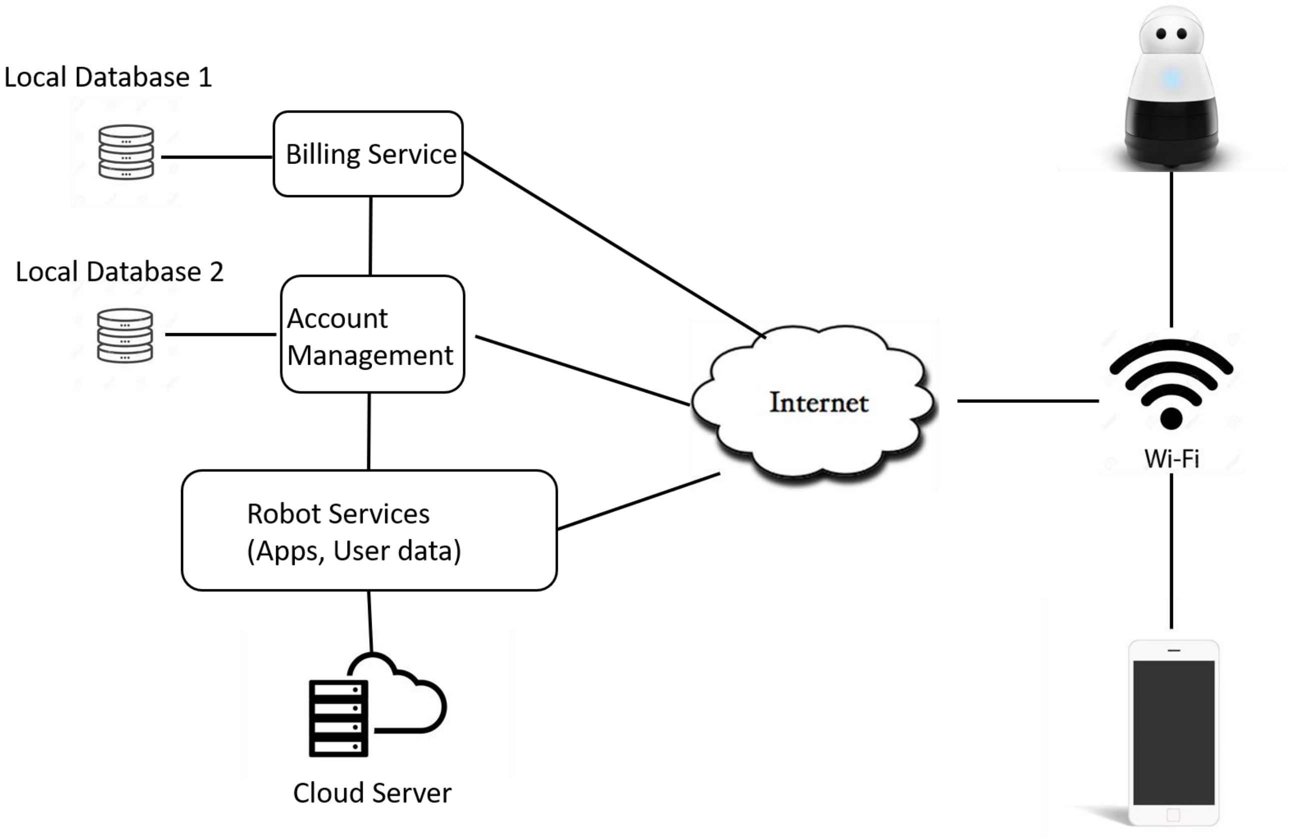
IoT Assignment 01

Problem Description

Consider a hypothetical mobile IoT robot that is having the following capabilities. The robot is equipped with a HD camera to capture images and video which is a useful feature for providing home security. The captured data will be stored in a third-party cloud server. The captured data is also accessible by the user/owner of the robot via his or her smart phone which can communicate with the robot via home wi-fi connection. The user also has the capability in accessing the captured data from the cloud platform when necessary. The robot is also equipped with microphones so that it can listen to the voice commands from the user/owner as well as pick-up other noises. The captured voice will also be stored in the cloud server in the form of text transcripts. It also has a speaker to interact with the people in the home environment. Speaker can be used to play music, interact with kids at home. The system architecture of the IoT robot is illustrated in the following diagram.



Note that Local Database 1 (stores billing information) and Local Database 2 (stores account information of robot owner) are local storages managed by the manufacturer of the robot. Since, the manufacturer has limited storage capability, the manufacturer uses a third-party cloud platform to store robot apps as well as user data (pictures, video, text transcripts). Robot applications are not free. So, the users need to pay when they configure the robot with new apps.

Task

Your task is to carry out a privacy impact assessment (PIA) on this hypothetical IoT Robot. You are allowed to work in groups. A group can have a maximum of **4 students.**

Deliverables

- Report (3-5 pages).

- The report should clearly describe how you carry out the PIA. You should explain how the IoT system is broken down to different life-cycle phases, information generated in each of the phase, your categorization of sensitivity of the generated information as well as how do you ensure the safety of critical PIIs via appropriate security mechanisms. Any assumptions you make should also be documented in the report.

deadline: 03.02.2020, 23:59