Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

A case study on the use of Amazon visual ID facial recognition metadata in investigation

Scott Lorenz[a], Stanley Stinehour[a], Anitha Chennamaneni[b,*], Abdul Subhani[a], Mohammad Nadim[b]

[a] Centex Technologies, Killeen, Texas 76549, USA
[b] Texas A&M University - Central Texas, Killeen, Texas 76549, USA

HIGHLIGHTS

- Demonstrated how forensic examiners can extract data from Amazon IoT devices using Visual ID technology.
- Identified the devices in the study and described the types of evidence and human presence indicators involved.
- Detailed nondestructive methods for carefully disassembling devices and obtaining forensically sound physical images.
- Demonstrated the Amazon IoT devices' ability to collect and store data locally, without needing an internet connection.
- Provided insights on using IoT device data in investigations, focusing on forensic extraction and metadata analysis.

ARTICLE INFO

Keywords:
Digital forensic
Forensic analysis
Internet of things

ABSTRACT

Crime investigators rely on gathering and synthesizing information from various sources to reconstruct events and identify criminal activities. Internet of Things (IoT) devices can play a pivotal role in these efforts by capturing events that transpire before, during, and after a crime. However, extracting and analyzing data from IoT devices can be complex without prior technical knowledge and clear procedural guidance. In this case study paper, we outline the methodology for configuring Amazon IoT devices within a controlled laboratory environment to facilitate data collection. We demonstrate how forensic examiners and crime investigators can retrieve data and utilize it in investigations using Amazon IoT hardware and Visual Identification (Visual ID) technology. Specifically, data from Amazon IoT devices such as the Amazon Echo Show can autonomously log human presence without direct interaction, providing critical insights. This extracted information offers valuable evidence to more precisely reconstruct events for investigations.

1. Introduction

The Internet of Things (IoT) is now becoming a key part of our daily life by providing smart and connected devices. These devices play a major role in advancing digitalization, with applications that extend beyond convenience and create new opportunities in different fields. The IoT business market is projected to grow 40 times its size from 10 years ago by 2030 (Al-Sarawi et al., 2020). The rapid growth of IoT brings new challenges and opportunities in various fields, including criminal investigations, where devices can serve as evidence sources for events. Crime investigations rely on reconstructing events before, during, and after a crime. Precise timelines, like determining the time of death, can be difficult without reliable witnesses. IoT devices, now part of daily life, provide a new opportunity in forensics by offering logged data to support or reveal critical evidence (MacDermott et al., 2018). Advances in connectivity, new protocols, and affordable miniaturization are transforming forensic methods through these devices.

Although the field of IoT forensics in crime investigation is relatively new, it already features numerous intriguing research studies and practical applications. In December 2015, a Connecticut man reported that

* Corresponding author.
Email addresses: slorenz@centextech.com (S. Lorenz), stanley@centextech.com (S. Stinehour), anitha.chennameneni@tamuct.edu (A. Chennamaneni), asubhani@centextech.com (A. Subhani), mohammad.nadim@tamuct.edu (M. Nadim).

https://doi.org/10.1016/j.fsidi.2026.302089
Received 25 February 2025; Received in revised form 7 January 2026; Accepted 27 February 2026
Available online 6 March 2026
2666-2817/

his wife had been murdered by an unknown intruder (Yankowski, 2022). Investigators secured a warrant for multiple electronic devices, including the victim's Fitbit, which logged critical data that contradicted the husband's account and provided probable cause for his arrest. Similarly, back in September 2018, the discovery of a deceased woman in her San Jose, California, home was linked to evidence from her Fitbit. The device data helped establish her time of death and implicated a suspect in her murder (Smiley, 2019). Evidence obtained from IoT devices can be crucial for crime investigations, but investigators must understand how to extract this evidence and link the information to reconstruct events accurately.

Experimenting with and extracting critical information from the hardware of IoT devices presents significant challenges (Stoyanova et al., 2020). These challenges involve two distinct tasks. The first task, data extraction, requires accurate methods and access to the IoT hardware technical details. The second task involves understanding and analyzing the extracted data, including how it is created and stored on the device. In forensic investigations, examiners often undervalue or misinterpret metadata, which can be equally or even more informative than primary data in reconstructing events. Identifying and leveraging metadata from IoT devices for crime event reconstruction demands careful consideration, as its forensic potential is not always immediately evident. To address these challenges, scenario-based testing is essential to account for ongoing advancements in IoT hardware and software, ensuring the effectiveness of investigative techniques.

The ongoing development of forensic tools and methodologies for collecting and analyzing data from IoT devices remains critical. Furthermore, there is a pressing need to validate and evaluate the privacy safeguards implemented by IoT hardware and software manufacturers to ensure compliance with legal and ethical standards (Atlam and Wills, 2020). In this case study paper, we demonstrate the connection between Amazon's efforts to ensure consumer privacy and the unintended creation and storage of data, such as potential crime scene evidence, on IoT devices. We present techniques and an analysis of visual ID metadata to establish the presence of individuals at crime scenes without relying on actual video or photographs. Additionally, this case study paper offers a practical guide for criminal justice professionals and private businesses to address Amazon IoT devices during investigations, workplace incidents, or business activity reconstructions. We provide a step-by-step framework equipping forensic practitioners with the tools and knowledge required to seize, preserve, and process Amazon IoT hardware effectively. The contributions of this research study can be summarized as follows:

- Comprehensive Analysis of Amazon IoT Devices: Defined and identified devices covered in this research, detailing stored evidence types and human presence indicators, including Visual ID functionalities.
- Forensic Methodologies: Provided step-by-step, nondestructive tear-down techniques, along with methods to extract forensically sound physical images of device storage.
- Testing and Validation: Evaluated the reliability of Amazon's facial recognition technologies and verified their policies on avoiding cloud storage of facial identification data.
- Offline Data Storage Demonstration: Showcased how Amazon IoT devices can collect and store data locally without requiring an internet connection.
- Practical Guidance for Law Enforcement: Provided key insights on leveraging IoT device data in investigations, focusing on the proper forensic extraction and analysis of metadata.

The rest of the paper is organized as follows: Section 2 covers the related research studies in the field of digital forensics and crime investigation. Section 3 explores the background of smart assistant technology. Section 4 and Section 5 summarize the experimental setup for testing Amazon IoT devices and the tear down and in-system programming of Echo Show devices, revealing offline Visual ID functionality, facial feature representations, assigned ID usage, and face-logging behavior. In Section 6, we discuss the implications of Amazon Echo Show devices for forensic analysis from multiple perspectives, and in Section 7, we conclude the case study.

2. Related work

IoT forensics is challenging due to the diversity of devices, proprietary architectures, and lack of standardization in data storage and access methods. Additionally, the sheer volume of data, along with privacy and ethical concerns, further complicates evidence extraction and analysis (Bu, 2021). Stoyanova et al. explore the key challenges in IoT-based investigations, focusing on legal, privacy, and cloud security issues (Stoyanova et al., 2020). They review theoretical models in digital forensics, highlighting privacy-preserving frameworks, blockchain-based evidence integrity, the Forensics-as-a-Service (FaaS) paradigm, and innovative data reduction techniques. Rana et. al. provide an overview of cyber-crimes and the digital forensic processes used in investigations (Rana et al., 2017). They discuss various forensic tools, detailing their benefits, challenges, and limitations, along with a comparative analysis. Similarly, Bouchaud et al. propose tools for locating IoT devices, develop the concept of digital footprints, and introduce a classification table while discussing its limitations (Bouchaud et al., 2018). It is very important to relocate IoT devices from their original environment to a secure, controlled space to preserve evidence for future analysis without altering or damaging valuable data (Bouchaud et al., 2021).

