17-645 Final, Fall 2019

Christian Kaestner and Eunsuk Kang

Name: _____

Andrew ID: _____

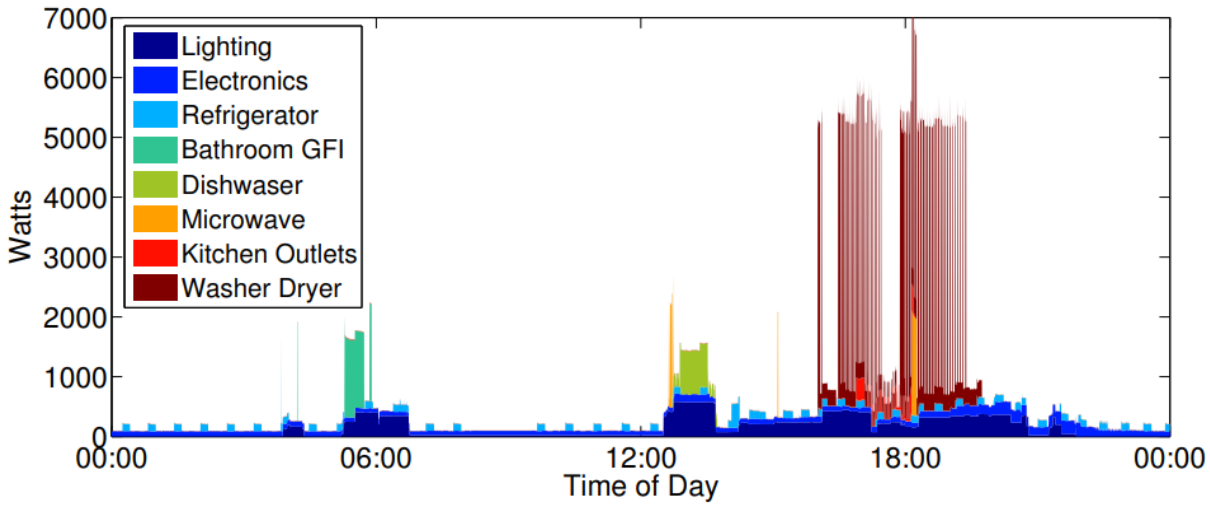
Instructions:

- Not including this cover sheet, your exam should have **13** pages. Make sure you're not missing any pages. **Write your Andrew ID on every page.**
- All questions in this midterm refer to the scenario on the first page.
- The exam has a maximum score of **100** points. The point value of each problem is indicated. We allocated approximately one point per minute.
- Clearly indicate and write your answers in the space provided for each problem. We cannot give you points for answers we cannot find or read. Write concise, careful answers; short and specific is much better than long, vague, or rambling.
- We give an amount of space commensurate with what we expect you to need for each question. If you need more space, use this cover sheet, the scenario page, or other pages and make it obvious in your first answer where to find the rest of the answer. **Do NOT write answers on the back side of pages.**
- You may not use calculators, cell phones, laptops, or any other electronic or wireless devices, nor consult with your friends or colleagues. **You may consult handwritten or printed notes and books**.
- Good luck!

Scenario

Consider the following fictional scenario for the remainder of the exam: After graduation, you have just been hired to work with the software team of Duquesne Light Company, Pittsburgh's local utility company that provides most of the region with electricity. Duquesne Light is a large company with 1200 employees and a long tradition going back to 1912, but it was always a utilities company first, never focused on innovative software solutions. It largely buys standard software for operating its power grid, for collecting meter readings, and for billing customers. Its customer-facing web page, which allows customers to sign up, report outages, track their energy consumption and pay their bills is run by a small team of three web developers and one web designer that largely just interface with purchased industry-standard backend systems.

