UNIVERSITÄT BONN

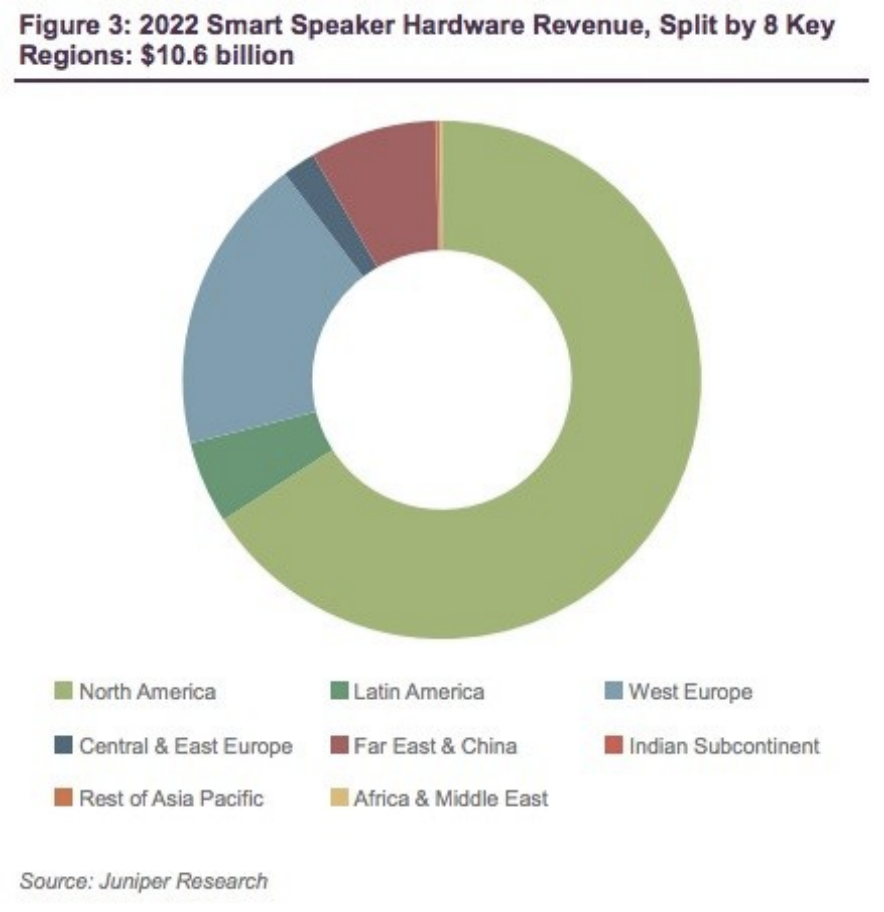
Platform for Investigating Privacy Concerns In Intelligent Voice Assistant

