# FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things (FAIoT: Hacia la Construcción de un Sistema Ecológico Forense para Internet de las Cosas)

**Abstracto:**

El Internet de las cosas (IoT) involucra numerosas cosas inteligentes conectadas con diferentes tecnologías y estándares de comunicación. Si bien IoT abre nuevas oportunidades en varios campos, presenta nuevos desafíos en el campo de las investigaciones forenses digitales. Las herramientas y procedimientos existentes de análisis forense digital no pueden cumplir con la infraestructura altamente distribuida y heterogénea de IoT. Los investigadores forenses enfrentarán desafíos mientras identifican las pruebas necesarias del entorno de IoT y recopilan y analizan esas pruebas. En este artículo, proponemos la primera definición de trabajo de análisis forense de IoT y analizamos sistemáticamente el dominio forense de IoT para explorar los desafíos y problemas en esta rama especial de análisis forense digital.

**Publicado en:**[2015 IEEE International Conference on Services Computing](https://ieeexplore.ieee.org/xpl/conhome/7194374/proceeding)

**Fecha de la conferencia:** 27 de junio-2 de julio de 2015

**Fecha de adición a IEEE *Xplore* :** 20 de agosto de 2015

**Información del ISBN:**

**Número de acceso de INSPEC:** 15411583

**DOI:**[10.1109 / SCC.2015.46](https://doi.org/10.1109/SCC.2015.46)

**Editorial:**IEEE

**Lugar de la conferencia:** Nueva York, NY, EE. UU.

**SECCIÓN I.**

## **Introducción**

La naturaleza dominante de Internet y la miniaturización rentable de dispositivos electrónicos inteligentes introduce un nuevo paradigma informático: Internet de las cosas (IoT). El IoT se considera como la evaluación futura de Internet que se da cuenta de máquina a máquina (M2M), identificación por radiofrecuencia (RFID), computación sensible al contexto, computación portátil y ubicua [1] . La idea básica de IoT es permitir una conexión e intercambio de datos autónomos y seguros entre dispositivos y aplicaciones del mundo real [2] .

Todos los días, cientos de cosas físicas se conectan a Internet para compartir información local en el ciberespacio. El Consejo Nacional de Inteligencia de los Estados Unidos (NIC) estima que para 2025 los nodos de Internet pueden residir en la mayoría de nuestros paquetes de alimentos, muebles, documentos en papel y muchos más [3] . Según un informe de Gartner, habrá 26 mil millones de dispositivos IoT en los próximos cinco años [4] . International Data Corporation (IDC) pronostica que el mercado de IoT alcanzará $ 3.04 billones y habrá 30 mil millones de cosas conectadas en 2020 [5] . Estas cosas pueden variar en diferentes atributos: poder de procesamiento y cálculo, medio de comunicación, dimensión, etc. [6] .

Sin embargo, el rápido crecimiento de IoT también trae algunos desafíos nuevos en términos de seguridad. Dado que miles de millones de cosas están interconectadas para realizar actividades personales y comerciales, los atacantes pueden encontrar que IoT es un objetivo muy atractivo de ataques. Un individuo malintencionado también puede lanzar ataques desde el entorno IoT. La Oficina Europea de Policía (Europol) afirma que se espera que la primera muerte del mundo causada por el IoT ocurra antes de finales de 2014 [7] . Un atacante puede explotar la debilidad de los equipos cruciales de salud y seguridad o el canal de comunicación y activar instrucciones maliciosas para poner en peligro la vida de un paciente. Para investigar tales ataques, necesitamos ejecutar procedimientos forenses digitales en el paradigma IoT, al que nos referimos como *IoT Forensics* .

