# Original Project Aims

An increasing number of smart-home devices are being developed to provide surveillance solutions for customers. While these devices have proved successful in improving the security of people’s homes, they introduce new unprecedented privacy risks. This project aimed to investigate homomorphic encryption as a solution to privacy concerns without detracting from the security benefits. To this end, it intended to use existing homomorphic encryption libraries to implement privacy-preserving unsupervised machine learning algorithms that can extract moving objects from surveillance footage. As extensions, the project would implement a bespoke encryption algorithm, investigate further inference algorithms, and validate the security of such algorithms.

# Work Completed

All core requirements of this project were fulfilled. A client-server application was designed and implemented to emulate the machine learning as a service business model, and an investigation into optimising data transmission was performed. Moreover, an investigation and evaluation of moving-object detection inference algorithms in the homomorphic encryption domain was completed, highlighting the limitations of privacy-preserving machine learning. Furthermore, as an extension, a bespoke homomorphic encryption scheme was implemented to further understanding and investigate potential optimisations through specialisation.

# Special Difficulties

The majority of the project was completed with relatively few unexpected disruptions. However, contracting COVID-19 in December resulted in the project falling several weeks behind schedule. Consequently, significant extra work had to be done to get back on track and ensure the project was completed before the deadline.