Privacy-aware Medical Voice Applications

Faysal Hossain Shezan
fs5ve@virginia.edu

Yuan Tian
yt2e@virginia.edu



Motivation



Los Angeles Times

Column: Alexa may be key to Amazon's looming domination of the healthcare market

Amazon.com + Add to myFT

Amazon expands healthcare services with Alexa deals

Source:
https://developer.amazon.com/blogs/alexa/post/ff33dbc7-6cf5-4db8-b203-99144a251a21/introducing-new-alexa-healthcare-skills
https://www.ft.com/content/9c3fb428-56e7-11e9-a3db-1fe89bedc16e
https://www.latimes.com/business/lazarus/la-fi-lazarus-amazon-healthcare-privacy-20190716-story.html

Motivation



MAD LONDON

AROUND THE NET

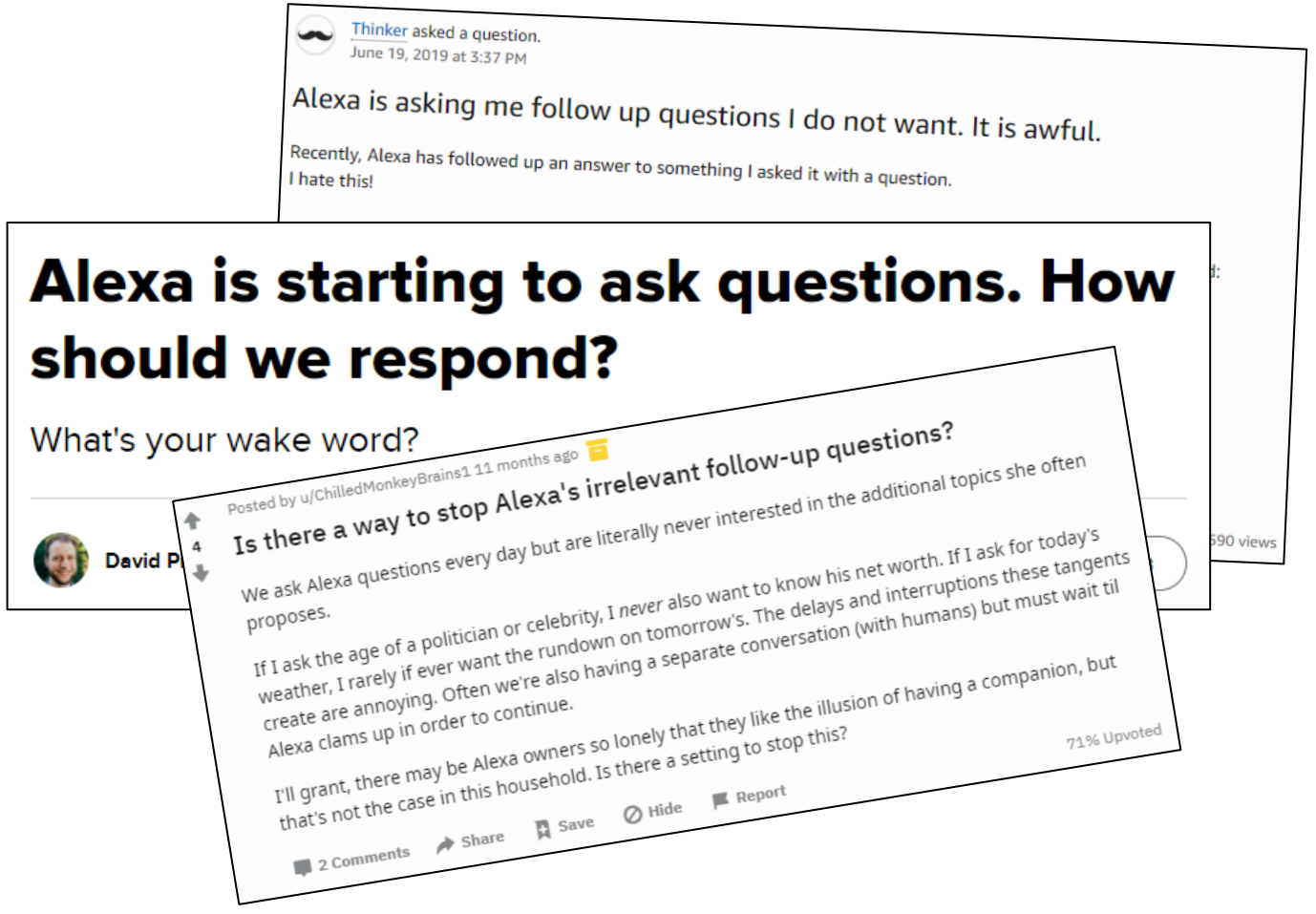
NHS Signs Deal With Amazon For Medical Information

