Artificial Intelligence Assistants: Convenient vs. Security and Privacy

Isaac Collins
Department of Computer Science
Hampton University
isaac.collins1@my.hamptonu.edu

Chutima Boonthum-Denecke
Department of Computer Science
Hampton University
chutima.boonthum@hamptonu.edu

ABSTRACT:

Artificial Intelligence, intelligence demonstrated by machines, has emerged as one of the most convenient and personable applications of everyday life. Specifically, AI powers digital personal assistants to answer user questions and automate everyday tasks. AI Assistants listen continuously to answer the user, even when not in use. Why is this a problem? For a hacker, this makes any digital assistant a potential listening device, a major security and privacy issue. While some companies are handling this situation well, others are falling behind as their AI components are slowly dying in the consumer market. Which digital assistant is best and most secure you may ask? This paper will first detail how each AI assistant works from a technical perspective. Then based on survey results, this paper will detail how AI Assistants rank in terms of overall security and performance.

CCS CONCEPTS

- **Security and privacy → Personal Information security**
- **Security and privacy → Software and application security →** Software security engineering

Keywords

Artificial Intelligence, privacy, personal information, vulnerabilities, natural language processing

ACM Reference format:

1. MOTIVATION

I've always been intrigued by Artificial Intelligence and its ability to assist one in performing everyday tasks. I remember when my parents gifted me an iPhone 4s with the brand-new Siri integration, using her to call and text people. Fast forward to today, I rely heavily on my Amazon Alexa daily to set morning alarms, create routines, play music, and remind me of daily tasks. Nevertheless, now I am motivated to look under the hood of Artificial Intelligence to see how they truly operate to give the user the best experience while keeping their personal and private information safe from cybercriminals.

2. INTRODUCTION

Artificial Intelligence is defined as the ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity [1]. AI enables technical systems to perceive their environment, deal with what they perceive, solve problems and act to achieve a specific goal. The computer receives data - already prepared or gathered through its own sensors such as a camera - processes it and responds. AI systems/devices can adapt their behavior to a certain degree by analyzing the effects of previous actions and working autonomously. Why is AI so important? Artificial intelligence is seen as central to the digital transformation of society [1]. Future applications are expected to bring about vast changes, nevertheless, AI is already present in our everyday lives. The following are some AI-powered applications: Online shopping and advertising, web search, smart homes/cities, cars, machine translations, and of course digital personal assistants. Being used to answer questions, provide recommendations [1], and help organize daily routines, AI assistants are becoming ubiquitous in millions of living rooms, smartphones, and even car sound systems. The

leaders in AI systems include: Amazon's Alexa, Apple's Siri, Google's Google Assistant, and Microsoft's Cortana. AI assistants are basically cloud-based programs that require internet-connected devices or applications to work with their capabilities [3]. They use Natural Language Processing (NLP), the automatic manipulation of natural language by software [4], to match user text to voice input to run commands. Digital assistants are basically cloud-based programs that require internet-connected devices or applications to work with their capabilities [3]. AI systems rely on machine learning algorithms to provide accurate answers and provide a better experience to the user based on past experiences with the

assistant [3]. Additionally, Amazon recently announced Ais may soon be able to assist with everything from conference calls to supply orders [2]. While this a great milestone for Artificial Intelligence to accomplish, it may come at a cost of security since AI devices are vulnerable to potential hacking.

3. PROBLEM STATEMENT

As stated before, AI Assistants are in a constant battle with security flaws that are causing real concerns. The problem at stake is individuals don't know how well each big-name AI Assistant is at protecting their data. This research will prove one with which AI Assistant is most secure and the ones they should avoid.

