ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 9, September 2022

Forensic Data Analysis using the Case Studies on Anti Forensic Devices

[1] Kavya P, [2] Keerthi G Ganiga, [3] Chethana L, [4] Amber Srivatsava,
[5] Dasari Venkata Siva Surya Kumar, [6] Dr Pooja Nayak S

Email: [1] kavyatmk2001@gmail.com, [2] keerthigganiga@gmail.com, [3] chethana0410@gmail.com,
[4] ambersrivatsava19@gmail.com, [5] surya.1dt19is036@gmail.com, [6] pooja-ise@gmail.com

Abstract*— Individuals' interactions with machines would change. The technology which started with using buttons have developed to the touchpad screen, which allows people to control devices. merely conversing with them Intelligent house assistants (IHAs), which allow customers to manage their smart devices, read their mail, and occasionally place orders, are becoming increasingly popular. As a result, it's possible that they'll be discovered at a crime scene shortly for this reason. and are capable of carrying the weight of digital evidence. This research looked into the most famous Alexa Echo and Google Home devices. Documentation was uncovered when this came to forensic research and evidence that made up metadata. Then, by fabricating operations, Changing the device's name, establishing a bogus routine, and so on talent improvement on an individual basis. As a result of the research, cyber defence experts and professors working in this field were given information on the several sorts the digital evidence that can be found in home automation system acts. Anti-forensic was also used to elicit the distinction between actual and false activities.

***Index Terms*— IoT Forensics, Alexa, Google Assistant, and Anti Forensic, Fake activity**

I. INTRODUCTION

Forensic analysis of data is a type of forensic data analysis (FDA). It investigates organized information in the context of fraudulent activity. The purpose is to identify and evaluate patterns of fraudulent behaviour. Information acquired from application systems or their accompanying data warehouses is referred to as organised data.

Mankind have invented opportunities for connecting via technology in history. People began using floppy disks and QWERT keyboards, and today's virtual assistants, such as Google Assistant, Amazon Alexa, Siri, and Cortana, use touch screens with spoken commands.

IVAs (intelligent virtual assistants) have ushered in a new era in which you may ask a technology the same queries you would a human. Chatbots, which seem to be software agents which can converse with users via text or speech, gave birth to IVAs. System logs are found in many modern electronic devices, including cameras, drones, and automobiles. For forensic investigations, these are valuable assets. It's not just about technology. It makes people's lives easier, but criminals also utilize it for anti-social purposes.

As a result, cyber security specialists are concerned should act first to safeguard those who are innocent. The Echo Plus 2nd Generation digital speakers has been linked with Amazon Alexa., while Google Assistant has been paired with the Google Home Mini smart speaker are checked to see if there is any digital evidence. Anti-forensic scenarios were generated and compared [1] to the electronic data in the first section. We now have central control of gadgets in the palm of our hands thanks to the Internet of Things. The IoT's powerful monitoring and reactive characteristics have ensured that the automation runs smoothly. All of these characteristics have contributed to boosting the work's efficiency. As a result, we've saved time.

II. BACKGROUND

A smart speaker is a speaker with an integrated microphone that allows users to use their voice to interact with other smart devices or internet services. The virtual assistant is the brain behind the smart speaker's intelligence. A virtual assistant is a software service that takes the user's voice as input, recognizes a command or query, communicates with other services if needed, and responds with a spoken response. To activate a virtual assistant, users use a wake-up expression such as Alexa or OK Google. Smart speaker microphones are turned on indefinitely unless users turn them off in order to identify wake-up expressions. When the smart speaker begins recording voice data, the device turns on a light to alert consumers.

Virtual assistants are built-in smart devices that accept vocal input, transform it to text, apply natural language processing (NLP)

to the text, take action, and answer to the user with an instructional voice clip. They can take advantage of Embedded applications, such as smart homes, to operate them, order items from afar, and transmit money. Smart speakers differ from traditional computers in that they do not have a graphical user interface (GUI). Therefore, devices are always listening to the surroundings till the user speaks specific wake-up phrases to turn on the voice assistants.

Through Intelligent virtual assistants (IVAs) you may ask a computer question and have it done chores as if it were a human. For instance, "Hey, can you tell me what's on my

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 9, September 2022

to-do list for today?" upon waking up, till “Turn out the bedroom lights” before going to sleep. Such interactions should, in theory, be limited to only you and the equipment aiding you. But are they really? How can you be certain?

As per current news reports, famous voice-activated assistants such as Voice Assistants, Apple's Siri, and Voice Commands aren't necessarily trustworthy.

Alexa has skills, while Google Assistant has actions, in order to fulfil user commands. More abilities or actions signify more capability in this type of equipment. Both offer development kits for developers, and both have nearly identical skills and actions. The number of smart speaker units sold is growing at an[2] exponential rate. Between 2016 and 2018, global smart speaker unit sales climbed 8.5 times, from 4.2 million to 38.5 million, according to a survey. According to a report by research firm Arizton, the smart speaker market was worth $991 million in 2016 and would be worth $4.8 billion in 2022.

