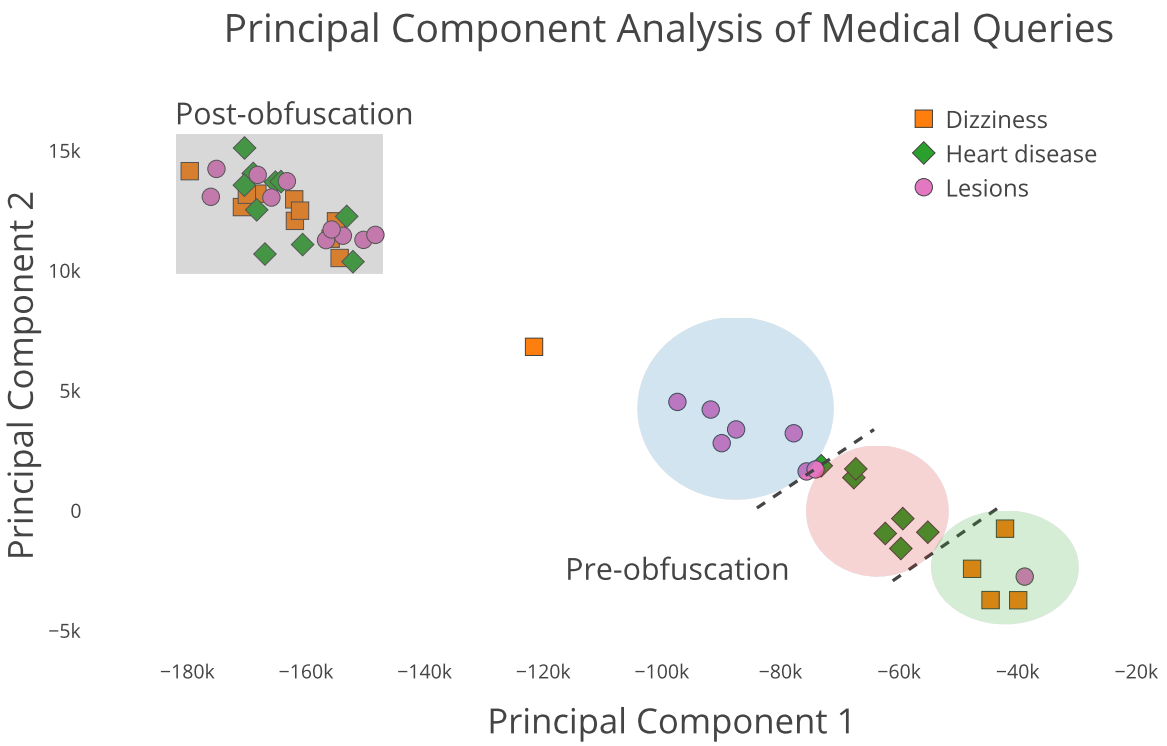

Figure 1: Principal Component Analysis of pre- and post-obfuscation on medical database queries. Each point represents memory requests performed over time when querying admitting diagnosis information for different patients. Pre-obfuscation, there is a clear separation between the input (disease) to the query, as shown by the dashed lines. Post-obfuscation, the memory request activity over time is too similar between the different queries for there to be any such separation.