A framework for IoT forensics is essential to standardize evidence collection, ensure data integrity, and address the diversity of IoT devices and data formats (Sathwara et al., 2018). Additionally, such frameworks can serve as a valuable guidelines for investigators and be beneficial in training emerging professionals in the field. Many research works have focused on developing standardized frameworks to address the challenges, incorporating solutions such as Blockchain integration (Li et al., 2019), Fog-based architecture (Al-Masri et al., 2018), Deep learning techniques (Koroniotis et al., 2020), Generic approaches (Kebande and Ray, 2016), Integrated generic approaches (Kebande et al., 2019), Federated learning environments (Mohamed et al., 2023), and Cloud independent frameworks (Islam et al., 2019). These advancements in developing IoT forensic frameworks aim to enhance the reliability, scalability, and efficiency of IoT forensic investigations while effectively addressing the associated legal, privacy, and technical challenges.

Amazon has become a leader in the IoT field with devices like Echo and Ring, leveraging its Alexa ecosystem to connect millions of smart home products. As of 2024, Amazon's IoT market share exceeded 30%, with over 500 million Alexa-enabled devices sold globally, highlighting its dominance in the smart device industry (Herzlich, 2024). Amazon Echo devices, like other IoT devices, pose notable security challenges (Pathak et al., 2022). However, they also provide valuable opportunities for forensic analysis, enabling law enforcement to gather critical evidence for crime investigations (Li et al., 2019). Jackson and Orebaugh discuss the security and privacy issues of Amazon Echo, some criminal investigation cases involving the utilization of Amazon Echo by law enforcement, and its implications under the Fourth Amendment (Jackson and Orebaugh, 2018). Lorenz et al. introduced a novel methodology to extract information from Amazon Echo devices that will assist law enforcement in drafting search warrants demonstrating probable cause for evidence on IoT devices (Lorenz et al., 2023). Giese and Noubir uncover vulnerabilities in Amazon Echo Dot that allow sensitive user data, such as Wi-Fi credentials and location information, to remain on the device even after a factory reset (Giese and Noubir, 2021). While IoT devices with facial recognition enhance access control (Khairuddin et al., 2021), security (Majumder and Izaguirre, 2020), and surveillance (Fushshilat and Yogasmana, 2020) capabilities, they risk violating consumer data protection rights without proper legal safeguards (Romero-Moreno, 2021).

Recent work by Crasselt and Pugliese reveals a non-invasive method to access Echo Show 15's unencrypted file system and uncover local artifacts, including Visual ID logs, media activity, and user interactions (Crasselt and Pugliese, 2024). Additionally, the authors leverage an insecurely stored token and newly identified Amazon APIs to access related cloud-based artifacts such as Alexa voice requests, contacts, calendars, and multimedia content. While their work exposes vulnerabilities in the Amazon Echo Show 15 similar to our case study, we employ an alternative approach by using In-System Programming (ISP) to access the eMMC and provide a step-by-step tear down techniques, which differ from their procedure.

3. Background

This section explores the environment surrounding smart assistant technology, examining the factors driving the rapid proliferation and design of interactive smart devices that are increasingly integrated into homes and workplaces. Our research and experiments focused specifically on the use and functionality of Amazon-manufactured smart displays equipped with facial recognition capabilities.

3.1. Public distrust and perception of new technology

Concerns about consumer data stored in the cloud primarily revolve around security and privacy. Security breaches can lead to stolen data or unintended leaks, while privacy violations, whether real or perceived, often involve the collection and use of consumer information by platforms (Wright and Xie, 2019). In 2019, reports of eavesdropping by popular smart assistants such as Alexa, Siri, and Google Assistant attracted widespread media attention. Notable headlines included *The New York Times* blog Wirecutter's article, "Amazon's Alexa Never Stops Listening to You. Should You Worry?" (Clauser, 2019), *Forbes Cybersecurity*'s "Apple Siri Eavesdropping Puts Millions of Users at Risk" (O'Flaherty, 2019), and *USA Today*'s "Google workers are eavesdropping on your private conversations via its smart speakers" (Bote, 2019). While these articles explained that companies reviewed a small percentage of voice recordings to improve device functionality, the sensational headlines shaped consumer perceptions of privacy concerns, influencing both public opinion and device design. By 2022, privacy concerns had also driven a renewed interest in local storage solutions for security cameras. While the number of security cameras with local storage options seemed to be declining, consumers increasingly sought alternatives to cloud-based storage in response to recent data breaches and privacy scandals. This trend reflects a growing consumer preference for solutions that minimize reliance on the cloud.

3.2. Amazon devices with facial recognition

Amazon performs facial recognition calculations directly on IoT device hardware, making the functionality dependent on the device's hardware capabilities to execute the facial recognition algorithm. While Amazon claims to use its Neural Edge Technology for processing voice and Visual ID, not all Amazon devices with display screens support facial recognition. Currently, only three Echo Show devices and the Amazon Astro are advertised with facial recognition capabilities. Table 1 shows details of Amazon devices that support facial ID.

3.3. Amazon's facial recognition and IoT hardware design

In response to growing concerns about privacy and data security, Amazon has adopted a "hands-off" approach to facial recognition on its Echo Show devices, differentiating itself from competitors like Google. While Google's Nest Hub Max uses cloud-based processing for facial recognition profiles, Amazon ensures that Visual ID data is processed and stored locally on the device without being transmitted to the cloud. This is possible through advanced hardware design, such as the Echo Show 15, which features increased local storage, and the AZ1 processor for processing facial recognition and voice data directly on the device. This local data storage design allows Amazon to address privacy concerns while still offering sophisticated features like facial recognition. Our experiments found that Echo Show devices, such as the Echo Show 10 (3rd generation), track and log human presence and movement, including detecting torsos and hands. This data is valuable for forensic investigations, as it can document interactions with the device and track individuals in view, even when users are not actively engaging with it. Such data could provide crucial insights into event reconstruction and crime scene investigations, highlighting the significant role of locally stored metadata on IoT devices.

Table 1
Amazon echo show devices supporting Facial ID.

Device name	Echo Show 10 (3rd Gen)	Echo Show 8 (2nd Gen)	Echo Show 15
Release Price	259	129.99	249.99
Diagram	ISP Diagram	ISP Diagram	ISP Diagram
Video Teardown	Teardown	Teardown	Teardown
FCCID	2AUPE-8959	2AWTZ-8462	2AXFL-4269
External Model #	T4E4AT	A8H3N2	H6Y2A5
Internal Model #	AEOTA	AEOAT	AEOHY
Screen	10.1" HD	8"	15"
Released	February 2021	June 2021	December 2021
Processor	MediaTek MT8183V and MT8512 AZ1	MediaTek MT8183V	AMlogic Pop1-C
Storage	8GB eMMC and 4GB eMMC	8GB eMMC	16GB eMMC
Encrypted	No	No	No
Extraction Type	Physical	Physical	Physical
Extraction Method	ISP	ISP	ISP
Device Family	KNIGHT	KNIGHT	KNIGHT
OS	9 and 7.1.2	9	9
Internal Name	theia and mopac	athena	Hoya
Build ID	PS7542 and NS6542	PS7547	PS7550

3.4. Intentional design versus forensic benefits of IoT hardware

IoT devices, including smart displays and cameras, are typically not designed for continuous surveillance but to record audio and video when actively controlled or triggered by the user. This intentional design addresses privacy concerns, as companies like Amazon emphasize privacy controls and user consent in their marketing. However, this design has an incidental benefit for forensic investigations: IoT devices can create valuable data related to crime scene activity.