Since industry conferences talk too much about smart homes, smart grids, smart meters, and about using AI for sustainability, Duquesne's CTO has decided to try to invest in AI. The CTO currently has significant say in the company and a fairly generous budget. She reached out to CMU's energy and AI researchers to discuss collaborations and ideas and has sponsored a research project on detecting at fine granularity which electric consumers are responsible for the energy consumption from measurements with a single smart reader for the entire household -- known as **energy disaggregation** (studies have shown that just presenting such a breakdown to users, so that a homeowner can see precisely how much energy is being used by which appliance, can automatically lead to energy-saving behavior). The idea is that smart meters provide very fine resolution measurements of energy consumption in a home and most electric consumers have a certain pattern of how much energy they draw, for how long, and how stable the consumption is (e.g., a washing machine has a fairly characteristic profile of energy spikes as visible in the graphic below, runs for a characteristic duration and at a characteristic time). Two machine-learning graduate students have built a novel experimental model for this energy disaggregation with very promising results, published at a top level machine-learning conference. Models have been built and evaluated based on labeled data collected from 100 Duquesne customers in the Pittsburgh area observed over 3 month, where additional power meters for individual devices provided the label information about which devices actually consumed energy in those houses.



The research project has been going well and the CTO wants to build a team to deploy the solution, showing customers on the Duquesne web page, both through regular reports and as a real-time tracker, how much energy they are consuming and for what. With a generous salary offer, Duquesne manages to hire one of the PhD students who worked on the original project and another recent graduate with a data science specialization. In addition, two web developers who were part of Duquesne's existing IT team for the web frontend have been assigned to help this project in about 40% of their time (continuing to maintain the existing web system in the other 60% of their time).

The team has worked hard to produce and deploy a prototype, which initially worked quite well, but soon the problem started. While the resulting reports on the web site worked quite well for most customers, some customers got very misleading results and were quite unhappy with the service, causing some bad media coverage. The system could not handle the demand and became quite unstable, now costing quite a bit to run, relying heavily on cloud resources. Every time the team has tried to release an update, it was a massive struggle with delays and outages. Due to mounting frustrations, the web developers and data scientists have largely stopped talking to each other beyond the absolute essential.

You have been brought in as consultant and engineer for the next 6 month to try to help the team to build a system that they can maintain and evolve more easily and that can be offered with lower operating costs and higher quality.

Question: Team/Process [11 points]

Your first goal as a consultant is to resolve the current team issues and build an effective team.

(a) [3 points] The web developers and data scientists barely talk to each other due to mounting frustrations. What do you think are the frustrations? Name two conflicts between the data scientists and web developers what may plausibly occur in this scenario.

(b) [4 points] Suggest one plausible intervention (e.g., introducing a tool, changing the process, changes to the implementation) to improve teamwork and briefly justify why you think this intervention will improve teamwork and will address at least one of the conflicts from the previous question.

(c) [4 points] The CTO has tasked you to bring in two experts to resolve the scalability and availability issues that the team is facing. What kind(s) of expertise (e.g., deep knowledge about a technique or a tool) do you think the team needs and why? Make sure your answer is grounded in the scenario.

Question: Data Provenance [8 points]

[5 pts] When customers complain about incorrect results of the energy disaggregation feature (e.g., the heater's energy consumption is explained as "lighting"), you have a hard time debugging your system because you cannot reproduce the problem or even identify which component caused the problem. To improve the situation, what additional data would you track or version and why?

[3 pts] Assuming a customer complains about a prediction of your system, briefly describe how you would use the data (from the previous answer) to reproduce the prediction.

