation.

Technologies used:
Redline, IOC Editor, VMware, Kali Linux, System Internals, Open source intelligence.

Student Name: Adrian Coleman	**Supervisor:** Cliona Mcguane
Project Title: TinyDuino Wearable Device	
Research Question: How can a device to monitor a runner's stride be used to improve a runner's speed and reduce impact on their joints?	
Project Abstract: Runners aim to run the fastest time they can while minimising the damage to their joints. This project aims to connect a wearable device to an Android app using Bluetooth TinyShield. The device uses an accelerometer to measure a person's stride turnover and stride length. This data will be processed and the resultant information used by runners to improve their speeds and decrease the impact on their joints. This application will run in the background and can be checked at any time.	
Technologies used: Arduino IDE, TinyDuino, TinyShields, Android Studio, Android	

Student Name: Michael O'Reilly	**Supervisor:** John Creagh
Project Title: Using Natural Language Processing to make an interactive game	
Research Question: Can Natural Language Processing be used to create a more organic and social game?	

Project Abstract:

Playing video games is one of the most popular hobbies among children and adults from all over the world. It is a great way to detach yourself from your life and immerse yourself in another. However, many video games nowadays rely on limited dialogue options or dialogue trees to advance the plot which reduces the involvement of the player on the overall story. While this is understandable for games with a linear game design, I believe that my approach to a more dynamic story telling could pave the way for a new genre of games, one which allows the player to truly dictate the pace and direction of the story.

The objective of this project is to create a game driven by dialogue which does not limit the players options, but instead adapts to the sentences the player types. I will be using natural language processing in an attempt to make an engaging and interactive game between the user and NPCs. Using the Stanford NLP library in conjunction with machine learning I hope to achieve an artificial intelligence which can derive information from the user and generate coherent sentences that shape the games story and deliver a more organic and fluid game play experience.

Technologies used:
Unity3D, C#, Stanford CoreNLP, Java, Python, Eclipse

Student Name: Robert Burns	**Supervisor:** Irene Foley
Project Title: A LOCAL STORE EVENT MANAGEMENT SYSTEM	
Research Question: Can a system be created to allow for the easy creation and accessibility of small events.	
Project Abstract: I have worked in a store in Cork city which regularly gets new customers and hosts gaming events for customers. I would like to create a system for this store or a similar one that makes it easier to plan such events. I feel like this would be a very useful system to have for the store to help run events and business on a day to day basis. The goal is to have the event management be the major part of this system. The users of this application can create, view and run events very easily. A system can be put in place to allow customers to apply to these events that may have a limited number restriction. This application can improve upon the events that a business already runs frequently. Customers could also use this to sign up to events early so the owner can gauge interest of each upcoming event as well as how much room to use for similar events in the future. This system also has room for expansion to multiple stores/store owners, different businesses and other areas of industry. Many businesses could benefit from this system including gaming stores, book stores/comic book stores, hardware stores or gardening stores.	
Technologies used: Android, Android Studio, Firebase	

Student Name: Ryan Monaghan	**Supervisor:** Dr. Sean McSweeney & Deirdre Dunlea
Project Title: Unwrapping Obfuscated Intrusion Vector Techniques Through Automation	
Research Question: Is it possible to decrease triage times and increase the accuracy of alerts through the automation of obfuscated intrusion vectors?	

Project Abstract:

The obfuscation methods employed by malicious actors require Security Operation Center Analysts to undergo training in order to fully understand and decode. As these security incidents are reviewed in real-time, it is important that the activity is decoded and communicated to the client in a timely manner, in order to satisfy time sensitive service-level agreements, as well as provide a list remediation steps.

By automating the steps required to decode more complex forms of obfuscated intrusion techniques, we can decrease overall triage time, while simultaneously supplying clients with more informative and meaningful alerts.

I intend to achieve this design through the use of Carbon Black and the esArtemis dashboard to monitor and analyse several examples of obfuscated intrusion attempts, decoding the contents of the commands and presenting them in plain-text to the user. I then plan to employ the steps required to de-obfuscate the commands to develop an application which will allow the user to feed an obfuscated string, and return the contents of the command in plain-text.