4. METHODOLOGY

This study will use a combination of information gained from literature reviews and user surveys to collect data and gather results directly related to my thesis. Each methodology is explained as follows:

4.1 Survey

We will collect data from users through conducting surveys. The purpose of my survey is to understand how AI Assistants rank in terms in overall performance and security amongst the public. I will analyze my findings along with other sources of information to find patterns, make conclusions, and recommendations related to my problem statement. The number of questions in the survey varied for everyone as the more AI Assistants one used, the more questions one had to answer. If they only use one AI Assistant, they must answer 7 questions. If they use two, they answer must 12 questions. If they use three, they must answer 15 questions. If they use all four assistants, they must answer all 22 questions provided. The survey will be comprised of a wide range of questions pertaining to the user's grading of their use of Digital Assistant(s).

4.2 Literature Review

The researcher will discuss how Digital Assistants work from a technical perspective, comparing popular Digital Assistant privacy practices, and the vulnerabilities associated with the use of AI Assistants. Reading through these reports will provide the researcher with a foundation to build research on and will serve as support to findings from other methods of data collection.

5. RESULTS

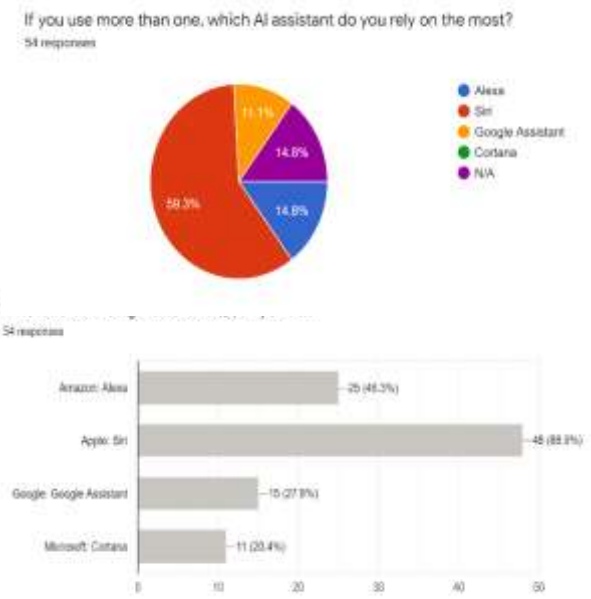
This section will cover the cumulative results obtained from researching methodologies outlined in the previous section.

5.1 Survey Results

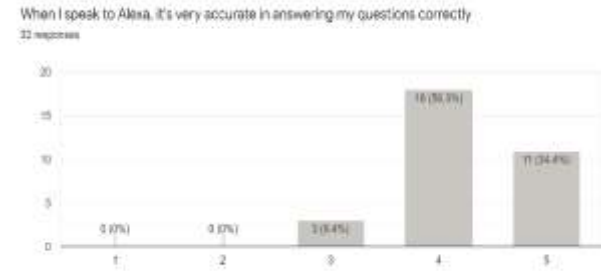
To conduct this research sufficiently and successfully, the researcher had to create a survey to record individual's experience with AI Assistants, which assistants they use, and how they score each one in terms of performance and overall security. The number of questions in the survey varied for everyone as the more AI Assistants one used, the more questions one had to answer. If they only use one AI Assistant, they must answer 7 questions. If they use two, they answer must 12 questions. If they use three, they must answer 15 questions. If they use all four assistants, they must answer all 22 questions provided. The survey was used to try and draw the conclusion of determining which AI Assistant is most secure and reliable. There was a total of 54 active participants who completed the survey. The observation the researcher expected to see was that Alexa or Siri would rank highest among survey responses as they are the two most popular assistants on the market. The researcher used the survey to prove the importance of this topic.

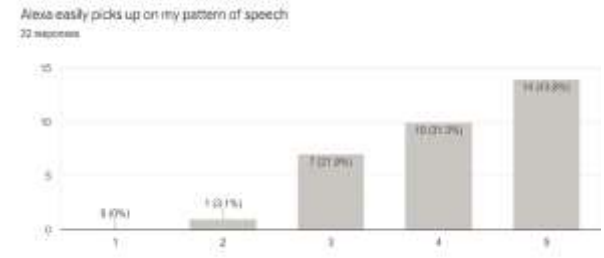
Total of 54 responses (n=54).

