Advances in Knowledge-Based Systems, Data Science, and Cybersecurity Received 30-03-2025; Accepted 23-04-2025; Published 30-04-2025

Assessing Vulnerabilities in Voice Assistants: Comparative Analysis of Google Assistant, Siri, and Alexa

Aakanksha aakanksha.1@rajguru.du.ac.in
Shaheed Rajguru College of Applied Sciences for Women
University of Delhi, Delhi, India

Kashish Jain kashish.jain@rajguru.du.ac.in
Shaheed Rajguru College of Applied Sciences for Women
University of Delhi, Delhi, India

Neha Giri neha.giri@rajguru.du.ac.in
Shaheed Rajguru College of Applied Sciences for Women
University of Delhi, Delhi, India

Anamika Gupta anamikargupta@sscbsdu.ac.in
Shaheed Sukhdev College of Business Studies
University of Delhi, Delhi, India

Corresponding Author: Neha Giri

Abstract

Voice assistants (VAs), such as Google Assistant, SIRI, and Alexa, have changed the way people use technology by making information and services easily available. VAs provides assistance with web searches, smart home control, and scheduling tasks. VAs make daily tasks more convenient. Although there are many concerns regarding security, privacy, and general performance of the VAs as their use has increased over the period. The majority of research concentrates on their usability and functioning; little is known about their security vulnerabilities, which include threats to data privacy, background noise interference, and unauthorized voice access. This study assess the VAs security methods, response accuracy and authentication methods along with evaluating potential risks of data leakage and eaves-dropping. Improving the security of voice interactions can be achieved by being aware of these security risks. Tests were conducted to determine how well these assistants authenticate users, limit access to sensitive data, and answer user inquiries to assess their security and performance. Tests were conducted with situations like illegal voice attempts, background noise interference, and voice history access. A comparative study was also conducted on the results generated by the test case. The findings of the study were that although all three assistants can successfully execute complicated requests, their security systems vary. Google Assistant is more vulnerable to background noise activation, unauthorized access, and voice history accessibility. SIRI offers the best security measure by imposing restrictions on the access to stored data and avoiding unauthorized activations. Alexa provides privacy and correct responses by striking a balance between security and dependability. These findings

Citation: Aakanksha et al. Assessing Vulnerabilities in Voice Assistants: Comparative Analysis of Google Assistant, Siri, and Alexa. Advances in Knowledge-Based Systems, Data Science, and Cybersecurity. Research 2025;2(1):10. Pages-197-214

stresses on how crucial it is to protect user data by using better encryption practices, more strong access controls, and improved voice authentication systems. As VA continues to develop and become integral part in our daily life, these problems must be resolved to make them safer and more reliable.

Keywords: Voice Assistant, Vulnerabilities, SIRI, Google Assistant, Alexa, Smart Personal Assistant

1. INTRODUCTION

Communication has been improved with the rapid increase of smart mobile devices. To continue this engagement of smart mobile devices, the manufacturers have introduced the Voice-Controlled Personal Assistants, which resulted in achieving new heights of human and technological intersection [1]. With advancements in science and technology, AI-powered tools have become an integral part of every person's daily life. You can find Voice Assistant's (VA) and Smart Personal Assistants (SPA) in all sorts of devices, from smartphones to Internet of Things (IoT) gadgets and smart speakers, making it super easy for users to handle tasks like planning trips, controlling media, and even tackling more complex jobs like data analysis. This easy access to these AI tools has increased their popularity, making voice commands a natural and intuitive way to engage with technology. Voice-enabled interaction is well known because it is simple and convenient, allowing us to control devices and services without effort [1]. The growth of AI-based Assistants has given us exciting new ways to connect and control multiple devices in smart homes, allowing us to check traffic, play music, or control appliances all from a single location. Unlike older voice systems that consistently demand exact commands, modern Voice-based Assistants use Natural Language Processing (NLP) to understand what users mean and respond accordingly, breaking down the rigid barriers to command structures. As a result, these intelligent systems have found their way into a wide range of devices, becoming essential in many households. As AI, the popularity of SPAs is growing, making them an important home technology setup. The increased integration and connectivity pose a great concern about the security and privacy of user data. As AI-based voice assistants handle a lot of user data like location, contacts, calendar info, and microphone access, their safety measures need to be strong to give protection against unauthorized access and data misuse. The rise of virtual assistants comes with some risks, especially because they need permissions that may affect privacy [2]. Take navigation, for instance— VAs require access to your location, they need to always be ready, and they rely on network access for pulling data and communicating with the cloud. These permissions help boost their functionality but also open the path for misuse of data, if not handled correctly. The most integral part of VAs is the voice commands, without which VAs are of no use. This has sparked worries about privacy due to the risk of unauthorized listening and data harvesting that could put sensitive personal information at risk. These security issues are made even more pressing by the ever-evolving landscape of cybersecurity threats, where malicious actors might take advantage of the vulnerabilities in VAs. Studies [2] have also shown that voice-based assistants have more permissions than required, which can be misused if proper measures are not taken. A proper examination of these vulnerabilities is essential, as these vulnerabilities can lead to security threats or misuse of the personal data of the user. Risk analysis tools like MobSF, RiskInDroid, and AndroBugs are used to check for potential security flaws, leading to the development of stricter access controls and more transparent data-handling practices [2]. Following