Technologies used:
esArtemis & esNetwork by eSentire, Carbon Black, BASH, SED, AWK, Sublime Text 3, Visual Studio Code, GIT

Student Name: David Nti	**Supervisor:** Arthur Tobin
Project Title: Exploiting Database Vulnerabilities in Web Applications	
Research Question: Vulnerabilities in Web Application	

Project Abstract:

The world is fast approaching a new era of the Data Age where every information gathered is vital to the growth and advancement in the business world at large. Most organization spend huge percentage of their budget on web application and general IT security in order to secure their application and also protecting the generated data. Although Web Application security has been a top priority for most leading companies, the threats against web applications has taken a new turn where hackers with little knowledge can exploit vulnerabilities in web application over the internet. Attacks on target companies has lead to exposure of dozens of private information one of such is Sony PlayStation. The attack on the Sony PlayStation expose close to 100 million user accounts. Interestingly this attack is one of the most common vector attack on networks-SQL injection attack. Why the recurrence of these flaws the answer lies in the technologies themselves and undoubtedly the human factor.

The popularity of web browser among different industries which has become one stop for all application and information gathering has allow hackers to plant malware's for exposing private information. Web applications provide easy platform for cyber-crime due to various technology that support it's platform. The 24 hour online presence has contributed to the vulnerabilities exploited by these attackers. It has ultimately allow hackers to leverage their attack, consequently gaining access to organizational systems through the end user devices. In attempt to secure web application by security expert various mechanism has been deploy such as application layer firewall, DMZ, IPS devices and BYOD has only increase the attack surface for attackers.

In this project ill be using Pen testing to estimate the security of network and it's web application. The goal is to identify possible vulnerabilities and threats that could be exploited by a malicious attacker. Having right security fixes can secure and prevent grass-root attack on a system. This project is targeted at helping the IT security consultants with detecting and securing the most common web application exploits that companies are vulnerable to today.

Technologies used:
Multillidae, bWAPP, OWASP, Linux, Burp Suit,

Student Name: Magloire Hateka	**Supervisor:** Dr Ruairi O Reilly
Project Title: Proof of Identity Platform for Consumer Services	
Research Question: Can a digital proof-of-identity platform be provided as a simplified means of enabling contractual service undertakings?	

Project Abstract:

Proof of identity for an individual in Ireland is typically reliant upon both proof-of-identity and proof-of-address an individual. This typically requires number of documents pertaining either to the individual (Passport, birth certificate, drivers' licence, PPS. card) and the property at which they are resident (lease, utility bill, deeds of property). This is a cumbersome process will delay the undertaking of transactions between consumer and service provider while still being susceptible to scams such as identity fraud.

This project indents to provide a platform based on web application where Irish residents and Irish based companies could simply and securely register their details and home addresses. After a user's registration is successfully completed, the system will proceed by checking the authentication of the information provided with partners (Residential Tenancies Board, Property Registration Authority or Housing Authorities). The system will then generate a document which can serve as Proof-of-address with a unique lifetime Proof-of address Number.

Using this technology can reduce identity frauds for Irish residents, public and private institutions can check their customers home addresses when they are subscribing for services or when posting to them mails, government and local authorities could use the platform database for a census and help local authorities for their future development plan.

Technologies used:
Drupal 8, Acquia Dev Desktop, Bootstrap 4, Apache Web Server, PHP and MySQL

Student Name: Dean Coakley	**Supervisor:** Ruairi O'Reilly
Project Title: Nginx server configuration simplified	
Research Question: Can human error be reduced when configuring nginx servers?	
Project Abstract: The project aims to reduce the complexity of nginx configuration away from the user, ensure best practices, provides client side validation, and assist in applying of configuration changes. The main aim is to reduce the amount of times an nginx server is configured incorrectly, possibly causing downtime on any production services that may be running on the server. An attempt to reconfigure a server incorrectly should fail locally with no interaction with the server. To shorten the feedback cycle to the user.	
Technologies used: Golang, Python, Linux, Git, Aws and Bash	

