Overall, the project was a success. All core success criteria and one of the extensions were met, and the remaining extensions were thoroughly considered. In its final state, the project contains an investigation into the applicability of HE in ensuring user privacy is preserved when using modern MLaaS surveillance technology. For this, a client-server system allowing data to be homomorphically encrypted using the CKKS scheme and transferred across a network was implemented. Moreover, several background subtraction algorithms were implemented, and more were investigated to attempt to find the limit of HE pertinency. Also, the results of these algorithms were evaluated against traditional algorithms operating on plain data, revealing similar accuracy but significantly increased running time due to increased computational complexity. Similarly, network activity was compared between plain and encrypted data, highlighting the cost of increased ciphertext size through increased data manipulation running times and transmission times between client and server. Furthermore, a bespoke implementation of the CKKS scheme – called MeKKS – was created to increase understanding and highlight opportunities for application-specific optimisations.