privacy-focused design methods—like controlling the limit of data collection to what's necessary and giving users more control over their data sharing—is increasingly seen as a best practice for ensuring the security of VAs and SPAs. On a broader scale, the security and privacy implications of SPAs in a household context are particularly noteworthy. For example, in homes with kids, the lack of proper control measures in SPAs to shield children from inappropriate content or unauthorized access makes their safe use a bit tricky. With the increase in always-on devices, there are concerns about how user data might be misused. The [3] General Data Protection Regulation (GDPR) in the EU has labeled voice data as sensitive, which means users need to give consent for their data to be processed. Unfortunately, many commercial AI-based voice assistants do not stand up to these security standards, revealing a major difference in how privacy-by-design principles are put into practice to protect users. Moreover, the increasing use of social networks, especially among younger people, thus signifies the need for digital safety and privacy. Social media has changed how communication is done, but it also gives rise to increased risks, like non-consensual image sharing and cyberbullying. Research by [4]shows that children are particularly vulnerable in online spaces, facing threats like privacy threats and the spread of harmful content. Sexting, which involves sharing sexually explicit messages and images, is one of the Virtual interactions that can be misused, causing serious psychological and social consequences. Cases of illegal sharing, commonly known as non-consensual intimate content, have raised concerns about the dangers of global connectivity. Apps like SafeSext, which help prevent the sharing of private content without permission, are a great step toward making digital communication safer.(Franco et al., 2023). Similarly, social platforms like Mastodon [1] are becoming popular because they give users more control over their data and reduce the risks of storing everything in one central place. As technology is growing fast, keeping the digital world safe is becoming more important for both users and developers. To protect our privacy and security, we need a strong and well-defined strategy. Something that looks at not just technical flaws but also other important factors. If we stay aware of the risks and improve how we handle data and user permission, we can create real trust in virtual assistants, social media apps, and online platforms.

The goal of this study is to find out the security breaches in voice assistants such as Alexa, Siri, and Google Assistant. It focuses on evaluating their privacy methods, methods of user authentication, and response accuracy. The study identifies risks such as voice commands, disturbance caused by background noises, and illegal access by unauthorized users. The results of this study would help in creating stronger security methods to improve user safety, data privacy, and the general dependability of AI-powered voice assistants in day-to-day life.

The paper is structured as follows: Section 2 reviews related work, highlighting previous research on voice assistant security and identifying existing gaps. Section 3 describes the methodology used to compare Google Assistant, Siri, and Alexa, focusing on their authentication methods, privacy protections, and response accuracy. Section 4 presents observations from real-world test cases, analyzing security risks and system vulnerabilities. Section 5 concludes the paper by summarizing the key findings and their implications.

The flowchart given in FIGURE 1 illustrates the step-by-step methodology used in the research process.It highlights the steps taken to analyze vulnerabilities in voice assistants.

[1] https://www.bing.com/ck/a?!&&p=cf793b8d5d4a4ad1932d8355274eb76bf2c83a6620ab855c4e0f21479a72c48bJmltdHM9MTc0MzI5MjgwMA&ptn=3&ver=2&hsh=4&fclid=27a15273-f1af-6c58-153f-47cdf0a96dc4&psq=mastodon&u=a1aHR0cHM6Ly9tYXN0b2Rvbi5zb2NpYWwv&ntb=1