NetImperative, Thursday, July 11, 2019 9:24 AM

Source: https://www.mediapost.com/publications/article/338031/nhs-signs-deal-with-amazon-for-medical-information.html

Motivation





Source:
https://www.amazonforum.com/s/question/0D54P00006zSsCz/alexa-is-asking-me-follow-up-questions-i-do-not-want-it-is-awful
https://www.reddit.com/r/alexa/comments/gqsjsr/is_there_a_way_to_stop_alexas_irrelevant_followup/
https://www.cnet.com/home/smart-home/alexa-is-starting-to-ask-questions-how-should-we-respond/

Contribution

1. New Tool
   - unfold the behavior of collecting unnecessary personal information

Contribution

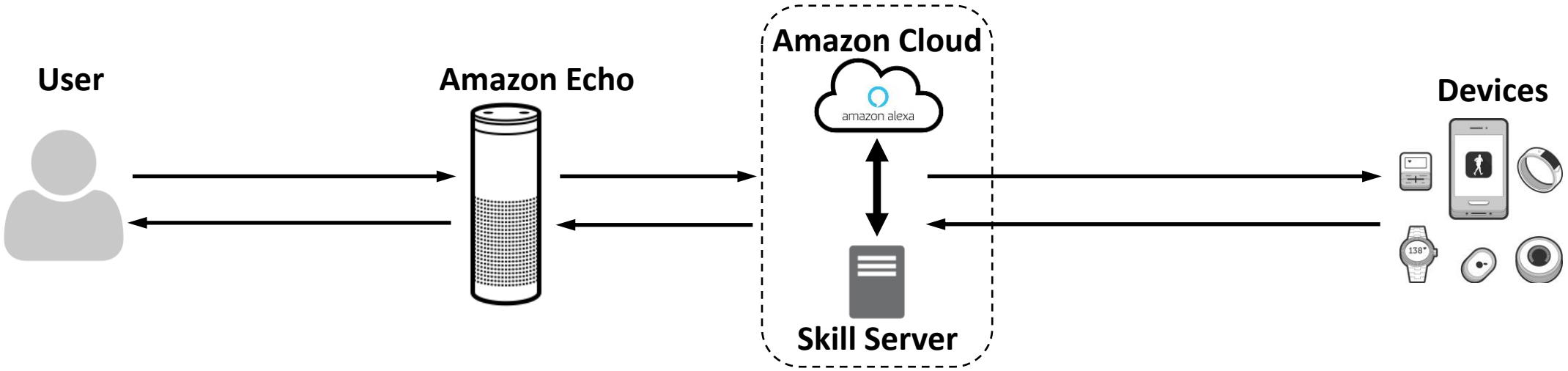
1. New Tool
   - unfold the behavior of collecting unnecessary personal information
2. New Measurement
   - explore the risky surface of the current state

Contribution

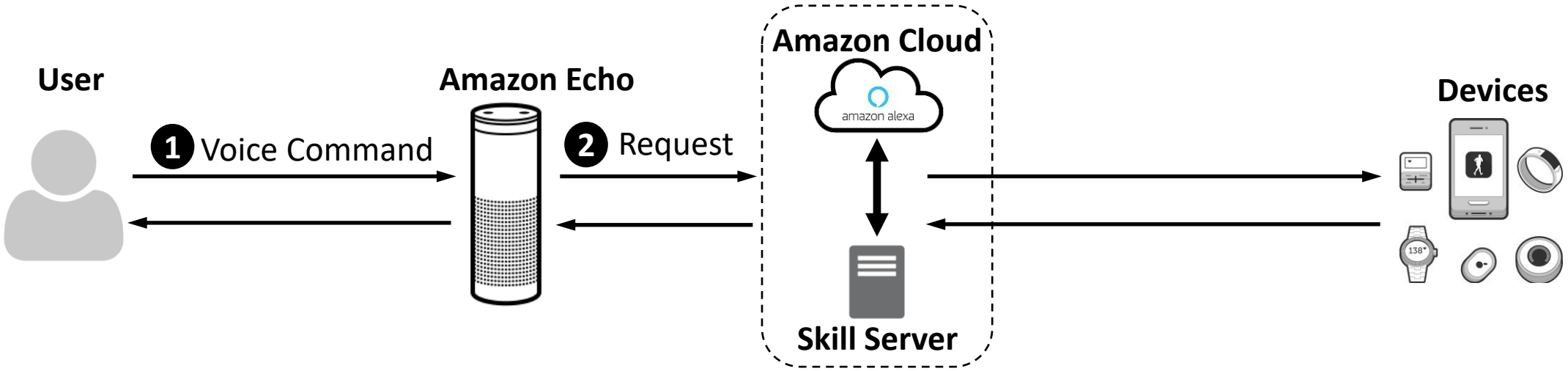
1. New Tool
   - unfold the behavior of collecting unnecessary personal information
2. New Measurement
   - explore the risky surface of the current state
3. Suggestion for Future Skills
   - ensure privacy of user’s private data

