Forensic Examinations of Alexa for Smart Home Privacy and Cybercrime Investigation

Bashaer Aljneibi, Mahra Alameri, Noora Alhashmi, Richard Ikuesan and Farkhund Iqbal
Computing and Applied Intelligence, College of Technological Innovation, Zayed University, Abu Dhabi, UAE

202106480@zu.ac.ae
202110496@zu.ac.ae
202103945@zu.ac.ae
Richard.ikuesan@zu.ac.ae
Farkhund.iqbal@zuac.ae

Abstract: Integrating Internet of Things (IoT) devices into smart homes has necessitated the development of novel strategies to address the difficulties and complexities of cyber-attacks and privacy concerns in the current digital threat landscape. One unaddressed challenge is the lack of clarity of information collected and stored by these IoT devices in smart homes. The data storage process and privacy compliance of smart home appliances, such as security cameras, thermostats, and smart speakers, are examined in this study. More specifically, this study focuses on sensitive data storage and potential breach exposure, including user commands, timestamps, and network traffic logs of these devices. To achieve this, forensic tools were deployed to collect and examine data from gadgets like Google Nest and Amazon Alexa/Echo following an experimental setup. These technologies were used in a hypothetical investigation that intentionally breached a restricted smart home network and replicated criminal activities. The gathered data was examined to determine the proof of the breach and ensure the chain of events. The findings provided a thorough forensic investigation into the potential digital artifacts within the device and exposed prevalent vulnerabilities of IoT ecosystems regarding usage privacy. This study advances the fields of digital forensics and smart home security by offering useful insights and suggestions for improving the security of IoT devices.

Keywords: Internet of things (IoT) forensics, Smart home security, Data storage vulnerabilities, Amazon Alexa, IoT ecosystem vulnerabilities

1. Introduction

Smart home systems have brought a powerful, realistic change for homeowner-occupants: comfort, convenience, and the ability to control their homes effectively. These homes contain interrelated appliances designed to enable occupants to manage different aspects of their surroundings, including lighting, temperature, and security, among others, through smartphone apps, voice recognition, or pre-installed systems. Consequently, where smart homes are already gaining prevalence, they have evolved into vast mini-networks of interconnected IoT systems designed to enhance the overall functionality of everyday living. However, as homes become smarter, the risk of cyber threats, vulnerabilities, and even cyber forensics begins to emerge. Smart home devices, though improving the quality of consumers' lives, can be easily exploited by attackers because of their permanent connection to the internet and often weak protection measures. From security cameras and locks to smart thermostats and light systems, these devices produce enormous data that can prove useful in supervising the behaviour of the residents and potential burglars (Do et al., 2018). Increased demand for protecting this data and privacy and investigating smart home cyberattacks has triggered the emergence of smart home forensics, which deals more with examining artifacts of the smart home environment to detect, analyze, and respond to a security breach.

Smart home forensic analysis has several distinctions from the recognized practice of digital forensics today. The decentralized and heterogeneous nature of computing devices, their various communication protocols, and their interaction with cloud-based services complicate investigations (Olegard, 2020). Also, most internet-connected consumer devices are built with cloud support from third parties for processing, storage, and data mining, which consequently brings an added layer of risks. Therefore, the calls for an overarching forensic model that can handle these issues have emerged louder. Smart home forensics is not only the detection of security breaches but also checking whether there is enough evidence to be used in court. Due to the diverse types of appliances in the smart home, the number of types of attacks is also numerous (Olegard, 2020). Smart home systems can be manipulated by hackers for access to a house, launching DDoS attacks with the help of vulnerable devices, or obtaining other information like live video feeds or people's data. Establishing a connection in such cases goes through different layers of the network and device storage, clearing the data to form the attack. The security and forensic issues of smart homes are, therefore, present a growing challenge that requires urgent attention.

In recent years, a forensic readiness framework has been identified as a proactive way to counter smart homes' security and forensic issues. These frameworks seek to endow smart home systems with the intelligence to automatically record potential forensic data on the occurrence, thereby eliminating investigation delays (Mahmood et al., 2024). Smart home manufacturers can comprehensively address the problem of cyberattacks by incorporating forensic readiness into constructing a smart home. This research intends to uncover the issue and research potential in the smart home forensic context, emphasizing the necessity of an overall framework that meets the security and forensic needs of smart homes. With regard to the current state of smart home technologies, their insecurity, and conventional forensic processes, this research posits an integrated model that helps secure and prepare smart homes for forensic applications (Do et al., 2018). AI, machine learning, and blockchain as part of smart home forensic workflows will also be discussed, as well as the contribution of these solutions and how such tools can be a valuable addition to smart home forensic workflows and enhance the detection and prevention of cyber threats. To the best of the Authors' knowledge, this is the first study to provide a practical insight into the privacy exposure of smart home devices. Furthermore, this study presents an empirical insight into the characteristics of potential digital evidence that could be extracted from a smart home device, justifying the forensic relevance of smart home devices in cybercrime. A synopsis of smart home history, related cybercrime, and a corresponding forensic perspective of smart homes is given in the next section.

