# FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger (FIF-IoT: un marco de investigación forense para IoT utilizando un libro público digital)

**Abstracto:**

La mayor implementación de dispositivos de Internet de las cosas (IoT) los convertirá en blanco de ataques. Los dispositivos IoT también se pueden usar como herramientas para cometer delitos. En este sentido, proponemos FIF-IoT, un marco de investigación forense que utiliza un libro de contabilidad digital público para encontrar hechos en incidentes criminales en sistemas basados ​​en IoT. FIF-IoT recopila interacciones que tienen lugar entre varias entidades de IoT (nubes, usuarios y dispositivos de IoT) como evidencia y las almacena de forma segura como transacciones en una red de blockchain pública, distribuida y descentralizada que es similar a la red de Bitcoin. Por lo tanto, FIF-IoT elimina el control de una sola entidad sobre el almacenamiento de evidencia, evita un solo punto de falla en los medios de almacenamiento y garantiza una alta disponibilidad de evidencia. FIF-IoT presenta un marco que garantiza integridad, confidencialidad, anonimato, y no repudio de la evidencia almacenada en el libro digital público. Además, FIF-IoT proporciona un mecanismo para adquirir evidencia del libro mayor y para verificar la integridad de la evidencia obtenida. Presentamos un estudio de caso de una investigación forense para demostrar que FIF-IoT es seguro contra la manipulación de pruebas. También implementamos un prototipo para evaluar el rendimiento de FIF-IoT.

**Publicado en:**[Congreso Internacional IEEE 2018 sobre Internet de las Cosas (ICIOT)](https://ieeexplore.ieee.org/xpl/conhome/8457595/proceeding)

**Fecha de la conferencia:** 2-7 de julio de 2018

**Fecha añadida a IEEE *Xplore* :** 27 de septiembre de 2018

**Información del ISBN:**

**Número de acceso de INSPEC:** 18115877

**DOI:**[10.1109 / ICIOT.2018.00012](https://doi.org/10.1109/ICIOT.2018.00012)

**Editorial:**IEEE

**Lugar de la conferencia:** San Francisco, California, EE. UU.

**SECCIÓN I.**

## **Introducción**

El concepto de Internet de las cosas (IoT) ya ha sido implementado por numerosos dominios de aplicaciones, como el hogar inteligente, la atención médica, los vehículos y los dispositivos portátiles [1] - [2] [3] . Los dispositivos de IoT realizan operaciones críticas de seguridad, como el monitoreo de las condiciones de salud de los pacientes, y almacenan información confidencial, como registros de salud [4] . Como tal, los sistemas basados ​​en IoT son de gran interés para los atacantes [5]. Un ataque exitoso en estos sistemas puede poner en peligro la vida de sus usuarios. Puede ser mortal para un paciente si el marcapasos habilitado para IoT del paciente se ve comprometido. Del mismo modo, los ataques contra un vehículo inteligente pueden provocar un accidente. Además, los adversarios pueden comprometer los electrodomésticos inteligentes, como las cámaras de vigilancia, para espiar a los residentes de una casa inteligente.

Los enfoques forenses convencionales, como los medios [6] , la nube [7] y la red forense [8] , no se pueden aplicar tal cual para establecer hechos en los sistemas basados ​​en IoT debido a las siguientes limitaciones: *a)* adquisición de registros almacenado en el almacenamiento de un dispositivo (análisis forense de medios [6] ) puede no ser posible para los dispositivos implantados en el cuerpo o los dispositivos que deben permanecer siempre en línea; *b)* Registros de nubes [7]utilizado para investigar los ciberataques basados ​​en el servicio en la nube no puede utilizarse como evidencia en escenarios en los que se accede localmente a los servicios que se ejecutan en dispositivos IoT: los clientes y los dispositivos IoT se ubican en la misma red y los clientes acceden directamente a los dispositivos IoT; *c) Los* registros de red utilizados en análisis forense de red [8] pueden no ser útiles para analizar incidentes en sistemas móviles basados ​​en ioT porque en estos sistemas los dispositivos están asignados con direcciones temporales de Protocolo de Internet (IP) y las topologías de red cambian con el tiempo (por ejemplo, redes ad-hoc). Aunque la investigación actual funciona [9] - [10] [11] [12] [13] [14] [15] [16] [17]en IoT, los forenses destacan las fuentes de evidencia en IoT y brindan instrucciones sobre los procedimientos de examen de incidentes, no brindan respuestas a las siguientes preguntas: *i)* ¿Cómo recolectar y almacenar evidencia de los sistemas basados ​​en IoT? *ii)* ¿Cómo garantizar la integridad, confidencialidad, anonimato y la procedencia segura de la evidencia? *iii)* ¿Cómo evitar un solo punto de falla en los medios de almacenamiento de evidencia y lograr una alta disponibilidad de la evidencia? *iv)* ¿Cómo verificar la integridad de la evidencia obtenida durante una investigación?