Background

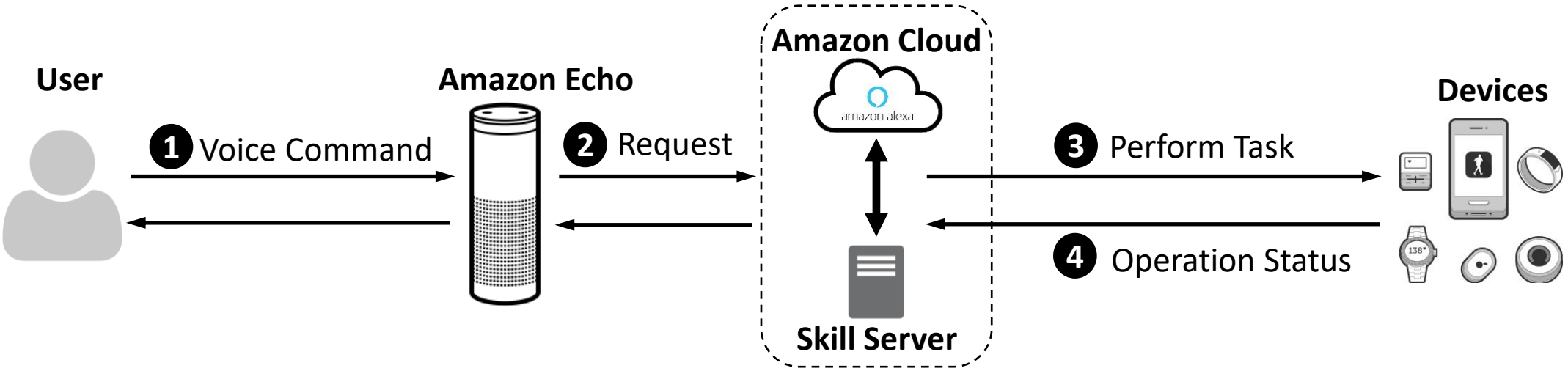
Voice Personal Assistant



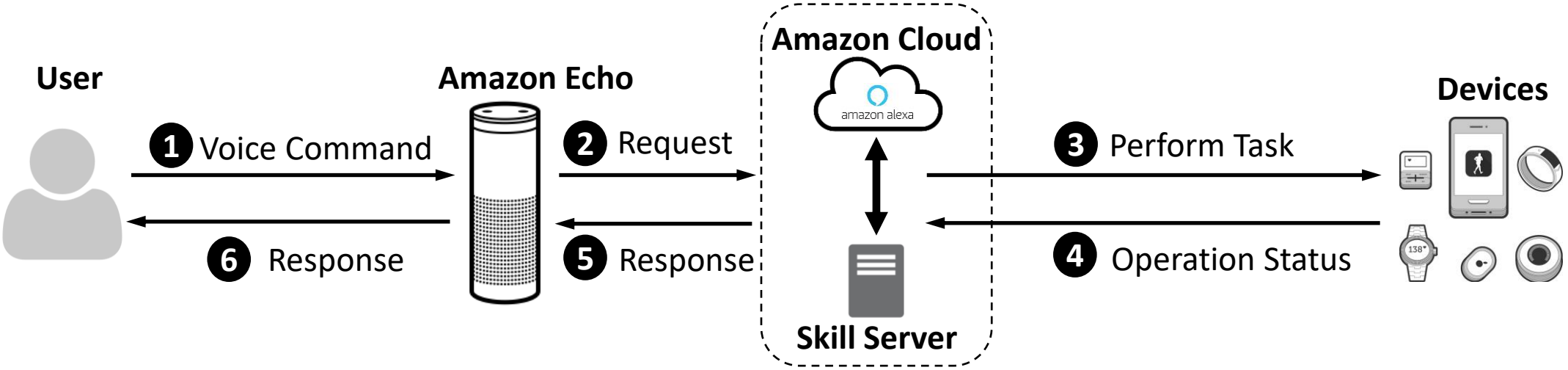
Voice Personal Assistant



Voice Personal Assistant



Voice Personal Assistant



Prior Work

- Privacy in VPA: Guo (2020), Tabassum (2019), Lau (2018)