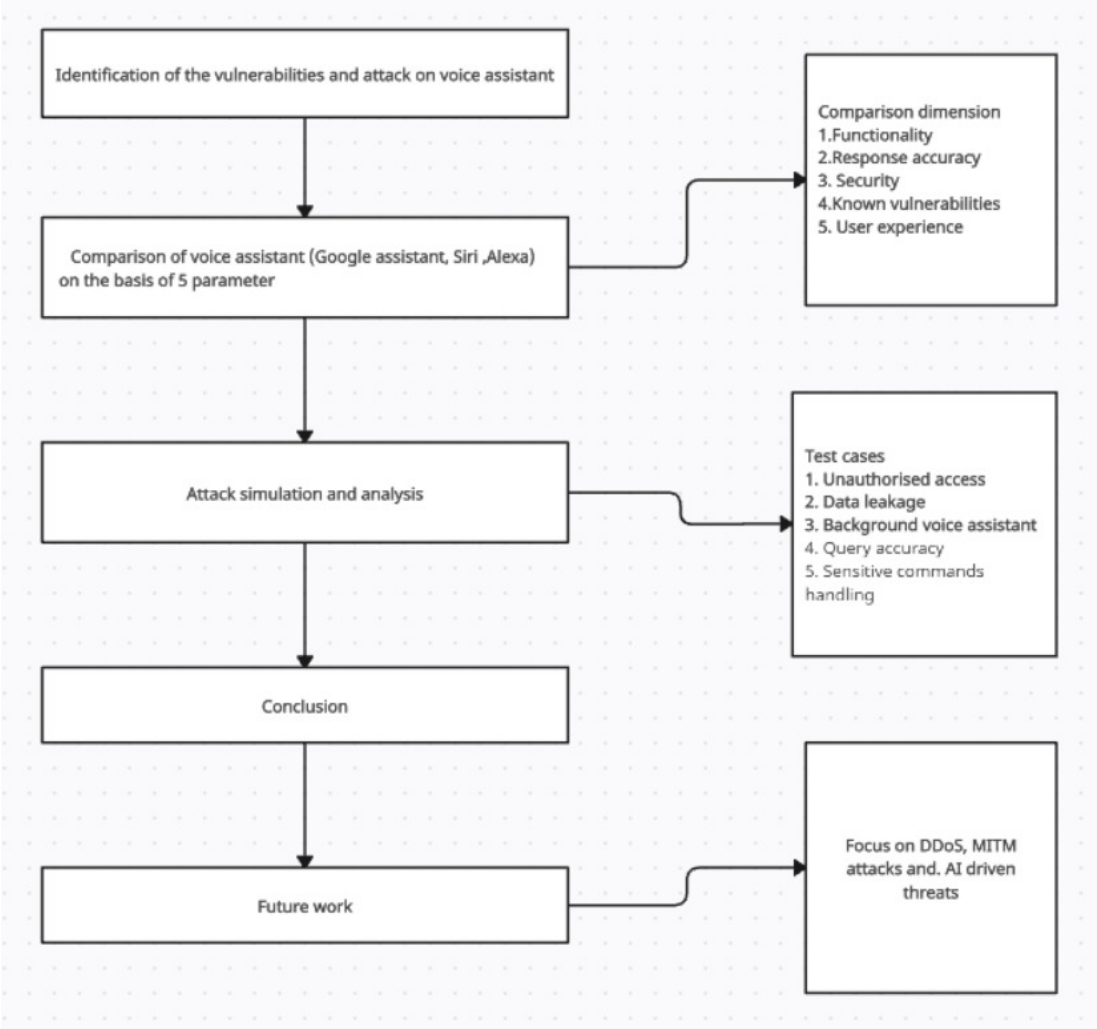

Figure 1: Flowchart depicting the flow of this research paper.

2. RELATED WORK

In the twenty-first century, a voice assistant powered by artificial intelligence is a necessity for everyone. Nearly everyone in the world is drawn to this new technology in numerous ways, including computers, laptops, and smartphones. Among the notable voice assistants are Alexa, Google Assistant, and Siri. Research on the security and privacy of AI-driven systems has been growing. This section looks at VA security and privacy studies, combining findings from different research works. One of the major issues related to voice-based assistants is managing user data and privacy risks. Paper by [5] focuses on the virtual assistants based on cloud-based processing. Where user command is sent, stored, and analyzed by service providers [6]. Several research findings indicate that voice assistants can record user conversations without apparent consent. Situations where Amazon employees reviewed private voice recordings from Alexa users have brought up ethical concerns about data tracking and authorization [5]. Moreover, many researchers found instances

where voice-based assistants unintentionally activated and captured sensitive audio and transmitted it to third parties.[5]. Privacy regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) highlight users' control over data storage and access. Yet, Current studies suggest that voice assistants have unclear policies regarding data storage and user approval, leading to potential policy breaches.(Bolton et al., 2021)[3]. Many voice assistants trust wake words like" OK Google"," hey Siri", and "Alexa" for activation. Which fails to possess a strong authentication mechanism. In contrast to biometric authentication in smart devices, voice authentication is highly vulnerable to spoofing, creating a significant threat of unauthorized access [5]. [7] Analyze security threats and proposed a classification of VA attacks, dividing them into three key categories. [8].The first category is ***Unauthorized Access Attacks***(Taking advantage of weak authentication to execute unauthorized commands). The second category is ***Voice Privacy Threats*** (Illegal recording and processing of voice data). And the last one is ***Sound-Based Attacks*** (Retrieving environmental details using Voice Assistant microphones). Their work Displays that many existing defenses focus on individual threats rather than giving a holistic security framework [7]. Likewise, [9] classified adversarial attacks, malicious skill injections, and voice spoofing techniques indicate that VAs are highly vulnerable to Exploitation. Most modern VAs allow third-party developers to create voice applications **"skills"** for Alexa (apps that help Alexa to perform tasks like ordering food, checking the weather, or controlling smart devices) and **"actions"** for Google Assistant (Like Alexa services, these let Google Assistant connect with third-party apps for tasks like booking cabs, playing music, or giving news updates). However, these skills introduce severe security risks due to Weak verification methods. [10] [11] Recognized the Voice Squatting Attack (VSA), where a malicious skill is audibly similar to a legitimate one. This tricks the VA into activating the malicious application rather than the desired one. [12] finds a different vulnerability, known as Voice Masquerading Attack (VMA), involves a malicious skill pretending to be an authentic virtual assistant service. The malicious skill fails to end after execution but rather continues listening, collecting sensitive user data such as passwords, personal details, and financial transactions.These findings represent major weaknesses in Voice assistant security policies, where third-party skills can execute unauthorized commands without proper validation [10] Adversarial attacks exploit weaknesses in AI-powered speech recognition systems used by voice assistants.[13], [14]and [9] describe two major Attack techniques: hidden voice commands and hidden disruptions. In hidden voice command, attackers hide inaudible voice commands inside background noise. Humans cannot detect these commands, but AI-powered voice-based systems can recognize and execute them [13]. In a hidden disruption attack, attackers change sound waves in a way that confuses the VA into thinking they are real commands. These disturbances are undetectable to the human ear but successfully bypass voice authentication systems [13]. We are enabling our houses with voice assistants and making the houses smarter at the cost of our privacy. These voice assistants pose great vulnerability to our privacy in the form of eavesdropping, data leakage [15]. Single-Factor Authentication in Alexa and Google Assistant uses only wake words to verify users This means anyone with the device, even attackers, can give commands without extra security [15]. Always-Listening Mode in smart voice assistants makes them vulnerable to eavesdropping attacks. Attackers can even use laser-based techniques to trigger commands remotely from hundreds of meters away, posing serious security risks [16]. These findings suggest that voice assistants should integrate multi-factor authentication and detect physical presence to improve security

3. METHODOLOGY

A voice-based assistant is an AI-powered software that uses voice commands to get assistance with various tasks or access to services. Virtual assistants are powered by AI and Machine Learning (ML). Together, these technologies help the voice assistant to understand the context and intent of the user's voice command, search for relevant information, and provide the required service as asked. The most commonly used voice assistants are Google Assistant, Siri, and Alexa. The integration of AI-based voice assistants powered by advanced natural language processing algorithms equipped with home automation technology offers a unique chance to develop a smart and adaptive living space. This system enables a wide range of functions, from regulating lighting and climate to enhancing security. Voice assistants have become an essential problem-solving tool in today's world; with just a voice command, users can find a solution to a wide range of queries. NLP is an essential component of AI-based voice assistants that helps them understand and process human language. By using NLP, voice digital assistants can transform voice into text (Converts the spoken words into text, allowing the voice assistant to understand user input), Recognize the speaker's purpose (Helps the voice assistant understand the user's intent or objective behind the query and deliver relevant answers to users' questions). [11]