Student Name: Amy O Connor	**Supervisor:** Byron Treacy
Project Title: Pipeline Builder	
Research Question: Can we create an application to assist development teams in creating CI/CD pipelines used to deliver their software?	
Project Abstract: The Pipeline Builder will aid in the development of CI/CD pipelines. A pipeline is a well-defined software delivery mechanism used by development teams to deliver their products. Currently there are many tools developers need to integrate with, all requiring configuration within a pipeline and a large amount of documentation. Research shows more than half of developers want easier configurations for CI tools and services. The Pipeline Builder is an application for developers, allowing easier configuration and creation of pipelines. Having a clear, well-defined method of building and delivering products will help increase the quality of code and the speed of delivery for all teams.	
Technologies used: Java, Intellij, JavaScript, HTML, CSS, Bootstrap, React, Spring Boot and Thymeleaf	

Student Name: Shane O Donovan	**Supervisor:** Ruairi O Reilly
Project Title: Pluggy – A Secure Website Plugin Architecture	
Research Question: How might one develop a secure plugin architecture such that users can write functionality which works on websites with different code bases?	

Project Abstract:

Website plugin architectures such as Trello Power-Ups and the Zendesk Apps Framework exist, allowing users insert sandboxed JavaScript code (plugins) which adds custom UI elements such as interactive buttons onto Trello and Zendesk. Plugins are also often allowed to fetch data from the API of the sites they're enabled on, such as Trello's REST API. The problem is each site uses its own architecture, so plugins must be totally rewritten to work on different sites.

Pluggy is a website plugin architecture in whose plugins will work on any site with minimal changes required. Websites using Pluggy allow users create their own JavaScript plugins, adding functionality to said websites. Plugins can insert interactive UI elements such as buttons and modal dialogs.

Websites can tell Pluggy to override plugin element styling to better match the website design. Buttons could be styled as a link on one site and as a dropdown item on another, for instance. The plugin simply says to create a button, specifying its attributes such as its label, and the site itself creates the HTML element and sends any callbacks back to the plugin. This prevents plugins from introducing Cross-Site Scripting vulnerabilities onto the site as they have no access to the DOM of the website they are on. All plugin code is sandboxed.

Pluggy has a built-in plugin which adds a button that displays a dialog allowing users to upload, enable and disable plugins. This plugin can be swapped for another plugin by site operators should they wish to customise how plugins are loaded.

Technologies used:
Apache, HTML, JavaScript (ES6), Vue CLI 3 (VueJS), Webpack 4, Sass, PostCSS, Babel, ESLint, Golang, GORM, MariaDB, Tampermonkey

Student Name: Darragh Cahill	**Supervisor:** Mary Davin
Project Title: GlobalSight User Management System	
Research Question: McAfee currently has no way to manage users on an internal application. If a user forgets their password or a user needs to be created it takes management in McAfee up to twenty five minutes to resolve these issues.	
Project Abstract: This project aimed to create a web application for McAfee that helps management administer 1500+ users on various servers, along with other administrative tasks such as defining permissions and the management of servers and locales. This project will severely help productivity in McAfee while saving time. This is of upmost importance when working on real world projects.	
Technologies used: C Sharp, Visual Studio, GitHub, Angular JS, HTML, CSS, SQL, Jenkins	

Student Name: Conor Allen	**Supervisor:** Byron Treacy
Project Title: An in-depth analysis of EMM solutions for SMEs BYOD environments	
Research Question: Implementing a security policy and EMM solution for a SME which has adopted a BYOD workplace environment.	

Project Abstract:

Bring Your Own Device (BYOD) technology has increased dramatically since its introduction in 2010. Early adopters of BYOD were typically large organisations that used BYOD in association with Enterprise Mobility Management software. In recent years there has been a significant increase in the number of Small to Medium sized Enterprises (SMEs) implementing BYOD. This is due to the many benefits that comes with successful BYOD implementation. However, unlike large enterprises, SMEs often lack the necessary funds and expertise needed for securing these environments. In many cases SMEs allow the use of personal devices in the workplace without implementing the required policies for both ethical and secure use by the employee.

This project investigates the risks facing SMEs who adopt a BYOD policy. A draft BYOD policy was drawn up and put through an iterative process using feedback gathered through one such enterprise. A key feature of this project is the development of a metric for comparative analysis that employed aggregation of three comparative techniques. The SME referenced throughout this project is Local Link.