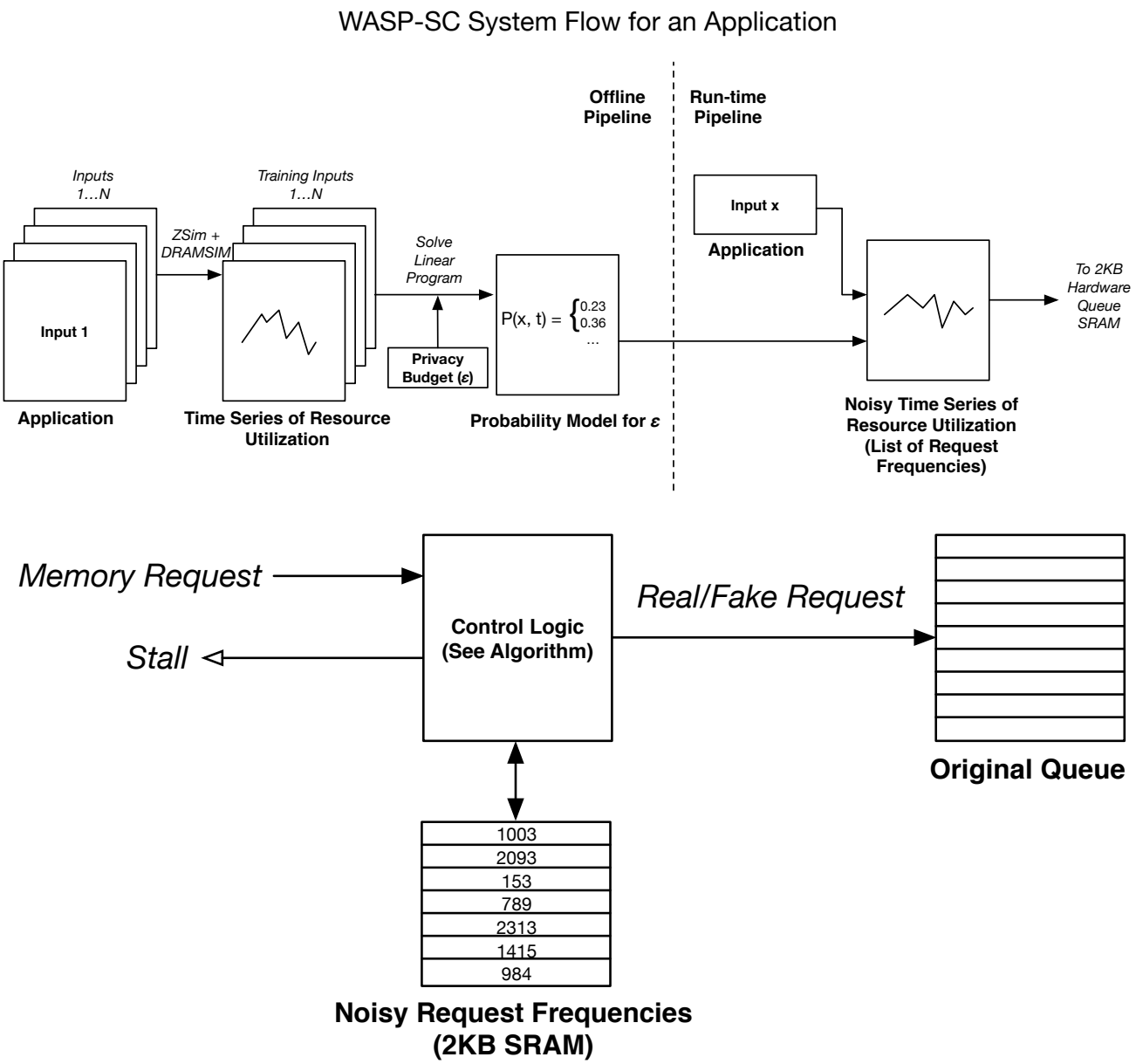

Figure 2: Diagram of the WASP-SC system flow. First, we create a model of each input's time-series of execution for ease of processing. Next, we determine the probability of selecting the private median value by solving the linear program. Finally, we generate a noisy time-series during run-time by sampling from the probability model, so the traces are not deterministic. This noisy time-series is then loaded into a small SRAM connected to the control logic that ensures real/fake requests are sent according to the time-series.

Algorithm 1 WASP-SC Queue Control Logic

```
if Interval Changed then
    Load frequency from SRAM into register
end if

counter−− = 1
if counter = 0 then
    counter = IntervalSize/Frequency
    if Real Request Pending then
        Enqueue real request
    else
        Enqueue fake request
    end if
end if

if Real Request Received then
    Pend Real Request until counter = 0
end if

stall = RealRequestPending
```