- Google Assistant is an AI-powered virtual assistant software application developed by GOOGLE that is commonly available on smart home devices and Android phones. Google Assistant launched in May 2016 as a part of the Google messaging app Apollo and its voice-activated speaker Google Nest. Users mainly engage with Google Assistant through natural voice, and through keyboard input, which is also supported. The assistant is also able to answer questions, schedule alarms, schedule events, adjust phone settings on the user's device, and display data from the user's Google account and Play Store. Google Assistant also allows users to activate and modify the command to perform actions on systems.
- Alexa allows users to activate the wake word called "Alexa", "Alexa play music", and "Alexa wake up". Alexa is a cloud-based virtual assistant technology that allows users to interact with devices using voice commands. Alexa is used to perform various tasks like playing music, setting alarms, controlling smart home systems, reading podcasts, reading audiobooks, playing games, sending messages, making calls, creating to-do lists, accessing real-time information, and many more. Alexa can also be used in the investigation as a voice data storage, legal request (Amazon cannot release data freely, but they can provide the data by the court order or warrant), and smart home data. Alexa can provide timestamps and movement history [17].
- Siri stands for Speech Interpretation and Recognition Interface. Siri is a digital virtual voice assistant developed by Apple in 2011, which is included in iOS, iPadOS, macOS, tvOS, etc. It uses voice queries, gesture-based control, and a Natural language user interface to answer questions, make recommendations, and perform actions by giving approval requests to a set of internet services. Siri can perform a variety of tasks like performing mathematical calculations, creating calendar events, reminders and alarms, coordinating payments through Apple Pay, playing music from various media applications, translating languages, and smart home control [17].

Understanding NLP in Voice Assistants and the Security Concerns It Brings: Voice assistants like Alexa, Siri, and Google Assistant depend on Natural Language Processing (NLP) to understand

and respond to users' voices. NLP helps these systems understand speech, figure out the user's intent, and generate relevant replies — all in real-time. To make the conversation more efficient and natural, different strategies are used, which include context analysis, intent detection, and speech recognition. Models like ChatGPT have also enhanced the abilities of NLP, which in turn helps to get accurate awareness of human language, including slang and difficult inquiries. But with this advancement comes risk. If the NLP system makes a mistake in understanding a command or is exposed to misleading or manipulated audio, such as background noise, spoofed recordings, or commands hidden in music, the voice assistant might give wrong outputs. This can cause accidental purchases, data leakage, or physical security issues in smart homes. Furthermore, some attackers have found ways to change inputs that sound normal to machines but are not recognized by human ears, raising serious concerns about unauthorized access. Most NLP operations need to send voice data to remote servers, which raises privacy concerns. If this data is not handled securely, it could be misused. Although NLP makes voice assistants powerful and user-friendly, it also opens the door to a range of vulnerabilities that must be addressed carefully during both development and deployment.

The automation and hence the functionality of these voice assistants using NLP brings in a lot of issues and concerns regarding the security, vulnerability and data privacy of the users. In this paper, we have done a comparative study on the three most frequently used VAs, Google Assistant, SIRI, and Alexa, to find vulnerabilities and hence security and privacy breaches in each one of them. Our study accesses the vulnerabilities in these VAs based on the following parameters:

1. Functionality Functionality refers to how well the assistant works, does it respond accurately to the right voice,follow commands, and does its job as expected? If a voice assistant allows someone who isn't the owner to issue commands, that's not just a security issue, it also messes with the functionality of the device.
2. Response Accuracy Response accuracy tells how well a voice assistant understands what a person is saying and carries out the right task based on that input. It shows whether the assistant can catch the actual words,understand the meaning, and then respond properly. When a voice assistant has high accuracy, the assistant usually gives the correct answer or performs the right action. However, if the accuracy is low, it might not understand the command and take the wrong action.
3. Security In voice assistants, security is all about ensuring that only authorized users can access and interact with the system. This includes preventing unauthorized access and ensuring that sensitive data, like voice recordings or personal details, is kept safe. security involves ensuring that the assistant correctly identifies authorized users and prevents unauthorized access to personal data or the execution of commands.
4. Known Vulnerabilities A vulnerability refers to any weakness in the system that can be exploited to bypass security mechanisms or cause unintended behavior. In the case of VAs, vulnerabilities might be technical flaws (e.g., poor voice recognition algorithms, weak authentication processes) or design flaws (e.g., data not being encrypted during storage or transmission). These vulnerabilities expose the system to potential exploitation, which can result in privacy breaches, unauthorized access, or malicious interference.
5. User Experience with respect to Data Privacy: Data privacy is all about being sure your personal information is secure and isn't shared with anyone who should not access it. For

voice assistants, this means keeping things like your voice recordings private and making sure no one gets access to your details, like your calendar or contacts, unless they're authorized. If someone unauthorized can access this information, then your privacy is being violated.

TABLE 1 gives a comparison study on Google Assistant, SIRI, and Alexa based on the parameters mentioned above.