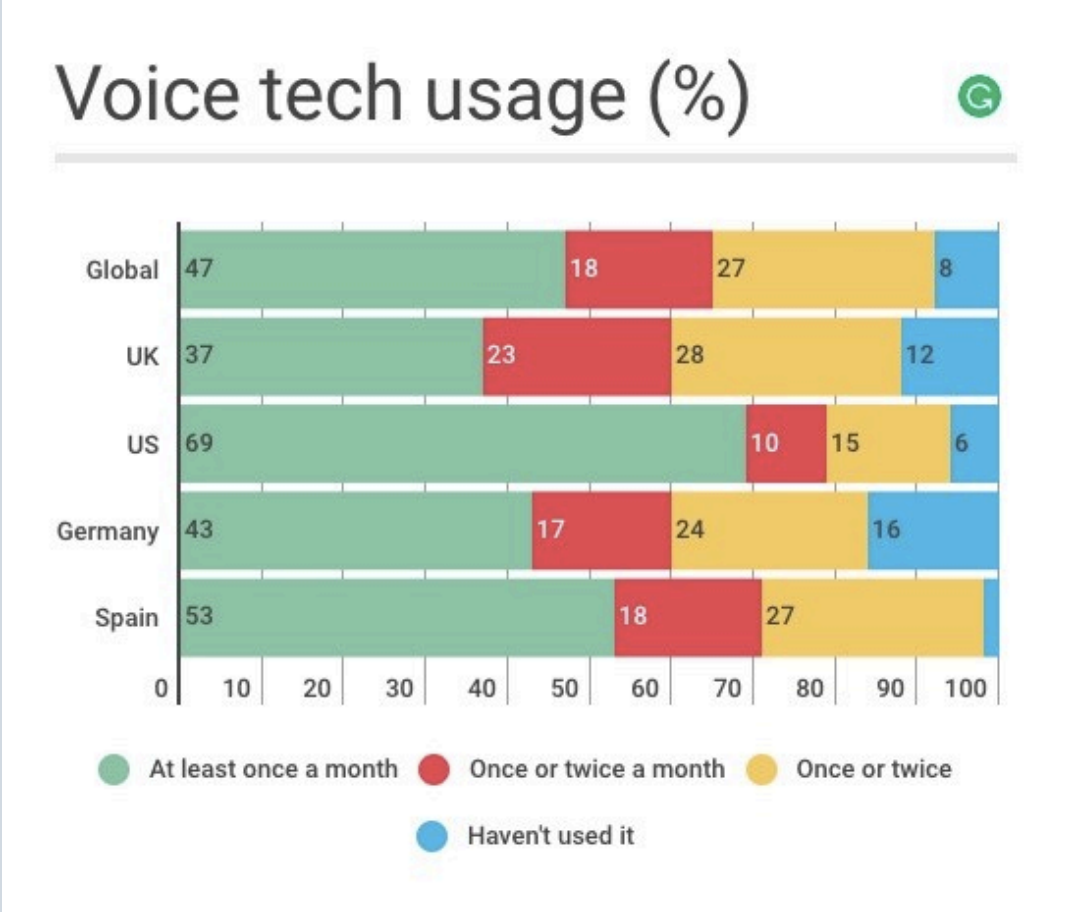
RAHUL LAO

Virtual Voice Assistant

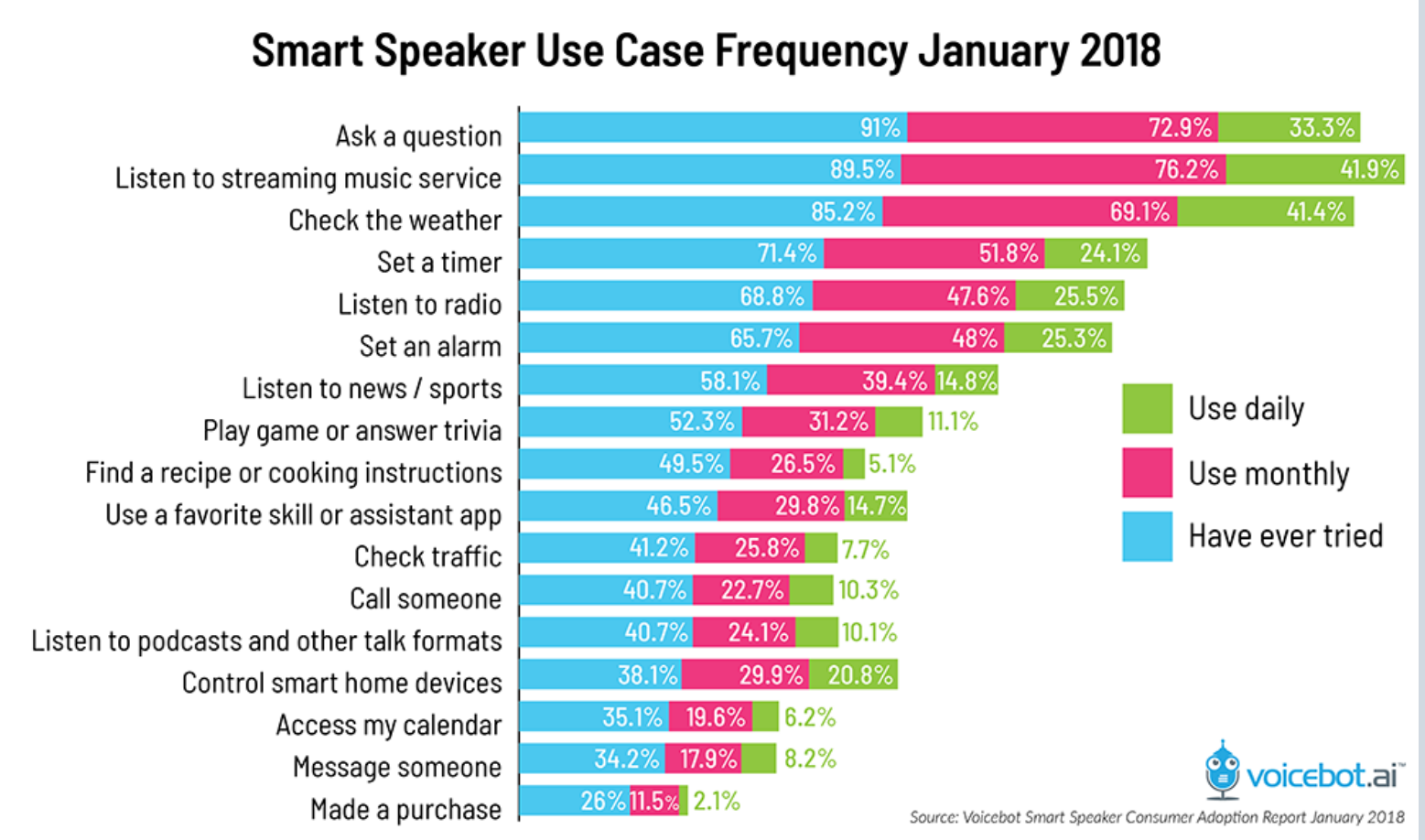
A virtual assistant, also called AI assistant or digital assistant, is an application program that understands natural language voice commands and completes tasks for the user.