Desafortunadamente, el análisis forense digital en la era de IoT es un desafío porque las herramientas y procedimientos forenses digitales existentes no se ajustan al entorno de IoT. La gran cantidad de dispositivos IoT generará una gran cantidad de evidencia posible, lo que traerá nuevos desafíos para todos los aspectos de la gestión de datos. A los investigadores les resultará muy difícil recopilar pruebas de las infraestructuras de IoT altamente distribuidas. La gran variedad de dispositivos IoT también planteará problemas en el análisis de datos debido a los formatos heterogéneos de datos. La fiabilidad de la evidencia también puede ser cuestionable ya que el atacante puede alterar la evidencia que reside en los dispositivos IoT. Por otro lado, el IoT puede ofrecer nuevas oportunidades a los investigadores. Dado que los dispositivos IoT comparten información física local,

En este documento, abordamos los análisis forenses de IoT desde dos perspectivas: *primero* , la ejecución de procedimientos forenses digitales en las infraestructuras de IoT, cuando el IoT es blanco de ataques o se utiliza para lanzar un ataque; *segundo* determinar hechos nuevos / desconocidos utilizando la infraestructura de IoT. Con base en las características de IoT y los procedimientos forenses digitales, identificamos los desafíos de ejecutar cada uno de los procesos de forense digital, donde la evidencia permanece en las infraestructuras de IoT. Proponemos FAIoT, un modelo con conocimiento forense para las infraestructuras de IoT para apoyar ambas perspectivas.

### Contribución

Las contribuciones de este trabajo son las siguientes:

* To the best of the authors knowledge, this is the first work to formally define IoT forensics. The two different perspectives of IoT forensics introduced here can spawn future research in this area.
* We systematically analyze the challenges and opportunities for IoT forensics and propose a model for forensics-aware IoT - FAIoT. Our analysis can help researchers to focus on specific research sub-problems of the IoT forensics problem domain.

### Organization

The rest of the paper is organized as follows: Section II provides the background knowledge about digital forensics, IoT, IoT forensics, and a hypothetical case study. In section III, we present the challenges of IoT forensics. Section IV presents the FAIoT model. Section V presents the related work and finally, we conclude in Section VI.

**SECTION II.**

## **Background**

In this section, we first present a brief overview of digital forensics and the IoT. Next, we define IoT forensics and present a hypothetical case study of digital forensics involving the IoT environment.

### A. Digital Forensics

Before 2006, there had been no separate US Federal law for using electronically stored information (ESI) as evidence in civil cases. Federal Rules of Civil Procedure (FRCP) broadened the scope of evidence in the 2006 amendment and included ESI to be used in civil litigation [8]. FRCP defines the discoverable material and under this definition, data stored in hard disk, RAM, or Virtual Machine (VM) logs, all are discoverable material for the forensic investigation. According to a definition from NIST [9], digital forensic is “*an applied science to identify an incident, collection, examination, and analysis of evidence data*”. From the above working definitions, we note that digital forensics comprises four main processes:

* *Identification*: There are two main steps in identification: identification of an incident, and identification of the evidence, which will be required for successful investigation thereof, with potential correlation to other incident(s).
* *Collection*: In the collection process, an investigator extracts digital evidence from various media (*e.g*., hard disk, cell phone, e-mail, and many other types of data). The investigator also preserves the integrity of the evidence.
* *Organization*: There are two main steps in the organization process: examination and analysis of the digital evidence. In the examination phase, an investigator extracts and inspects the data and its characteristics. In the analysis phase, he or she interprets and correlates the available data to come to a conclusion, which can serve to prove or disprove civil, administrative, or criminal allegations (when interpreted legally).
* *Presentation*: In this process, an investigator makes an organized report to state his or her findings about the case. This report should be appropriate for presentation to the competent court or proceedings.

In digital forensics, maintaining the integrity of the information and strict chain of custody for the data is mandatory. Several other researchers define computer forensic as the procedure of examining computer system to determine potential legal evidence [10], [11].