Con respecto a las preguntas planteadas anteriormente, proponemos FIF-IoT, un marco de investigación forense para sistemas basados ​​en IoT que utilizan un libro digital descentralizado, distribuido y público. En FIF-IoT, el libro mayor mantiene una lista creciente de registros, llamada blockchain. Un bloque contiene una lista de transacciones, y una transacción incluye información sobre las interacciones entre las diversas entidades de un sistema basado en IoT, como dispositivos IoT, usuarios y servicios en la nube. Como tal, el libro digital mantiene una procedencia de interacción. El libro mayor está disponible públicamente y se distribuye entre las partes interesadas de un sistema basado en IoT. Los usuarios, los proveedores de servicios de IoT, los fabricantes de dispositivos de IoT, las compañías de seguros, los organismos encargados de hacer cumplir la ley, las firmas de auditoría, etc., son las partes interesadas de un sistema basado en IoT y mantienen una copia del libro mayor. Así, se elimina el control de una entidad única y central (inserción, eliminación y modificación) sobre la cadena de bloques de interacción, y se garantiza una alta disponibilidad de la evidencia. Antes de almacenar las interacciones en la blockchain pública, estas son firmadas por las partes involucradas y encriptadas usando la clave pública de un tercero confiable (un servicio de depósito de garantía). En consecuencia, el propósito de FIF-IoT es garantizar la integridad, confidencialidad y no repudio de las interacciones de modo que los bloques de interacción se utilicen como evidencia durante la investigación de un incidente de preocupación forense. Las interacciones también se pueden usar para resolver disputas en los sistemas basados ​​en IoT, como la violación de los acuerdos de nivel de servicio por parte de los proveedores de servicios de IoT o las leyes de tránsito en los sistemas de transporte inteligentes. y modificación) sobre la cadena de bloques de interacción se elimina y se garantiza una alta disponibilidad de la evidencia. Antes de almacenar las interacciones en la blockchain pública, estas son firmadas por las partes involucradas y encriptadas usando la clave pública de un tercero confiable (un servicio de depósito de garantía). En consecuencia, el propósito de FIF-IoT es garantizar la integridad, confidencialidad y no repudio de las interacciones de modo que los bloques de interacción se utilicen como evidencia durante la investigación de un incidente de preocupación forense. Las interacciones también se pueden usar para resolver disputas en los sistemas basados ​​en IoT, como la violación de los acuerdos de nivel de servicio por parte de los proveedores de servicios de IoT o las leyes de tránsito en los sistemas de transporte inteligentes. y modificación) sobre la cadena de bloques de interacción se elimina y se garantiza una alta disponibilidad de la evidencia. Antes de almacenar las interacciones en la blockchain pública, estas son firmadas por las partes involucradas y encriptadas usando la clave pública de un tercero confiable (un servicio de depósito de garantía). En consecuencia, el propósito de FIF-IoT es garantizar la integridad, confidencialidad y no repudio de las interacciones de modo que los bloques de interacción se utilicen como evidencia durante la investigación de un incidente de preocupación forense. Las interacciones también se pueden usar para resolver disputas en los sistemas basados ​​en IoT, como la violación de los acuerdos de nivel de servicio por parte de los proveedores de servicios de IoT o las leyes de tránsito en los sistemas de transporte inteligentes. Antes de almacenar las interacciones en la blockchain pública, estas son firmadas por las partes involucradas y encriptadas usando la clave pública de un tercero confiable (un servicio de depósito de garantía). En consecuencia, el propósito de FIF-IoT es garantizar la integridad, confidencialidad y no repudio de las interacciones de modo que los bloques de interacción se utilicen como evidencia durante la investigación de un incidente de preocupación forense. Las interacciones también se pueden usar para resolver disputas en los sistemas basados ​​en IoT, como la violación de los acuerdos de nivel de servicio por parte de los proveedores de servicios de IoT o las leyes de tránsito en los sistemas de transporte inteligentes. Antes de almacenar las interacciones en la blockchain pública, estas son firmadas por las partes involucradas y encriptadas usando la clave pública de un tercero confiable (un servicio de depósito de garantía). En consecuencia, el propósito de FIF-IoT es garantizar la integridad, confidencialidad y no repudio de las interacciones de modo que los bloques de interacción se utilicen como evidencia durante la investigación de un incidente de preocupación forense. Las interacciones también se pueden usar para resolver disputas en los sistemas basados ​​en IoT, como la violación de los acuerdos de nivel de servicio por parte de los proveedores de servicios de IoT o las leyes de tránsito en los sistemas de transporte inteligentes. y el no repudio de las interacciones de modo que los bloques de interacción se utilicen como evidencia durante la investigación de un incidente de preocupación forense. Las interacciones también se pueden usar para resolver disputas en los sistemas basados ​​en IoT, como la violación de los acuerdos de nivel de servicio por parte de los proveedores de servicios de IoT o las leyes de tránsito en los sistemas de transporte inteligentes. y el no repudio de las interacciones de modo que los bloques de interacción se utilicen como evidencia durante la investigación de un incidente de preocupación forense. Las interacciones también se pueden usar para resolver disputas en los sistemas basados ​​en IoT, como la violación de los acuerdos de nivel de servicio por parte de los proveedores de servicios de IoT o las leyes de tránsito en los sistemas de transporte inteligentes.

### Contribuciones

Las contribuciones de este artículo son las siguientes:

1. Proponemos un marco de investigación forense para IoT utilizando tecnología blockchain descentralizada y distribuida.
2. Proponemos un modelo para recolectar evidencia y un esquema de evidencia de manipulación para almacenar evidencia de manera confiable.
3. Realizamos un análisis de seguridad de FIF-IoT e implementamos un prototipo FIF-IoT utilizando dispositivos IoT habilitados para Contiki.

### Organización

En la Sección II , brindamos motivación detrás de nuestro trabajo. Discutimos el modelo de amenaza en la Sección III . La sección IV presenta la arquitectura de FIF-IoT. El análisis de seguridad de FIF-IoT se proporciona en las secciones V y VI . Presentamos la evaluación experimental de FIF-IoT en la Sección VII . Presentamos la revisión de la literatura en la Sección VIII . Finalmente, concluimos este artículo en la Sección IX .