2. Background of the Study

This section explores existing studies on smart technologies related to home automation, the corresponding and applicable security threats, and the overall need for a forensic framework towards a proactive security suite in the dynamics of smart technologies.

2.1 Historical Background on Smart Homes

Smart Homes began to evolve through the mid-20th century as technology advanced, giving rise to the X10 protocol in the 1970s. X10 was one of the most significant technologies that permitted electronic devices in a home to interact using the home's electrical wiring. X10 allowed for dimming or switching lights, appliances, or any other system and had drawbacks like unreliability and slow data transfer speed (Philomin et al., 2020). It also paved the way for the later developments of substance to elaborate on the study of changes in the progression of X10. The technology products from the 1980s, such as the Clapper sound-activated electrical switch, were a new technology where users switched their lights and appliances off by clapping. Lacking the complexity of the current technologies, the Clapper attracted consumers with home automation integrated into day-to-day use. It was not until the 1990s that the concept of an interconnected layer was introduced and turned home automation into what it is today. While the basic overviews of smart homes were introduced in the late 20th century, the present age of internet-connected smart homes started with the smart thermostat, followed by garage door openers and security cameras (Surange & Khatri, 2022). These technologies also brought the initial computer security issues into homes, as these new homestead systems were no longer secure from remote intrusion. A new device like the Nest thermostat came into play in the 2000s, and the increased use of smartphones became an important innovation. The combination of Wi-Fi and Bluetooth was more helpful in linking home devices to a base or a smartphone. Specifically, Nest products like the Nest Thermostat exemplified these systems, allowing users to control their home's climate remotely based on their habits, enabling the gadget to set the temperature automatically. This device embodied convenience, energy efficiency, and machine learning that could be incorporated into the home automation solution. In the 2010s, voice-control-based assistants such as Amazon Alexa and Google Assistant became considerably popular because direct control is more natural than using an app or a remote. These technologies introduced home automation to millions of homes; specific devices became controllable by voice command, including lighting, appliances, and security systems (Philomin et al., 2020). New technologies such as augmented reality (AR), virtual reality (VR), and hand gestures offer users a new way to control their homes. In addition, Zigbee, Z-Wave, and Thread have been created to enhance compatibility between devices regardless of the manufacturers, making smart homes more intuitive (Kim et al., 2024).

2.2 Security Attacks Against Smart Homes

Smart homes are highly vulnerable to infotech systems due to multiple IoT devices in the household network. These devices deployed in environments have fundamental protection mechanisms, giving attackers several access points. The Mirai attack is one of the first known smart home attacks that targeted IoT devices for large-scale DDoS attacks (Liu et al., 2022). The Mirai botnet showed that smart devices can easily be exploited to influence other systems outside individual homes. Smart home attacks commonly can be divided into categories: unauthorized access, listening, data leakage, and malware installation. One standard threat model is

unauthorized access obtained by the attacker controlling the devices a home may house, such as cameras, smart locks, or even heating and air conditioning systems, which compromises the safety and privacy of such a home (Surange & Khatri, 2022). Some attacks involve intercepting conversations between devices and, thus, result in data leakage that may contain people's information. Criminals can also use ransomware to make users surrender control of their smart home devices, demanding payment for their return. At the same time, malware allows for complete control of smart home systems, which grants criminals control of other devices (Mazhar et al., 2022). The smart home system is also subjected to internal threats whereby the residents or a service provider with access to a given smart home system engages in malicious activities against the system.

Encryption is the most common type of protection because it guarantees that only the communicating devices can see the information exchange and cannot alter it. Nevertheless, the heterogeneous nature of smart home IoT devices complicates the ability to standardize encryption across all devices (Surange & Khatri, 2022). Apart from encryption, intrusion detection systems (IDS) and firewalls are some of the tools used to protect smart homes from attack. They are used to watch the relationship between the traffic passing through the network and the behaviour of the devices on the same network. In recent years, intrusion detection systems based on machine learning have been implemented in smart home systems to enable real-time detection of cyber-attacks and misuse by seeking patterns that resemble a specific behaviour likely to be an attack (Liu et al., 2022). Some recent solutions have been directed toward implementing blockchain on IoT devices to enhance data security and confidentiality in communication (Kebande et al., 2018). A comparison of these security solutions shows that although IDS systems based on machine learning are very effective in threat identification, they consume many computing resources and may introduce delays, especially for low-power IoT devices (Mazhar et al., 2022). On the other hand, encryption is cheaper and more straightforward in terms of implementation since it does not cover all the possible threats, such as firmware attacks and cloud services attacks. Thus, while using blockchain to improve data reliability and openness is inspiring, the problem has weaknesses.