Question: Big Data [8 points]

Measurement data is received from the users' smart meters regularly and stored in an append-only database in its raw format. To create usage reports, you need to apply the energy-disaggregation model to the data of the report's period. In addition, customers can optionally indicate in an interface which appliances they actually ran, providing labels for retraining. You consider how you perform the prediction or training:

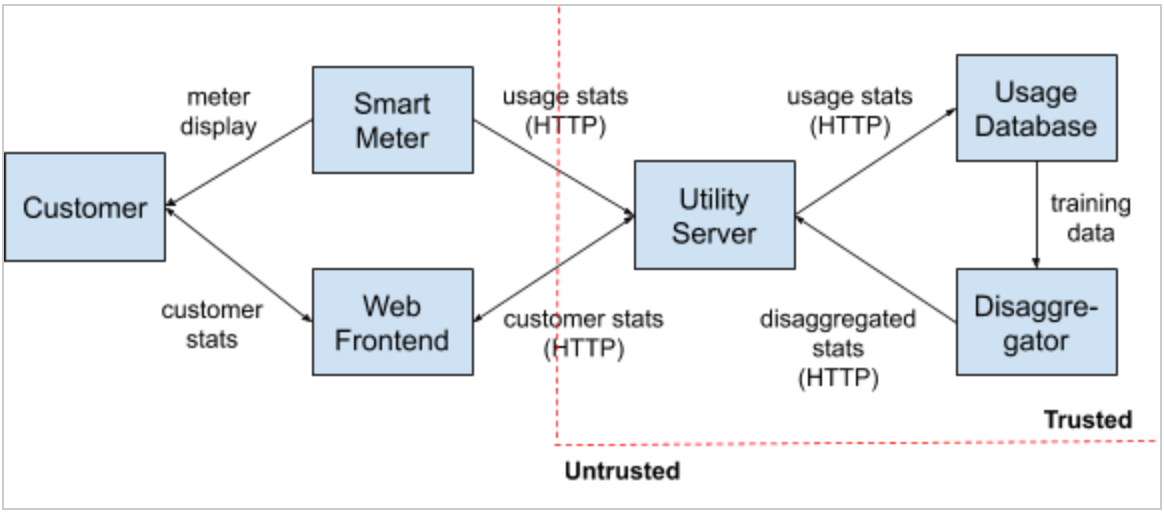
- Option 1: On demand processing (e.g., creating the report when the user requests the web page/updating the model whenever a prediction is needed)
- Option 2: Batch processing (e.g., caching reports overnight/updating the model in regular intervals)
- Option 3: Stream processing (e.g., continuously updating reports/models)
- Option 4: Combined batch and stream processing using the lambda architecture

[4 pts] Which option would you choose for creating reports? Briefly justify why you prefer this option over the alternatives.

[4 pts] Which option would you choose for retraining the model with new labeled data? Briefly justify why you prefer this option over the alternatives.

Question: Security [17 points]

As you continue to work on the energy disaggregation features, you are concerned about malicious or mischievous customers tampering with the smart meter or the communication from the meter to your server. To identify potential security threats and mitigations, you've constructed the following architecture diagram:



(a) [3 pts] Give an example of an **integrity** requirement that the system must ensure.

(b) [7 pts] Regarding **spoofing attacks**, state which connection(s) may be vulnerable to the attack, how the attack can lead to the violation of the integrity requirement that you stated above, and a corresponding mitigation strategy.

Vulnerable connection:

Attack scenario:

Mitigation:

(c) [7 pts] Regarding **poisoning attacks**, state which connection(s) may be vulnerable to the attack, how the attack can lead to the violation of the integrity requirement that you stated above, and a corresponding mitigation strategy.

Vulnerable connection:

Attack scenario:

Mitigation:

Question: Model Quality and Telemetry [20 points]

Based on the energy-disaggregation model's outputs and other inputs (e.g., temperature, user inputs, set target temperature) you plan to develop a new "unusual consumption" model that identifies warning signs that an owner's heating or cooling unit might malfunction because it consumes an unusually high amount of energy. If this case is detected, a system built with the model sends a message to the customer, encouraging the customer to reach out to a service company to inspect their heating/cooling unit.

You plan to design telemetry to be able to measure the model quality of the "unusual consumption" model in production. Specifically, you want to see whether you can reliably identify malfunctioning heating and cooling units without too many false warnings. In the context of the scenario, suggest a realistic way to assess the quality of your "unusual consumption" model in production.