Amazon has adapted its IoT hardware design to balance user privacy with functionality, particularly by processing data locally on devices rather than in the cloud. The inclusion of local storage and advanced processing capabilities, like the AZ1 Neural Edge processor in the Echo Show 10, has enhanced the forensic potential of these devices. Our experiments revealed significant amounts of user data stored directly on the devices, including event tracking and facial recognition data. Amazon's shift towards local processing, with the introduction of the Echo Show 15 and the continued use of Neural Edge Technology, allows for better privacy while also providing forensic examiners with critical data that could be pivotal in crime scene investigations. This evolution in design demonstrates how privacy concerns can shape the hardware and functionality of IoT devices, creating opportunities for more robust forensic analysis.

4. Experimental setup

In this section, we outline the experimental setup used to test Amazon IoT devices, detailing the device environment, network monitoring

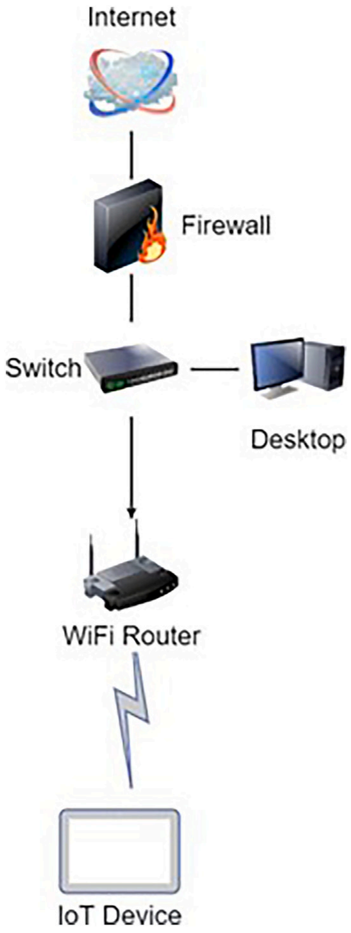


Fig. 1. Network diagram of experimental setup.

procedures, and the step-by-step process followed during our experiments. This comprehensive approach ensures accurate data collection and analysis for our investigation.

4.1. Device test environment

In this experiment, the IoT devices were mounted on a wooden frame with a plexiglass wall. Power was supplied via an extension cord connected to a fuse box and a doorbell transformer for devices requiring 24 volts, while an electrical outlet provided 110 volts for other devices. The Echo Show 15 was mounted on the wall and plugged into the outlet for our experiments. Two cameras were used: one faced outward to capture the Echo Show 15's camera view, and the other recorded its screen to document inputs and responses. A desktop with recording software was placed nearby to save videos and display timestamps in Unix Epoch Time, UTC, and Central Time.

4.2. Network monitoring

Internet access was provided through a PfSense router, with static IP addresses assigned to each IoT device based on their MAC addresses via the router's interface. A switch, connected to the router, had port mirroring enabled to replicate all data traffic passing through it to a designated port. A desktop computer running Wireshark was connected to this mirrored port, allowing the logging of all internet traffic to and from the connected devices. Additionally, a wireless router configured in access point mode was connected to the switch to provide a wireless network for the IoT devices. The network configuration for the experiments is illustrated in Fig. 1.

4.3. Experimental process

Our research began with a teardown and examination of the device hardware to identify the components used. We determined the appropriate in-system programming (ISP) method for data extraction, documenting the process with photos and videos. The eMMC chip location, shown in Fig. 2, was identified, and we removed it using hot air to trace and mark ISP access points for future experiments. The eMMC chip was read using a chip reader to preserve the device's condition, allowing us to observe the creation of databases and files triggered by user activation of features like Visual ID. After marking ISP locations, we reballed and reinstalled the eMMC chip to ensure the device remained functional without altering its data.

Following the establishment of a reliable and repeatable extraction process, we prepared the device for real-world testing by setting up an Amazon user account and connecting the device to the internet, mimicking average consumer use. External lab cameras were configured to record the device's screen, sounds, and precise interaction times. Post-testing, we extracted and analyzed data, employing forensic methods to power down or disconnect the device as an investigator would at a crime scene. Using timestamps from our experiments, we located and parsed data relative to our interactions, identifying artifacts, databases, and logs associated with normal device operation. Repeated testing ensured consistency and thoroughness in our findings. The step-by-step process of this experiment is listed below:

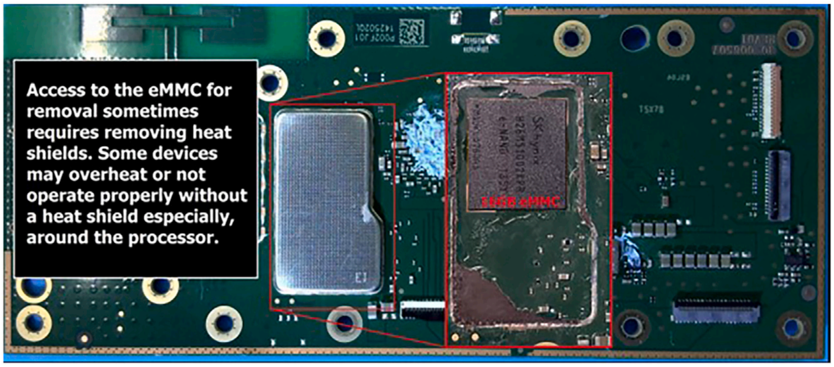
1. Record the tear-down and chip removal process through video and photographs.
2. Disassemble the device and remove the main logic board.
3. Detach the eMMC chip from the main board.
4. Identify and mark the ISP access points on the main board.
5. Reattach the eMMC chip to the circuit board through soldering.
6. Use video cameras and network monitoring tools to document the experiment.
7. Interact with and manipulate the IoT device during testing.
8. Power off the device, disassemble it, and solder an ISP adapter to the identified ISP points.
9. Extract data from the eMMC chip using a chip reader and create a forensically sound physical image.
10. Analyze the physical image using forensic tools.
11. Capture and analyze network traffic data alongside data recovered from the device.
12. Thoroughly document all findings and observations.

5. Experiment

In this section, we describe the teardown and in-system programming of Echo Show devices, uncovering Visual ID capabilities without an internet connection. We explore the numerical representations of facial characteristics, the creation and use of assigned Visual ID numbers, and examine the logging of enrolled individuals and unknown faces, highlighting the vulnerabilities of IoT facial recognition software.

