# Introduction

* *Explain the difference between anomaly behaviour and suspicious behaviour.*
* *Point out challenges that make the problem difficult to solve in general.*
* *Present the scope of the project, the problem we are trying to solve and discuss our contributions.*
* *Present some related work and their approaches when solving similar problems.*
* *Organisation section to explain the structure of the report.*

## How are Anomalous and Suspicious behaviour different?

Anomalous behaviour or anomalies are patterns in data that are different from a predefined notation of normal (normal model). Those patterns might be a result of malicious activity, system failure or just noise in the data. Therefore, the relevance of anomalies to real life is a key feature in anomaly detection.

Novelty detection is also closely related to anomaly detection [1, 2]. Unlike anomaly detection, novelty detection is concerned with finding new or unknown patterns that a system was not aware of during training. The main difference between the two is that novel patterns are typically later incorporated in the normal model.

While anomalous behaviour can be described as behaviour which differs from the expected, suspicious behaviour is not that simple to model. Suspicious behaviour is detected through subjective interpretation and present a challenge even for human observers. Human observers rely on their experience sometimes described as ‘sixth sense’ or ‘gut feeling’ to correctly detect suspicious behaviour [3]. Context is another very important part of suspicious behaviour detection. Behaviour that is considered normal can become suspicious if the context changes. Because of that the normal behaviour model needs to be updated over time as the context changes. This makes labelling data for training nearly impossible and it is also impossible to generate a data set capturing all possible human behaviours.

## Challenges

Since anomalies are considered deviations from the normal model, detecting them should be straight forward, define a normal region and all observations outside that region are abnormal. However, several issues arise when trying to implement that approach. And it gets even more challenging when the purpose is detecting suspicious behaviour.

* It is very difficult to define a normal region that correctly represents every possible normal behaviour. Also, the separation between normal and abnormal is not always clearly defined.
* When the anomalies are caused by malicious actions, those actions are usually made to appear normal.
* The normal behaviour changes, and the current normal model might not be sufficient in the future.
* It is hard to find labelled data for training models used in anomaly detection systems
* Detecting suspicious behaviour is very subjective and depends on how actions are interpreted.
* Given behaviour might be considered suspicious in one context but normal in another and because the context changes the system needs to account for that.

Because of those challenges it is not easy to create a general solution for detecting suspicious behaviour. Instead most solutions are focused on very specific formulation of the problem.

## Problem Statement

## Related Work

## Organisation

**REFS:**

1. MARKOU, M. AND SINGH, S. 2003a. Novelty detection: A review-part 1: Statistical approaches. *Sig.*

*Proc. 83*, 12, 2481–2497.

1. MARKOU, M. AND SINGH, S. 2003b. Novelty detection: A review-part 2: Neural network based approaches.

*Sig. Proc. 83*, 12, 2499–2521.

1. [Crime and CCTV in Australia: Understanding the Relationship](http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1071&context=hss_pubs)