**SECCION II.**

## **Antecedentes y motivación**

Las herramientas y procedimientos forenses digitales convencionales no se ajustan al entorno de IoT [18] - [19] [20] debido a la movilidad, la naturaleza distribuida y descentralizada de los dispositivos y servicios de IoT, como Internet de vehículos y IoT portátil. Además, la gran cantidad de dispositivos inteligentes generará una gran cantidad de evidencia posible, lo que traerá nuevos desafíos para todos los aspectos de la gestión de datos [15] . A los investigadores les resultará muy difícil recopilar pruebas de las infraestructuras altamente distribuidas y descentralizadas de IoT [12] . La gran variedad de dispositivos IoT también generará problemas en el análisis de evidencia debido a los diversos formatos de datos [10]. La fiabilidad de la evidencia también puede ser cuestionable ya que el atacante puede alterar la evidencia almacenada en los dispositivos IoT [21] , [22] . 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 de la evidencia

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, el número 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. Recolección de evidencia y adquisición

Después de identificar la evidencia, los investigadores recolectan evidencia para analizar y encontrar los hechos. Los errores ocurridos en la fase de recolección pueden afectar el resultado de una investigación. Las siguientes características de los sistemas basados ​​en IoT hacen que el proceso de adquisición de datos en el análisis forense de IoT sea más difícil que el análisis forense informático tradicional.

#### Cantidad masiva de datos Iot

El IoT involucra numerosos nodos conectados con diferentes tecnologías y estándares de comunicación. Un investigador puede encontrar muy difícil recopilar evidencia de esta infraestructura altamente distribuida. 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.

#### Redes multiprotocolo

Los dispositivos IoT pueden usar protocolos no IP mientras se comunican con dispositivos proximales ubicados en el área del cuerpo, el área personal o la red de área local. Al mismo tiempo, estos dispositivos pueden comunicarse con proveedores de servicios en la nube a través de la red IP. Es posible que los esquemas, herramientas y tecnologías forenses digitales contemporáneos no estén diseñados teniendo en cuenta todas las propiedades de cada protocolo de comunicación para proporcionar registros significativos a los investigadores.

#### Limitación de almacenamiento en el dispositivo

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 nubes se aplican para el análisis forense de IoT, como la inaccesibilidad física a las nubes [23] . Además, es posible que los investigadores no puedan obtener evidencia de algunos dispositivos IoT que están implantados en el cuerpo humano o que requieren estar encendidos todo el tiempo.

#### Sistemas operativos en tiempo real (RTOS)

Los dispositivos IoT están integrados con RTOS que procesan los datos a medida que entran. Por ejemplo, los sensores portátiles y los actuadores médicos ejecutan aplicaciones en tiempo real que procesan una solicitud de inmediato para enviar actualizaciones sobre las condiciones físicas de un paciente. Estas aplicaciones están diseñadas para procesar datos en la memoria no volátil para evitar retrasos de almacenamiento en búfer. Eso significa que los datos no se almacenan en la memoria volátil. Como resultado, puede ser difícil para los investigadores adquirir evidencia digital de dispositivos IoT.

#### Topología de red dinámica

Los dispositivos IoT móviles, como los automóviles inteligentes y los sensores portátiles, pueden unirse o salir de una red en cualquier momento. Una topología de red se vuelve dinámica debido a las propiedades de unión y salida de dispositivos temporales y espaciales. Sin embargo, las herramientas y procedimientos forenses digitales existentes pueden no ser capaces de manejar tales cambios repentinos en la topología de la red.

#### Manipulación de nodos

Los adversarios pueden usar técnicas anti-forenses para desactivar el soporte forense del dispositivo. Por ejemplo, los adversarios pueden alterar el software incorporado o los registros del dispositivo para destruir o modificar la evidencia. Sin embargo, no se puede garantizar que todos los dispositivos inteligentes estén integrados con un embalaje resistente a la manipulación para proteger dicha técnica.

### C. Organización de la evidencia

Analizar registros de diferentes fuentes juega un papel vital en la investigación forense digital [24] . 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 tarea de análisis de evidencia. Organizar los registros recopilados de diferentes fuentes (como múltiples dispositivos IoT) es un desafío porque existen diferencias entre los registros en los diferentes sistemas. Es posible que algunos de los registros ni siquiera proporcionen información crucial para un propósito forense, por ejemplo, quién, cuándo, dónde y por qué se ejecutó un incidente [25] . Podríamos correlacionar los registros recopilados de diferentes dispositivos de IoT e identificar información crucial si hubiera un formato estándar para los registros.

### D. Examen de evidencia

La evidencia se puede recuperar de varias fuentes, como nubes, redes y dispositivos, bajo ciertas circunstancias. Las herramientas y métodos forenses digitales convencionales pueden no ser capaces de establecer una conexión entre la evidencia recopilada de varias fuentes. Por ejemplo, estas técnicas pueden no rastrear un incidente que se origina en la nube y termina en la red perimetral o viceversa. Como tal, se hace difícil para un examinador determinar la evidencia crucial que se analizará primero cuando se le presente al examinador una gran cantidad de registros de nube, red y dispositivos.

**SECCION III.**

## **Modelo de amenaza**

En esta sección, primero, presentamos algunos incidentes hipotéticos de preocupación forense en sistemas basados ​​en IoT. A continuación, presentamos escenarios de colusión que pueden afectar el resultado de la investigación de un incidente.