III. RELATED WORKS

There've been research into Forensic analysis and voice assistants. The phrase "wake up" causes voice assistants to respond to its surroundings once they encounter it. A study is currently underway to determine if Siri, the voice assistant, should respond to the surrounding till the wake-up words or record it all in order to interpret data. They used network forensic techniques for 21 days. The information was transmitted in an encrypted format. They cannot really find any evidence that Siri is always monitoring. Another study's scope includes cloud-based infrastructure testing, voice recognition evaluations, application assessment, and hardware assessment. The idea was to draw attention to Alexa's Flaws.

As a result, they discovered that Alexa records environmental sounds even if the speech has no significance, noises upon listening wake-up phrases Crime investigation strategies of home automation system are being researched. Researchers looked into the Echo Dot using Alexa and discovered evidence. To identify Alexa's API, they first looked at network traffic statistics. Then they make a request for proof to be gathered. They discover activity logs, personal information, and other items.

As a conclusion, they created a fictional device because of this.

"Skill squatting attacks" is the name of a study about Alexa vulnerability that emphasises on command tone. They tested 11.460 American English phrases to see how many mistakes Smart speaker had. They attacked with these remarks after recognizing there was a systematic misunderstanding on Alexa. This form of attack was dubbed "skill squatting attacks" [9]. In general, one susceptibility research report that used Amazon Voice commands to order something fake and automatically open a door. Many forensic tests on voice assistants, according to the researchers, were theoretically sound. They demonstrated that there have been various studies on the Amazon Echo voice assistant and Digital forensics Z-wave protocol in practise, and also underlined those academics should pay attention to the problem.

IV. METHOD

In this study, the methodology was set up to generate information. The LG ThinQ Q7 smartphone with model number LM-G710EM and Android 8.0.0 is utilised. With their Android mobile applications, Google Home Mini H0A and Amazon Alexa Echo Plus 2nd Generation L9D29R were employed as voice assistance in the smart home setting. The Google Home program was updated to version 2.11.1.8, and Amazon Alexa was updated [3] to version 2.2.271281.0. In Turkey, the Alexa Voice app doesn't really function. As a result, the United States has been included in the Google Play account settings. The GE C-Life Digital Bulb A19 is seamlessly connected to google Voice Assistant Mini, while the SENGLED bulb R11-G13 was actually provided to Echo.

Alexa Service were developed with the help of Amazon Web Services Lambda functions and the Alexa Skills Kit. In order to construct a false activity, a node.js intent code was built. When a user requests the total of two numbers, Alexa responds by multiplying the two numbers. Using Google Dialog Flow Fulfilment inline editor, Google Actions for the same capability were created.

Four commands were made to Voice Assistant of google and Alexa for the crime site. The cases are listed in Table 1 along with their information.

TABLE I

Cases	Command	Comm and Type	First Case	Expect ed Result	Actual Result
1	Switch on the light	Everyday	Lights turned off	Lights turned on	Lights turned on
2	Switch on the horse	Device Renamed	Lights turned off	Lights turned on	Lights turned on
3	Switch on the TV	Customized Routine	Lights turned off	Lights turned on	Lights turned on
4	“Fake activity”, “Add 5 and 6”	Skill/ Action	-	Add	Multiply

In the very first case, one client instructs voice assistants to “Switch on light”. This is how smart home devices are used on a regular basis. As a result, this case was used as a benchmark against which other instances were compared.

The Anti-Forensic is using the other instances to deceive forensic investigators. In the later case, the item's renamed from "light" to "horse," and both voice assistants received the command "turn on horse."

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 9, September 2022

In the third case, the protocol was created. As with everyday activities, the protocol sentence's event handler was made to "Turn on TV," the protocol action was made to "Turn on the light," as well as the protocols response was made as "Ok." Dual devices were then given the message "Turn on TV."

The final case included creating custom abilities utilising developer tools between both device types. For the aggregate goal of two integers, a multiplying reaction was built. The "Add 5 and 4" commands are given for those devices first, followed by the invocation word. Your activities are tracked by both the Alexa and google Assistant. For the four examples, these action histories were found in the consumer privacy menu that appears; after clicking this, programmes navigate to website pages.

V. EVALUATION

As a consequence of the first "turn on lights" daily case, the physical evidence was found in Alexa & Google Assistant's trace. Tables II and III exhibit the activity details for Google Assistant and Alexa, respectively.

TABLE II

Google Assistant History	"Turn on Lights" Command
User Instruction's Text	Said turn on lights
User Command's audio Recording	Play Button to Listen Recording
Time stamp	Today at 1:18 PM
Assistant's Response	Ok, turning the Light on.
Type of device	Smart Speaker
Approximate Location of Device	Google Map Image
Started By	Hot word
sort of action	com. google. home automation

TABLE III

Alexa History	"Turn on Lights" Command
User Instruction's Text	"Turn on light"
User Command's audio Recording	Play Button to Listen Recording
Time stamp	Today at 02:07 PM
Assistant's Reaction	"ok"
Device Name	<user>'s Echo Plus

Both activity logs include the customer instruction text, its audio recording, meta data, and the supervisor's reply were included in activity history. Alexa just retains the device name, whereas Google saves the parameter type, like Google Home and maybe Android App. Google retains the device's approximate location, who initiated its action, and the sort of activity in contrast to Alexa.