### B. Internet of Things (iot)

The idea of Internet of Things (IoT) was first proposed by MIT's Auto-ID centre [12]. The International Telecommunication Union's (ITU) Internet report 2005 formally proposed the Internet of Things [13]. According to the report, we are heading towards the age of ubiquitous network society, in which networks and networked devices are omnipresent. All of our surrounding things will be interconnection through the Internet of things for data interchange; These things include personal computers, laptops, tablets, smart phones, insulin pump, tires, refrigerator, television, air cooler/heater, and many more. By 2020, there will be 10 connected IoT devices for every person of the world and 40 to 80 billion IoT devices in total [14]. Most of the IoT devices embed different sensors and actuators that can sense, perform computation, take intelligent decisions and transmit useful collected information over the Internet.

The Internet of Things involves many heterogeneous technologies. Among them, RFID (radio frequency identification) and wireless sensor technology are most mature. There is a wide range of applications for IoT such as home appliance control, health care management, automotive services, inventory management, and many more. In general, the IoT devices capture data from the physical environment through different sensors and sends the data to the cloud for intelligent decision making or for other data processing tasks.

### C. Iot Forensics

We define IoT forensics as an especial branch of digital forensics, where the identification, collection, organization, and presentation processes deal with the IoT infrastructures to establish the facts about a criminal incident.

We identify IoT forensics as a combination of three digital forensics schemes: device level forensics, network forensics, and cloud forensics, which are illustrated in the Figure 1.

**Fig. 1:**

Iot forensics

[View All](https://ieeexplore.ieee.org/document/7207364/all-figures)

* *Device level forensics*: An investigator may need to collect data from the local memory of the IoT devices. When a crucial piece of evidence needs to be collected from the IoT devices, it involves the device level foren-sics.
* *Análisis forense de la red* : la fuente de diferentes ataques se puede identificar a partir de los registros de la red. Por lo tanto, los registros de red pueden ser muy cruciales para condenar o exonerar a un sospechoso. Las infraestructuras de IoT incluyen diferentes formas de redes, tales como Red de área corporal (BAN), Red de área personal (PAN), Redes de área de hogar / hospital (HAN), Redes de área local (LAN) y Redes de área amplia (WAN). Se puede recopilar evidencia importante de cualquiera de estas redes.
* *Análisis forense de la nube* : uno de los roles más importantes en el dominio forense de IoT será el análisis forense de la nube. Dado que la mayoría de los dispositivos IoT tienen poca capacidad de almacenamiento y computación, los datos generados por los dispositivos IoT y las redes IoT se almacenan y procesan en la nube. Esto se debe a que las soluciones en la nube ofrecen varios beneficios que incluyen conveniencia, gran capacidad, escalabilidad y accesibilidad bajo demanda.

#### Estudio de caso hipotético

Alice sufre de un nivel alto de azúcar en la sangre y siempre usa un dispositivo monitor de azúcar en la sangre. En su casa, hay otros dispositivos inteligentes, como sistema de calefacción, televisión, refrigerador, dispensador de medicamentos inteligente, automóvil, etc. Todos estos dispositivos están conectados a Internet y son controlables desde el dispositivo móvil de Alice. Alice también trabaja en un hospital, donde hay miles de dispositivos IoT relacionados con la atención médica y el hospital permite a sus empleados conectar sus dispositivos inteligentes con la red del hospital. Mallory crea un malware inteligente para recopilar datos de los dispositivos inteligentes de atención médica. Primero, infecta el refrigerador inteligente de Alice, se conecta con el monitor de azúcar en sangre de Alice a través de la red compartida y, finalmente, infecta el monitor de azúcar en sangre. Más tarde, cuando Alice va al hospital a trabajar, El malware busca otros dispositivos que comparten la misma red que el monitor de azúcar en la sangre. De esta manera, Mallory puede infectar cientos de dispositivos inteligentes de atención médica ubicados en el hospital y roba registros médicos electrónicos (EMR) confidenciales. Cuando se identifica la violación de datos, Bob, un investigador forense, es asignado para investigar el caso. La cantidad y variedad de dispositivos IoT disponibles en el hospital harán que la investigación de Bob sea muy desafiante. Bob necesita ejecutar análisis forenses a nivel de dispositivo para todos los dispositivos disponibles. Más tarde, debe investigar los registros de red de todos los dispositivos para identificar la fuente de infección. Esto no solo incluye los dispositivos inteligentes para el cuidado de la salud, sino también el dispositivo móvil inteligente que los profesionales de la salud generalmente traen todos los días.