### A. Caso hipotético de preocupación forense

#### Iot Botnet

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 teléfonos inteligentes, sistemas de calefacción, televisores, refrigeradores, dispensadores de medicamentos inteligentes y automóviles. 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 teléfono 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 sangre. Si tiene éxito, Mallory puede infectar cientos de dispositivos inteligentes de atención médica ubicados en el hospital y roba registros médicos electrónicos confidenciales (EMR). Cuando se identifica la violación de datos, se asigna a Bob, un investigador forense, para investigar el caso.

#### Incidentes en Iot Healthcare

El nivel de azúcar en la sangre de Alice aumenta tanto que debe ser hospitalizada para un mejor tratamiento. Una enfermera instala una bomba de insulina inteligente que monitorea el nivel de glucosa de Alice y libera insulina si es necesario. La enfermera usa una computadora, que está conectada a la bomba de insulina a través de un medio inalámbrico, para emitir un comando a la bomba de insulina para controlar (aumentar o disminuir) la dosis de insulina. La computadora también muestra periódicamente el nivel de glucosa actual de Alice. La bomba de insulina también es lo suficientemente inteligente como para ajustar el nivel de dosis de insulina de acuerdo con el nivel de azúcar detectado. La enfermera nota un aumento repentino en la glucosa de Alice. La enfermera investiga y encuentra que la bomba de insulina está liberando una dosis alta de insulina y con una frecuencia alta cuando no es necesario. La administración del hospital presenta un reclamo de seguro contra el fabricante de la bomba de insulina debido a un mal funcionamiento del dispositivo. Bob es asignado para investigar el caso.

### B. Colusión durante una investigación

Las partes interesadas de un sistema basado en ioT pueden coludir para manipular el resultado de la investigación. Por ejemplo, las partes interesadas de un servicio de salud de IoT son un investigador, un paciente que usa sensores médicos, los fabricantes de sensores portátiles, el proveedor de la aplicación que se ejecuta en el dispositivo médico, un médico, el editor de las aplicaciones médicas instaladas en el médico. smartphone, el proveedor de un servicio en la nube que almacena registros médicos y permite al médico controlar la condición de salud del paciente de forma remota, y los proveedores de seguros. Durante una investigación, una o más partes interesadas pueden confabularse para enmarcar a una parte interesada inocente o para salvar a una parte interesada maliciosa de la acusación mediante la manipulación de pruebas, como registros falsificados y modificados.

Por ejemplo, el proveedor de seguros puede coludir con el proveedor de servicios en la nube (CSP) para proporcionar evidencia falsa o modificada a Bob para culpar a los fabricantes o al proveedor de aplicaciones de los dispositivos médicos. En otro escenario, un investigador deshonesto puede coludir con el médico y el paciente para enmarcar al inocente CSP. pornorte número de partes interesadas, el número total de escenarios de colusión ( Tc s) es la combinación posible ( c ) I de partes interesadas para grupos de tamaño variable ( i ); por lo tanto,Tc s se calcula como ∑i = 1norteCryo.

**SECCION IV.**

## **Bloques de construcción de Fif-Iot**

En la Figura 1 se muestra una descripción general de la arquitectura del sistema de FIF-IoT . FIF-IoT recopila interacciones de sistemas basados ​​en IoT. FIF-IoT crea transacciones utilizando la información intercambiada en las interacciones. Las transacciones se envían a la red de contabilidad pública. Los mineros reciben las transacciones y crean bloques de interacción combinándolos. Los bloques se agregan a una cadena de bloques pública, distribuida y descentralizada. De esta manera, el libro digital mantiene el orden cronológico (procedencia) de las interacciones. Los detalles del proceso de recolección, preservación y adquisición de evidencia son los siguientes.

### A. Tipos de interacciones

En un sistema basado en IoT, las interacciones se pueden dividir en las siguientes tres categorías ( Figura 2 ):

#### Cosas para los usuarios (T2U)

*a)* Un usuario (nodo iniciador) accede a un dispositivo IoT (nodo objetivo) de forma remota a través de un servicio en la nube (nodo intermedio) y puerta de enlace (nodo intermedio) o viceversa; *b)* Un usuario accede a un dispositivo IoT localmente a través de una puerta de enlace o viceversa.

#### Cosas a la nube (T2C)

Un dispositivo IoT publica datos en un servicio en la nube a través de una puerta de enlace o viceversa.

#### Cosas a las cosas (T2T)

Un dispositivo IoT se comunica con otro dispositivo IoT ya sea directamente o a través de una puerta de enlace.

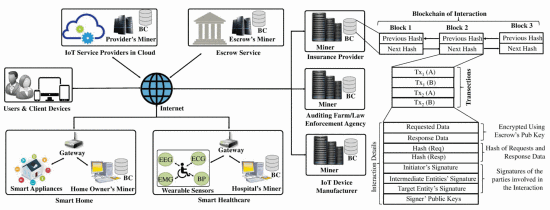
### B. Modelando una transacción de interacción

El objetivo de una transacción de interacción es registrar con precisión la interacción de dos entidades registrando la acción y las identidades de las partes involucradas. La información clave registrada en una interacción son las solicitudes y respuestas de la entidad iniciadora, intermedia y objetivo (ver Figura 3 ).

