# Dissertation Proposal: Develop a Machine Learning Application that is Able to Detect Real-Time Anomalies in User Behaviour.

## Motivation

In the United Kingdom, an estimated 4.2 million surveillance cameras watch us every day (Clive Norris & Michael McCahill, 2006). Found in businesses, homes, shops and on high streets we are one of the most watched nations in the world. CCTV is actively available in 96% of homicide investigations, where it added value to the case 80% of the time (Scotland Yard, 2010). However, this statistic does not hold true for all crimes within the UK, with reports showing that CCTV only solves one in every 1000 crimes. (Press Association, 2009) It is fair to say that the work force allocated to high profile crimes makes it possible to find, collect and search all the archived video footage for evidence. This illuminates the problem at hand; CCTV is solely deployed in a traceability capacity when it has the potential to provide a much richer source of information. If we were able to understand video footage as it occurred, then we can start making smarter decisions that can lead to earlier crime detection and reduce the need to store such vast amounts of video footage on file.

The problem we need to solve to achieve this is, once presented with a set of data points representing the events that have occurred in a video frame, how can we detect whether what we are shown is anomalous in nature? Furthermore, can we apply this on an individual basis and detect when a single person on video is acting out of the ordinary? If we can solve this, we are in a capacity to create a system that could alert a vested party of an anomaly in real-time, allowing for the event to be investigated and any necessary action to be taken. This creates a much more proactive approach to detecting crime along with removing the need for archival of video footage.

My approach will be to develop a system that can detect users in a video stream, extrapolate data points about them, and then apply machine learning models to classify their behaviour as anomalous or normal. I will be focusing on unsupervised learning methodologies, evaluating which models provide the highest level of accuracy while being as high performance as possible. The system will use a microservice-based architecture in order to provide scalability and high-performance data throughput, a key success criterion for a real-time system.

The solution will not require storage of any video footage, as the video processing happens at the video source. I am aiming to show that this proposed approach will enable higher performance than existing alternatives while being accurate in its ability to detect anomalous user behaviour. To develop a suitable and achievable application in the given timeframe I will confine the problem to a single room environment with a set of configured subjects for facial recognition.

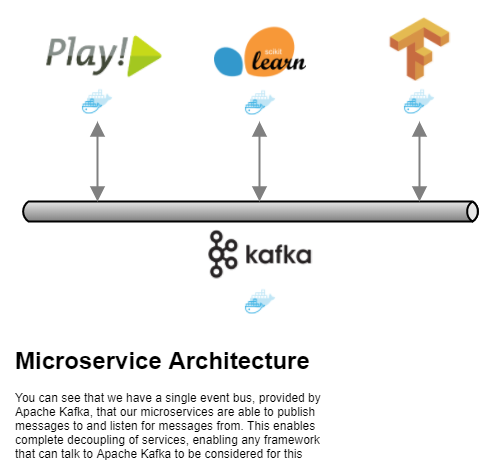
## Aim and Objectives

**Aim:** To develop a machine learning application that is able to detect real-time anomalies in user behaviour.

**Objectives:**

1. To research existing video processing techniques and available software in order to obtain as many data points with the highest degree of accuracy from a video stream.
2. To research machine learning techniques for detecting anomalies in time series data that can be applied to data sets produced from objective 1.
3. Develop testing scenarios that will allow the evaluation of machine learning models in their ability to detect anomalies in real-time.
4. Develop a micro-service based solution that allows interaction of services encapsulating video processing, machine learning models, an interactive web service and an anomaly notification service.
5. Using the test scenarios defined in objective 3, evaluate the applications ability to detect anomalies and alert users in real-time.
6. Compare and contrast the performance and storage requirements of the final system against existing CCTV systems and methodologies.

We are aiming to accomplish the development of a real world applicable system that will outperform existing solutions and methodologies when it comes to video processing and anomaly detection. To achieve this, we need to focus on objectives; 3, 4, 5 and 6 as a minimum, as they are concerned with producing the final product and evaluating its success in regard to the aim of this dissertation. The objectives preceding them provide support and increase the solutions chance of success, but time could be withdrawn from them once a single viable methodology has been found.

Through my initial work on my dissertation, I have been able to produce first architectural diagram of my proposed solution based off the papers described in the background section of this document. This should aid in the description of what a microservice based architecture looks like and show initial direction towards the final solutions shape.

In the diagram above, you can see how we can utilise microservices by running the different components of our application independently of each other, solely relying on the common event bus provided by Apache Kafka for communication. This means, during the Delivery phase of my project, I will be unrestricted when considering tools to implement features required of my final solution.

In the diagram below, you can see how we can leverage the cloud to perform the tasks of; providing an interface to the solution; and running machine learning models over received data. You can further see how we defer the video processing complexity to the video source, meaning we only transmit the event data to the cloud, reducing the storage and network traffic required to supply this solution.



## Background

**Paper:** A Survey on Behaviour Analysis in Video Surveillance for Homeland Security Applications

**Description:** The paper shows an overall look at the stages involved in creating an intelligent video stream solution. It gives insight into object classification, object tracking, extracting motion information, and behaviour analysis.