Prior Work

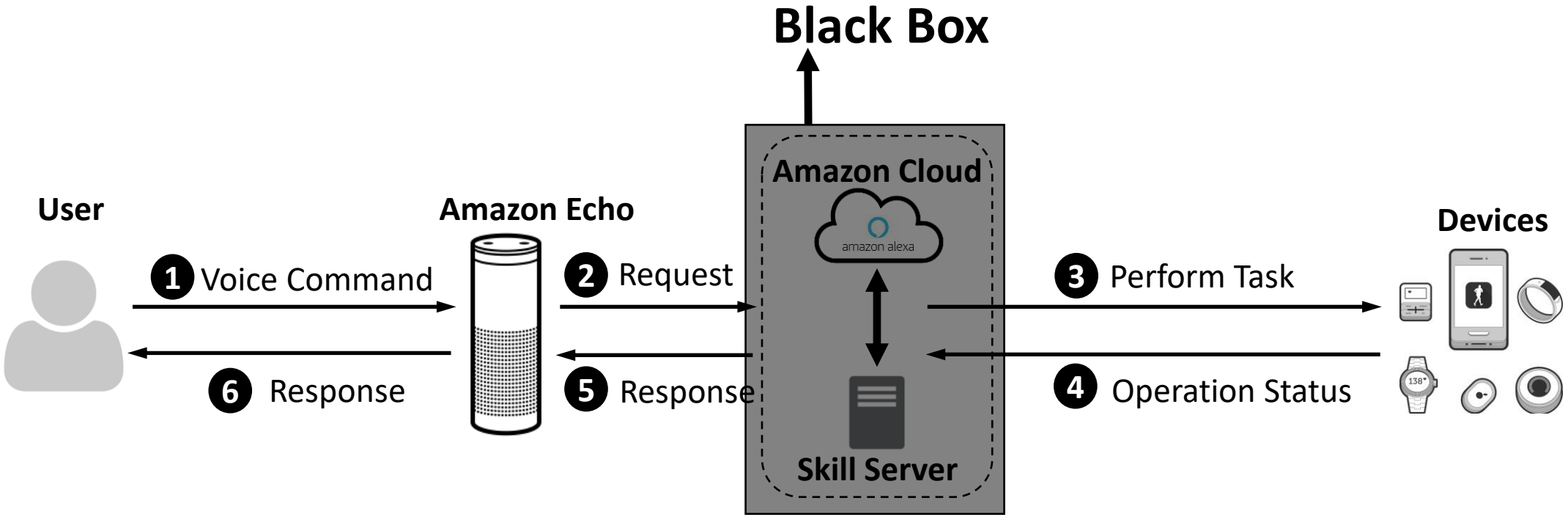
- Privacy in VPA: Guo (2020), Tabassum (2019), Lau (2018)
- Healthcare using VPA: Ahmed (2018), Maor (2020)

Prior Work

- Privacy in VPA: Guo (2020), Tabassum (2019), Lau (2018)
- Healthcare using VPA: Ahmed (2018), Maor (2020)
- Safety analysis of skill: Bickmore (2018), Spitzer (2018)