(a) [4p] Describe what data you would gather in production and how

(b) [4p] Describe how you would determine recall of your "unusual consumption" model with that data (be precise about the computation):

(c) [4p] Describe how you would determine precision of your "unusual consumption" model with that data (be precise about the computation):

(d) [4p] Do you have any concerns regarding cost or privacy with this approach and, if yes, how would you address it? Briefly explain your answer.

(e) [4p] The data scientists keep improving the energy disaggregation model and regularly release new versions. You are worried about the impacts this may have on the "unusual consumption" feature. The data scientists argue that they are careful and only release model updates of the energy-disaggregation model with higher accuracy than the previous version. They further argue that since accuracy improves for energy disaggregation so should also improve the accuracy for the dependent "unusual consumption" model, as it now receives better inputs. Do you agree with their argument? Explain why or why not.

Question: Fairness and Ethics [20 points]

When an unexpected power shortage occurs (e.g., unusual winds, wildfire, snow storm), your company may not have enough electricity for all customers, and must temporarily cut supply to some subset of the households. A company-internal initiative is exploring options of how to make decisions in such emergency cases and asks the data scientists on your team to explore whether they can predict which customers are less likely to pay their bill on time to select them for the needed power cut. To predict whether a customer is likely to pay their bill on time, your team experiments with learning a binary classifier that uses various features, including age, occupation, household income, past payment behavior (i.e., number of late payments), and neighborhood.

Concerned about the project, you push the data scientists to consider fairness, especially with regard to customers from diverse backgrounds. In particular, you think that the *neighborhood* attribute is sensitive. There are two major neighborhoods that your company serves: Richville and Springfield. You have trained and tested your classifier on historical data (with a sample size of 500 households in each neighborhood) to produce the following statistics:

Results for Richville		Results for Springfield	
TPs: 462	FPs: 21	TPs: 413	FPs: 21
FNs: 7	TNs: 10	FNs: 21	TNs: 45

TPs: true positives, FPs: false positives, FNs: false negatives, TNs: true negatives

The binary classifier returns 1 (i.e., positive) for an input sample if the corresponding household is expected to pay the bill on time.

(a) [16 pts] Given the above statistics, state whether the model satisfies the following definitions of fairness: (i) group fairness, (ii) equalized odds, and (iii) predictive parity. Include the formulas and intermediate steps used to derive your conclusion.

(i) Group fairness:

(ii) Equalized odds:

(iii) Predictive parity:

(b) [4 pts] Which of the three definitions of fairness in (a) is most appropriate for this task? Briefly justify your answer.

Question: Startups & Usability [16 points]

You start thinking about what to do after your consulting contract with Duquesne expires. You have talked to a few friends and think about starting a company to develop a revolutionary smart home device designed to help customers use electricity more efficiently and reduce utility costs. In particular, your device will be (i) connected to other Internet-connected IoT devices in a household (e.g., Nest thermostat or a smart washer), (ii) use advanced ML to learn the appliance usage pattern, and (iii) automatically turn on/off those other devices when they do not adhere to the expected usage pattern (e.g., turn off lights and heating during the day when everyone is at work).

You are confident that this product will be a huge hit and your company will reach a $1 billion valuation in no time.

(a) [4 pts] Describe one ML-related risk that may pose a serious obstacle to the success of your startup (briefly explain why it is a risk).

(b) [4 pts] Describe a minimum viable product (MVP) that you can use to test whether the risk you identified in (a) can be addressed.

You are also thinking about developing a mobile app that users would use to monitor and control the IoT devices at home. Before you start further exploration, you want to think about what types of user interactions would be most suitable for your product.

(c) [4 pts] Give an example of a situation where the system should prompt the user for a decision instead of fully automating an IoT device.

(d) [4 pts] Discuss one strategy that could be used to reduce the possibility of a customer being surprised by automated decisions made by the system.