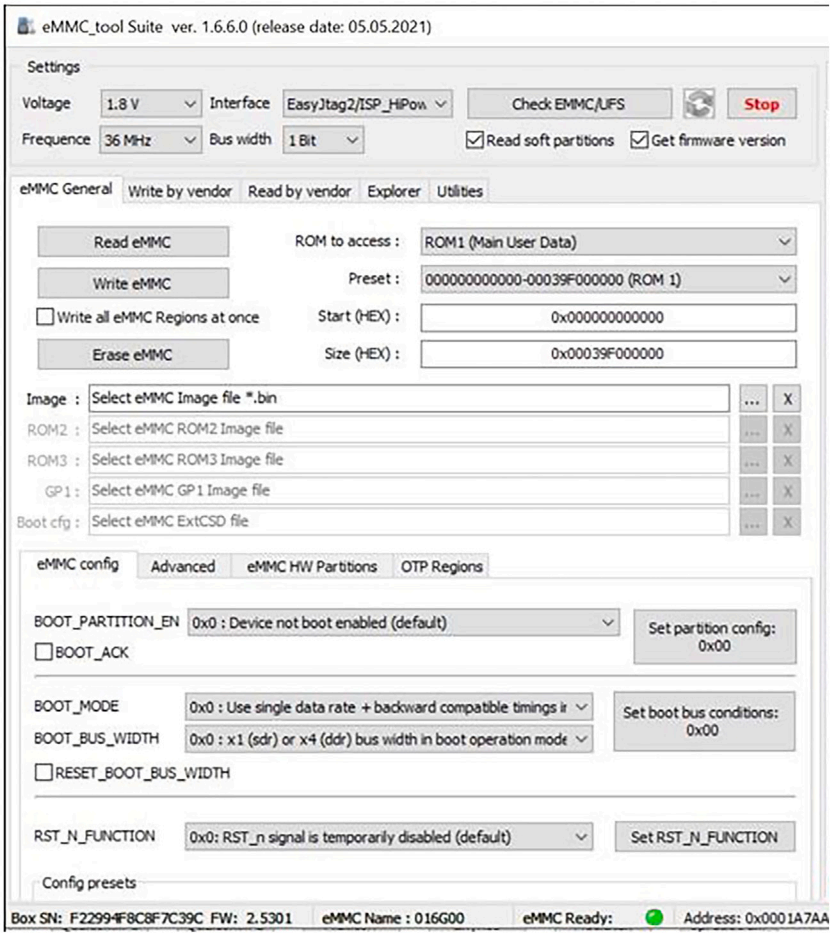
5.1. Teardown and in-system-programming of echo show devices

The Amazon Echo Show 15, equipped with 16GB of eMMC storage, allows for straightforward access to its hardware through a non-complex teardown procedure. Detailed diagrams and videos demonstrating the teardown and data extraction process for three Echo Show devices supporting Visual ID, including the latest Echo Show 15, are available upon request. Utilizing In-System Programming (ISP), we successfully extracted data from the eMMC chip and wrote data back to the storage during experiments. This approach was particularly useful for analyzing and experimenting with the facial recognition avatar database, as illustrated in Fig. 3. Our comprehensive documentation ensures the reproducibility of the process, making it an invaluable resource for researchers and practitioners conducting forensic analysis on similar



Access to the eMMC for removal sometimes requires removing heat shields. Some devices may overheat or not operate properly without a heat shield especially, around the processor.

Fig. 2. eMMC chip Removal for Amazon Echo Show 15.



eMMC_tool Suite ver. 1.6.6.0 (release date: 05.05.2021)

Settings

Voltage: 1.8 V
Interface: EasyJtag2/ISP_HiPow
Frequence: 36 MHz
Bus width: 1 Bit
☑ Read soft partitions
☑ Get firmware version

ROM to access : ROM1 (Main User Data)
Preset : 000000000000-00039F000000 (ROM 1)
☐ Write all eMMC Regions at once
Start (HEX) : 0x000000000000
Size (HEX) : 0x00039F000000

Image : Select eMMC Image file *.bin
ROM2 : Select eMMC ROM2 Image file
ROM3 : Select eMMC ROM3 Image file
GP1 : Select eMMC GP1 Image file
Boot cfg : Select eMMC ExtCSD file

BOOT_PARTITION_EN: 0x0 : Device not boot enabled (default)
☐ BOOT_ACK
Set partition config: 0x00

BOOT_MODE: 0x0 : Use single data rate + backward compatible timings ir
BOOT_BUS_WIDTH: 0x0 : x1 (sdr) or x4 (ddr) bus width in boot operation mode
☐ RESET_BOOT_BUS_WIDTH
Set boot bus conditions: 0x00

RST_N_FUNCTION: 0x0: RST_n signal is temporarily disabled (default)

Config presets

Box SN: F22994F8C8F7C39C FW: 2.5301 eMMC Name : 016G00 eMMC Ready: ● Address: 0x0001A7AA

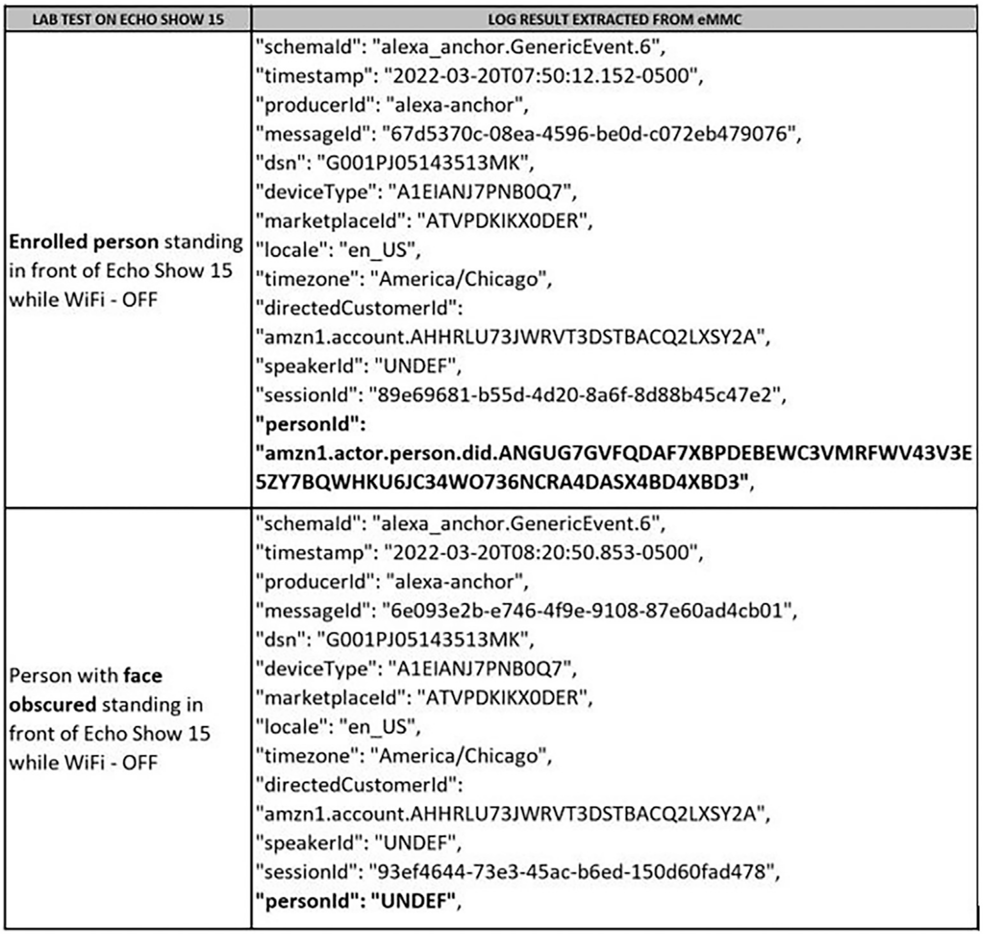
Fig. 3. In-System Programming (ISP) of Amazon Echo Show 15.

devices. This method allows for the preservation of device integrity while enabling a deeper understanding of the data structures and artifacts stored within these advanced IoT devices.