4. EXPERIMENT AND DISCUSSION

With the rapid use of voice assistant in our daily lives, ensuring their security has become a crucial concern. Google Assistant, Siri, and Alexa are the most commonly used AI-driven voice-based assistants, enabling users to perform tasks effortlessly without using their hands. However, these assistants have vulnerabilities related to voice recognition, data privacy, response accuracy, etc. This study aims to analyze their performance through an experimental approach by performing test cases on voice-based assistants and identifying strengths and weaknesses in their security mechanisms. These test insights will play a crucial role in determining their effectiveness and security in real-world use. The observations are shown in TABLE 2.

Test Case-1: Unauthorized Access via Voice Recognition Bypass

Test Description This test evaluates whether the voice assistant grants access or executes commands when prompted by a voice that does not belong to the authorized user, thereby exposing the system to an unauthorized access attack.

Input and Output: When the authorized user (owner) gave the voice command: "Hey Google, what's my name?", the assistant correctly recognized the user and responded with: "Your name is Neha." This confirms that the assistant can execute commands when the owner is speaking, as shown in FIGURE 2 and 3. However, when the same voice command was spoken by an unauthorized person, the assistant still responded with: "Your name is Neha."—despite the voice being different from the enrolled one. This is demonstrated in FIGURE 2 and 3.

Observation and Security Analysis: This test clearly reveals a security vulnerability in the form of weak voice authentication. The assistant fails to distinguish between the voice of the owner and an unauthorized user, thereby allowing unintended access to personal data. This is how this issue affects functionality (perform commands given by unauthorized user) as well as data privacy, as personal information like name or calendar entries may be exposed. While Alexa required the authorized user's voice to respond, Google Assistant and Siri performed commands for unauthorized users during testing. This shows a major gap in voice-based security protocols and falls directly into the 'Unauthorized Access Attacks' category defined in the threat model.

Test Case-2: Data Leakage via Voice History

Test Description This test evaluates whether a voice assistant shows previously provided voice commands (i.e., voice history) without asking for user authentication. If accessible, such data can pose serious privacy threats by exposing sensitive personal interactions to any user with physical access to the device.

Table 1: Comparison of Siri, Google Assistant, and Alexa

Parameters	Siri	Google Assistant	Alexa
Functionality	• Making calls • Managing messages • Controlling gadgets • Seamless Apple integration • Limited third-party support	• Robust online searches • Intelligent home automation • Smooth app connections • Google Nest and Android compatible	• Broad third-party service support • Designed for home automation • Highly versatile for smart homes
Response Accuracy	• Improved but lags behind Google Assistant • Limited web-based search • Relies on Apple's ecosystem	• Extensive Google Search integration • High response accuracy • Strong navigation capabilities • Supports multilingual interactions	• Superior smart home control • Excels in shopping-related tasks • Slightly less proficient in general queries
Security	• On-device processing • Minimal data collection • Most privacy-focused • End-to-end encryption	• Sophisticated safety techniques • Advanced encryption methods • Collects a large amount of user data • Enhances services via data analysis	• Stores voice recordings on Amazon servers • Data can be removed • Raises privacy concerns
Known Vulnerabilities	• Apple security updates • Prevents unauthorized access via voice	• Vulnerable to hostile attacks • Risks in third-party apps • Susceptible to speech recognition flaws	• Vulnerabilities in third-party "Skills" • Risk of accidental eavesdropping • Potential for data leakage
User Experience	• Best for Apple users • Restricted third-party integration • Limited flexibility	• Most intelligent AI experience • Natural conversational interactions • Strong contextual awareness	• Best customization for smart homes • Seamless home automation

Table 2: Security Vulnerability Test Cases for Voice Assistants

Test Case ID	Scenario	Google Assistant (Secured/ Unsecured)	Siri (Secured/ Unsecured)	Alexa (Secured/ Unsecured)	Observation
1	Unauthorized Access via Voice Recognition Bypass	Unsecured	Unsecured	Secured	Google Assistant and Siri are unsecured, but Alexa is secured.
2	Data Leakage via Voice History	Unsecured	Secured	Secured	Google Assistant exposed data, while Siri and Alexa protected it.
3	Activation via Background Audio	Unsecured	Secured	Secured	Google Assistant activated; Siri and Alexa prevented it.
4	Response Accuracy for Complex Queries	Secured	Secured	Secured	All assistants responded accurately.
5	Handling of Sensitive Commands (e.g., Payments, Calls, Smart Home)	Secured	Secured	Secured	Secure execution with confirmation.

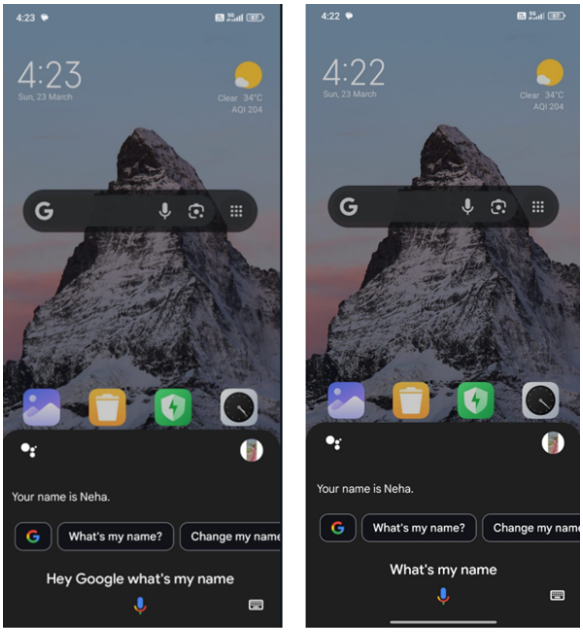

Figure 2: Google Assistant

Figure 3: SIRI

Input and Output: When the command "Show my activity" was given to Google Assistant, it instantly presented a list of previous voice commands, without confirming it with the authorized user (which could be done by asking for a password, PIN or any other type of biometric authentication). This output allowed unauthorized users to view the owner's past communication with the assistant, such as calendar requests, names mentioned, or location-related queries, as shown in FIGURE 4. In contrast, when the same command was issued to Siri and Alexa, both systems prompted the user for authentication (Face ID or device passcode), as shown in FIGURE 4. This additional layer of authentication confirmed that voice history was not visible to unauthorized users.