2.3 Forensic Analysis of Attacks

Smart homes use forensic detection to determine the type of attack and the assailant and to prevent further incidents in the future based on data obtained from smart devices. This entails gathering logs, device memory, and other digital objects left behind by IoT devices. The data that may be found in such artifacts include network logs, system logs, and registry keys. The artifacts provide insight into the activities of the smart home devices and their interactions with other entities. Unlike the more conventional model of forensics, which is aimed at personal computers and servers, the smart home environment is characterized by decentralization. Due to the nature of a smart home, the various devices and operating environment can complicate matters for a forensic investigator. Smart thermostats, security cameras, and door locks produce various data types; the data must be synchronized to recreate an event timeline during an attack (Surange & Khatri, 2022). Furthermore, analyzing and investigating the data source is challenging because IoT data may be overwritten or lost due to limited storage. The Digital Forensic Readiness Framework for Smart Homes highlights the call for anticipatory data capture to capture the proper evidence before a hacker's attack (Philomin et al., 2020). This approach entails programming smart devices to store information in an arrangement that facilitates retrieval when conducting an inquiry, cutting the time needed to search for evidence after an incident. Some other advances have been introduced into analysis in smart homes, especially in machine learning and artificial intelligence. These technologies enable forensic investigators to streamline the data aggregation and analysis process and discern patterns and bulges likely to suggest compromise (Liu et al., 2022). With the help of machine learning algorithms that review traffic flows in networks and devices' behaviours, investigators can define the attacks during the process before significant losses appear.

2.4 Existing Forensic Frameworks for Smart Homes

Due to the high rate at which smart home technology is being implemented, it has become imperative to find specific forensic frameworks that fit the smart home complex systems. Some of the papers have proposed frameworks that can be used to improve digital forensic operations in smart home systems. For example, there are specific frameworks for the IoT regarding the distinct and distributed nature of the devices, such as the Integrated Digital Forensic Investigation Framework (IDFIF-IoT) recently suggested by Kebande et al. (2018). This framework targets a single methodology of gathering digital evidence from various devices, making up an efficient investigation process. Building upon Finkle and Lin's (2018) concept of SDR in SHs, Philomin et al. (2020) put forward a framework that promotes the active acquisition of evidence. This is consistent with the ISO/IEC 27043 Digital Forensics Standard, which contains a structured and planned approach to conducting digital investigations and, therefore, a systematic way to look for digital evidence. This has often become critical,

especially with smart home systems, since data is usually overwritten and, as such, requires timely evidence gathering. Strange and Khatri (2022) also further developed the field, proposing an integrated intelligent IoT forensic framework that uses open-source tools for data acquisition. This framework recognizes the heterogeneity and dynamism of smart home technologies. Therefore, it proposes that forensic frameworks must address the variations in the architecture of these devices and the data they generate. Their work highlights the importance of working on frameworks that would help deal with the many kinds of data from smart home devices for more accessible forensic investigations in ununiform spaces. However, current frameworks also have drawbacks in terms of extensibility and compatibility. The lack of standardization in IoT protocols enables the combining of different forensic tools across different devices. This stands out as the main problem that smart home forensic investigators face. There is one significant difference—the degree to which the framework applies. For instance, Kebande et al. (2018) discuss the overall structure of their framework and the proposal that it must be compatible with other IoT devices. At the same time, Philomin et al. (2020) go one step further in their procedural focus by spelling out the procedures for sound evidence acquisition. This divergence in focus illustrates a broader challenge in forensic frameworks: how to find the middle ground between the encyclopedic approach and its applicability. The other important attribute is usability. The tools in the framework proposed by Surange and Khatri (2022) should be open source, the authors write, as the investigators that may use them often do not have funds for commercial tools. Liu et al. (2022) discuss data acquisition strategies that do not disrupt the smart home environment's functioning. However, the trade-off here is that investigations may suffer from partial data, making it hard to understand what went wrong. This variability suggests that there is a growing need for a methodology on data management that will capture all forms of evidential information while at the same time preserving the integrity of the smart home setting.

