The project encountered two recurring limitations of HE that would benefit from further investigation. Firstly, the memory requirements resulting from ciphertext size resulted in a significant bottleneck during the networking stage of the application. Consequently, research into reducing this cost would make HE more applicable to MLaaS applications. Secondly, the variety of operations available in the HE domain must be expanded if more advanced moving object detection algorithms are to be implemented. This would enable GMMs to produce much more accurate inference results.

Regarding security, other methods could be investigated to preserve privacy. For example, techniques exist for storing private keys in hardware to prevent visibility to users [LORCH]. This would reduce the risk of malicious actors performing unauthorised access. Moreover, \textit{functional cryptography} is an asymmetric cryptographic protocol that allows properties of ciphertexts to be extracted [BONEH]. An investigation into this could produce a potential alternative to HE, and compare the advantages and disadvantages of the two approaches.

More specifically for surveillance applications, further research considering the hardware aspect of the problem would be beneficial for obtaining a more precise measure of practicality. Some potential topics include: evaluating and reducing energy usage to accommodate battery-powered devices, improving computational complexity for execution on lower-powered processors, or developing specialised accelerators to design devices specific to HE computations.