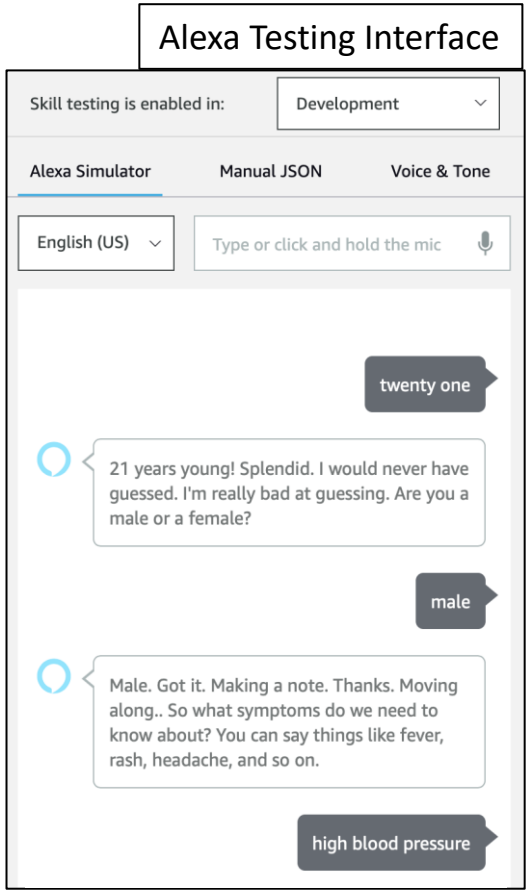
Challenges

C1. No executable files



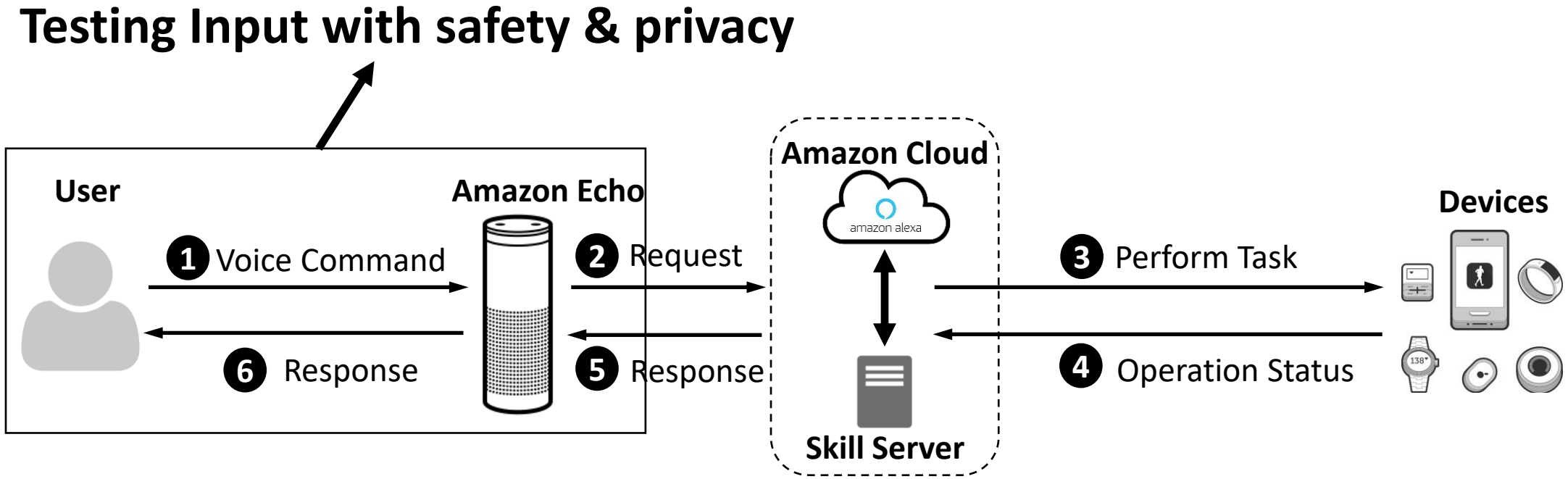
Challenges

C1. No executable files



Challenges

C2. Sophisticated testing input



Challenges

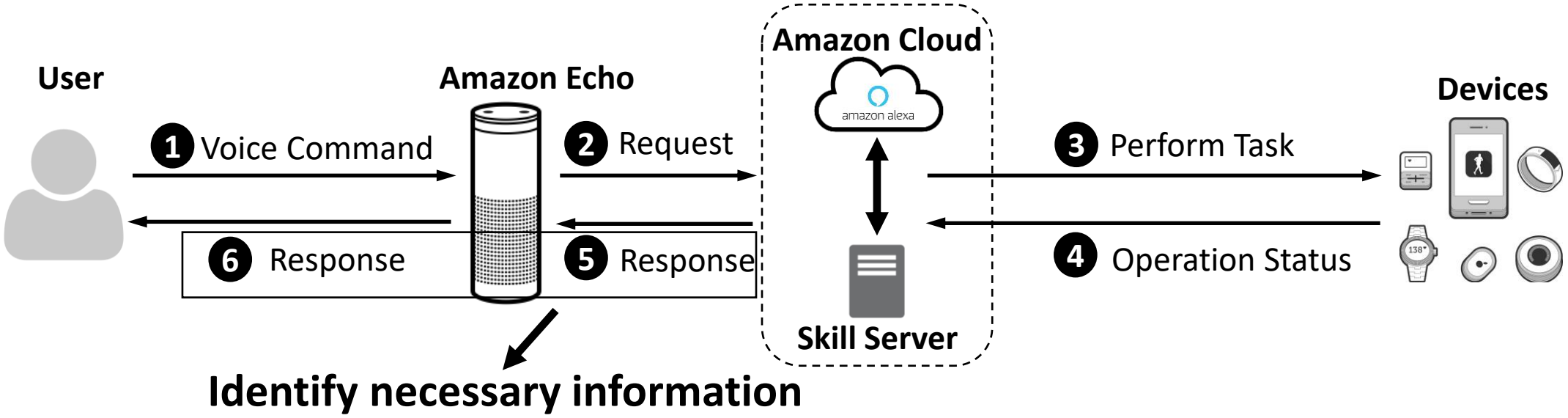
C2. Sophisticated testing input

Our Tool

1. Multiple rounds of interaction
2. Leading question/answer generation
3. Rephrasing commands

Challenges

C3. Required expertise in medicine and healthcare domain



Challenges

C3. Required expertise in medicine and healthcare domain

Consult Domain Expert