Observation and Privacy Impact: This test shows a major vulnerability in voice data privacy for Google Assistant. By making voice history accessible without authentication, it breaches the core principles of data protection and user confidentiality. Sometimes, without any voice-match verification, an attacker could use this issue to figure out a user's habits, interests, or even personal events. This is a serious concern and is related to the "Voice Privacy Threats" discussed earlier in the literature. It also supports the reviewer's point that we need to study the risks of data exposure more closely. On the other hand, Siri and Alexa do a better job of protecting voice data because they ask for authentication before giving access.

Test Case-3: Activation via Background Audio

Test Description: This test shows whether voice assistants can be activated by background audio, such as pre-recorded wake words or speech, which could allow attackers to easily activate the assistant without direct voice interaction. This test creates scenarios where an assistant can be accidentally activated by loudspeakers, television, or a public announcement.

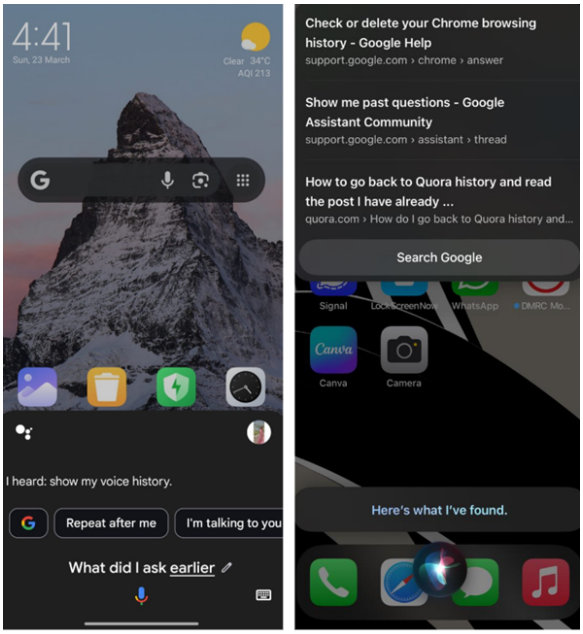

Figure 4: Data leakage via Voice History in Google Assistant and SIRI

Input and Output: A pre-recorded voice clip having the assistant's wake phrase, like "Hey Google," along with a command, was played using a media player, as shown in FIGURE 5. When this audio was played near Google Assistant, the device activated and responded to the command, thereby demonstrating that it could not differentiate between live and recorded voices. In contrast, Siri and Alexa did not respond to the same recorded input under similar testing conditions, showing resistance against such audio-based triggering attempts. The result is depicted in FIGURE 6, where Google Assistant responds, but Siri remains inactive.

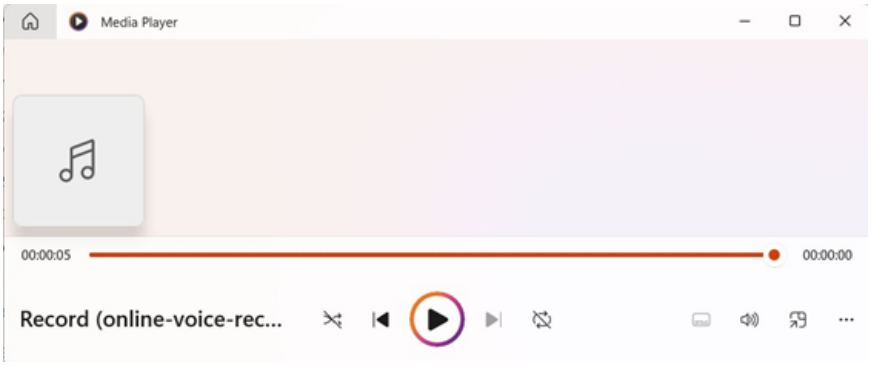

Figure 5: Recorded Voice

Observation and Security Impact: This test highlights a sound-based vulnerability in Google Assistant, where even background or recorded audio can be used to misuse the system. In some situations, voice assistants can be triggered by audio played from everyday devices like speakers

Figure 6: Activation via Background Audio in Google Assistant and SIRI

or televisions. This means that without physically interacting with the device, someone could still get it to respond to commands, for example, sending a message or accessing a calendar, without the user noticing. This becomes even riskier in places like hostels, offices, or cafes, where such things can go unnoticed.

Compared to this, Siri and Alexa seemed more secure. They didn't activate as easily, probably because of better filters or stricter voice checks. This kind of issue fits into what we called "Sound-Based Attacks" in our threat categories and clearly shows why it's important to study these audio-related risks more closely, just like the reviewer suggested.

Test Case-4: Response Accuracy for Queries

Test Description: This test looked at how well voice assistants can understand and respond to everyday questions—like doing simple conversions or answering facts. We wanted to see if they could handle natural, conversational language and still give correct answers.

Input and Output: We asked all three assistants some common questions, like "What's 10 inches in centimeters?" and "What's the capital of France?" Google Assistant and Siri both gave the right answers, and their responses are shown in FIGURE 7. Alexa also got it right, but we couldn't include a screenshot because of privacy settings.