Revenue And Usage (%)

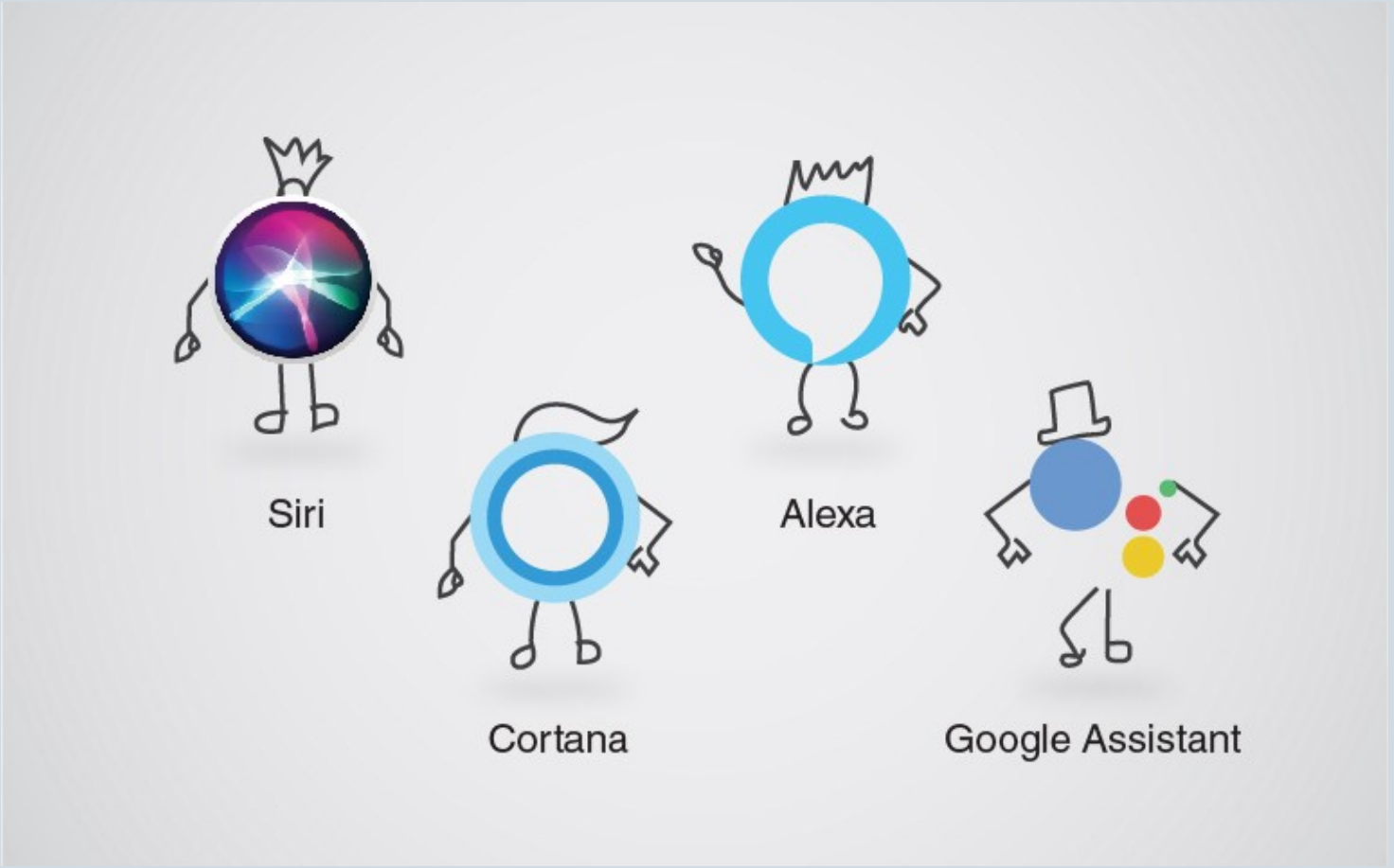




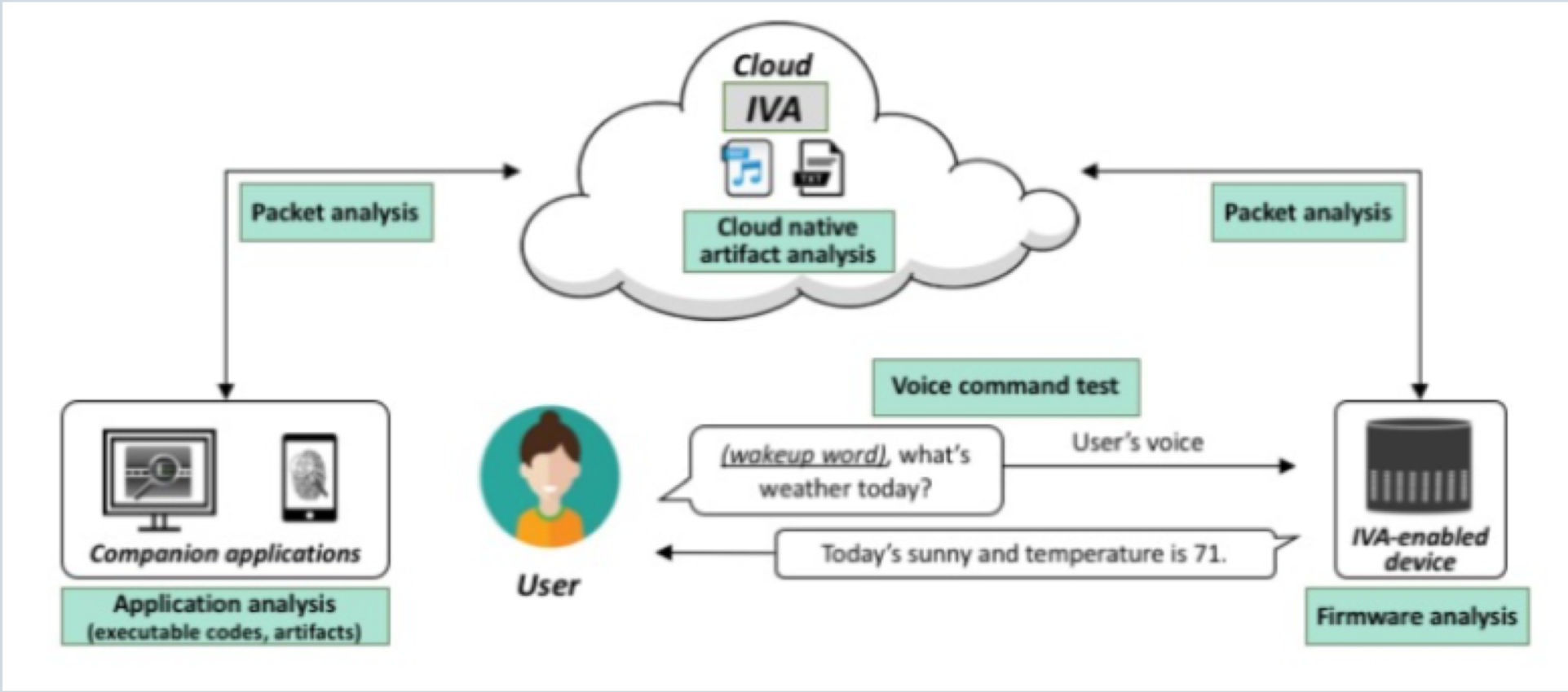
Use Cases


Smart Speaker Use Case Frequency January 2018
Ask a question
Listen to streaming music service
Check the weather
Set a timer
Listen to radio
Set an alarm
Listen to news / sports
Play game or answer trivia
Find a recipe or cooking instructions
Use a favorite skill or assistant app
Check traffic
Call someone
Listen to podcasts and other talk formats
Control smart home devices
Access my calendar
Message someone
Made a purchase
91%
72.9%
33.3%
89.5%
76.2%
41.9%
85.2%
69.1%
41.4%
71.4%
51.8%
24.1%
68.8%
47.6%
25.5%
65.7%
48%
25.3%
58.1%
39.4%
14.8%
52.3%
31.2%
11.1%
49.5%
26.5%
5.1%
46.5%
29.8%
14.7%
41.2%
25.8%
7.7%
40.7%
22.7%
10.3%
40.7%
24.1%
10.1%
38.1%
29.9%
20.8%
35.1%
19.6%
6.2%
34.2%
17.9%
8.2%
26%
11.5%
2.1%
Use daily
Use monthly
Have ever tried
voicebot.ai
Source: Voicebot Smart Speaker Consumer Adoption Report January 2018