5.2. Visual ID without internet connection

To investigate the creation and storage of metadata in crime scenes or critical incidents, we tested whether Echo Show devices could operate and generate metadata without internet connectivity. During trials, we disconnected the Echo Show 15 from WiFi by disabling it in “Network Settings” on the device interface. Despite this, the device continued to log the presence of both unidentified individuals and those previously enrolled in Visual ID. It recognized our faces and displayed personalized greetings, including our profile names and photos. We tested three scenarios: (1) with non-enrolled individuals, (2) with faces obscured, and (3) in low lighting. Non-enrolled individuals or those with obscured faces received no visible response, while enrolled users were correctly identified in well-lit conditions.

After disconnecting WiFi, we extracted and analyzed the device’s 16GB eMMC storage and found logs of our interactions. For visible faces, the logs recorded a unique Visual ID identification number *(amzn1.actor.person.did)*, consisting of 72 characters per enrolled individual, along with timestamps in Central Time for when faces were recognized. For



LAB TEST ON ECHO SHOW 15	LOG RESULT EXTRACTED FROM eMMC
Enrolled person standing in front of Echo Show 15 while WiFi - OFF	"schemaId": "alexa_anchor.GenericEvent.6", "timestamp": "2022-03-20T07:50:12.152-0500", "producerId": "alexa-anchor", "messageId": "67d5370c-08ea-4596-be0d-c072eb479076", "dsn": "G001PJ05143513MK", "deviceType": "A1EIANJ7PNB0Q7", "marketplaceId": "ATVPDKIKX0DER", "locale": "en_US", "timezone": "America/Chicago", "directedCustomerId": "amzn1.account.AHHRLU73JWRVT3DSTBACQ2LXSY2A", "speakerId": "UNDEF", "sessionId": "89e69681-b55d-4d20-8a6f-8d88b45c47e2", **"personId":** **"amzn1.actor.person.did.ANGUG7GVFQDAF7XBPDEBEWC3VMRFWV43V3E** **5ZY7BQWHKU6JC34WO736NCRA4DASX4BD4XBD3"**,
Person with **face obscured** standing in front of Echo Show 15 while WiFi - OFF	"schemaId": "alexa_anchor.GenericEvent.6", "timestamp": "2022-03-20T08:20:50.853-0500", "producerId": "alexa-anchor", "messageId": "6e093e2b-e746-4f9e-9108-87e60ad4cb01", "dsn": "G001PJ05143513MK", "deviceType": "A1EIANJ7PNB0Q7", "marketplaceId": "ATVPDKIKX0DER", "locale": "en_US", "timezone": "America/Chicago", "directedCustomerId": "amzn1.account.AHHRLU73JWRVT3DSTBACQ2LXSY2A", "speakerId": "UNDEF", "sessionId": "93ef4644-73e3-45ac-b6ed-150d60fad478", **"personId": "UNDEF"**,

Fig. 4. Visual ID enrollment detection while internet is turned off.

obscured faces, the *personId* was logged as *UNDEF*. These findings confirm that, even without internet connectivity, the Echo Show 15 logs and identifies enrolled users based on facial recognition, Fig. 4. This capability highlights the device's potential for reconstructing events in critical environments, such as business settings or crime scenes.

5.3. Numeric representations of facial characteristics

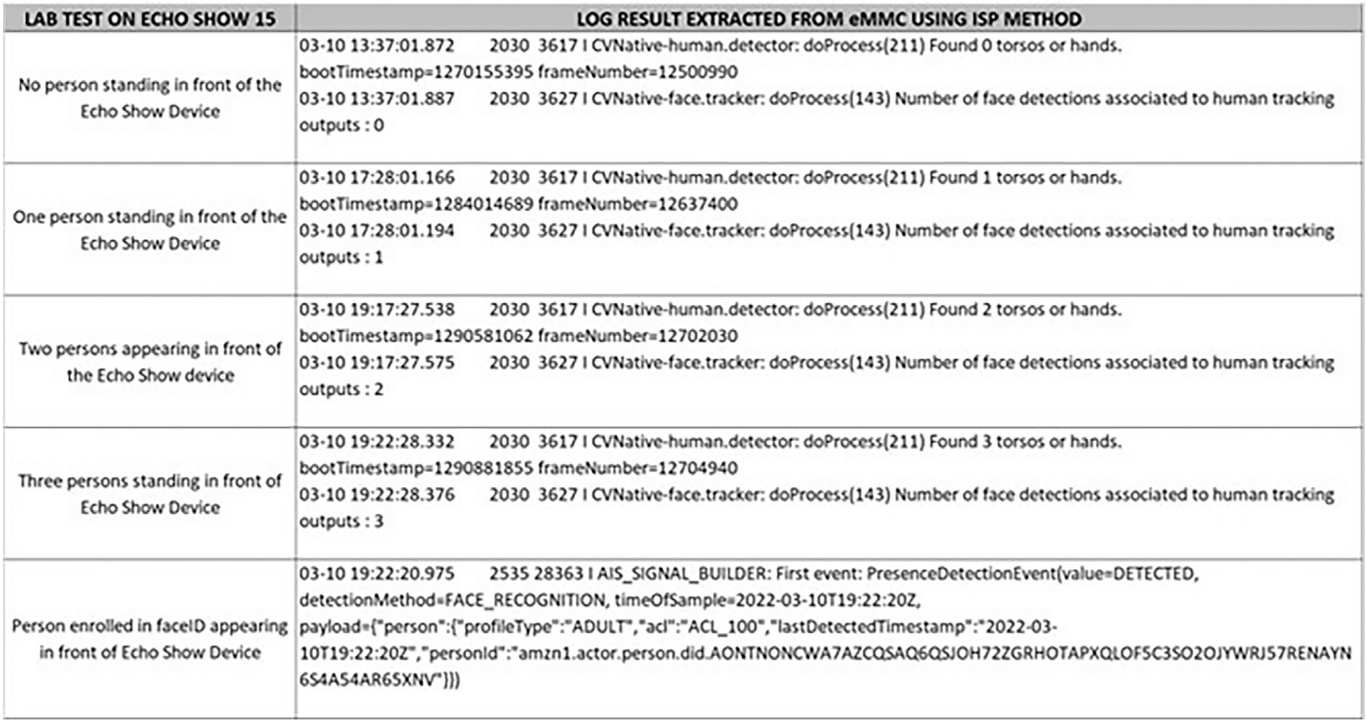
Amazon requires users to opt-in before creating a Visual ID profile, a process detailed on their website. During enrollment, the Echo Show captures photographs of the user's face as they look up, down, left, and right. The user can select a personalized name for greetings and take a profile photo to appear in a circular display when recognized by the device. Amazon states that these enrollment photos are used to generate numeric representations, long character strings that uniquely identify Visual IDs. According to Amazon, these vectors are stored only on the device and are not transmitted to the cloud. In our testing, we found these vectors stored in an SQLite database named *DomainApplicationVUIEnrollment_Alexa.Identify.db* on devices after Visual ID enrollment. Notably, this database did not exist on the Echo Show 15 storage we extracted before enrolling in Visual ID. The numeric representations for enrolled profiles were substantial, with one exceeding 9100 characters in base64 and another surpassing 13,200 characters.