**Relevance:** The paper proposes a general architectural design from the initial capture of video, making sense of what is in the feed to then making smart decisions based off this information. The paper examines the most common approaches to object detection and classification, the extraction of motion information and how to apply behaviour analysis and understanding. I will be using this paper for its capacity in behaviour analysis, giving me a high-level overview of some of the most effective models in behaviour classification.

**Paper:** A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data

**Description:** The paper aims to achieve a comparative universal evaluation between the most common unsupervised learning models using public domain datasets for comparative evaluations in performance and accuracy.

**Relevance:** During my work, I will be required to detect anomalies in human behaviour within video feeds. This paper gives a good basis for selecting and exploring known machine learning models within this space, looking at not only accuracy and success of the models but also on their performance. It compares and contrasts unsupervised learning mechanisms on a variety of datasets allowing me a good foothold when choosing what models to adopt for my own data set.

**Paper:** Unsupervised Learning Techniques for an Intrusion Detection System

**Description:** The paper proposes a two-tier architecture for detecting anomalies in network traffic using solely unsupervised learning methodologies. It looks at how you can initially perform clustering of data to reduce dimensionality and then enable more sophisticated anomaly detection algorithms to categorise.

**Relevance:** The mentioned paper investigates the use of unsupervised machine learning models; K-means algorithm, Principle Direction Partitioning and Self Organising Maps, in order to provide anomaly detection on network traffic. The investigation of these models is extremely useful for my work, when evaluating which methodologies to adopt when detecting anomalous human behaviour. It further proposes an architectural approach that adopts an initial filtering of data using clustering algorithms to then enable more traditional anomaly detection methods. This approach is relevant to my work as I will be looking at how best to gain real-time analysis of video streams, which may require data transformations to make possible, and this approach could be adopted to my work.

**Paper:** Real-Time Network Anomaly Detection System Using Machine Learning

**Description:** The paper proposes a novel framework for real-time network traffic anomaly detection using machine learning algorithms.

**Relevance:** The paper proposes a suitable architecture for my dissertation project, though with a slightly different aim and data source. It will allow me a basis to work from and insight into problems to overcome when attempting to provide real-time processing of data streams. They adopt real-time technologies including Apache Kafka, Apache Storm and Apache Hadoop, which will greatly influence my final design of my dissertation project.

**Paper:** Microservice Architectures for Scalability, Agility and Reliability in E-Commerce

**Description:** The paper presents how microservice architectures facilitate scalability, agility and reliability using an industrial case study.

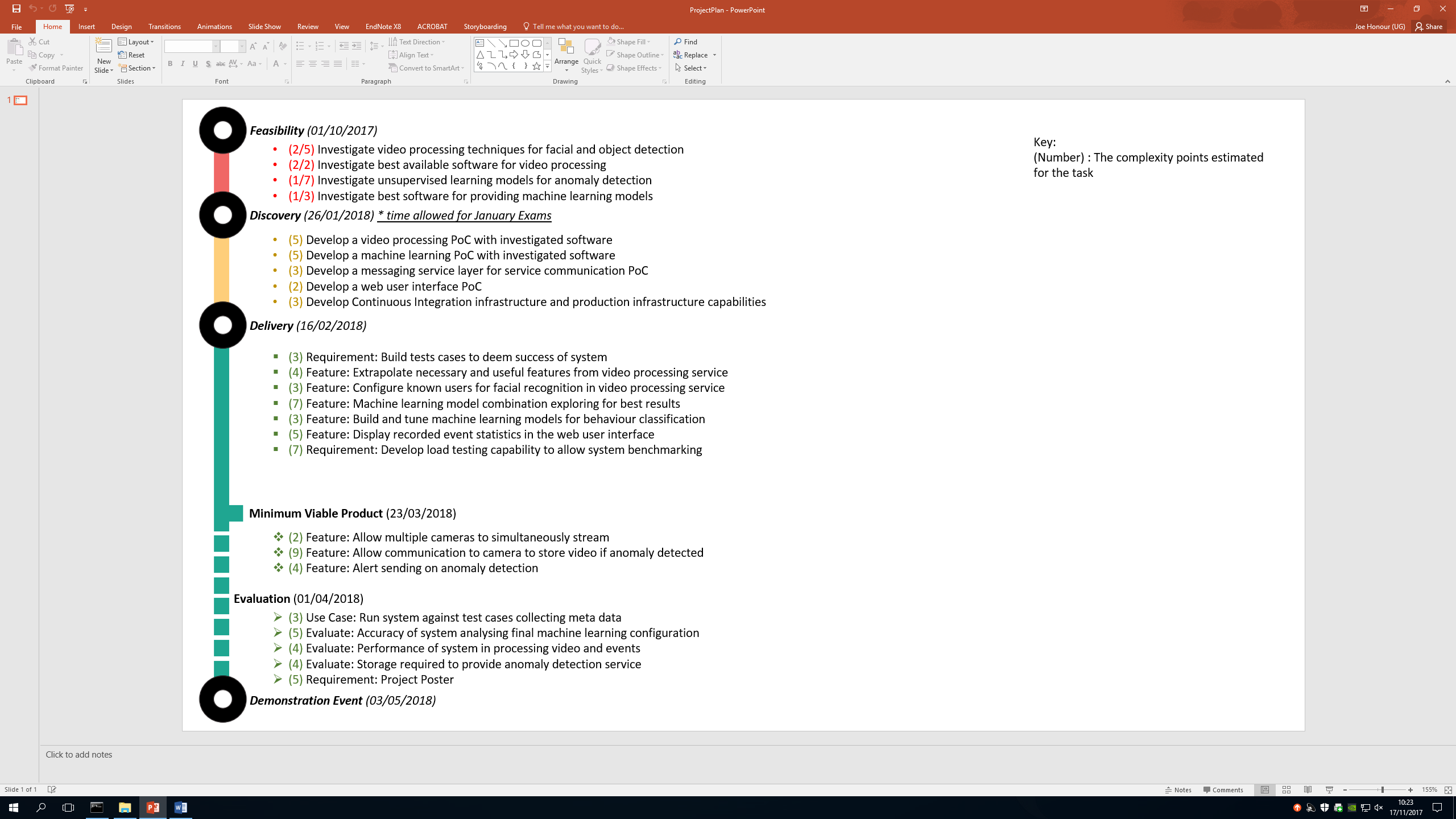
**Relevance:** My dissertation will need the key features of the microservice-based architecture, mainly focused on scalability and agility. This paper allows a firm understanding of how we can achieve this and the design decision required to create a successful solution. It also provides a real-world success story based on this approach, which allows me confidence in the achievability of my solution.