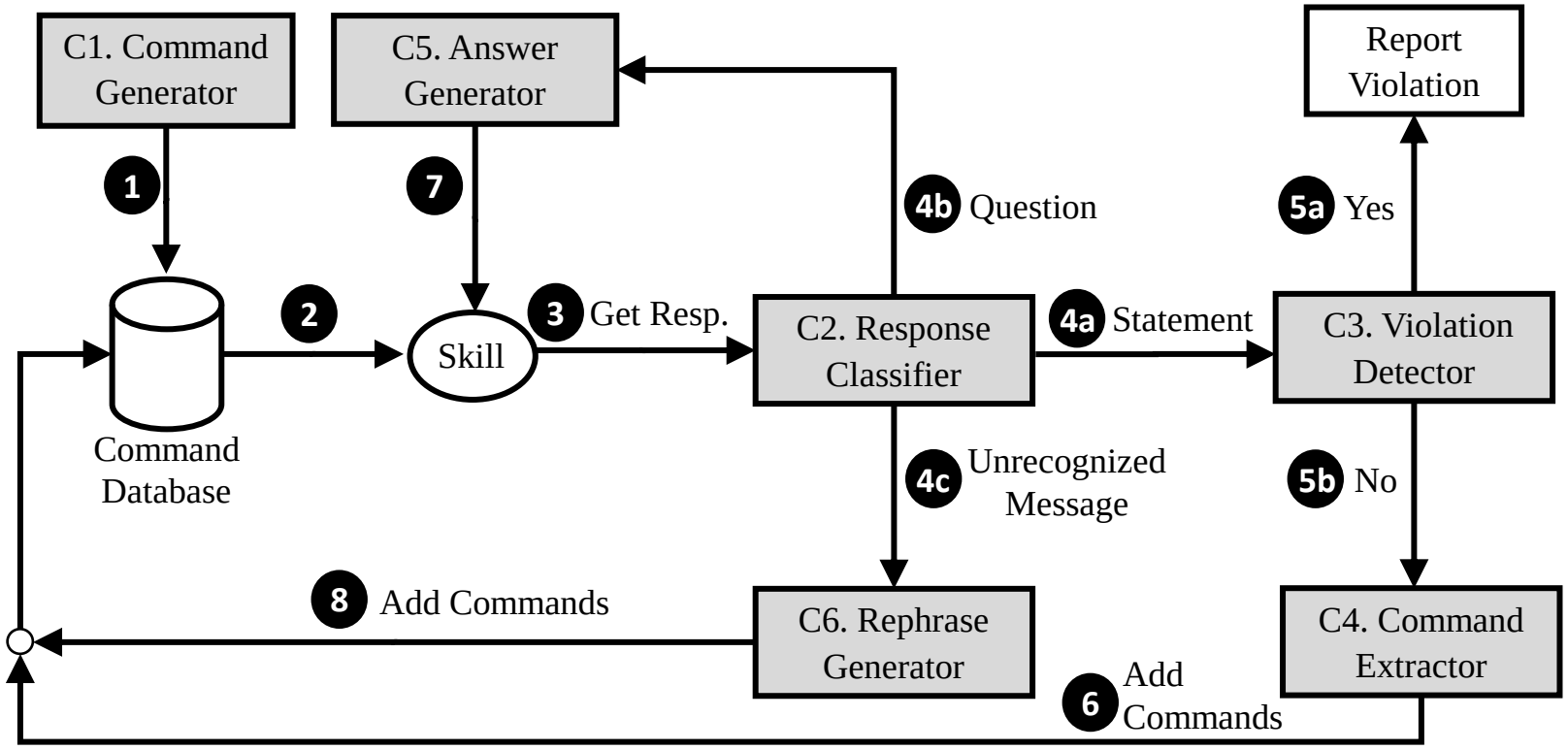
1. Consult experts from medical domain
2. Provide them syndrome name along with the corresponding follow up questions from skills
3. Identify necessary collected information

System Design

Data Collection

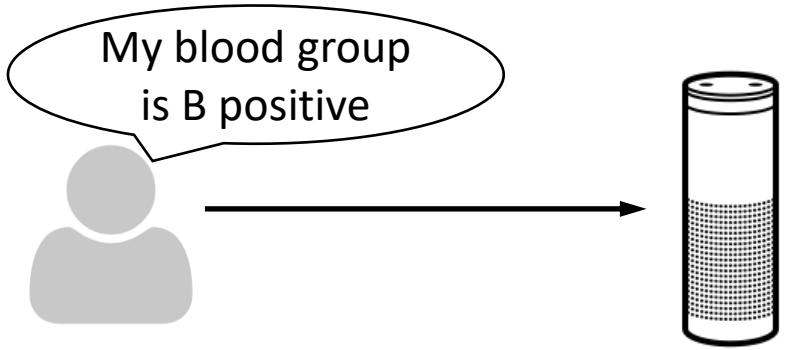
- Python Crawler
- 31,413 Alexa Skills from 23 different categories
- 80,129 voice commands
- **Data**- skill name, invocation name, category, description, account linking details, developer information, user review, category information, voice commands