Observations and security impacts: All three assistants did a good job, showing they are pretty dependable for basic info and quick questions. We didn't run into any security issues during this

test. Even though we couldn't show Alexa's answer, it still performed just as well. Getting these kinds of questions right matters a lot—it helps avoid confusion and makes sure tasks aren't

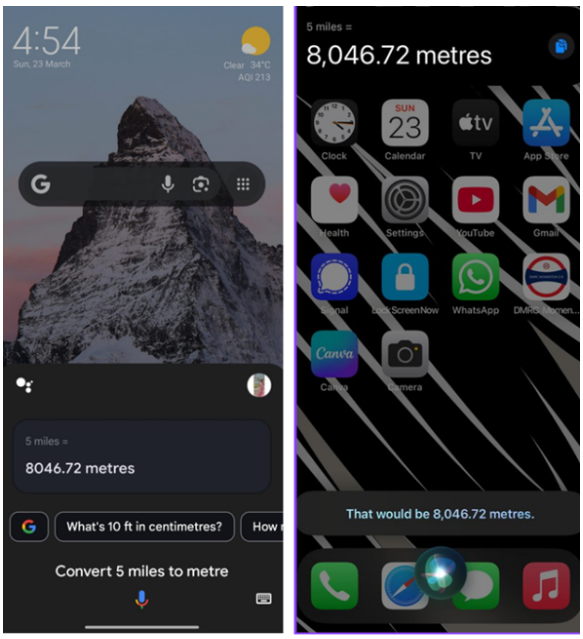

Figure 7: Response Accuracy in Google Assistant and SIRI

Test Case-5: Handling of Sensitive Commands (e.g., Payments)

Test Description: This test looked at how voice assistants handle commands that involve sensitive actions—like sending money or checking your bank balance. The main goal was to see whether they ask for confirmation before carrying out something important.

Input and Output: We tested each assistant with commands like "Send Rupees 100 to Rahul" and "Show my bank balance." In every case, Google Assistant, Siri, and Alexa paused the process and asked for confirmation before continuing. This confirmation came in different forms—such as a fingerprint scan, password, or a simple "Yes" from the user. FIGURE 8 shows how Google Assistant and Siri responded. Alexa followed the same process, but due to privacy restrictions, we couldn't include a screenshot of its response.

Observation and Security Impact: When handling sensitive tasks such as sending money or checking bank balances, each of the three voice assistants responded with extra caution Instead of immediately acting on the command, they paused and asked for some form of confirmation—whether it was a fingerprint, a password, or a simple "yes" from the user. This extra step provided extra security. It made sure that even if an unknown voice tried to make a payment, the assistant wouldn't go through with it without confirming the request. Earlier tests showed that assistants could respond to voices they didn't recognize, but this behaviour shows they're more careful when it comes to tasks that could affect the user's money or safety

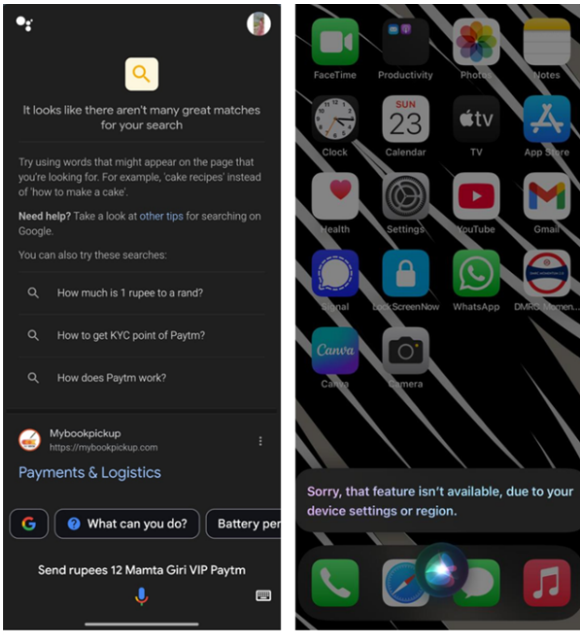

Figure 8: Handling of sensitive commands by Google Assistant and SIRI

5. CONCLUSION

This research explores the vulnerabilities and hence security issues and privacy breaches in Google Assistant, Siri, and Alexa, drawing attention to the risks these AI assistants pose to users. It focuses on real-world scenarios for attack vulnerabilities and their effects on user privacy and data security. This research aimed to identify the three types of attacks that are caused by the vulnerabilities in these voice assistants. The findings showed some serious flaws like *unauthorized access*, *data leaks, and the manipulation of voice commands*—threats that undermine user safety. The research indicates that using these voice assistants for the mundane tasks exposes the users to various threats and risks their data privacy. These flaws underline the serious need for stronger security measures, including multi-layer authentication, real-time threat detection, and AI-powered anomaly detection. Beyond theoretical analysis, the study calls for developers to improve encryption, implement stricter authentication, and raise user awareness to mitigate these risks. With virtual assistants becoming an integral part of daily life, their security is more important than ever. This research aims to inspire better practices in AI development, pushing for safer, more reliable systems and encouraging further exploration in NLP and security testing to strengthen AI protections.

6. LIMITATIONS AND FUTURE WORK

Our study focused on three popular voice assistants—Google Assistant, Siri, and Alexa—and examined how they perform with respect to various features. These assistants are widely used in

everyday devices, making them important to study when looking at privacy and security concerns. However, we didn't include newer or less common voice assistants, like those in tools like Gemini or Microsoft Copilot. These assistants are not widely used in everyday life, they are still relatively new, and many people aren't aware of them . In future, it's important to look at more types of voice assistants as new AI tools keep improving and becoming an important part of our daily lives. Future research work will focus on one or more of the following aspects under the umbrella of Cybersecurity, which indeed is an area that requires more research to protect against and evade the new cyber-attacks :

- Tackling AI-Powered Cyber Threats in Voice Assistants

  As voice assistants like Alexa, Siri, and Google Assistant become a bigger part of everyday life, they're also becoming a bigger target for cyber attacks. Going forward, our research is shifting focus toward how attackers might start using AI to launch more complex threats—especially things like DDoS (Distributed Denial of Service) and MITM (Man-in-the-Middle) attacks. These kinds of attacks can either flood systems to the point of failure or secretly intercept what users are saying. We're looking into smarter ways to detect and block this behavior early, using tools like machine learning and real-time anomaly detection.

