The idea is that we concern about the security and privacy about the voice assistant (like Apple Siri, Amazon Alexa…).
The privacy part is: as these kinds of voice assistant always detecting our voice to find the word like "Hey Siri" to wake themselves up. And they need to upload our voice to the cloud to manipulate our voice and turn back the result. Then, here is the privacy concern that they will definitely upload more words than we supposed it to upload. And as they are detecting our voice all the time, we want to know whether it uploads our voice to the cloud in our daily life when we are not saying "Hey Siri". We are supposed to measure this problem in the transportation part (i.e. to see the package that a device sends out to the cloud).

The security part is: people can wake up the Alexa by saying some words, which means even someone else can wake it up and control other device in our house (e.g. a stranger can wake up the Alexa to open the door from the outside). This is ridiculous. However, now, Google, Apple have announced that they use Neural Network to learn the person's voice and make the device can only be waked up by that person. However, here is a security concern that we want to learn: If there are another choice to wake it up, like another person says "Hi Sorry"(Lol) and suddenly wakes the Siri up. Or in another way, we can detect if we can activate the Siri with accent (like Chinese accent or Indian accent or any other accent) to see how strong the deviation the device can bear.

Here we want to choose either privacy or security to be our course project. The following are some brief survey of them.

Seems like a similar concern:
https://www.zdnet.com/article/google-home-mini-flaw-left-smart-speaker-recording-everything/
https://www.theverge.com/2017/10/5/16430822/mattel-aristotle-ai-child-monitor-canceled
https://digital-library.theiet.org/content/journals/10.1049/et.2017.1005
https://www.tandfonline.com/doi/full/10.1080/02763869.2018.1404391 (See the security and privacy part)
Apples announcement about how Siri works:
https://www.imore.com/how-hey-siri-works

But interestingly, as the concern about the security and privacy rises really early (at about 2017). I have not found a paper designed to measure the privacy in our way (i.e. detecting the upload package).

The question is:
We need to detect how the device encrypt its package?
https://www.apple.com/privacy/approach-to-privacy/
https://www.cnet.com/news/apple-will-keep-conversations-with-siri-and-homepod-a-secret/
Find a way to make sure how many redundancy information will Siri send before it wakes up and after all the message has been sent?
https://arxiv.org/pdf/1708.05044.pdf
https://arxiv.org/pdf/1705.06805.pdf
Will the cloud store our voice message or not?

How can we define whether the device spy our daily life voice?

For the security thing, we need to learn the how these devices detect the voice and translate them from speech to text: https://skywell.software/blog/how-does-siri-work-technology-and-algorithm/
And how will the accent or something else influence the algorithm?
https://www.theguardian.com/technology/2016/feb/10/texas-regional-accent-siri-apple-voice-recognition-technology
https://www.cbc.ca/radio/spark/292-what-you-say-will-be-searched-why-recognition-systems-don-t-recognize-accents-and-more-1.3211777/here-s-why-your-phone-can-t-understand-your-accent-1.3222569
http://www.bokorlang.com/journal/61dictating.htm
https://www.researchgate.net/profile/Rishabh_Upadhyay4/publication/319042404_Accent_Classification_Using_Deep_Belief_Network/links/598c8725a6fdcc58acba45a0/Accent-Classification-Using-Deep-Belief-Network.pdf
Then things going on to either test the frequency of the voice or something else that can help us solve this problem.