Data Summary

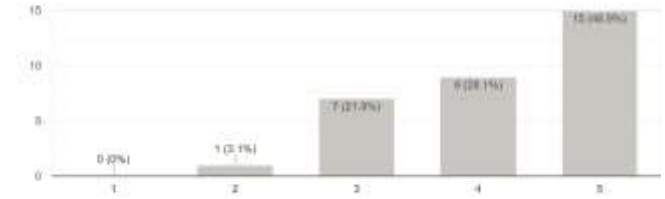


Ranking Amazon's Alexa:

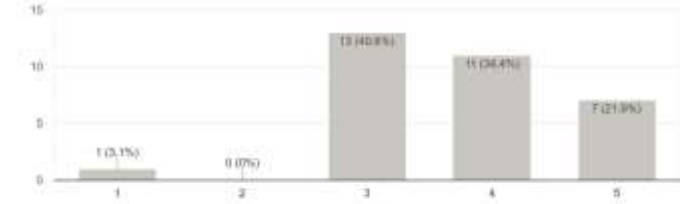




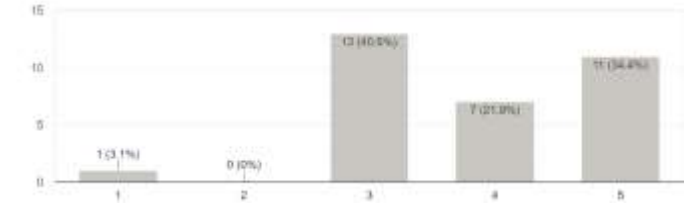
After asking Alexa a question, it responds very quickly and without delay
32 responses



The "Alexa" command always activates Alexa without having to repeat myself
32 responses

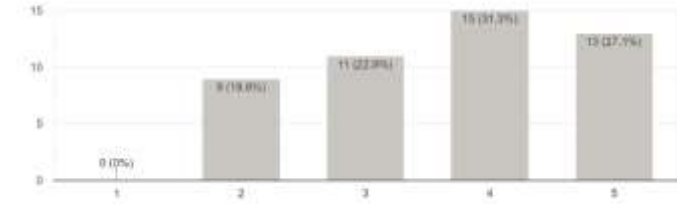


Alexa keeps my personal information secure and private
32 responses

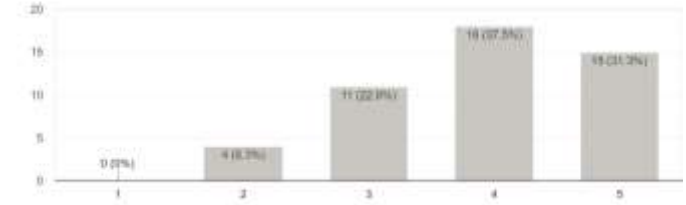


Ranking Apple's Siri:

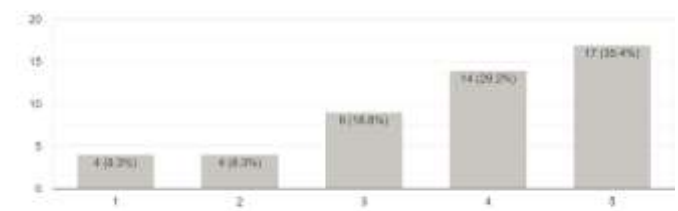
When I speak to Siri, it's very accurate in answering my questions correctly
48 responses



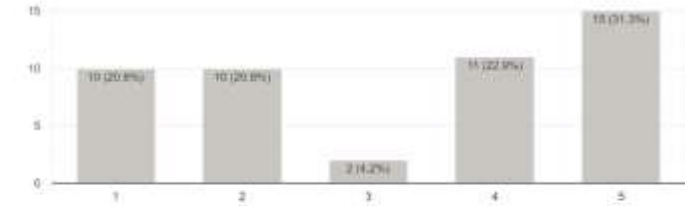
Siri easily picks up on my pattern of speech
48 responses