### C. Modelo operacional

#### Creación de transacciones

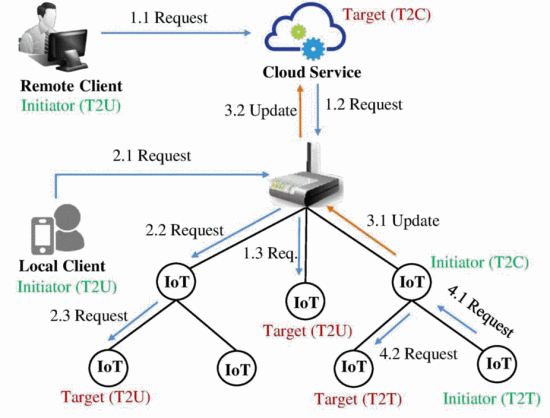
La Figura 3 muestra el proceso de creación de una transacción para una interacción T2U. Se sigue el mismo proceso para crear transacciones para las interacciones T2C y T2T. El iniciador de una interacción inicia una transacción. Las partes involucradas en la interacción firman la transacción utilizando sus claves públicas emitidas por un servicio de depósito de garantía. La transacción finaliza cuando la última parte ubicada en la ruta de reenvío de la interacción firma la transacción. Cuando se completa la transacción, se envía a la red blockchain.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-1-source-large.gif)

**Figura 1:**

Resumen del sistema. BC = blockchain.

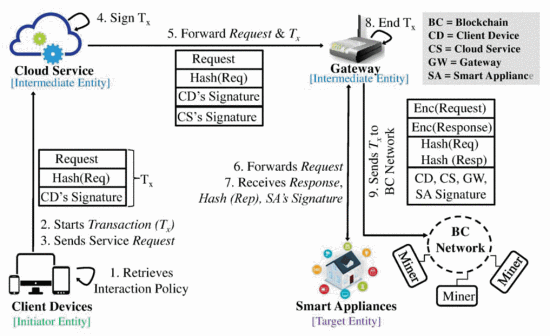
[Ver todo](https://ieeexplore.ieee.org/document/8473437/all-figures)

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-2-source-large.gif)

**Figura 2:**

Interacciones en sistemas basados ​​en iot.

[Ver todo](https://ieeexplore.ieee.org/document/8473437/all-figures)

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-3-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-3-source-large.gif)

**Fig. 3:**

El proceso de crear una transacción.

[Ver todo](https://ieeexplore.ieee.org/document/8473437/all-figures)

#### Servicio de fideicomiso

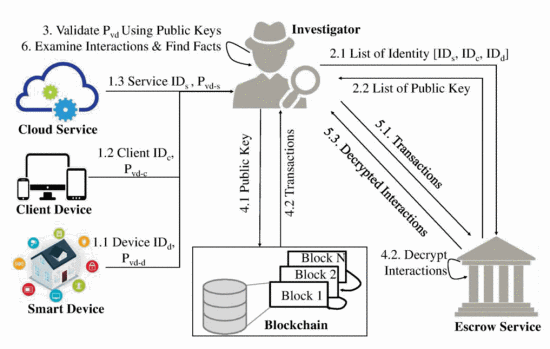
El servicio de depósito de garantía emite claves **públicas** para las entidades de IoT. Por ejemplo, el servicio de depósito de garantía proporciona credenciales Elliptic Curve Qu-Vanstone (ECQV) [26] a una entidad que la entidad utiliza para calcular sus pares de claves privadas y públicas. El servicio de depósito mantiene una asignación entre la identidad de una entidad y su clave pública. La asignación de la clave pública y la identidad de una entidad se almacena de forma segura en el servicio de depósito como una tupla *[identidad, clave pública]*. Las claves públicas de las partes involucradas en una interacción se incluyen en una transacción. Sin embargo, las identidades de las partes no se revelan en la transacción. Los datos de solicitud y respuesta encontrados en una transacción se cifran con la clave pública del servicio de depósito antes de que la transacción se envíe a la red blockchain (consulte el registro de detalles de interacción en la Figura 1 ).

#### Inserción en el libro mayor de Blockchain

Los mineros asignados por las partes interesadas recolectan transacciones periódicamente. Un minero compila transacciones para un período de tiempo particular. El minero valida las firmas adjuntas a las transacciones. A continuación, crea un bloque de interacción que contiene las transacciones. Finalmente, el minero agrega el bloque en la cadena de bloques.

#### Etapa de investigacion

Durante la investigación de un incidente, se proporciona al investigador identidades (ID) de las entidades involucradas en el incidente y los datos de validación de clave pública de las entidades ( Figura 4 ). Una entidad calcula sus datos de validación de clave públicaPAGv dcomo sigue: *i)* selecciona un nonce N; *ii)* firma el nonce y su ***ID*** con su clave privadas como SyoG N( N∥ yoD ) )s; *iii)* concatenaSyoG N( N∥ yoD )s y norte para generar PAGv d= N∥ SyoG N( N∥ yoD )s. El investigador presenta las identidades al servicio de depósito de garantía y recibe las claves públicas de las entidades. El investigador valida elpagv dde cada entidad que usa la clave pública de esa entidad. Por lo tanto, el investigador se asegura de que una identificación proporcionada por una entidad no se falsifique y la clave pública de esa entidad proporcionada por el Fideicomiso corresponde a la identificación. A continuación, el investigador recupera las transacciones del libro público que contienen las claves públicas. El investigador recopila las transacciones que se crearon dentro del intervalo de tiempo del incidente. El investigador luego proporciona las transacciones al servicio de depósito de garantía. El servicio de depósito de garantía descifra los datos de solicitud y respuesta incluidos en las transacciones utilizando su clave privada y los envía de vuelta al investigador a través de un canal seguro. Finalmente, el investigador analiza y examina las interacciones no encriptadas para establecer hechos en un incidente criminal o resolver una disputa.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-4-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-4-source-large.gif)

**Fig. 4:**

El proceso de investigación.