Technologies used:
Trello (Project Management), Google Trends, VMWare Airwatch, IBM MaaS360, MobileIron, SOPHOS

Student Name: Alec Owens	**Supervisor:** Ruairi O'Reilly
Project Title: Download and Storage of the App Stores Statistics	
Research Question: Can all available statistics be downloaded and stored in a database periodically?	

Project Abstract:

The overall goal of this project is to be able to use the information pulled down from Google Play Console and App Store Connect as a data source when using reporting tools, like Power BI. Giving people access and controlling the level of information available to each user leading to greater and easier access.

As of now connectivity to the information that is provided by the app stores is not possible through Power BI. Creation of a link between the app stores and Power BI would prove useful for any company who wishes to make reports regularly and on a large set of data over a period of time.

Information is pulled down at regular intervals, and will then be stored in a database which will have the ability to connect to the reporting tool chosen by McAfee being Power BI. Key investigations here will be how we download the information from the two app stores, either command line tools or is there an API that we can use, and also, what are we going to store and maintain the data in.

The database will need to be updated periodically, refreshing the database at a certain times throughout the day is the main goal. Providing access to users who register on the web page and controlling what permission each user has provides the security to the database. Using an API to connect to the database from Power BI, by passing the username as a parameter returns back content available to that user.

Technologies used:
C#, Angular, CoffeeScript, Sass, SQL Server, HTML, Jira, Jenkins, Microsoft Power BI

Student Name: David Hurley	**Supervisor:** Paul Rothwell
Project Title: Simple Animator	
Research Question: Are animation software applications more complex than they need to be?	

Project Abstract:

Much of today's media with which we interact uses animated graphics. These animations are produced using a wide variety of animation software applications. However, it can be difficult to understand the technologies behind these applications and thus to learn how to use them. Added to that, they may be limited in the formats they can produce. A novice in this area may have to spend more time than they would prefer in learning the user interface and experimenting with what the software can offer before starting to make animations of their own within the software.

The proposed application will provide a simpler interface compared to many of the more popular applications available. Users can create projects from scratch or can use a pre-existing image to make their own animations. A preview will allow the user to view their work and the user can their export project to a variety of formats.

Technologies used:
C++ Qt

Student Name: Keith Kenneally	**Supervisor:** Paul Rothwell
Project Title: Smart Queuing System	
Research Question: Can a system be developed which allows a person, who is waiting in a long queue, to leave that area and get notified through an app when their number is called?	
Project Abstract: This project involves the research and development of a Mobile Application/Web Application system that allows a user to enter a virtual queue for a service. The user can join the electronic queue by scanning a QR Code and then physically leave the waiting room to do other things while waiting. They will receive real time notifications of their queue position, expected waiting time and when their ticket is called. Our system will look at previous data for estimating the time remaining in the queue for each customer so they can plan their journey accordingly. Our system will also keep track of the users' GPS coordinates; if the users were to stray too far from the waiting area and risk missing their spot, they will receive warning notifications. This system could potentially save people hours of their day. Instead of sitting in a waiting room, they can proceed with their daily chores and rely on the mobile application to notify them when they reach the top of the queue.	
Technologies used: Android Studio, Java, C#, ASP.Net API, Microsoft Azure Server, React, MLKit, Google Maps, Github	

Student Name: Alex O Regan	**Supervisor:** Donna O' Shea
Project Title: An AI-Driven, Self-Learning Image-Sharing Platform.	
Research Question: "Can deep learning data-sets be diversified using a public image-sharing application?" "Is it feasible to implement a deep neural network in a web-based environment?" "What is the minimum number of images required to train an effective deep neural network?"	

Project Abstract:

Deep Neural Networks(DNN's) are a highly-powerful, but computationally-expensive means of providing machines with human-like intelligence in specific tasks. One such use for DNN's is in the field of Computer Vision (CV), where, after extensive training, an image recognition system can determine the contents of images with over 90% accuracy. However, these models can only achieve these levels of performance after being trained on data-sets that
are comprised of millions of example images, and this training process can often take weeks of constant computation on powerful machines. While online resources exist to supply this many images, there is very little variety in their shape and format, which can lead to models under-performing when introduced to more diverse examples.