5.4. Creation and use of assigned visual ID numbers

Amazon outlines a two-step process for Visual ID on supported devices, facial detection and facial recognition, which can be invaluable for forensic examiners and event reconstruction. While Amazon states that the numeric vectors representing enrolled profiles are stored only on the device hardware and not sent to the cloud, the *personId* number, a 72-character identifier generated by Amazon, is shared with the cloud. This *personId* is consistent across multiple Amazon devices that support Visual ID, provided they are linked to the same user account. In our test trials, we located the *personId* in device logs and databases on Echo Show devices. This identifier can serve as a critical tool for forensic examiners to link specific individuals enrolled in Visual ID to their interactions with the Echo Show's camera, Fig. 4.

5.5. Logging of enrolled individuals and unknown faces

When an individual steps into the view of an Amazon device's camera, their presence is logged if they are enrolled in Visual ID, with the event tied to a unique 72-character ID *("amzn1.actor.person.did…")* assigned to each user. Even if a person is not enrolled in Visual ID, the device logs the presence of unknown faces. Our analysis revealed thousands of log entries from Echo Show devices, documenting and counting faces detected by the front-facing camera. These logs also record the absence of a face with entries like … *Number of face detections associated with human tracking outputs: 0*, which are generated every few seconds, even when there is no activity. Additionally, the logs document the presence or absence of torsos or hands, with entries ending in … *Found 0 torsos or hands*. In our experiments, the logs consistently and accurately recorded both enrolled and unidentified individuals, Fig. 5. Network analysis using Wireshark indicated that no Visual ID data was transmitted to Amazon servers during or after enrollment, suggesting that facial data remains device-local. This finding was corroborated by



LAB TEST ON ECHO SHOW 15	LOG RESULT EXTRACTED FROM eMMC USING ISP METHOD
No person standing in front of the Echo Show Device	03-10 13:37:01.872 2030 3617 I CVNative-human.detector: doProcess(211) Found 0 torsos or hands. bootTimestamp=1270155395 frameNumber=12500990 03-10 13:37:01.887 2030 3627 I CVNative-face.tracker: doProcess(143) Number of face detections associated to human tracking outputs : 0
One person standing in front of the Echo Show Device	03-10 17:28:01.166 2030 3617 I CVNative-human.detector: doProcess(211) Found 1 torsos or hands. bootTimestamp=1284014689 frameNumber=12637400 03-10 17:28:01.194 2030 3627 I CVNative-face.tracker: doProcess(143) Number of face detections associated to human tracking outputs : 1
Two persons appearing in front of the Echo Show device	03-10 19:17:27.538 2030 3617 I CVNative-human.detector: doProcess(211) Found 2 torsos or hands. bootTimestamp=1290581062 frameNumber=12702030 03-10 19:17:27.575 2030 3627 I CVNative-face.tracker: doProcess(143) Number of face detections associated to human tracking outputs : 2
Three persons standing in front of Echo Show Device	03-10 19:22:28.332 2030 3617 I CVNative-human.detector: doProcess(211) Found 3 torsos or hands. bootTimestamp=1290881855 frameNumber=12704940 03-10 19:22:28.376 2030 3627 I CVNative-face.tracker: doProcess(143) Number of face detections associated to human tracking outputs : 3
Person enrolled in faceID appearing in front of Echo Show Device	03-10 19:22:20.975 2535 28363 I AIS_SIGNAL_BUILDER: First event: PresenceDetectionEvent(value=DETECTED, detectionMethod=FACE_RECOGNITION, timeOfSample=2022-03-10T19:22:20Z, payload={"person":{"profileType":"ADULT","acl":"ACL_100","lastDetectedTimestamp":"2022-03-10T19:22:20Z","personId":"amzn1.actor.person.did.AONTNONCWA7AZCQSAQ6QSJOH72ZGRHOTAPXQLOF5C3SO2OJYWRJ57RENAYN6S4A54AR65XNV"}})

Fig. 5. Log result extracted from eMMC using ISP method.

cross-device testing, in which enrolled individuals were recognized on the Echo Show 15 but not on a separate Visual ID–enabled device, Echo Show 8, under the same account until enrollment was repeated.

5.6. Statistical accuracy

Three individuals were enrolled in the Amazon Visual ID system and six unenrolled individuals were tested for evaluation. Interactions with the device were conducted under typical operational conditions to generate analyzable metadata. Test scenarios included both enrolled and unenrolled individuals interacting with the device. Multiple enrolled individuals were simultaneously positioned within the device's field of view to evaluate recognition. In these scenarios, the system consistently identified and logged the recognized individuals until the recognized subjects exited the field of view, at which point the device returned to an idle state. When combinations of enrolled and unenrolled individuals were present, log data reflected the presence of multiple subjects through metadata. Additional tests evaluated recognition performance under varying conditions, including the use of hats, glasses, and other facial obstructions by enrolled individuals. Environmental factors, such as lighting conditions and facial coverings, were observed to negatively impact recognition accuracy, thereby reducing the system's ability to correctly identify registered individuals. Finally, controlled modifications were made to the Visual ID database to assess the data integrity. By altering stored facial metadata, the system was observed to misattribute recognition events, identifying one enrolled individual as another. This demonstrated that recognition outcomes were directly dependent on the integrity of stored facial data and highlighted the potential impact of database manipulation on system accuracy.

5.7. Vulnerability of IoT facial recognition software

Our research focuses on leveraging metadata from IoT hardware to create timelines and reconstruct events involving IoT devices, while also investigating potential exploits to deceive or manipulate facial recognition software and hardware. While much of our work centers on the protection and preservation of data during forensic processes, experimenting with data manipulation on IoT devices offers valuable insights into their intended functions and potential vulnerabilities. Amazon markets its facial recognition technology, Visual ID, as a means to deliver more personalized content and experiences for customers, essentially functioning as a form of access control. Studies, such as those by Sharif et al., highlight the dual use of biometric systems for access control and surveillance, as well as their susceptibility to impersonation attacks where external manipulation fools facial recognition software (Sharif et al., 2016). In our experiments with Echo Show devices, enrolling in Visual ID allowed us to trigger personalized displays, such as tailored lists, music preferences, and news feeds, based on facial recognition. Unlike external impersonation methods, our approach involved internal manipulation of the IoT device's facial recognition software to explore its vulnerabilities and behavior.

6. Discussion

Our research and experiments with Amazon Echo Show devices supporting Visual ID reveal significant implications for forensic investigators in reconstructing events and timelines at crime scenes. They also provide a method for assessing Amazon's commitment to balancing user convenience and functionality with consumer privacy and data control. While Amazon appears to have developed a strategy to meet consumer demands for intuitive, personalized IoT devices while minimizing data collection, the Echo Show devices still rely heavily on cloud connectivity for core functionalities. Nonetheless, Amazon's approach to combining personalization with privacy has resulted in the creation of a rich layer of metadata stored on IoT hardware, which can serve as a valuable resource for forensic investigations.