3. Related Works

A study by Li et al. (2019) identified that when studying smart home forensic frameworks, devices like Amazon Echo or Google Assistant, for example, are a special challenge because they are tightly integrated into users' lives and complicated ecosystems. As Haack et al. (2017) asserted, complications drawn from popular smart devices such as the Amazon Echo are linked to other smart devices in the IoT, making distinguishing between traditional device-centric and ecosystem-based investigation techniques challenging. Even with the implemented security measures, the Echo collecting personal information could potentially be vulnerable to having its data integrity threatened. This leaves investigators responsible for collecting the required data and ensuring a critical vulnerability does not corrupt them. Akinbi and Berry (2020) explain that devices such as Google Assistant contain a huge amount of personal data, from the logs of interactions to voice commands, as well as deleted records on companion devices like smartphones. This, of course, brings into question and criticizes the extent to which data is being collected and its necessity to be collected for forensic purposes. Building on that, Chung et al. (2017) go a step further with a cloud-native and client-side forensic approach to the like of the Echo, a realization that IoT forensics is no longer about what is on the device. Since the Amazon Echo can communicate directly with Alexa, a cloud-based intelligent virtual assistant (IVA), data has been cached locally and on Amazon's cloud systems. Forensic investigators must chase electronic fingerprints on mobile gadgets such as Alexa. For instance, Alexa learns from the Echo and saves voice inputs to the cloud, making the addition of cloud-based analysis crucial. Chung et al. (2020) present a novel approach: a complex integrated forensic tool (CIFT) that can consider both local and cloud-based devices since investigating ecosystems such as Amazon Echo would be unthinkable only within the local sphere. Technical and privacy issues are not the only considerations closely related to these legal aspects. Contrasting an important privacy aspect and the exigency to have access to data stored by Amazon Echo, Orr and Sanchez (2016) raise the question regarding the admissible evidence of the digital information of an involved party. With time, IoT devices such as the Echo remain part of a user's daily life; the data generated could be the basis of a legal case; however, issues to do with the admissibility of the data, the Fourth Amendment's infringement, and consent are still issues. The IoT forensic frameworks should be technically sound and legally compliant in terms of compliance with legal requirements on privacy rights and ensuring that evidence can be legally obtained from the IoT devices and used in legal processes. Krueger and McKeown (2020) explored the possibility of using Alexa APIs as a source of digital evidence. The data found through Amazon Alexa APIs provided digital evidence from voice interactions to user behaviour, which is integral in any criminal investigation. In addition, the data found through the APIs can be used to clarify timelines in a crime through timestamps, locations, and device IDs. Iqbal et al. (2023) also shed light on user privacy concerns, where third parties and Amazon gather voice commands and metadata from users' interactions with Alexa. Researchers intercepted network traffic to analyze data collection. Those interactions collected are utilized to display targeted ads to the user, increasing advertisement auction bids. The

study continued to develop a framework to measure data collection and sharing, revealing that Amazon synchronizes cookies with advertisers and shares data with third parties. Iqbal et al. (2023) findings stress the requirement for improved transparency in privacy policies and users' ability to control data usage to ensure data privacy and accountability when handling data.

4. Methodology

The methodology followed in this study is shown in the operational framework presented in Figure 1. The framework comprises the set-up phase and three use cases.

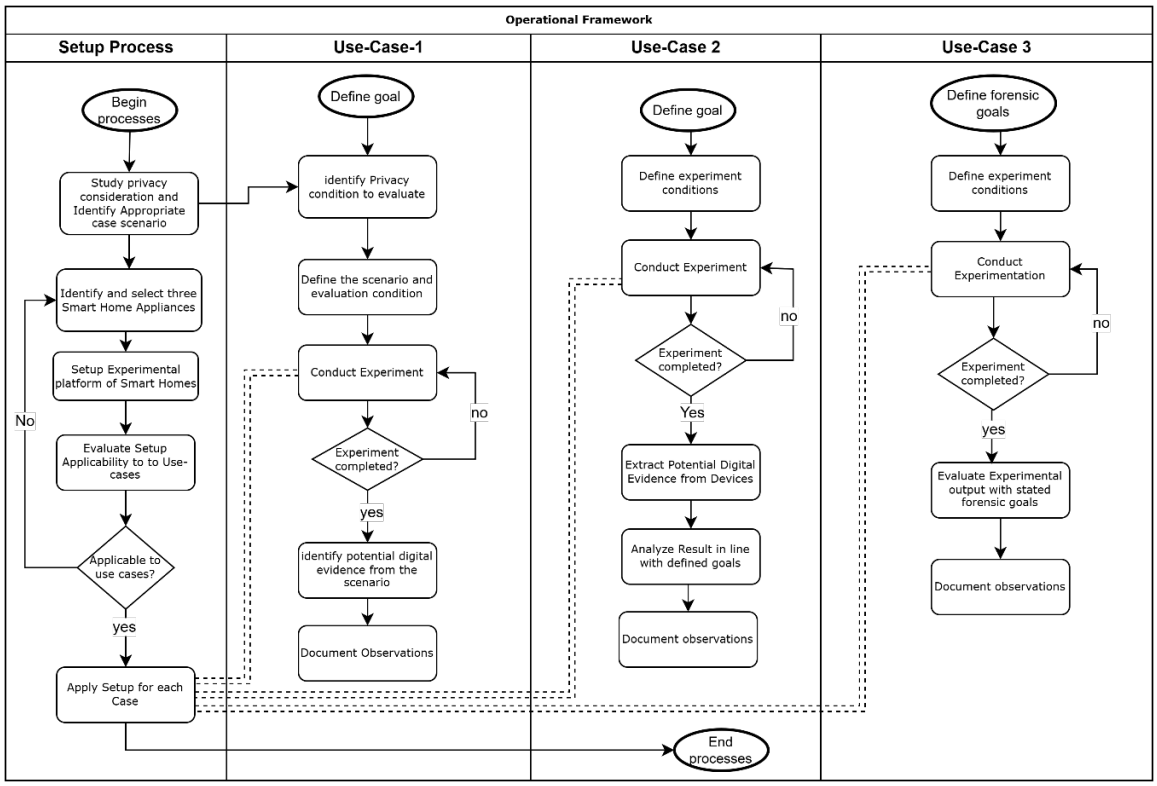

Figure 1: Operational Framework of the Study

Three generations of Alexa smart home devices were set up in a smart lab in the setup process. The details of the devices, including the OS and the corresponding mobile application, are shown in Table 1. The privacy conditions for each device were extracted and studied for onward use in the use-case development process, as highlighted in Figure 1. Details of each process are further presented.