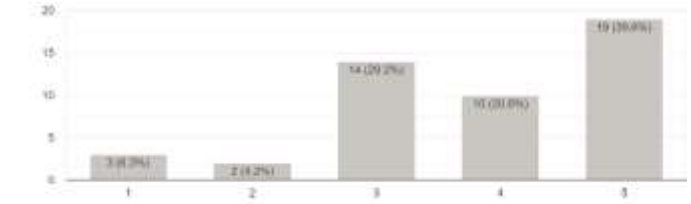
After asking Siri a question, it responds quickly and without delay
48 responses



The "Hey Siri" command always activates Siri without having to repeat myself
48 responses



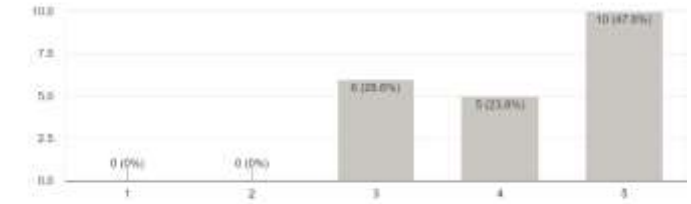
Siri keeps my personal information secure and private
48 responses



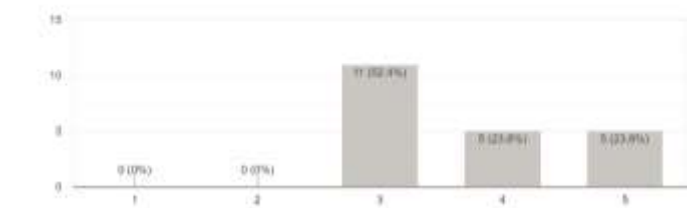
Ranking the Google Assistant:

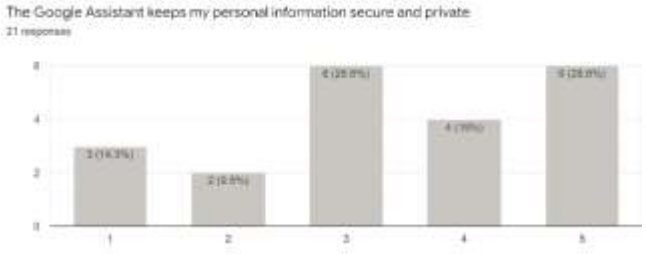
When I speak to the Google Assistant, it's very accurate in answering my questions correctly
21 responses

The Google Assistant easily picks up on my pattern of speech
21 responses

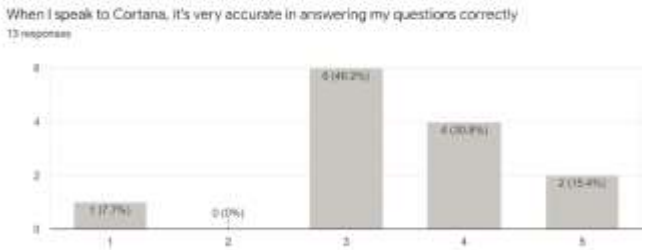


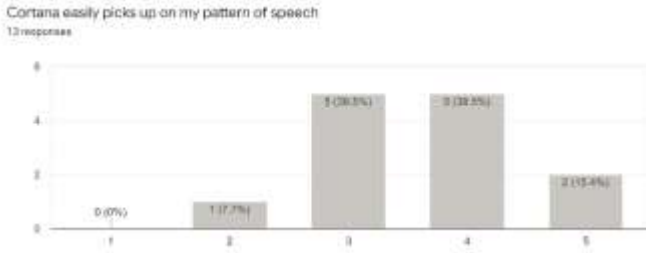
After asking the Google Assistant a question, it responds quickly and without delay
21 responses