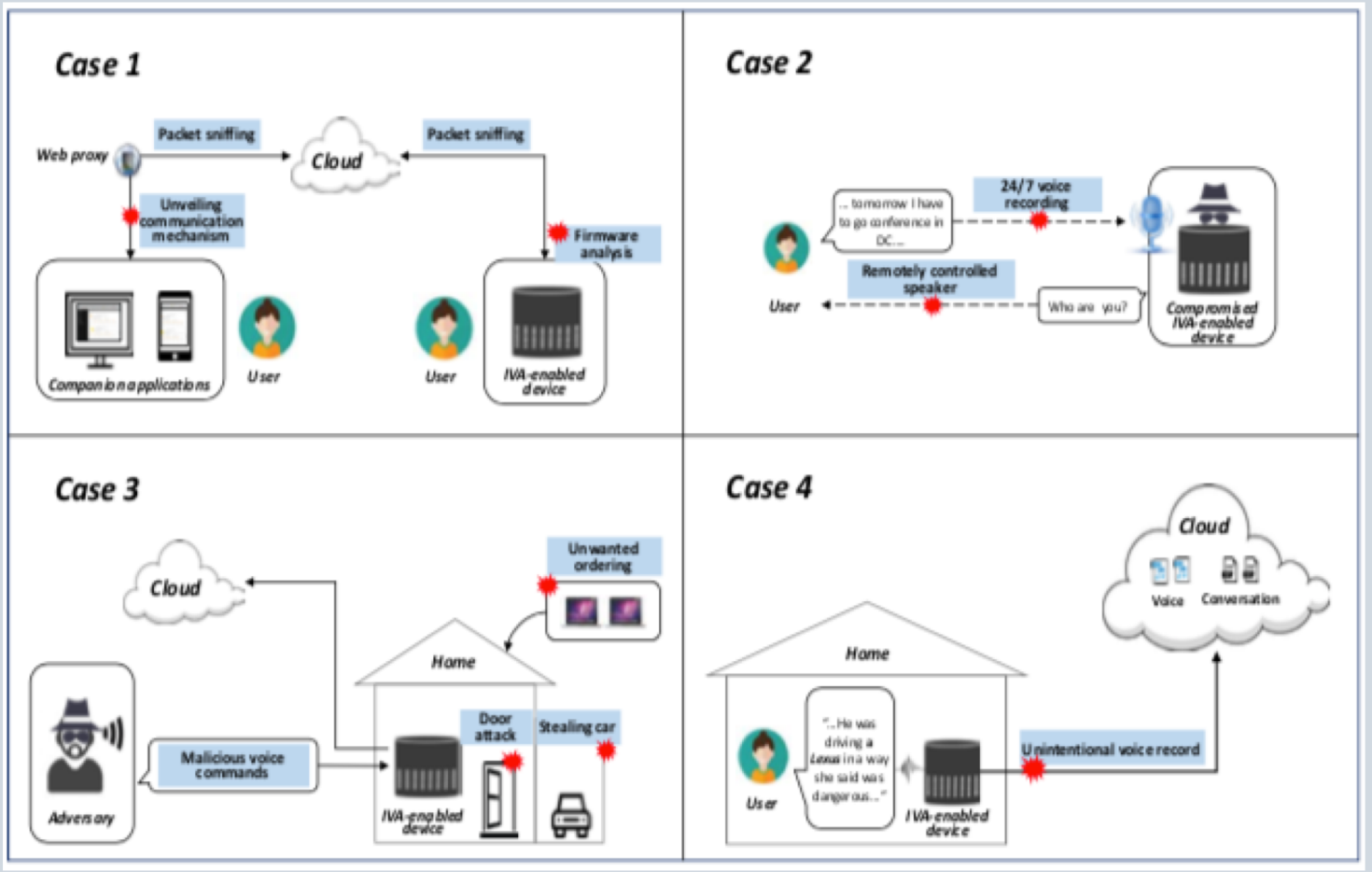
The Big Four



IVA Eco System



Rogue IVA


Case 1
Web proxy
Packet sniffing
Cloud
Packet sniffing
Unveiling communication mechanism
Firmware analysis
Companion applications
User
User
IVA-enabled device
Case 2
.. tomorrow I have to go conference in DC...
24/7 voice recording
User
Remotely controlled speaker
Who are you?
Compromised IVA-enabled device
Case 3
Cloud
Unwanted ordering
Home
Door attack
Stealing car
Malicious voice commands
IVA-enabled device
Adversary
Case 4
Cloud
Voice
Conversation
Home
"..He was driving a Lexus in a way she said was dangerous..."
User
IVA-enabled device
Unintentional voice record

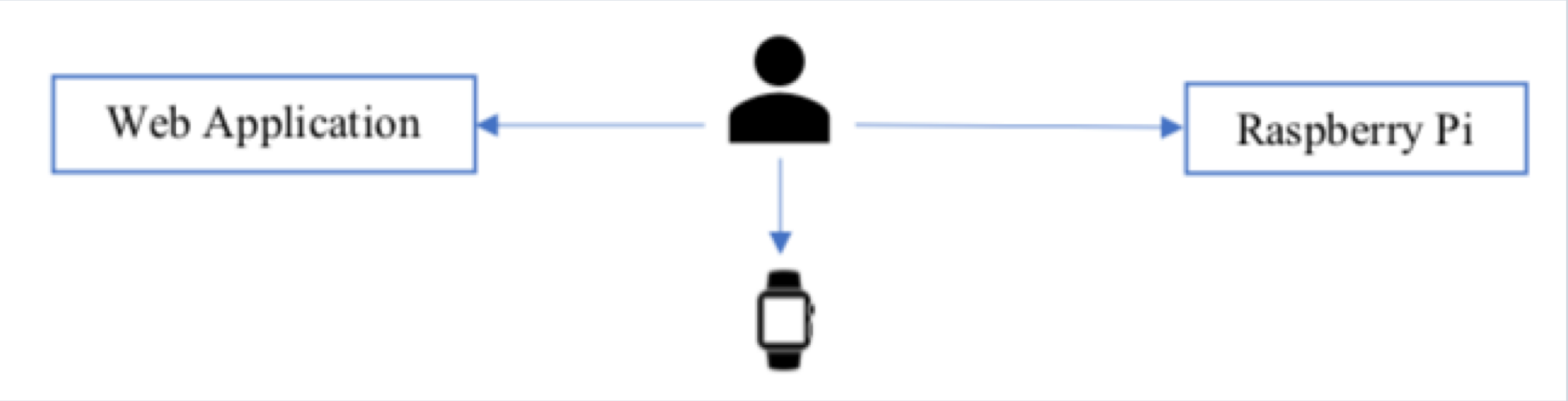
Privacy Concerns

- Who actually owns user‘s data?
- What exactly can and can‘t the digital assistant vendors do?
- Can the vendor give any third parties access to user data?
- What level of technical skill might be sufficient to hack into user data?
- Is there a retention policy for user data?
- Can a user allow another user to access their data?