Table 1: Description of tools and devices used

Item	Description
Alexa Echo Dot 3rd Generation	The Alexa Echo Dot 3rd-generation, released in October 2018, comes in a compact circular shape that measures 3.9"x 3.9" x 1.7" and weighs 10.6 oz. 1.6-inch front-firing speaker
Alexa Echo 4th Generation	Alexa Echo 4th generation, released in October 2020, comes in a rounded shape that measures 5.0" x 5.0"x 4.7" in size and weighs 970 grams. Supports 802.11 a/b/g/n/ac (2.4 and 5 GHz) networks. Does not support connecting to ad-hoc (P2P) WiFi networks
Alexa Echo Dot 5th Generation	Alexa Echo Dot 5th generation, released in October 2022, comes in a compact, rounded shape, measures 3.9" x 3.9" x 3.5" in size, and weighs 10.7 oz. 1.73" Front-firing speaker, Lossless High Definition
Connected Phone-1	iPhone 13 Pro Max, Released September 14, 2021, iOS 17.6.1, A15 Bionic, 6-core CPU, 5-core GPU, 6GB RAM,256GB, Screen Size of 6.7 inches, Alpine Green.
Connected Phone-2	iPhone 14, Released September 7, 2022, iOS 18, A15 Bionic, 6-core CPU, 5-core GPU, 6GB RAM,256GB, Screen Size of 6.1 inches, Blue.
Application	Alexa App, AMZN Mobile LL, 381.3 MB, Version 2.2.635412.0

Case 1: The primary digital forensic experiment was designed to test if Alexa devices follow the privacy claim that "they only commence recording when wakened by a wake-up phrase or an actual touch." The methodology involved three key stages: using staged interactions, acquiring evidence from the device, and synchronizing data with the device and associated cloud accounts in search for such cases. Firstly, the study organized several controlled test interactions to evaluate the device's behaviour under different conditions. These include intentional situations consisting of speaking the wake word 'Alexa' or touching the device and unintentional situations where the device was interacted with to capture an authentic comparison between expected and unexpected recordings. The duration of each interaction and accurate timestamps against the device records and voice recordings in the assessment were captured. Afterward, by employing the FTK Imager, a forensic imaging tool, a full image of the storage of an Alexa-enabled device was made. A summary of the process is further depicted in Table 2. This includes viewing logs and associated metadata while maintaining tamper-proof data on the device. In addition, Alexa's voice history was pulled from the linked Amazon account. Alexa records voice interactions and related data on Amazon servers. This step allowed for comparison and differentiation of any data that would be recorded, whether locally or in the cloud. The last step involves the analysis of the gathered forensic image and cloud data, which was carried out using the Autopsy forensic tool.

Table 2: Controlled Interactions and Expected Activations

Interaction ID	Timestamp	Action Taken	Expected Activation	Actual Recording	Privacy Status
001	2024-11-03 10:00:00	Said "Alexa, what's the weather?"	Yes	Yes	Expected recording
002	2024-11-03 10:05:00	No voice/touch interaction	No	No	Privacy claim upheld
003	2024-11-03 10:10:00	Said "Alexa, play music"	Yes	Yes	Expected recording
004	2024-11-03 10:15:00	Background conversation (no wake-up phrase)	No	Yes	Privacy concern noted
005	2024-11-03 10:20:00	Tapped Alexa for settings access	Yes	Yes	Expected recording
006	2024-11-03 10:25:00	Normal background sounds	No	No	Privacy claim upheld

Table 2 shows that 80% of Alexa's interactions adhered to privacy guarantees, recording only when triggered by a wake phrase or touch. However, in 20% of situations, Alexa made unintentional recordings, such as during background conversations, without being explicitly activated. This poses concerns about the device accidentally activating and capturing audio when not authorized. However, this also implies that Alex could be used as a potential witness in a crime scene where voice-based evidence is required. Furthermore, the information transmitted to the cloud application is presented in Table 3.

Table 3: Alexa Voice History from Cloud Account

Recording ID	Timestamp	Recorded Content	Activation Method	Privacy Status
RH001	2024-11-03 10:00:00	"What's the weather?"	Voice wake word	Expected recording
RH002	2024-11-03 10:10:00	"Play music"	Voice wake word	Expected recording
RH003	2024-11-03 10:15:00	Background conversation	None (no activation)	Privacy concern noted
RH004	2024-11-03 10:20:00	"Settings access"	Tap	Expected recording

Table 3 shows that these unintentional recordings were also transferred to the cloud, storing private conversations without the user's permission. While most predicted recordings matched the wake word, undesired data in the cloud reveals flaws in Alexa's capacity to maintain privacy, posing a danger to user data security.