**Paper:** About Microservices, Containers and their Underestimated Impact on Network Performance

**Description:** This paper aims to investigate the cost associated with using a container-based approach within a microservice architecture. It sets out to prove that although microservices provide scalable high-performance systems, there is a cost associated with them.

**Relevance:** As my dissertation will require high-performance to be viable, and to achieve this I will be adopting a microservice architecture, this paper allows me the appropriate information in the cost I incur in making that decision. It can also provide reason if performance issues are encountered during the development of the final solution. This is a good counter argument to containerisation, and shows the considerations that need to be made for horizontal scalability.

## Project Plan



KEY:

* (NUMBER) = Estimates the amount of work required to complete the task.
* (N/NUMBER) = The amount of work done towards completing the task.
* PoC = Proof of Concept

I am currently working through the feasibility phase of the project lifecycle. You can see from the above diagram, based on the Enterprise Agile model (BJSS, 2008), that I have completed tasks within the feasibility stage of the project and will be moving onto the discovery phase after the January exam period.

I have chosen this delivery methodology as it allows me an achievable and measurable journey to completion, while allowing the flexibility to adapt to change as I move through the phases of delivery. The Discovery phase enables me to prove the technologies are compatible and work for their chosen tasks, and if they do not I am able to pivot quickly to replace them. This development style is known as a fail fast approach.

Once I have a proven technology stack I move on to the core of the implementation, developing features in the priority displayed in the project plan, however this priority can change at any time based on problems I may encounter or future knowledge gain. I believe this gives me the greatest chance of success, not only in completing the dissertation, but also in producing a viable product.

## References

Clive Norris, Michael McCahill; CCTV: Beyond Penal Modernism?, The British Journal of Criminology, Volume 46, Issue 1, 1 January 2006, Pages 97–118.

Retrieved from <https://doi.org/10.1093/bjc/azi047>

Scotland Yard (2010) CCTV in Homicide investigations.

Retrieved from: <https://goo.gl/oS5Tgn> (Accessed: 15th November 2017).

Press Association (2009) 'CCTV cameras help to solve one in every 1000 crimes', The Independent, 24 August 2009

Retrieved from: <https://goo.gl/cRnpaE> (Accessed: 15th November 2017)

Wilson, N. (2016) *BJSS Enterprise Agile*, 4th edition., Leeds, United Kingdom: BJSS Limited.

ISBN: 978-0-9565371-2-6

Ko, T., 2008, October. A survey on behavior analysis in video surveillance for homeland security applications. In *Applied Imagery Pattern Recognition Workshop, 2008. AIPR'08. 37th IEEE* (pp. 1-8). IEEE.

Goldstein, M. and Uchida, S., 2016. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PloS one*, *11*(4), p.e0152173.

Zanero, S. and Savaresi, S.M., 2004, March. Unsupervised learning techniques for an intrusion detection system. In *Proceedings of the 2004 ACM symposium on Applied computing* (pp. 412-419). ACM.

Zhao, S., Chandrashekar, M., Lee, Y. and Medhi, D., 2015, March. Real-time network anomaly detection system using machine learning. In *Design of Reliable Communication Networks (DRCN), 2015 11th International Conference on the*(pp. 267-270). IEEE.

Hasselbring, W. and Steinacker, G., 2017, April. Microservice Architectures for Scalability, Agility and Reliability in E-Commerce. In *Software Architecture Workshops (ICSAW), 2017 IEEE International Conference on* (pp. 243-246). IEEE.

Kratzke, N., 2017. About microservices, containers and their underestimated impact on network performance. *arXiv preprint arXiv:1710.04049*.