# Requirements Analysis

The requirements for this project are listed below. The nature of the project required the development of theoretical knowledge before implementation began. Consequently, the requirements subtly evolved as understanding matured. The original requirements are given in Appendix \ref{app:proposal} for comparison. The final requirements have been grouped into two categories. The first, labelled $A$, are the core requirements deemed essential to the project’s success. The second, labelled $B$, are considered extensions, aiming to improve understanding or further the investigation into HE and surveillance.

## Core

* \textit{implement a client-server application allowing videos to be homomorphically encrypted and transmitted in both directions.}

This component provides the foundation for implementing and integrating all other components. It is essential for emulating the MLaaS software stack. While conceptually simple, incorporating HE data adds challenges that formed a significant portion of the investigation into HE applicability.

* \textit{implement background subtraction models that can extract moving objects from homomorphically encrypted videos.}

This requires designing and implementing the five moving object detection algorithms detailed in §\ref{sec:movingObjectDetection} within the HE domain.

* \textit{evaluate the accuracy of HE inference to investigate its applicability to real systems.}

This involves analysing different metrics to understand the efficacy of moving object detection on HE data. Comparisons can be made between inference methods and between plain and encrypted data.

## Extensions

* \textit{implement a bespoke HE scheme and integrate it into the core application, providing the same functionality as the established scheme already used.}

While this implementation will likely have worse performance than existing implementations, it will offer helpful insight into the inner workings of HE. Also, it may provide opportunities for specialisation optimisations.

* \textit{analyse the security of the encryption schemes used in the project.}

This will be useful in ensuring HE can overcome both security and privacy concerns of existing surveillance solutions and doesn’t accidentally introduce insecurities that could allow adversaries to extract information.

* \textit{implement an object recognition algorithm acting on HE data using neural networks.}

Implementations like Cryptonets [DOWLIN] have demonstrated the application of neural networks to HE. This would allow further services offered by surveillance companies to be emulated and reveal a greater insight into the limitations of HE.

# Methodology

The different stages of the project were best suited to different development methodologies. For the core components, a waterfall development methodology was adopted [WATERFALL]. The requirements were detailed and unambiguous, so the project lent itself to a structured methodology, not requiring the flexibility of an iterative approach. The stages of the model are detailed below.

DIAGRAM

The results of the \textit{requirements analysis} stage have been detailed in §\ref{sec:requirements}. This stage is where most of the research was performed so that the project’s design would be better informed.

The \textit{design} phase involves expanding on the requirements into a physical project; this includes, for example, creating the class diagram shown in Figure \ref{fig:class}.

The \textit{implementation} and \textit{testing} stages were intertwined where possible in order to promote a test-driven approach to development. This was made easier by the object-oriented methodology and unit testing practices adopted.

The \textit{evaluation} stage replaces the \textit{maintenance} stage of the traditional Waterfall model. This stage involves running experiments to evaluate the project.

When working on extensions, an iterative model was more appropriate. The main reason for this was that less time had been dedicated to researching these components, so implementation was riskier. Consequently, a rapid cyclical development model requiring components to be decomposed would allow any problems to be discovered sooner, limiting impacts. Therefore, the Agile model, depicted in Figure \ref{fig:agile} was selected. Moreover, regular supervisor meetings allowed Agile’s sprint system to be utilised so that a project prototype could be presented in each meeting to ensure thorough progression tracking.

A Gantt chart of the project’s timeline is shown in Figure \ref{fig:gantt}.

## Testing

Unlike traditional software engineering, machine learning does not provide precise criteria against which correctness can be verified. The models used for background subtraction are probabilistic, so the outputs cannot be precisely predicted. Consequently, a variety of testing methodologies were required.

### Unit Tests

Designed for testing atomic units of source code, unit testing utilises the independent nature of components written following object-oriented principles to elements in isolation. It does this by providing known expected, boundary, and erroneous data and ensuring function results match the expected. Unit tests can be automated, making them easy to run repeatedly as changes to the source code are made, ensuring errors aren’t introduced.

Unit tests were particularly useful when completing the first extension for verifying the correctness of the encoding, encryption, and decryption functions and the HE Boolean circuits.

### Integration Tests

Integration tests increase the scope of functionality covered by each test. Their goal is to ensure separate modules interact correctly. Once unit testing has been completed, these tests aggregate verified modules and provide similar data to ensure the output is correct.

Integration testing was useful in verifying that the software stack functioned correctly. For example, ensuring the client and server communicated correctly. While some integration testing can be automated, more complex engineering work was prioritised over creating a more comprehensive testing suite, so manual integration testing was the primary technique used.

### Manual Verification

Manual verification was used to overcome the challenges of testing the background subtraction models. Since the project involves video data, human inspection provides a good intuition of if a background has been correctly removed. If a more detailed analysis is required, pixel values can be compared to check for expected results or verify consistency across multiple tests.