Case 2: This study set out to determine whether Alexa retains user commands, how long the commands are retained, where the data is stored, and whether command deletion influences the data retention period. This experiment was to be performed for 32 days with the command given, its availability, storage locations, and performance after deletion taken at 8-day intervals. It started with four commands given to the Alexa device on Day 1 of the experiment. The commands were, for instance, “play music,” “set an alarm,” “What is the weather like?” and "Turn off lights." Every command was written down in the logbook so that the command could easily be recalled. Subsequent to these commands’ implementation, an evaluation of both local application storage and cloud storage was conducted initially. After the first day, the respondents positively confirmed that all four commands remained accessible, therefore achieving a retention rate of 100%. As the study progressed, data collection continued at specified intervals: A new course of treatment should be recalled as 8-day Treatment, 16-day.

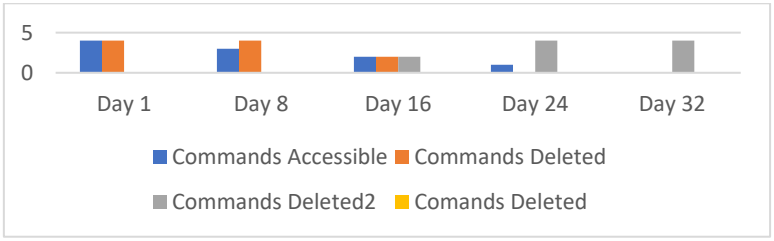

Figure 2: Command Accessible, Commands found Post-Deletion, Commands Deleted Permanently

Treatment, 24-day Treatment, and 32-day Treatment. Thus, at each interval, the availability of the previously issued commands was assessed using the mobile app and the FTK Imager and Autopsy tools. The data collected included the number of commands and details such as how many remain available to the users, those commands’ usage retention rates, and where their records were stored, either locally within the app or in the cloud. Two of the commands given earlier were intentionally removed from the Alexa app to investigate the effects of command deletion on data retention on Day 16. Further efforts to recall the deleted commands were made on Day 24, with an additional trial on Day 32 to determine how many commands remained visible after the deletion commands and the efficiency of this technique. Forensic analysis tools were used to determine the storage locations of commands and flux and establish their storage type. The lifespan of given commands is depicted in Figure 2, emphasizing deletion status, post-deletion retrieval, and command accessibility. All commands are initially recoverable and available, and none are erased. As the retention rate declines over the next several days, command accessibility progressively declines as more commands are removed or rendered inaccessible. Instructions discovered after deletion also diminish over time, demonstrating that while certain commands may be recovered, the retrieval rate falls with increasing time, indicating more stringent adherence to deletion procedures.

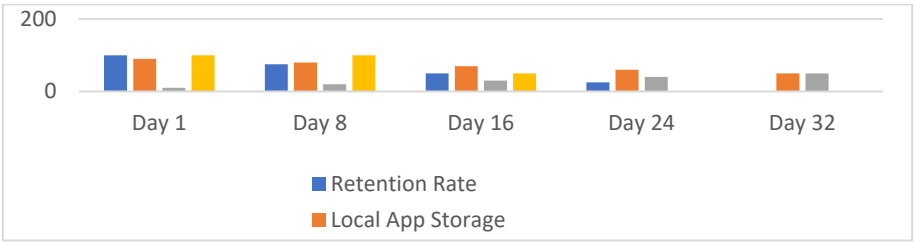

Figure 3: Retention Rate (%), Local App Storage (%), Cloud Storage (%), Retrieval Rate Post-Deletion (%)

The availability of all commands given to the device on Day 1 was 100% retention, which proves that the device stores user interactions. However, as the study extended to Days 8, 16, 24, and 32, the overall command accessibility diminished, and the retention rates reached zero by Day 32. This implies that commands might not remain perpetually in local application storage, as the changing percentages hinted at cloud storage. Commands were deleted deliberately on Day 16 to show the effect of user activity, and the number of commands that could be recovered decreased to a bare minimum.

Case 3: The investigation sought to examine the efficiency of Alexa’s command deletion process and attempt to discover whether these commands could be retraced utilizing digital forensic techniques. The experiment was conducted under restricted conditions utilizing an Amazon Alexa device and the Alexa app on a mobile device. First, commands were made to the Alexa device and voice calls, including announcing a song, setting an alarm, asking about the climate, and switching off lights. Instructions given at each time point were recorded so that a

similar experiment may be repeated as an affirmation of sanity. After the commands were given, the user used the Alexa app to clear the commands from the history list. This deletion process entailed going to the command history part of this app and typing delete to erase the entries. Following the deletion of commands, a cyber forensic action was taken through cyber forensic utilities, including FTK Imager and Autopsy. Due to the task expected in this analysis, deleted commands and the possibility of recovering information in the mobile device's local app storage were investigated. After performing the recovery assessment, the details collected were grouped based on the command type, whether it had been deleted/found, the type of command, such as text command, voice, log entry, and the location and duration of storage. This was achieved through careful documentation of each category to inform further analysis. The result of this process is presented in Table 4. It reveals the investigation's discovery and presents an aggregated summary of data retention and an analysis of the efficiency of the deletion process. This methodological approach attempted to evaluate the validity of the removal process in Alexa's command deletion, concluding the concerns for user privacy and data erasure in smart technology usage.