[Ver todo](https://ieeexplore.ieee.org/document/8473437/all-figures)

**SECCION V.**

## **Seguridad de la evidencia pública**

En esta sección, proporcionamos un análisis de varias propiedades de seguridad de la evidencia pública.

### Confidencialidad

La información de interacción (datos de solicitud y respuesta) disponible en el libro público se cifra utilizando la clave pública del servicio de depósito. Los mineros y adversarios no tienen acceso a la clave privada del servicio de depósito de garantía. Por lo tanto, no pueden aprender la información intercambiada entre entidades a partir de la evidencia cifrada disponible públicamente. Por lo tanto, la confidencialidad de la evidencia está protegida.

### No repudio

Las partes involucradas en una interacción firman datos de interacción. Además de los datos de interacción cifrados, se incluyen en la transacción los hash de los datos de interacción y las firmas de las partes involucradas. Por lo tanto, una parte no puede negar su participación en una interacción encontrada en el libro mayor.

### Anonimato

Una transacción contiene claves públicas de las partes involucradas además de hashes y firmas. Sin embargo, las identidades de las partes no están incluidas en la transacción. El servicio de depósito de garantía tiene la asignación entre identidades y claves públicas, y solo sabe a qué partes pertenecen las claves públicas encontradas en el libro mayor público. Por lo tanto, no se puede determinar qué partes están involucradas en una interacción de las claves públicas encontradas en una transacción.

**SECCION VI.**

## **Estudio de caso hipotético**

### Una parcela

Consideramos un incidente hipotético en un servicio de IoT Healthcare que requiere un examen forense. Un paciente fue ingresado en un hospital con diabetes aguda. Una enfermera del Hospital conectó un dispositivo de monitoreo de glucosa en sangre (GMD) conectado a Internet y una bomba de insulina (IP) al cuerpo del paciente. Un médico puede controlar de forma remota el nivel de glucosa del paciente, así como ajustar la dosis de insulina utilizando su teléfono inteligente. Desafortunadamente, durante la última actualización de software, el dispositivo estaba infectado con malware. Un adversario explotó el firmware vulnerable integrado con el GMD para instalar el malware. Como tal, el GMD proporciona lecturas incorrectas de glucosa en sangre al médico. El médico ajusta la dosis de insulina de acuerdo con las lecturas falsas. La paciente experimenta una condición física terrible debido a la dosis de insulina que no debe recibir. La administración del hospital identifica esta anomalía y designa un investigador para examinar este problema. Según FIF-IoT, todas estas transacciones se agregaron a blockchain y finalmente se publicaron en un libro público. Aquí, se pueden observar todo tipo de transacciones.

### B. Investigación

Un investigador requiere una identificación válida para comenzar la investigación. En el primer paso, el investigador recopila la información necesaria. El investigador requerirá identidades de los dispositivos que participaron en este incidente. Aquí, los dispositivos involucrados son: 1) dispositivo de monitoreo de glucosa (GMD), 2) bomba de insulina (IP) y 3) teléfono inteligente (SP) del médico. En el siguiente paso, el investigador debe identificar el servicio en la nube. Aquí, estuvieron involucrados los siguientes servicios: 1) actualización de firmware de GMD 2) monitoreo de glucosa de GMD y 3) control de dosis de IP. Al obtener estas identidades, el investigador puede recuperar las transacciones relacionadas de la cadena de bloques publicada. Pero en blockchain, todos estos dispositivos y servicios se grabaron con sus claves públicas. Entonces, el investigador también requerirá las claves públicas relacionadas. Para servir a este propósito, en**FIF-IoT** , tenemos un servicio de custodia. Con una identificación válida y el privilegio adecuado, un investigador puede recuperar las claves públicas de dispositivos y servicios. Por lo tanto, el investigador pudo recuperar todas las claves públicas relacionadas con este incidente. Después de eso, las transacciones se pueden adquirir del libro mayor público. **Pero**, dado que este libro de contabilidad público es una gran cadena de bloques, el investigador necesita fijar una hora de inicio y una hora de finalización. Como el hospital informó que la anomalía ocurrió después de la última actualización de firmware, el investigador solicitará todas las transacciones desde la última actualización de firmware hasta que se produjo la anomalía. Después de este paso, el investigador tendrá todas las transacciones requeridas y puede comenzar a analizarlas. Después de validar estas interacciones, el investigador examinará estas transacciones y proporcionará el veredicto final.

### C. Modelo de colusión

#### Motivos adversarios

En nuestro modelo de colusión, el fabricante de GMD, el fabricante de IP, el médico y el adversario real pueden coludir entre sí para proporcionar transacciones falsas al auditor. Su objetivo es enmarcar una entidad honesta o salvar a una entidad deshonesta de la convicción.