**SECCION III.**

## **Desafíos en Iot Forensics**

Las herramientas y tecnologías tradicionales de análisis forense digital no están diseñadas para manejar completamente la infraestructura de IoT. En esta sección, identificamos los desafíos en cada uno de los pasos del análisis forense digital, al mismo tiempo que tratamos con el entorno de IoT.

### A. Identificación

Los miles de millones de dispositivos IoT generarán una gran cantidad de datos. Cuando la cantidad de evidencia posible es muy grande, es difícil identificar las pruebas importantes que se pueden usar para determinar los hechos sobre un incidente criminal. Por ejemplo, hay miles de dispositivos IoT en un hospital y solo uno de los dispositivos puede estar compuesto y filtrar registros médicos electrónicos confidenciales (EMR). Sin embargo, la cantidad de registros generados a partir de los miles de dispositivos IoT del hospital puede ser muy grande, y encontrar evidencia para identificar el dispositivo comprometido puede tratarse como encontrar una aguja en el pajar.

### B. Colección

After identifying the evidence, investigators need to collect the evidence to analyze and find the facts. Any errors that have been occurred in the collection phase will propagate to the evidence organization and reporting phase, which will eventually affect the whole investigation process. Hence, this is one of the most crucial steps of forensic procedure.

Some of the factors that make the data acquisition process in IoT forensic harder than traditional computer forensics are discussed below:

El Internet de las cosas involucra numerosos nodos conectados con diferentes tecnologías y estándares de comunicación. Un investigador puede encontrar muy difícil recopilar evidencia de estas infraestructuras altamente distribuidas. Para un entorno hospitalario, donde hay miles de dispositivos IoT, es posible que ni siquiera sea posible recopilar evidencia de todos los dispositivos IoT del hospital en un corto período de tiempo.

Debido a la limitación de almacenamiento de los dispositivos IoT, la mayoría de los datos generados por los dispositivos IoT se almacenan en la nube. Dado que las nubes serán una de las principales fuentes de evidencia para el análisis forense de IoT, algunos de los problemas de recopilación de evidencia de las nubes se aplican para el análisis forense de IoT, como la inaccesibilidad física a las nubes. Los procedimientos y herramientas forenses digitales establecidos suponen que tenemos acceso físico a los recursos informáticos, por ejemplo, disco duro, enrutador de red, etc. Sin embargo, en el análisis forense de la nube, la situación es diferente. A veces, ni siquiera sabemos dónde se encuentran los datos, ya que se distribuyen entre muchos hosts en múltiples centros de datos. Varios investigadores abordan este problema en su trabajo [15] , [16]

Dado que la información confidencial, como EMR, puede filtrarse del IoT, el proceso de recopilación puede sufrir problemas legales, especialmente las leyes de privacidad y protección de datos. Estas leyes pueden variar según la jurisdicción. Puede suceder que un investigador forense se encuentre en una jurisdicción y los datos residan en otra jurisdicción, donde las leyes de privacidad de estas dos jurisdicciones no están en armonía. Por lo tanto, las organizaciones deben considerar cuidadosamente las ramificaciones legales de dónde almacenan y procesan los datos para asegurarse de que cumplen con las regulaciones que enfrentan [17] .

### C. Organización

Hasta ahora, no existe un protocolo o estándar ampliamente aceptado para IoT. Los proveedores están utilizando sus protocolos patentados para la comunicación de cosas a cosas. La amplia variedad de estructura de los datos generados por los dispositivos IoT dificulta la fase de examen y análisis.