Table 4: Command Deletion Investigation

Command Issued	Deleted (Yes/No)	Recovery Status	Data Type	Storage Location	Storage Duration (Days)	Recovery Method
Play music	Yes	Found	Text Command	Local App Storage	16	Forensic analysis via Autopsy
Set alarm	Yes	Found	Text Command	Local App Storage	16	Forensic analysis via Autopsy
What's the weather?	Yes	Not Found	Voice Recording	Local App Storage	undetermined	N/A
Turn off lights	Yes	Found	Log Entry	Local App Storage	16	Forensic analysis via Autopsy
Play music	No	Found	Text Command	Local App Storage	32	Forensic analysis via Autopsy
Set alarm	No	Found	Text Command	Local App Storage	32	Forensic analysis via Autopsy
What's the weather?	No	Found	Voice Recording	Local App Storage	32	Forensic analysis via Autopsy
Turn off lights	No	Found	Log Entry	Local App Storage	32	Forensic analysis via Autopsy

As shown in Table 4, the findings from the investigation of Alexa's command deletion mechanism reveal that significant details of the deleted commands can be recovered. Furthermore, 75% of the instructions were recoverable despite being destroyed, showing substantial gaps in the deletion process. The result further shows unrecoverable deletion results for the "What is the weather?" voice command. Four of the eight commands issued were deleted, while data from three was recovered through forensic analysis, meaning that the app saves data even when the user deletes it. The result also shows a common storage – Local App Storage – suggesting that it is sustained as the main approach to data storage. Moreover, the storage durations of 16 days for deleted commands and 32 days for non-deleted commands indicate that data can remain persistent for extended periods beyond the assumed period. This can include sensitive information, thus indicating that deleted processes do not necessarily provide secure solutions.

5. Discussion

Accordingly, an evaluation of Alexa's behaviour helped determine that 80 percent of the captured interactions were consistent with the device's privacy assertion. The recordings were performed only when the device was activated verbally or by touching the gadget. However, in 20% of the cases, the Alexa device picked up what was being said in the background without users' awareness and consent, which poses a real question regarding how private the conversations are with Alexa. These unintended captures are also deposited in the Alexa Voice History, meaning the gadget does not always honour its declared privacy measures. The data show an important contradiction in how Alexa works, stating that most interactions align with Alexa's privacy statement and that

they never listen in. However, they also find that Alexa might listen in on families when it is meant to record a wake phrase. This finding is supported by prior studies that have revealed that voice-activated devices may sometimes accidentally record sounds or background noise as activation commands. Therefore, the existence of such unexpected recordings means there is a need for better technologies to increase reliability and protect users' privacy. These findings align with the research goal of employing digital forensics to validate Alexa's privacy concerns. Thus, the analysis of participants' responses indicates that some recordings were made even without activation while using Alexa. This difference underlines the indispensability of continuously reviewing and improving voice recognition technology, mainly in realizing how various background noises result in unintentional recording. The information obtained during this forensic inspection prompts questions as to the effectiveness of anonymity statements of wise devices, the need for further technology, and the development of clear high-tech boundaries.

The results of this experiment call into question some of the storage mechanisms in Alexa and how user commands are dealt with in the long term. The first idea that all the commands given were fully navigated encourages the discussion about Alexa's purpose in remembering users' interactions for convenience. However, the subsequent lower frequency of commands increases the question of their storage time in isolated interactions. Commands reduced to 0% accessibility by Day 32; this shows that although Alexa stores commands in their database, this data is only saved for a certain period and can be very helpful in showing the timeline of a command's accessibility within the Alexa database. Furthermore, the change of data storage from app local to cloud also suggests that users need to know where their data goes and how it is dealt with. The experiment showed that even though some percentages of data were kept in the cloud, the constant use of this approach over time threatens data confidentiality and integrity. The removal of commands brought an additional challenge to the image analysis. Even when it comes to deletion, users are the ones who directly delete the information, as the retrieval rate follows a steep decline after the deletion. Although users seem to appreciate the option of erasing their commands, the presence of this option was proven to lead to the loss of material that may be important or useful for further work. Such observation would have important implications for user ownership of their data and clarity of the data management strategies being implemented by smart devices.