#### Capacidades de adversarios

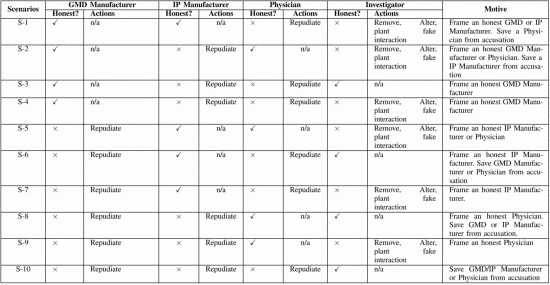
En **FIF-IoT** , las interacciones entre entidades se agregan a una cadena de bloques. Esta cadena de bloques se publica en un libro de contabilidad digital. Múltiples partes interesadas mantienen este libro mayor. Para un adversario, es bastante imposible comprometer (por ejemplo, falsificación de evidencia) esto. Un investigador o un auditor pueden verificar si está comprometido o no al verificar múltiples copias. Por lo tanto, podemos concluir que el libro mayor público contiene interacciones reales, no inventadas. En nuestra investigación, consideramos escenarios en los que una o más partes, como el fabricante de GMD, el fabricante de IP y el médico, pueden ser maliciosos. El investigador también puede ser malicioso. Sin embargo, suponemos que el paciente es honesto porque sufrió la consecuencia de la falta de dosis.

### D. Análisis de seguridad

#### Escenarios de colusión

En esta sección, mostramos que nuestro FIF-IoT propuesto no puede verse comprometido incluso si las entidades involucradas se confabulan entre sí. Cinco entidades están involucradas en nuestro estudio de caso: el fabricante de GMD, el fabricante de IP, el médico, el proveedor de servicios FIP-IoT y el investigador. Como FIF-IoT proporciona las transacciones de blockchain público, es bastante imposible comprometer el libro público. Para n número de entidades, el número total de escenarios se calcula como:∑n - 1i = 2Cnorteyo. Aquí, el proveedor de servicios FIF-IoT se considera honesto. Por lo tanto, el número total de escenarios se reduce a 10 ( Tabla I ).

**Tabla I:** escenarios de colusión. GMD-M = fabricante de GMD. IP-M = fabricante de ip. N / a = sin acción.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-table-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-table-1-source-large.gif)

#### Análisis de escenario

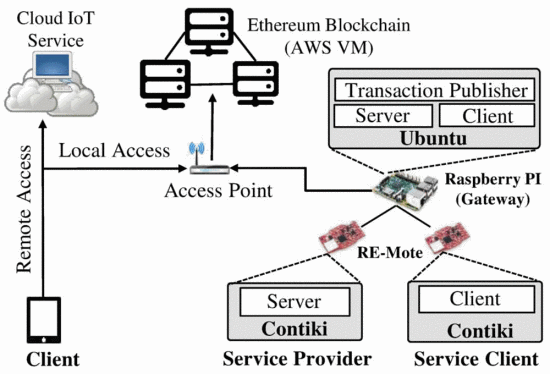
Presentamos el análisis de los escenarios de colusión en la Tabla II. Una entidad inteligente maliciosa no puede repudiar las interacciones enviadas anteriormente, ya que la entidad firmó la interacción antes de enviarlas a FIP-IoT. Del mismo modo, el proveedor FIF-IoT no puede falsificar o negar las interacciones publicadas, ya que todas estas interacciones se enviaron a blockchain público donde múltiples mineros acordaron. Además, un investigador deshonesto puede alterar, eliminar y plantar interacciones falsas o intencionalmente pasar por alto interacciones reales mientras presenta el caso ante el tribunal. Sin embargo, un auditor puede detectar la evidencia manipulada o el análisis engañoso utilizando el proceso de verificación. El auditor puede encontrar fácilmente la falta de coincidencia entre el informe del investigador y las interacciones del libro mayor público. Finalmente, concluimos que nuestro modelo propuesto puede detectar interacciones fabricadas en los escenarios adversos fuertes,

**SECCION VII.**

## **Experimentar**

### A. Configuración experimental

La Figura 5 presenta nuestra configuración experimental. Desarrollamos una aplicación cliente para un teléfono inteligente Android para enviar solicitudes. Utilizamos la biblioteca Java de *bouncy castle*[27] para operaciones criptográficas. Utilizamos un dispositivo Raspberry Pi como puerta de enlace para conectar dispositivos IoT a Internet. En la puerta de enlace Raspberry Pi, alojamos dos servidores para recibir datos tanto del dispositivo de usuario como del dispositivo IoT. Para nuestra configuración, utilizamos dos dispositivos RE-Mote [28] IoT con el sistema operativo Contiki [29] . Se usó un dispositivo para enviar solo datos. El otro dispositivo actuó como receptor y como remitente. Para dispositivos IoT, utilizamos la biblioteca Relic [30]para operaciones criptográficas. Para la parte de la nube, alojamos una aplicación de servidor en una máquina virtual en la nube (VM) de AWS. Esta aplicación recibió datos del dispositivo del usuario y los reenvió a la puerta de enlace. La puerta de enlace fue responsable de enviar las interacciones a una red blockchain. Creamos una red blockchain usando la plataforma Ethereum [31] . Los nodos mineros Ethereum estaban alojados en las máquinas virtuales.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-5-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-5-source-large.gif)

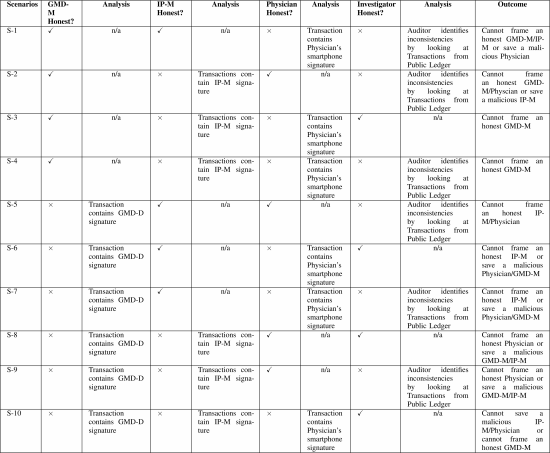
**Fig. 5:** Configuración experimental.