- Digging Into the Weak Spots in AI Systems

  Voice assistants depend heavily on AI to understand what we say and decide how to respond. But the more AI is involved, the more important it becomes to understand where the weak points are. Future work will explore how attackers might exploit the algorithms that drive natural language processing or the decision-making systems behind the scenes. It's about finding the cracks before someone else does.

- A Better Security Plan for Voice Assistants

  To really protect these devices, we need more than just patching problems as they come up. We're aiming to create a more complete security approach—one that covers both the voice interface and the AI behind it. That could mean layering defenses, like using AI to automatically detect suspicious traffic or behavior, and making sure the system can respond quickly before things get out of hand.

- Using AI to Defend Against AI

  With hackers starting to use AI to make their attacks smarter and sneakier, it only makes sense to fight back with the same tools. One idea we're exploring is using reinforcement learning so voice assistants can learn how to recognize patterns that look like attacks, like weird traffic spikes, and act accordingly. At the same time, we want to make sure that voice interactions are protected by strong encryption, so even if someone tries to intercept them, they get nothing useful.

- Protecting User Information Protecting user privacy remains one of our top priorities throughout this work. We're especially interested in finding ways to keep personal data safe, even if an attack gets through. That might involve using techniques like differential privacy or secure multi-party computation—basically, ways to protect the data itself, not just the system around it. The goal is simple: even if someone does get in, they walk away empty-handed.

- Testing Real-World Scenarios

Of course, the best way to understand these threats is to simulate them. We're planning to run real-world tests that mimic how DDoS and MITM attacks could hit voice assistants, especially if powered by AI. By watching how these systems respond under pressure, we'll be able to better understand where the vulnerabilities are—and how to fix them.

References

[1] Alepis E, Patsakis C. Monkey Says Monkey Does: Security and Privacy on Voice Assistants. IEEE Access. 2017;5:17841-17851.

[2] Kalhor B, Das S. Evaluating the Security and Privacy Risk Postures of Virtual Assistants. arXiv preprint: https://arxiv.org/pdf/2312.14633. 2023.

[3] Aleksanjan A. Data Protection in the Age of Virtual Personal Assistants PhD Thesis. Ghent Belgium: Ghent University. 2019.

[4] Franco M, Gaggi O, Guidi B, Michienzi A, Palazzi CE. A Decentralised Messaging System Robust Against the Unauthorised Forwarding of Private Content. Future Gener Comput Syst.

[5] Bolton T, Dargahi T, Belguith S, Al-Rakhami MS, Sodhro AH. On the Security and Privacy Challenges of Virtual Assistants. Sensors Basel. 2021;21:2312.

[6] Awojobi B, Landry BJL. An Examination of Factors Determining User Privacy Perceptions of Voice-Based Assistants. Int J Manag Knowl Learn. 2023;12:53-62.

[7] Cheng P, Roedig U. Personal Voice Assistant Security and Privacy—A Survey. Proc IEEE. 2022;110:476-507.

[8] Bispham MK, Agrafiotis I, Goldsmith M. A Taxonomy of Attacks via the Speech Interface. In: Think Third International Conference on Cyber-Technologies and Cyber-Systems CYBER. Mind Digital Library. 2018.

[9] Yan C, Ji X, Wang K, Jiang Q, Jin Z, et al. A Survey on Voice Assistant Security: Attacks and Countermeasures. ACM Comput Surv. 2023;55:1-36.

[10] Zhang N, Mi X, Feng X, Wang XF, Tian Y, et al. Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home. arXiv preprint: https://arxiv.org/pdf/1805.01525v1. 2018.

[11] Haque S, Eberhart Z, Bansal A, McMillan C. Semantic Similarity Metrics for Evaluating Source Code Summarization. In: Proceedings of the 30th IEEE/ACM international conference on program comprehension. New York USA: ACM. 2022:36-47.

[12] Zhang N, Mi X, Feng X, Wang XF, Tian Y, et al. Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. In: IEEE Symposium on Security and Privacy SP. IEEE. 2019:1381-1396.

[13] Kadam AV. Adversarial Attacks on Voice Assistants & Protecting Against Manipulation. Int J Comput Eng and Technol IJCET. 2023;14:163-171.

[14] Chen G, Chenb S, Fan L, Du X, Zhao Z, et al. Who Is Real Bob? Adversarial Attacks on Speaker Recognition Systems. In: IEEE Symposium on Security and Privacy (SP). IEEE. 2021:694-711.

[15] Lei X, Tu GH, Liu AX, Ali K, Li CY, et. al. The Insecurity of Home Digital Voice Assistants– Amazon Alexa as a Case Study. arXiv preprint: https://arxiv.org/pdf/1712.03327

[16] Lei X, Tu GH, Liu AX, Li CY, Xie T. The Insecurity of Home Digital Voice Assistants-Vulnerabilities, Attacks and Countermeasures. In: IEEE conference on communications and network security CNS. IEEE. 2018:1-9.

[17] Hoy MB, Alexa S. Alexa, Siri, Cortana and More: An Introduction to Voice Assistants. Med Ref Serv Q. 2018;37:81-88.