In the second example, the device names in both mobile applications were altered from "light" to "horse" to deceive the forensic investigator. As a result, there was no difference in activity history for the second case activity between the daily case and this instance. If indeed the operator did not update the device's id or name, the forensic investigator should utilize a mobile application to record device names in order to figure out what horse it is.

In the third scenario, the activity history recordings of the constructed routine command differed from the daily activity history. Despite the fact that it was specified in both activity histories, the agent's reaction was not included. The forensic investigators' hint is this. They should carefully note all of the routines at this time.

The latest instance's activity start history for custom actions and skills was identical to the daily case. The purpose activity records of Google Assistant were distinct from the daily scenario, the operator command's audio recording and the agent's reaction were both absent from the activity recording in this example. In Alexa's activity history, there was no missing segment, as was the case on a daily basis. The only indication for the forensic investigators. At this stage is Google Assistant's history. Criminals can construct anti-forensic false activities for the Alexa part.

Both products require cloud computing to store user data in order to develop their products, and they must provide this data to customers in a legible format in order to comply with GDPR. As a result, the lives of forensic investigators are considerably easier.

VI. CONCLUSION

Based on the amount of unit demand in the market and forensic examination, the Amazon Echo and Google Home Mini smart speakers were chosen for this study. To deceive forensic investigators, everyday user commands were sent against both devices, and their activity was recorded. This was then compared to anti-forensic false actions such as changing device names, generating routines, and constructing bespoke skills. Activity histories revealed clues and weaknesses in several circumstances.

By making unreasonable requests with modified abilities or actions, users can perform various activities and create phone activity history records. Alexa and the Google Assistant team can conduct preventative research.

The field of smart assistant forensic analysis is quite new. Although the study was conducted on Android smartphones, it is clear that there is no difference between the two platforms because both apps use the web browser to store activity history. Because all data is uploaded to cloud servers, criminal experts really had no way of obtaining an image of the device for analysis, but they can request this information from Amazon and Google.

REFERENCES

[1] D. Lillis, B. A. Becker, T. O'Sullivan and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," in the 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, FL, USA, 2016

[2] D. Lillis, B. A. Becker, T. O'Sullivan and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," in the 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, FL, USA, 2016. [2] B. Kinsella, "There are Now More Than 70,000 Alexa Skills Worldwide, Amazon Announces 25 Top Skills of 2018," 14 12 2018. [Online]. Available: https://voicebot.ai/2018/12/14/there-are-nowmore-than-70000-alexa-skills-worldwide-amazon-announces-25-topskills-of-2018/. [Accessed 06 06 2019].

[3] "Google Assistant Actions Total 4,253 in January 2019, Up 2.5x in Past Year but 7.5% the Total Number Alexa Skills in U.S.," 15 02 2019. [Online]. Available: https://voicebot.ai/2019/02/15/googleassistant-actions-total-4253-in-january-2019-up-2-5x-in-past-yearbut-7-5-the-total-number-alexa-skills-in-u-s/. [Accessed 06 06 2019].

[4] B. Kinsella, "Amazon Increases Global Smart Speaker Sales Share in Q4 2018, While Google Rise Narrows the Gap and Apple Declines," 20 02 2019. [Online]. Available: https://voicebot.ai/2019/02/20/amazon-increases-global-smart speaker-sales-share-in-q4-2018-while-googles-rise-narrows-the-gapand-apple-declines/. [Accessed 02 06 2019].

[5] Arizton, "Arizton Says Smart Speaker Market $4.8 Billion in 2022 - Voicebot," 4 1 2018. [Online]. Available: https://voicebot.ai/2018/01/04/arizton-says-smart-speaker-market-4- 8-billion-2022. [Accessed 5 5 2019].

[6] M. Ford and W. Palmer, "Alexa, are you listening to me? An analysis of Alexa voice service network traffic," Personal and Ubiquitous Computing 23(1), pp. 1-13, Temmuz 2018.

[7] H. Chung, M. Iorga, J. Voas and S. Lee, "“Alexa, Can I Trust You?”," Computer 50, pp. 100-104, 2017.

[8] J. P. S. L. Hyunji Chung, "Digital forensic approaches for Amazon Alexa ecosystem," Digital Investigation Volume 22, Supplement, pp. Pages S15-S25, August 2017.

[9] D. Kumar, R. Paccagnella, P. Murley, E. Hennenfent, J. Mason, A. Bates and M. Bailey, "Skill squatting attacks on amazon alexa," SEC'18 Proceedings of the 27th USENIX Conference on Security Symposium, pp. 33-47, 2018.