The Machine Learning as a Service (MLaaS) framework describes a business model in which customers send data to a server for machine learning inference to be performed; then, results are returned. Specifically for this project, security companies analyse video surveillance data remotely. Suppose that a subscriber to one of these services, \textit{Alice}, uses a camera to record activity at her front door. This exposes two critical threats: (i) an adversary, Eve, may eavesdrop on the transmitted data while it is in flight, and (ii) a malicious actor, Mallory, may exfiltrate the data while the server stores it, either by hacking the company or by having privileged access, revealing a range of privacy risks including identity theft, monitoring intimate behaviours of household members, identifying household objects, and more. Figure \ref{fig:threatModel} illustrates this succinctly. The first threat can be mitigated relatively easily using cryptographic protocols such as TLS [TLS]. However, the second threat is much more difficult to defend against, particularly because data must usually be decrypted before inference [BAE].

Fortunately, HE offers a potential solution to both risks. Firstly, HE is a secure cryptographic encryption scheme, so using it to encrypt data during transmission is sufficient to thwart eavesdropping adversaries. Secondly, HE allows computation to be performed on the data without decryption, so it can prevent the exploitation of plain data.