**Arrange the following paragraphs of the Introduction in the correct order.**

**Digital forensic approaches for Amazon Alexa ecosystem**

**Introduction**

1 **(5)**

While there are many legal questions regarding the use of this type of evidence, there are also important technical considerations. Most importantly, to efficiently investigate these types of cases, it is first necessary to understand the digital forensic characteristics of Amazon's Alexa and its ecosystem.

2 **(2)**

Gartner predicts that 25% of households using an intelligent virtual assistant (IVA) will have two or more devices by 2020 (Gatner). The ubiquitous use of wearables, personal smart devices, smart appliances, etc., will generate a large amount of digital data that can be a great source of digital evidence.

3 **(7)**

Also, for customizing these Alexa-related environments, users should access the cloud service using companion clients, such as PC or mobile (Android and iOS) devices. Thus, the ecosystem created by all these interconnected devices, third-party applications and companion clients is complex and heterogeneous (Amazon). In this paper, we will refer to this ecosystem as the Amazon Alexa ecosystem.

4 **(9)**

First, it requires valid user accounts in order to access the cloud. There is, of course, the potential to discover access information through investigation or interrogation, but this information is not always available. Second, it is difficult to recover deleted data on the cloud. Client-side forensics approaches are needed to overcome these limitations. That is, when it is impossible to acquire cloud-native artifacts, companion clients can offer important artifacts for digital investigations.

5 **(11)**

In a situation where existing tools and procedures cannot meet the demand for this emerging IoT system, our findings and proof-of-concept tool will be helpful for investigators attempting to work in the Amazon Alexa environment.

6 **(3)**

In several recent criminal investigations, law enforcement officials, legal experts and forensics experts attempted to use “always-on” IoT devices as sources of forensic artifacts similar to human-life black boxes. In particular, one recent criminal investigation case involving an Amazon Echo, gained widespread attention in the media.

7 **(12)**

The rest of the paper is organized as follows. Section Amazon Alexa and digital forensics describes the target system and Section Related works reviews existing works. Section Forensic artifacts on Amazon Alexa ecosystem presents our findings for digital forensics and Section Design and implementation introduces an implementation based on our findings. Section Visualization and evaluation evaluates results with visualization techniques. Finally, Section Conclusion and future works discusses conclusions and next steps.

8 **(10)**

As a result of our analysis, we introduce a proof-of-concept tool for cloud-based IoT environments, CIFT: Cloud-based IoT Forensic Toolkit, which can acquire cloud native artifacts from Alexa using unofficial APIs and analyze client-side artifacts associated with the use of a web-based application. We also tried to normalize all identified artifacts into a database file, and visualize them for evaluating our approach and further supporting the work of the digital forensics community.

9 **(6)**

When Alexa-enabled, Amazon Echo is not only a smart speaker, but operates as an intelligent, personal virtual assistant. As a cloud service, Alexa interacts with various Alexa-enabled devices such as Echo, and it can communicate with other compatible IoT devices and third-party applications by converting the voice requests to other services’ native communication protocol.

10 **(4)**

In November 2015, James Bates was charged with firstdegree murder of another man, who was found dead in Bates' hot tub. Police in Arkansas seized Bates' Alexa-enabled Echo smart speaker from his home, and asked Amazon to hand over any pertinent information regarding the device's communication with Alexa. However, Amazon denied the request in the absence of a valid and binding legal demand (Techcrunch).

11 **(1)**

The Internet of Things (IoT) is evolving rapidly along with the network of physical objects that contain embedded communication technology. Analysts predict that the worldwide IoT market will grow to $1.7 trillion in 2020 with a compound annual growth rate (CAGR) of 16.9% (IDC, 2015).

12 **(8)**

We propose a new digital forensic approach for the Amazon Alexa ecosystem combining cloud-side and client-side forensics. The acquisition of cloud-native artifacts from the Alexa is very important. Echo operations are based on Alexa, so the cloud includes many different types of artifacts related to user behaviors. Unfortunately, this approach has two limitations.