Our Tool


C1. Command Generator
C5. Answer Generator
Report Violation
1
7
4b Question
5a Yes
2
3 Get Resp.
Skill
C2. Response Classifier
4a Statement
C3. Violation Detector
Command Database
4c Unrecognized Message
5b No
8 Add Commands
C6. Rephrase Generator
C4. Command Extractor
6 Add Commands

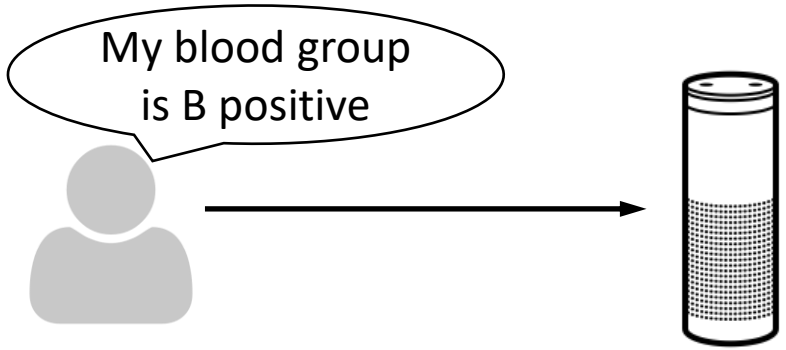
Storing information Detection

Provide Information



Storing information Detection

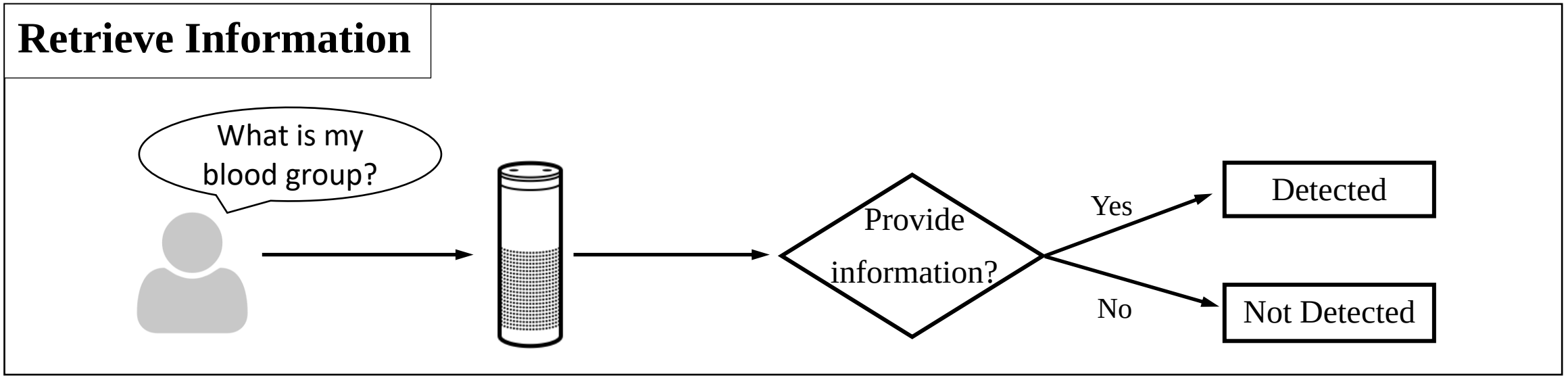
Provide Information



Approach:

1. Collect common physical and mental health conditions
2. Built template commands with conditions
3. Send those to top 20 skills (sorted by Amazon's featured rank)
4. Filter the conditions by the occurrences of valid responses
5. Use the reduced filtered conditions