This project aims to solve the issue of sourcing more diverse data-sets by offering an image-sharing online platform to the public. Images uploaded by users will be passed to an image-recognition model that will generate descriptive keywords for the content. The user can then determine if the tags are accurate, and can specify their own additional keywords. Periodically, the platform will gather images grouped by tags, and create new training data-sets, allowing the model to improve and adapt itself to the data it's most-often presented with.

Since potentially hundreds of thousands of images are required to create a viable neural network, a series of state-of-the-art techniques are used, such as the concept of "transfer learning", where a portion of a pre-trained, open-source neural network is adapted to function on a new data-set, essentially "transferring" it's previously-learned knowledge. This reduces the amount of data necessary for training by orders of magnitude.

Technologies used:
Keras ML Framework, Flask Web Server, MySQL, gRPC, Docker/Docker-compose, Python, HTML/JS/CSS

Student Name: Marko Cirkovic	**Supervisor:** Arthur Tobin
Project Title: IT Service Management	
Research Question: Can the implementation of an ITSM application provide businesses with the right tools to achieve asset handling and increased efficiency with IT service processes?	
Project Abstract: The development of an IT Service Management application (ITSM) capable of monitoring and recording stock is critical to businesses nowadays. Working in medium to large organisations as an IT technician or a helpdesk administrator can be challenging. Lack of technology offered to complete day to day tasks can lead to a decrease in productivity. Administrators can find it extremely difficult to monitor hardware and other assets, this can result in data loss and can lead to theft. The real question is, can the development and implementation of an ITSM application help a business achieve asset handling and reduction of overall cost? In other words, what are IT businesses missing that would implement, manage and deliver IT services in the best possible way to meet their goals? ITSM offers the appropriate mix of technological systems, people and processes. This concept offers a full range of complexity and interaction with other IT services and processes.	
Technologies used: WAMP, Visual Studio Code (VSC), PHP, PhpMyAdmin, MySQL, Java, jQuery and GitHub	

Student Name: Chris O'Riordan	**Supervisor:** John Barett, Garry Smith
Project Title: `Virtual Receptionist	
Research Question: Design Of A Virtual Receptionist	
Project Abstract: With the ever-increasing popularity of virtual assistants like Amazon Alexa and Google Assistant helping people lead more productive lives, technologies like these are quickly becoming a main stay of ordinary people's lives but little to none of these virtual assistants have yet to enter the professional market. The Virtual Receptionists platform will help office workers and the like to book meetings and greet guests upon their arrival to the organisation.	
Technologies used: Kotlin, Android, NodeJs, MySQL	

Student Name: Andrew Crowley	**Supervisor:** Dr. David Stynes
Project Title: Malware Worms: Initial Infection Vectors, Propagation Methods, & other capabilities	
Research Question: Categorisation of the evolved capabilities of a variety of worms & initial infection vectors	

Project Abstract:

The first malicious worm wreaked havoc on the internet in 1988, known as the “Morris” worm. Since then, Worms have evolved to carry payloads with more malicious intent. This includes data theft, backdoor access, and more destructive capabilities, such as ransomware and file-infectors.

The damage caused by a worm is reliant not only on the payload, but how many machines the worm manages to propagate to. Propagation methods have evolved to both try and evade detection, or spread more quickly. For example, USB propagation is slower but evades firewalls, network propagation is quicker, but also more likely to be flagged by a firewall.

The initial infection vectors, (ie. How a worm infects its first host), have also evolved. Phishing techniques have become increasingly convincing & documents with malware embedded in them have become better at evading AV detection. In this project, we explore and fully categorise the evolved capabilities of a variety of worms, as well as initial infection vectors employed by threat actors.

Technologies used:
VMWare Fusion, Windows 7, OllyDBG, IDA Disassembler, Fakenet, Sandboxie, WireShark, Network Miner

Student Name: Sinead Hegarty	**Supervisor:** Gerard MacSweeney
Project Title: Word Roar	
Research Question: Interactive Gamification-based Mobile App for Speech Therapist Sessions	

Project Abstract:

Speech therapy is the science that specializes in the evaluation, diagnosis, and treatment of communication disorders. It includes word-finding issues, social communication difficulties and structural language impairments.