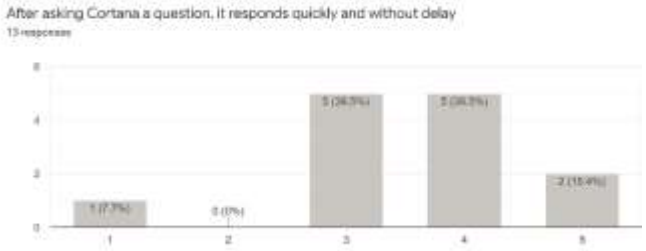


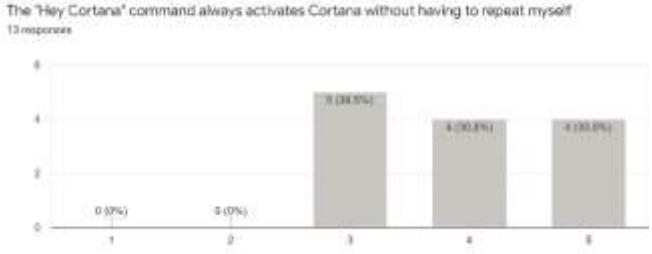


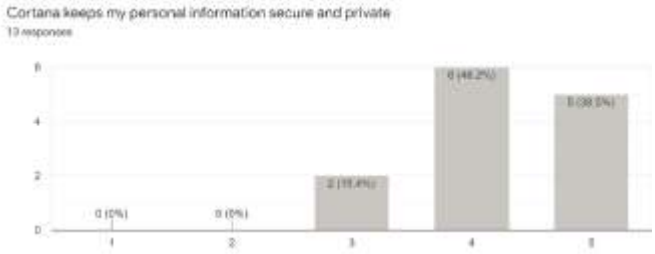
Ranking Microsoft's Cortana:











6. ANALYSIS OF RESULTS

Based on the results from question one it shows that the Apple's Siri is the most popular AI system as 48 of the 54 responses use it. Amazon's Alexa comes in at second with 25 users, the Google Assistant comes in at third with 15 users and Microsoft's Cortana finishes last with 11 users. This translates very accurately to the second question as 59.3 % rely on Siri the most. This makes sense as everyone has an iPhone, therefore everyone uses and relies on Siri the most. Nevertheless, there are those who think of other AI systems to be just as reliable: 14.8 % rely on Amazon's Alexa, 11.1% rely on Google Assistant, and 14.8% do not use more than one AI Assistant. Next, we have ranking individual AI systems. In this next series of questions, the respondent will have the option to score AI Assistants with a 1 to 5 scale, 5 being they strongly agree with the question statement and 1 being they strongly disagree with the question statement. Let's look at the first question asked about each AI system: "when I speak to [AI Assistant name], it's very accurate in answering my questions correctly". Of the 32 Alexa responses, 11 people strongly agree, 18 agree, and 3 are neutral. Translating this to a tally, Alexa scored 136 out of 160 possible points, a grade of 85. Of the 48 Siri responses, 13 users strongly agree with the statement, 15 agree, and 11 are neutral, and 9 disagree. Siri scored 176 out of 240 possible points, a grade of 73. Of the 21 Google responses, 5 strongly agree, 12 agree, 3 are neutral, and 1 disagrees. As a result, Google scored 84 out 105 possible points, a grade of 80. Of the 13 Cortana responses, 2 strongly agree, 4 agree, 6 are neutral, and 1 strongly disagrees. Cortana scores 45 out of 65 possible points, a score of 69.

Acknowledgements

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant award# 1754054.

References

[1] "What Is Artificial Intelligence and How Is It Used?: News: European Parliament." What Is Artificial Intelligence and How Is It Used? | News | European Parliament, 22 Oct. 2020, www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used.

[2] @SageSingleton, Sage Singleton Digital JournalistFollow. "AI in the Workplace: How Digital Assistants Impact Cybersecurity." Infosecurity Magazine, 29 Jan. 2018, www.infosecurity-magazine.com/opinions/ai-workplace-digital-assistants/.

[3] Gupta, Harsh. "Machine Learning by Virtual Assistants." What After College, 7 June 2020, whataftercollege.com/machine-learning/machine-learning-virtual-assistants/.

[4] Brownlee, Jason. "What Is Natural Language Processing?" Machine Learning Mastery, 7 Aug. 2019, machinelearningmastery.com/natural-language-processing/.