El análisis de registros de diferentes fuentes juega un papel vital en la investigación forense digital. Los registros de proceso, los registros de red y los registros de aplicaciones son realmente útiles para identificar varias actividades maliciosas y los usuarios detrás de esas actividades maliciosas. Un formato estándar de registros puede facilitar la fase de organización de datos. Organizar los registros recopilados de diferentes fuentes (como múltiples dispositivos IoT) es un desafío, ya que no hay formatos estándar para registros en diferentes sistemas. Es posible que algunos de los registros ni siquiera proporcionen información crucial para fines forenses, por ejemplo, quién, cuándo, dónde y por qué se ejecutó algún incidente [18] . Podríamos correlacionar los registros recopilados de diferentes dispositivos de IoT e identificar información crucial si hubiera un formato estándar para los registros.

Dentro de IoT, esperamos ver una explosión de datos debido a la mayor cantidad de dispositivos interconectados que se comunicarán e intercambiarán información a través de la autopista de información de IoT. Organizar un conjunto de datos tan grande para identificar los hechos sobre un incidente criminal puede ser un desafío. Para un conjunto de datos muy grande de evidencia, la revisión manual y la toma de decisiones no pueden funcionar. A menudo, requiere técnicas y herramientas especiales de minería de datos para identificar los hechos [19] , [20] .

### D. Presentación

El último paso de la investigación forense digital es la presentación, donde un investigador acumula sus hallazgos y los presenta ante el tribunal como evidencia de un caso. Los desafíos también se encuentran en este paso del análisis forense de IoT. Proporcionar la evidencia frente al jurado para la informática forense tradicional es relativamente fácil en comparación con la complejidad de administrar los datos de IoT. Los miembros del jurado posiblemente tengan conocimientos básicos de computadoras personales o, como máximo, de almacenamiento local privado. Pero los aspectos técnicos detrás de la identificación, el filtrado y el análisis de datos de un entorno de IoT altamente distribuido y heterogéneo pueden ser demasiado complejos para que puedan entenderlos.

**SECCION IV.**

## **Oportunidades y oportunidades con conocimiento forense**

En esta sección, primero presentamos un modelo para IoT forense-consciente (FAIoT). Luego, presentamos nuevas oportunidades disponibles para los investigadores forenses digitales de la FAIoT.

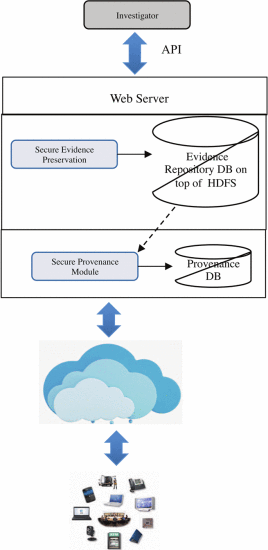
### A. El modelo Faiot

Dado que la infraestructura de IoT está altamente distribuida y no existe una estandarización entre los dispositivos, proponemos un repositorio de evidencia confiable centralizado en FAIoT para facilitar el proceso de recolección y análisis de evidencia. El depósito de pruebas también aplicará el esquema de registro seguro [21] para garantizar la fiabilidad de las pruebas. Podemos considerar esto como un nuevo servicio disponible para todos los dispositivos IoT. Los dispositivos solo necesitan registrar este servicio de repositorio de evidencia seguro. La Figura 2 ilustra nuestro modelo propuesto.

#### Módulo de preservación segura de evidencia

Este módulo supervisará constantemente todos los dispositivos IoT registrados y almacenará pruebas de forma segura en el repositorio de pruebas. La evidencia puede ser registros de red, registros de registro, lecturas de sensores, etc. Mientras se preservan los datos, este módulo puede encargarse de segregar los datos de acuerdo con los dispositivos IoT y su propietario. De esta manera, los datos de múltiples usuarios no se mezclarán. Este módulo también preservará la confidencialidad de los datos de los empleados maliciosos de la nube mediante el uso de cifrado basado en clave pública-privada, de modo que solo los investigadores puedan ver los datos.