On the other hand, gamification is the term used for the application of game-design elements and game principles in non-game contexts. In this project we want to create a mobile app allowing speech therapists to introduce interactive gamification-based activities during their sessions with children. The goals of the project are as follows:

1. Survey of the current speech therapy techniques applied for improving the speech of children.
2. Compare and contrast the gamification-based approaches available for existing mobile apps.
3. Survey of different algorithms/libraries for speech recognition.
4. Create an app that put all pieces together:
- It must propose a set of activities following a gamification-based approach.
- The activities must give support to an underlying speech therapy methodology.
- The app must be able to interact with the child, collecting some sound inputs and running some speech recognition algorithms in the background, so as to provide reports/feedback.

Technologies used:
Android, Java, Github, Android Studio, Google Speech, XML

Student Name: Mark Facon	**Supervisor:** Arthur Tobin
Project Title: Securing a Hadoop Environment Through Threat Modelling	
Research Question: How effective is a threat model when securing a Hadoop environment	

Project Abstract:

Digital data has become an inevitable consequence of our daily lives; large amounts of personal data is being collected from many different sources due to new trending technologies like IoT and is being used by big data technologies like Hadoop, an open-source software with distributed storage and processing capabilities. Securing these scaling environments from many possible threats and vulnerabilities can be a major undertaking for an administrator.

This project is aimed at improving big data security by providing Hadoop administrators a threat model to inform them about threats and vulnerabilities that could become a risk, explaining how it could happen and providing and testing mitigations for the risks. This is done using the STRIDE threat modelling methodology and the OWASP risk rating methodology.

Technologies used:
AWS, Ubuntu, Hadoop

Student Name: Cian Roddis	**Supervisor:** Byron Treacy
Project Title: Enabling a Neural Network to Recognize Key Features in Music	
Research Question: Classifying Music on a scale of genres to provide feedback to a user	

Project Abstract:

The goal of this project is to train a machine learning model to be able to categorize apiece of music. This will be done by user submitted audio via GUI. As it is an unseen piece of audio, the program will have to extract and analyze key features of the audio and try to classify it by comparing it to seen, classified data. This is known as supervised learning. A major factor when it comes to a piece of music is genre.

As music can be extremely complex, five algorithms, independent of each other are run on the piece of audio to get a more rounded outcome. The desired outcome is an accurate classification of the unseen audios genre. The classifications will be then fed through a graphing library for user friendly feedback.

Technologies used:
Python, Kivy, SciKit Learn, Librosa, Matplotlib, Ubuntu, Google API Manager

Student Name: Glenn Dunlea	**Supervisor:** Olivia Brickley & Pat McCarthy
Project Title: Optimizing Data Management in the Clustered Infrastructure	
Research Question: This project investigates how to automate multiple data management methods in a clustered infrastructure using virtual machines and open-source technologies.	

Project Abstract:

In today's technological age, the margin for error grows finer. Companies cannot afford to have any downtime and their dependence on data to support everyday operations is vital, with the use of new open-source technologies along with automative scripting languages companies can manage their data in more efficient and centralised manners. Organisations of any kind look to optimise how data is handled in their architectures in terms of priority. Organisations also must hold data for up to 7 years – moving non-prioritised data to suitable off-site locations to reclaim space in the infrastructure while upholding this regulation is a sought-after practice.

This project investigates the concept of efficient data management in a clustered infrastructure using virtual machines and open-source technologies. The system environment is designed to address the basic principles in clustering several independent computing resources. These include high availability, node redundancy, resource pooling and centralised administration with software provisioning.

Data management in the form of automated storage tiering and off-site archiving is implemented in this clustered environment. Data is moved between disks depending based on access times. Off-site archiving is also automated by policies that reflect on file size, file type, file access time. This is carried out using python; a very versatile and automating scripting language that allows users to automate tasks based on certain variables.

Technologies used:
VMware Workstation 15, Ubuntu 18.04 Server & Desktop, Python, Ansible, Kubernetes, Starwind vSAN, AWS S3, Microsoft Azure Blob Storage, iSCSI, Windows Server 2012 R2.