6.1. Implications for other IoT smart device manufacturers

Amazon's design and marketing of IoT devices prioritize addressing consumer concerns regarding privacy and the potential misuse of personal information by government or private entities. To balance privacy with functionality, Amazon has shifted its design approach to reduce reliance on cloud processing while maintaining advanced features. Traditionally, most IoT devices relied on low processing power and acted primarily as sensors or portals that transmitted data to the cloud for analysis and processing (Yaqoob et al., 2019). However, Amazon's Echo Show devices deviate from this trend, emphasizing local processing capabilities. While the ubiquity of IoT is built on affordable, simple devices connected to the cloud for sophisticated data processing, the growing mistrust among consumers regarding the handling of personal data has led companies like Amazon and Google to rethink their strategies.

Initially, functionalities like voice and facial recognition were performed in the cloud, but with increasing consumer concerns, both companies have reduced or eliminated the collection of sensitive data, such as voice recordings and facial recognition information, to regain trust. Amazon now avoids sending facial ID data to the cloud entirely, opting instead to store and process this information locally on IoT hardware. Similarly, Google's Nest Hub Max employs local storage and processing for face match profiles, ensuring video and images are not sent to the cloud. This shift requires IoT devices to become more sophisticated and robust in hardware design, allowing for high-performance local processing while preserving privacy.

As the world's largest manufacturer of IoT smart displays, Amazon's move toward more powerful and complex IoT hardware, combined with its by-design privacy limitations, sets a precedent for other manufacturers. By delivering functionality and convenience while minimizing data collection, Amazon's approach may drive other companies to adopt similar designs and improve their marketing strategies. Both Amazon and Google now emphasize advanced model performance relying on improved IoT hardware to perform tasks locally that were previously achievable only through cloud computing. This evolution not only reflects changing consumer priorities but also signals a potential transformation in IoT design and functionality across the industry.

6.2. Implications for law enforcement

Amazon's "Customer Help" section provides guidance on how the company handles law enforcement requests for information and publishes a bi-annual transparency report summarizing its policies and the number of such requests processed. Amazon does not fulfill subpoenas for content or non-content information but may comply with search warrants, distinguishing between these two categories. "Content information" refers to data stored in a customer's account, such as photographs, while "non-content information" includes basic subscriber details like names, addresses, and billing information. Amazon reviews all requests and challenges those deemed "overbroad" (Amazon, 2021). According to the most recent report, 99% of processed requests involved non-content disclosures, and only 0.7% resulted in the release of content information (Amazon, 2021).

For law enforcement officials, it is critical to understand that facial recognition data from Amazon IoT devices, classified as content information, will not typically be available from Amazon's cloud services and can only be retrieved from the devices themselves. This underscores the importance of identifying and securing IoT devices at crime scenes that may contain Visual ID metadata. Investigators must be prepared to establish probable cause for seizing and analyzing these devices, as this metadata could provide key insights for forensic investigations. In scenarios such as a homicide occurring within a residence where the victim is enrolled in the device's visual identification system, the logs can indicate the last confirmed interaction or visual recognition of the registered user. Furthermore, law enforcement must recognize Amazon's "hands-off" policy regarding such data, as the company can simply assert that it does not possess Visual ID metadata rather than contesting requests as overbroad. Obtaining biometric data from Amazon's cloud requires a subpoena or search warrant, and similarly, a search warrant is necessary at a crime scene to lawfully acquire data from the local device before conducting a forensic examination. These legal considerations, along with the technical skills needed to extract and analyze metadata from IoT hardware, will be essential components of future training programs for crime scene investigators and forensic examiners.

6.3. Implications for businesses

Amazon offers a service called "Alexa for Business," which enables businesses to integrate Alexa-powered smart assistants for use in personal workspaces or conference rooms, as well as extend functionality to Alexa devices already in use at employees' homes. Companies adopting "Alexa for Business" must thoroughly understand the devices' functionalities and capabilities to create effective policies and procedures for their use. This understanding is particularly crucial when addressing workplace incidents, as Alexa-based devices are capable of storing data that could serve as evidence. Such evidence may reside on company-deployed Alexa devices or on employees' personal Alexa devices used off-site. Recognizing and managing this potential data can play a key role in workplace investigations and policy development.

6.4. Implications for consumers

Consumer privacy concerns about IoT device design and criticism of companies like Amazon often center on the storage and sharing of customer information in the cloud. With the advent of IoT devices equipped with facial recognition technology, consumers now have greater access to information about how their data is processed and stored. For instance, Amazon requires customers to actively "opt-in" to use facial recognition features on specific smart displays. The shift toward devices capable of processing and storing data locally offers enhanced privacy but comes at a higher cost compared to devices that rely primarily on cloud-based processing. As such, consumers must remain vigilant and take responsibility for securing sensitive information that may be stored on their own IoT devices.

6.5. Limitations and future work

Our experiments primarily focused on recovering data from Amazon IoT device hardware. Due to limited access, we did not examine data stored in Amazon's cloud, nor did we include information that might be accessible through a search warrant during an actual investigation. While IoT devices are often located at the scene of a crime or incident, they may contain evidence of criminal activity, data breaches, or privacy violations originating from other sources. Additional research is also necessary to determine the log retention period and data persistence behavior of the device.

Future research will aim to provide a more detailed analysis of data recovered from IoT hardware, including decoding and parsing event-specific information linked to individual devices and quantifying accuracy under different environmental conditions. Developing forensic tools to efficiently parse and report this data is critical for enabling forensic examiners to effectively utilize extracted information. Additionally, validating findings from IoT hardware analysis by cross-referencing data from other connected devices and the cloud is essential to ensure accuracy and strengthen conclusions drawn from lab experiments.

7. Conclusion

In conclusion, our research highlights the significant role IoT devices, such as Amazon Echo Show devices with Visual ID capabilities, can play in forensic investigations and incident reconstructions. By examining the data stored locally on these devices, we demonstrated the potential to recover critical metadata, such as facial recognition logs, timestamps, and unique identifiers, even in scenarios where cloud data is inaccessible. These findings emphasize the importance of understanding IoT device functionality, storage mechanisms, and privacy limitations when conducting forensic analyses.

As IoT devices continue to evolve, incorporating advanced features like local facial recognition and data storage, the need for robust forensic methodologies and tools becomes more pressing. This paper underscores the value of developing specialized forensic tools and practices to decode and interpret data from IoT hardware while maintaining the integrity of evidence. Future work should explore complementary analyses involving cloud-stored data and connected devices to validate findings and provide a comprehensive understanding of IoT ecosystems in forensic contexts.

By bridging the gap between IoT technology and forensic sciences, we aim to enhance investigative capabilities while addressing critical concerns about privacy and data security. This research provides a foundation for both forensic examiners and IoT stakeholders to better understand the implications of IoT devices in legal, corporate, and consumer environments.

CRediT authorship contribution statement

Scott Lorenz: Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Conceptualization. **Stanley Stinehour:** Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Formal analysis, Conceptualization. **Anitha Chennamaneni:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Project administration, Methodology, Investigation, Funding acquisition, Conceptualization. **Abdul Subhani:** Writing – review & editing. **Mohammad Nadim:** Writing – review & editing, Writing – original draft, Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This research was supported in part by the Air Force Research Laboratory (AFRL) and the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate under award FA8750-19-C-0077. The views expressed are those of the author and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense, or the U.S. government.