Dicho repositorio necesita manejar un conjunto de datos muy grande. Por lo tanto, proponemos utilizar el Sistema de archivos distribuidos de Hadoop (HDFS) para el repositorio de pruebas. Hadoop 1 es una implementación de código abierto del marco de MapReduce patentado de Google. El HDFS es el componente del sistema de archivos de Hadoop, que está diseñado para almacenar conjuntos de datos muy grandes de manera confiable y para transmitir esos conjuntos de datos con un gran ancho de banda a las aplicaciones del usuario [22] . Por lo tanto, HDFS funcionará mejor que los sistemas tradicionales de administración de bases de datos al recuperar una pequeña información de un gran conjunto de datos de posible evidencia.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/7194374/7207317/7207364/7207364-fig-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/7194374/7207317/7207364/7207364-fig-2-source-large.gif)

**Figura 2:**

Un modelo conceptual de iot forense

[Ver todo](https://ieeexplore.ieee.org/document/7207364/all-figures)

#### Módulo de procedencia segura

This module ensures the proper chain of custody of the evidence by preserving the access history of the evidence. Using provenance aware file system (PASS) [23], the evidence repository can produce the provenance record for evidence usage. However, as all the evidence and the access history are under the control of secure evidence repository provider, they can always tamper with the provenance record. Moreover, from the provenance data in cloud, an attacker can learn confidential information about the data stored in cloud. To protect provenance information from these types of attack, we need a secure provenance scheme. This module will apply secure provenance chaining [24] to preserve the integrity of the provenance record.

#### Access to Evidence Through API

We propose to provide secure read-only APIs to law enforcement agencies. Only the investigators and the court will have access to these APIs. They can collect the preserved evidence and the provenance information by calling these APIs. To implement this feature, the secure evidence repository provider need additional web server, which will communicate with the previously described modules to collect the requested data by an API call. The web server provides Representational State Transfer (REST) based API using the synchronized data, and the provenance record as resources. To retrieve these evidence, GET operations can be used on the resources. Caller of a REST service can pass different parameters to retrieve his desired result.

### B. Opportunities

The availability of FAIoT can also brings new opportunities for digital forensics investigators. Since IoT share physical information to the virtual world, this can give new information to the investigator and can help to identify new insights for a criminal activity.

From the various on-board sensors and logs of these IoT devices, we can identify important information of the surroundings of the devices that can help us to determine facts about a criminal incident. For example, by correlating data of different IoT devices, we can determine the location of a suspect at a particular time. From the data of the IoT devices of the suspect's home or office building, we can determine whether the suspect was at either of these places. From the wearable activity monitors' data, we can also identify the approximate location of the suspect. An ideal solution to handle large amount of sensor data will quickly identify crucial information of a criminal case.

**SECTION V.**

## **Related Work**

La seguridad de la infraestructura de IoT ha sido abordada por los investigadores. Oren *y col* . demostró que un televisor inteligente podría verse comprometido con una antena barata y mediante la transmisión de mensajes, ya que se basa en un estándar de televisión híbrido de transmisión de banda ancha (HbbTV) [25] . Los investigadores de IOActive Labs [26] presentaron un mecanismo que puede usarse para atacar los sistemas de control de tráfico. Los sensores magnéticos utilizados en las calles (para recopilar y difundir datos) podrían verse comprometidos al usar transmisores profesionales o antenas de un par de millas de distancia, ya que existen pocos protocolos de seguridad.