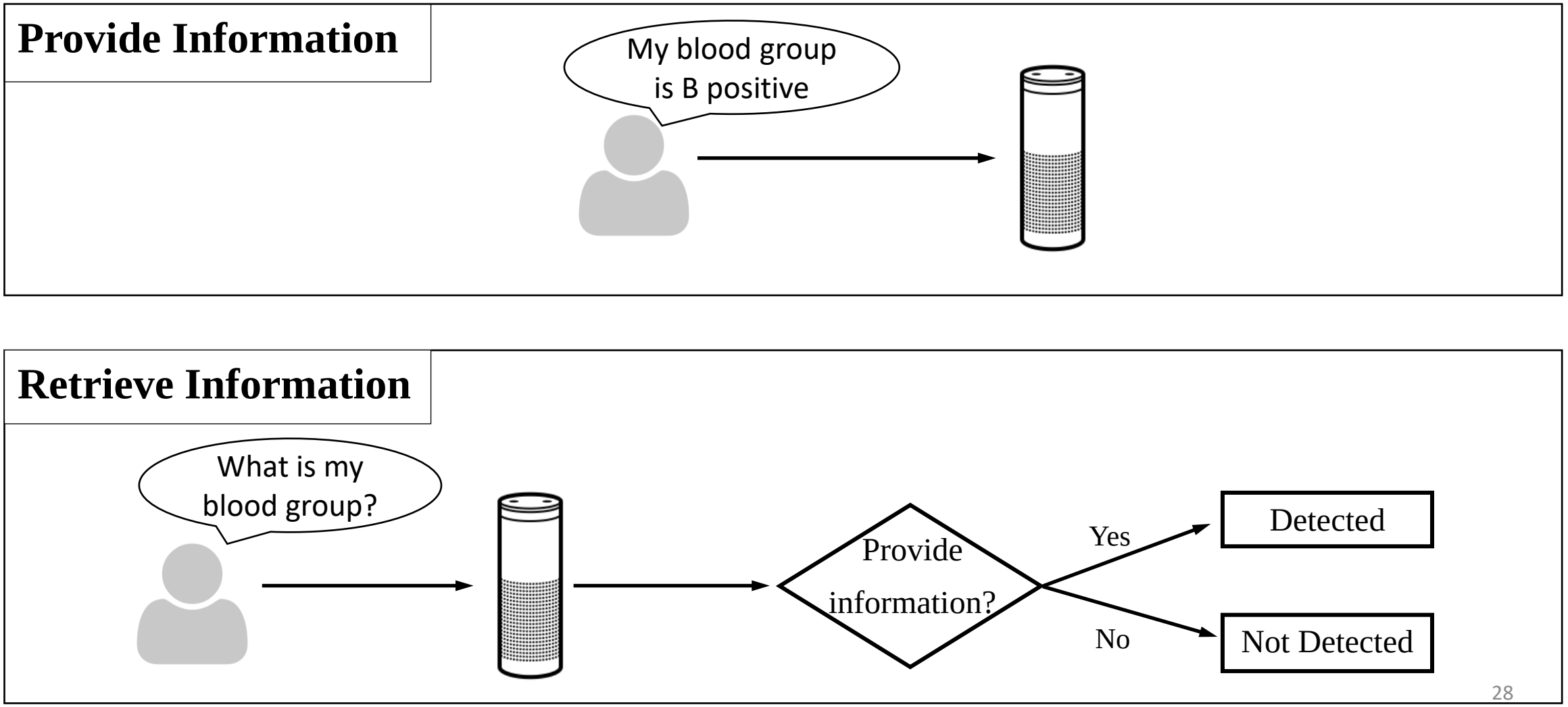
Storing information Detection



Approach:

1. Query for physical and mental health conditions
2. If found then it is violation
3. Otherwise not violation

Storing information Detection

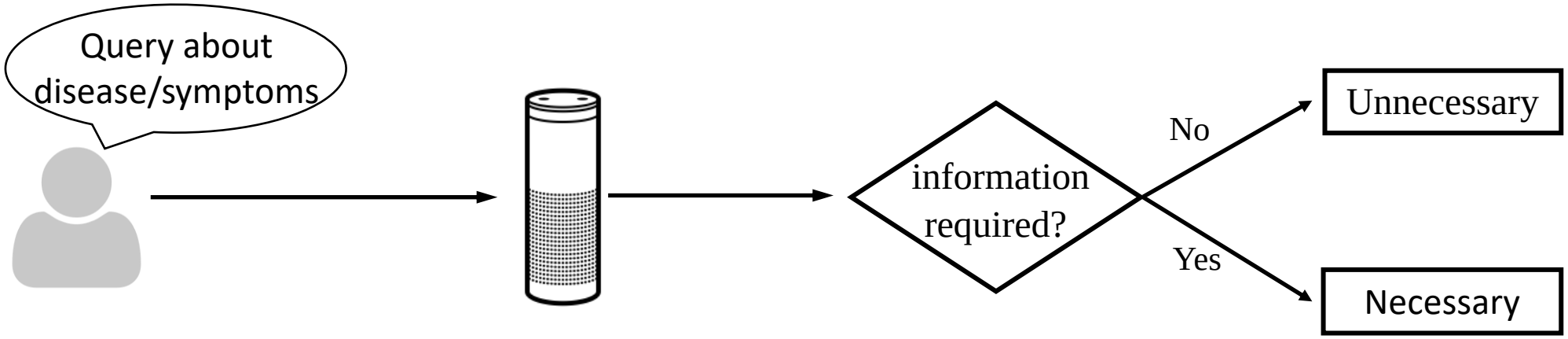


Results

Total Medical Skill: 813

Policy	#Skill
Storing Information	244 (30.23%)

Assessment by Domain Expert



Future Work

- Build a user medical profile for better user experience
- In critical conditions (analyzing voice patterns), connect them with medical professionals
- Incorporate medical history in a privacy preserving way to remind individual about their regular checkup
- Extend it to other voice application platforms (e.g. Google Assistant)

Thank you!

Email: fs5ve@virginia.edu

Questions?

Email: fs5ve@virginia.edu