6. Future Studies and Recommendations

Future research should ascertain users' awareness and attitudes toward data storage in voice-activated gadgets like Alexa. Research could focus on whether information campaigns could make users aware of durations for data retention, data storage, and the consequences of command deletion. Furthermore, it would be useful to compare the smart device manufacturers' privacy policies and security systems' approaches and viewpoints regarding perceptions of privacy concerns. The improvement recommendations for manufacturers presented in the work are increasing user transparency for commanding storage management, enforcing better data erasure, and providing proper information for further data utilization. Future research should extend this study by including other smart voice assistants, including Google Assistant and Apple Siri, to compare command deletion and data retention policies comprehensively. Moreover, market analysis—risking particular attention to the concerns related to data retention and potential threats connected with residual data—is essential. The relationships among technology developers, privacy activists, and policymakers may produce comprehensive rules that protect user rights in the data storage processes, enhancing the secure and reliable smart technology.

References

2022 Echo Dot 5th Gen Smart Speaker | Charcoal | Amazon. (2024). Amazon.com. https://www.amazon.com/dp/B09B8V1LZ3?ref=ods_ucc_aucc_co_rc_nd_ED_rc_nd_ucc&th=1

Akinbi, A., & Berry, T. (2020). Forensic Investigation of Google Assistant. *SN Computer Science*, 1(272). https://doi.org/10.1007/s42979-020-00285-x

Amazon Echo Dot (3rd Gen). (2024). Amazon.com. https://www.amazon.com/dp/b07fz8s74r#tech

Chung, H., Park, J., & Lee, S. (2017). Digital forensic approaches for Amazon Alexa ecosystem. *DFRWS USA 2017*.

Do, Q., Martini, B., & Choo, K. K. R. (2018). Cyber-physical systems information gathering: A smart home case study. *Computer Networks*, *138*, 1-12.

Echo (4th generation) | Smart speaker with premium sound, smart home hub, and Alexa (Arabic or English). (2024). Amazon.ae. https://www.amazon.ae/dp/B093R3XF9B?ref=ppx_yo2ov_dt_b_fed_asin_title&th=1#tech

Haack, W., Severance, M., Wallace, M., & Wohlwend, J. (2017). Security Analysis of the Amazon Echo. *Proceedings of DFRWS USA 2017*.

Iqbal, U., Pouneh Nikkhah Bahrami, Rahmadi Trimananda, Chen, H., Gamero-Garrido, A., DuBois, D. L., Choffnes, D., Athina Markopoulou, Roesner, F., & Shafiq, Z. (2023). Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem. *ArXiv (Cornell University)*. https://doi.org/10.1145/3618257.3624803

Kebande, V. R., Karie, N. M., Michael, A., Malapane, S., Kigwana, I., Venter, H. S., & Wario, R. D. (2018, August). Towards an integrated digital forensic investigation framework for an IoT-based ecosystem. In *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)* (pp. 93-98). IEEE.

Kim, S., Bang, J., & Shon, T. (2024). Forensic Analysis for Cybersecurity of Smart Home Environments with Smart Wallpads. *Electronics*, *13*(14), 2827.

Krueger, C., & McKeown, S. (2020, June 1). *Using Amazon Alexa APIs as a Source of Digital Evidence*. IEEE Xplore. https://doi.org/10.1109/CyberSecurity49315.2020.9138849

Li, S., Choo, K. -K. R., Sun, Q., Buchanan, W. J., & Cao, J. (2019). "IoT Forensics: Amazon Echo as a Use Case," *IEEE Internet of Things Journal*, 6(4), 6487-6497. https://doi.org/10.1109/JIOT.2019.2906946

Liu, X., Fu, X., Du, X., Luo, B., & Guizani, M. (2022). Machine Learning-Based Non-Intrusive Digital Forensic Service for Smart Homes. *IEEE Transactions on Network and Service Management*, *20*(2), 945-960.

Mahmood, H., Arshad, M., Ahmed, I., Fatima, S., & ur Rehman, H. (2024). Comparative study of IoT forensic frameworks. *Forensic Science International: Digital Investigation*, *49*, 301748.

Mazhar, M. S., Saleem, Y., Almogren, A., Arshad, J., Jaffery, M. H., Rehman, A. U., ... & Hamam, H. (2022). Forensic analysis on Internet of Things (IoT) device using machine-to-machine (M2M) framework. *Electronics*, *11*(7), 1126.

Olegård, J. (2020). Security & Forensic Analysis of an Internet of Things Smart Home Ecosystem.

Orr, D. A., & Sanchez, L. (2016). "Alexa, did you get that? Determining the evidentiary value of data stored by the Amazon® Echo." *Journal of Digital Forensics*.

Philomin, S., Singh, A., Ikuesan, A., & Venter, H. (2020, March). Digital forensic readiness framework for smart homes. In *International conference on cyber warfare and security* (pp. 627-XVIII). Academic Conferences International Limited.

Surange, G., & Khatri, P. (2022). Integrated intelligent IOT forensic framework for data acquisition through open-source tools. *International Journal of Information Technology*, *14*(6), 3011-3018.