En [27] , los investigadores presentaron un método de delegación de acceso con consideraciones de seguridad basadas en el modelo de Control de acceso basado en el contexto (CCAAC) basado en la capacidad destinado a la comunicación federada de máquina a máquina o redes IoT. Al usar el enfoque de control de acceso basado en identidad y capacidad junto con la información contextual y la IoT federada segura, el modelo propuesto proporciona escalabilidad y flexibilidad, así como una delegación de autoridad segura para un sistema altamente distribuido. Ning *y col* . propuso una arquitectura de seguridad basada en ciber-físico-social para abordar las perspectivas de seguridad de información, física y de gestión, y presenta cómo las abstracciones arquitectónicas apoyan el modelo de IoT [28] . En [29], los investigadores examinaron las evidencias digitales recopiladas de los dispositivos móviles y propusieron un esquema para correlacionar la ubicación del teléfono móvil con los contactos en función de las llamadas entrantes y salientes.

Los investigadores proponen varias soluciones para facilitar el proceso de análisis forense digital en la nube. Para que la red, el proceso y los registros de acceso estén disponibles para los clientes, Bark *et al* . propuso exponer las API de solo lectura por parte de los CSP [30] . Al utilizar estas API, los clientes pueden recopilar información valiosa y proporcionarla a los investigadores. Recientemente, Dykstra *et al* . implementó FROST [31] , una herramienta de recopilación de datos forenses para OpenStack. Usando FROST, los usuarios / investigadores de la nube pueden adquirir una imagen de los discos virtuales asociados con cualquiera de las máquinas virtuales del usuario, y validar la integridad de esas imágenes con sumas de verificación criptográficas. También es posible recopilar registros de todas las **API**solicitudes realizadas a los registros de firewall de CSP y OpenStack para las máquinas virtuales de los usuarios. Para obtener los registros necesarios del modelo de nube IaaS y preservar la integridad y confidencialidad de los registros, Zawoad *et al* . propuesta de registro seguro como servicio (SecLaaS) [21] . Al utilizar este servicio, los investigadores pueden recopilar varios registros importantes, por ejemplo, registros de red, procesos, registros y aplicaciones. SecLaaS también puede detectar cualquier alteración de los registros por parte de un CSP malicioso o un investigador forense malicioso. Thorpe *y col* . desarrolló un auditor de registro utilizando la relación 'sucedió antes' [32] en el entorno de la nube [33] . Delport y col. se centró en aislar una instancia para mitigar el problema de la tenencia múltiple en el análisis forense de la nube [34].

El trabajo de cierre relacionado con nuestro trabajo se presenta en [35] . En este documento, los investigadores presentaron el diseño del Sistema Forense de Administración de Bordes (FEMS), un sistema que proporciona de manera autónoma servicios forenses y de seguridad dentro del Internet de las Cosas (IoT) o el contexto del hogar inteligente. FEMS se enfoca en la solución definida por el usuario para administrar la evidencia basada en IoT. Si bien proporciona el control de los usuarios, el sistema propuesto también brinda a los usuarios maliciosos la oportunidad de alterar la evidencia.

**SECCION VI.**

## **Conclusión**

El rápido aumento de los dispositivos IoT crea nuevas superficies de ataque. Por lo tanto, existe una creciente necesidad de proporcionar soporte forense en el entorno de IoT. Sin embargo, la infraestructura de IoT, la gran cantidad de dispositivos de IoT y la gran variedad de dispositivos de IoT imponen nuevos desafíos para los investigadores forenses digitales. En este artículo, definimos el término análisis forense de IoT e identificamos los desafíos de ejecutar análisis forenses confiables en el dominio de IoT. También proponemos un modelo conceptual para ejecutar análisis forense digital en la infraestructura de IoT. Resolver todos los desafíos del análisis forense de IoT puede abrir la oportunidad de identificar muchas nuevas ideas que antes no eran posibles.

### RECONOCIMIENTO

Esta investigación fue apoyada por el National Care Foundation CAREER Award CNS-1351038, un Google Faculty Research Award y el Departamento de Seguridad Nacional Grant FA8750-12-2-0254.