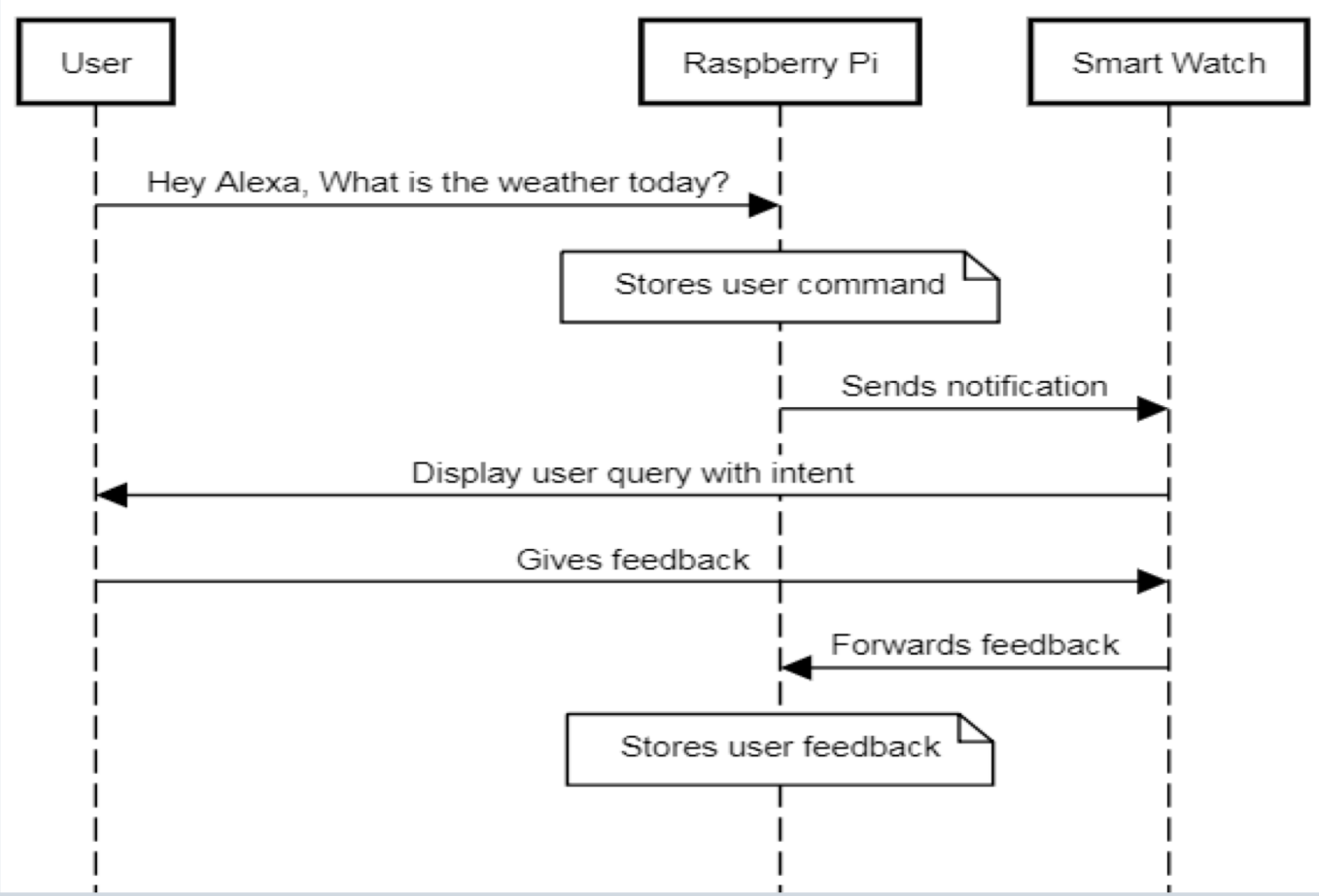
Goal

Our goal is to develop a platform that can be used to capture user voice commands which can be later used to perform studies related to privacy issues with intelligent voice assistants.