Data availability

Data will be made available on request.

References

Al-Masri, E., Bai, Y., Li, J., Sep 2018. A fog-based digital forensics investigation framework for IoT systems. In: 2018 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, pp. 196–201.

Al-Sarawi, S., Anbar, M., Abdullah, R., Al Hawari, A.B., Jul 2020. Internet of things market analysis forecasts, 2020–2030. In: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE, pp. 449–453.

Amazon, Jul-Dec 2021. Law enforcement information requests - Amazon customer service. from https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF (Retrieved 10 December 2024).

Atlam, H.F., Wills, G.B., 2020. IoT security, privacy, safety and ethics. Digital Twin Technol. Smart Cities 123–149.

Bote, J., 2019. Google workers are eavesdropping on your private conversations via its smart speakers. from https://www.usatoday.com/story/tech/2019/07/11/google-home-smart-speakers-employees-listen-conversations/1702205001/ (10 December 2024).

Bouchaud, F., Grimaud, G., Vantroys, T., Aug 2018. IoT forensic: identification and classification of evidence in criminal investigations. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, pp. 1–9.

Bouchaud, F., Vantroys, T., Grimaud, G., 2021. Evidence gathering in IoT criminal investigation. In: Digital Forensics and Cyber Crime: 11th EAI International Conference, ICDF2C 2020, Proceedings (15 October 2020), vol. 11. Springer International Publishing, Boston, MA, USA, pp. 44–61.

Bu, Q., 2021. The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. Int. Cybersecurity Law Rev. 2, 113–145.

Clauser, G., 2019. Amazon's alexa never stops listening to you. Should you worry? from https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/ (Retrieved 10 December 2024).

Crasselt, J., Pugliese, G., Started Off Local, Now We're in the Cloud: Forensic Examination of the Amazon Echo Show 15 Smart Display, arXiv preprint arXiv:2408.15768, 2024.

Fushshilat, I., Yogasmana, Y., May 2020. IoT Scheme for Surveillance System and Laboratory Security Access In IOP Conference Series: Materials Science and Engineering, vol. 850. IOP Publishing, No. 1, p. 012014.

Giese, D., Noubir, G., Jun 2021. Amazon echo DOT or the reverberating secrets of IoT devices. In: Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 13–24.

Herzlich, T., Jul 2024. Amazon Bleeding Billions of Dollars from Money-Losing Alexa Speakers: Report, from https://nypost.com/2024/07/23/business/amazon-bleeding-billions-of-dollars-from-alexa-speakers-report/ (Retrieved 6 December 2024).

Islam, M.J., Mahin, M., Khatun, A., Debnath, B.C., Kabir, S., May 2019. Digital forensic investigation framework for internet of things (IoT): a comprehensive approach. In: 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT). IEEE, pp. 1–6.

Jackson, C., Orebaugh, A., 2018. A study of security and privacy issues associated with the Amazon echo. Int. J. Internet Things Cyber-Assur. 1(1), 91–100.

Kebande, V.R., Ray, I., Aug 2016. A generic digital forensic investigation framework for internet of things (IOT). In: 2016 IEEE 4th International Conference on future Internet of Things and Cloud (FiCloud). IEEE, pp. 356–362.

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

Khairuddin, M.H., Shahbudin, S., Kassim, M., Aug 2021. A Smart Building Security System with Intelligent Face Detection and Recognition In Iop Conference Series: Materials Science and Engineering, vol. 1176. IOP Publishing, No. 1, p. 012030.

Koroniotis, N., Moustafa, N., Sitnikova, E., 2020. A new network forensic framework based on deep learning for internet of things networks: a particle deep framework. Future Gener. Comput. Syst. 110, 91–106.

Li, S., Qin, T., Min, G., 2019. Blockchain-based digital forensics investigation framework in the internet of things and social systems. IEEE Trans. Comput. Soc. Syst. 6(6), 1433–1441.

Li, S., Choo, K.K.R., Sun, Q., Buchanan, W.J., Cao, J., 2019. IoT forensics: Amazon echo as a use case. IEEE Internet Things J. 6 (4), 6487–6497.

Lorenz, S., Stinehour, S., Chennamaneni, A., Subhani, A.B., Torre, D., 2023. IoT forensic analysis: a family of experiments with Amazon echo devices. Forensic Sci. Int.: Digit. Investig. 45, 301541.

MacDermott, A., Baker, T., Shi, Q., Feb 2018. IOT forensics: challenges for the ioa era. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, pp. 1–5.

Majumder, A.J., Izaguirre, J.A., Jul 2020. A smart IoT security system for smart-home using motion detection and facial recognition. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, pp. 1065–1071.

Mohamed, H., Koroniotis, N., Moustafa, N., 2023. Digital forensics based on federated learning in IoT environment. In: Proceedings of the 2023 Australasian Computer Science Week, pp. 92–101.

O'Flaherty, K., 2019. Apple siri eavesdropping puts millions of users at risk. from https://www.forbes.com/sites/kateoflahertyuk/2019/07/28/apple-siri-eavesdropping-puts-millions-of-users-at-risk/ (Retrieved 10 December 2024).

Pathak, S., Islam, S.A., Jiang, H., Xu, L., Tomai, E., 2022. A survey on security analysis of Amazon echo devices. High-Confid. Comput. 2 (4), 100087.

Rana, N., Sansanwal, G., Khatter, K., Singh, S., Taxonomy of digital forensics: Investigation tools and challenges, arXiv preprint arXiv:1709.06529, 2017.

Romero-Moreno, F., Oct 2021. AI facial recognition and biometric detection: balancing consumer rights and corporate interests. In: 2021 International Carnahan Conference on Security Technology (ICCST). IEEE, pp. 1–5.

Sathwara, S., Dutta, N., Pricop, E., Jun 2018. IoT forensic a digital investigation framework for IoT systems. In: 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). IEEE, pp. 1–4.

Sharif, M., Bhagavatula, S., Bauer, L., Reiter, M.K., Oct 2016. Accessorize to a crime: real and stealthy attacks on state-of-the-art face recognition. In: Proceedings of the 2016 Acm Sigsac Conference on Computer and Communications Security, pp. 1528–1540.

Smiley, L., 2019. A brutal murder, a wearable witness, and an unlikely suspect. from https://www.wired.com/story/telltale-heart-fitbit-murder/ (Retrieved 1 December 2024).

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K., 2020. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Commun. Surv. Tutorials 22 (2), 1191–1221.

Wright, S.A., Xie, G.X., 2019. Perceived privacy violation: exploring the malleability of privacy expectations. J. Bus. Ethics 156, 123–140.

Yankowski, P., Mar 2022. Connecticut woman's fitbit tracker key evidence in murder trial. from https://www.ctinsider.com/news/article/Connecticut-woman-s-Fitbit-tracker-key-evidence-16977179.php (Retrieved 1 December 2024).

Yaqoob, I., Hashem, I.A.T., Ahmed, A., Kazmi, S.A., Hong, C.S., 2019. Internet of things forensics: recent advances, taxonomy, requirements, and open challenges. Future Gener. Comput. Syst. 92, 265–275.