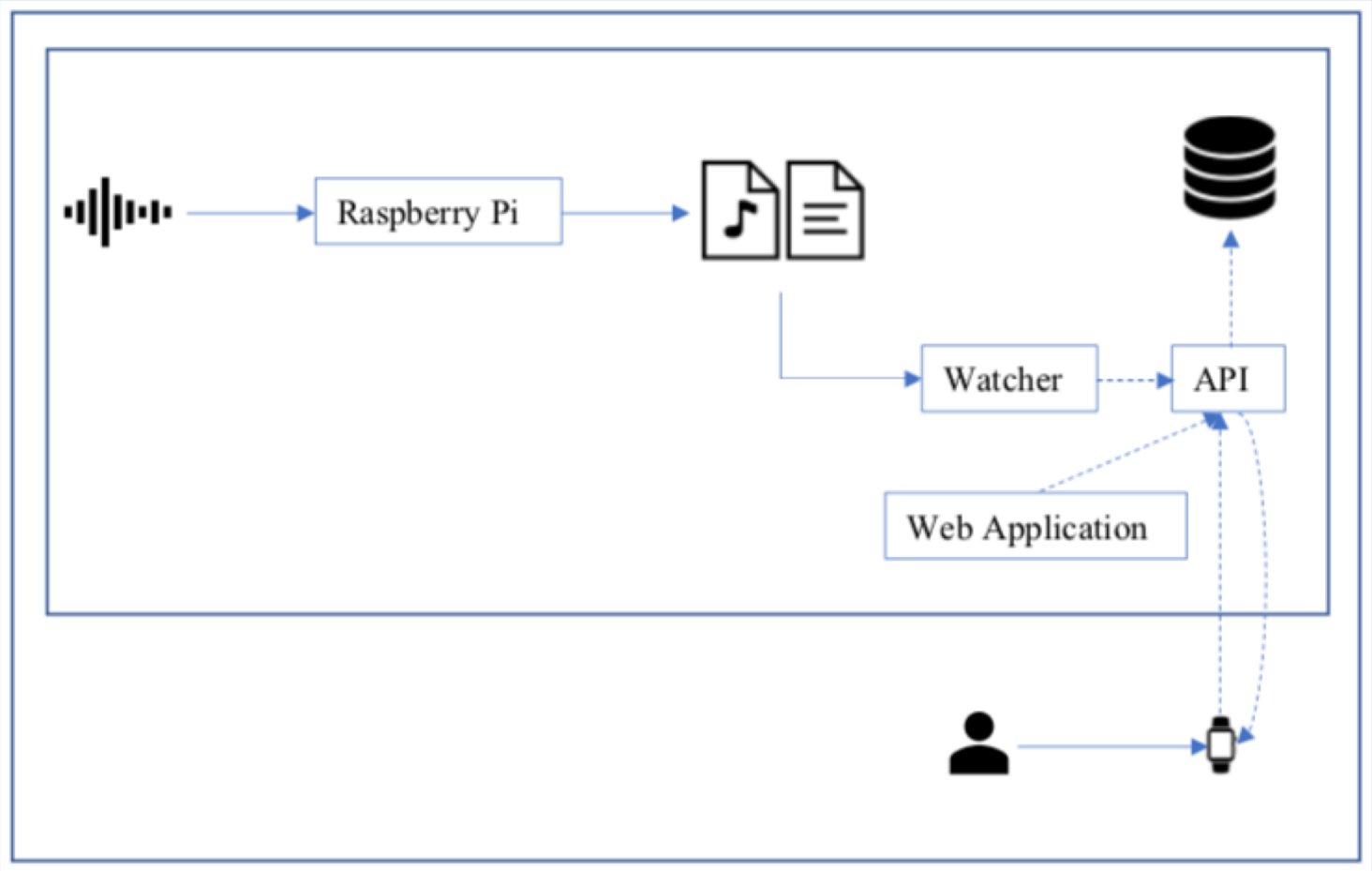
Main Components Of The Platform



Sequence Diagram



First Draft Of Platform Workflow



Thank You