### B. evaluación

#### Hora de finalización de la solicitud

Realizamos nuestros experimentos para diferentes tamaños de mensajes que varían de 32 bytes a 1024 bytes. En cada caso, medimos el retraso de extremo a extremo para calcular el tiempo de finalización de la solicitud. En nuestro modelo, había tres tipos de interacciones: a) cosas para los usuarios b) cosas para las cosas yc) cosas para la nube. Para los usuarios interesados, también realizamos el experimento tanto para el acceso remoto como para el acceso local. En todos los casos, observamos una leve sobrecarga en el retraso de extremo a extremo para FIF-IoT como se muestra en la Figura 6 . Para cosas para los usuarios ( Figura 6a), en caso de acceso remoto, la mayor sobrecarga de retraso de extremo a extremo fue del 9,7% para el tamaño del mensaje de 32 bytes. A medida que aumentaba el tamaño del paquete, la sobrecarga también comenzó a disminuir. Para el tamaño de paquete de 1024 bytes, la sobrecarga fue del 0,20%, lo que es insignificante. Observamos una tendencia similar en otros casos también. Para el acceso local a usuarios, la sobrecarga varió de 11.7% (32 bytes) a 1.95% (1024 bytes). En el caso de cosas a cosas ( Figura 6b ), observamos una variación de 13.04% (32 bytes) a 2.05% (1024 bytes). Finalmente, para que las cosas se nublen ( Figura 6c ), la sobrecarga en el retraso de extremo a extremo se desvía entre 13.44% (32 bytes) y 3.16% (1024 bytes). Podemos concluir que la sobrecarga en el tiempo de finalización de la solicitud es insignificante.

**Tabla II:** Resultado de escenarios de colusión. N / a = no requiere análisis.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-table-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-table-2-source-large.gif)

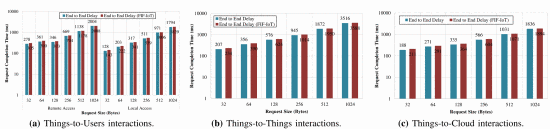
#### Consumo de energía

Medimos el consumo de energía en dispositivos IoT con recursos limitados. Nuestro objetivo era observar cómo FIF-IoT contribuye en los gastos generales de consumo de energía para la generación de firmas y el envío de cargas criptográficas, como firmas y hashes, que se incluyen en una transacción. Utilizamos la biblioteca de energía Contiki [32] para medir el consumo de energía de la CPU para el cálculo de la firma ( Figura 7) También medimos la cantidad de energía consumida por el transceptor de radio para transmitir cargas criptográficas. Aunque hubo un aumento mínimo en el consumo de energía para las solicitudes de menor tamaño, la sobrecarga del costo de energía disminuyó drásticamente a medida que aumentó el tamaño del mensaje. Varió de 25.71% (32 bytes) a 3.56% (1024 bytes). La sobrecarga de energía bajó a un nivel insignificante. Utilizamos la clave ECC de 160 bits para la firma. Por lo tanto, las firmas ECDA para las solicitudes fueron como máximo 320 bits. El costo de generación de la firma varió entre 3.94 y 9.8 milijulios.

**SECCION VIII.**

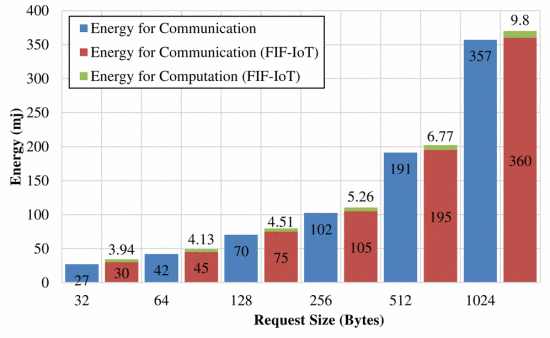
## **Trabajo relacionado**

Hay varios trabajos de investigación recientes que abordaron el análisis forense de IoT [9] - [10] [11] [12] [13] [14] [15] [16] [17]. Estos modelos forenses existentes discutieron principalmente los componentes del análisis forense digital de IoT, la fuente de evidencia y el proceso de investigación. En comparación con nuestro trabajo, los trabajos anteriores no consideraban un sistema distribuido y descentralizado para la preservación y adquisición de interacciones forenses de IoT que estén aseguradas contra la manipulación. También mostramos la robustez de nuestro marco en varios escenarios adversos. Además, a diferencia de FIF-IoT, ninguno de los modelos forenses mencionados proporciona esquemas para garantizar la disponibilidad, escalabilidad y propiedades de tolerancia a fallas del sistema de almacenamiento de evidencia. Además, ningún esquema o marco para mantener la privacidad de la evidencia preservada no se propuso en los trabajos de investigación citados anteriormente.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-6-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-6-source-large.gif)

**Fig. 6:**

Comparación del tiempo de finalización de la solicitud.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-7-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8457595/8473425/8473437/8473437-fig-7-source-large.gif)

**Fig. 7:**

Comparación del costo de la energía.

[Ver todo](https://ieeexplore.ieee.org/document/8473437/all-figures)

**SECCION IX.**

## **Conclusión**

En este documento, propusimos FIF-IoT, un marco de investigación forense para sistemas basados ​​en IoT que utilizan un libro de contabilidad digital público. FIF-IoT almacena interacciones dispositivo a dispositivo, dispositivo a usuario y dispositivo a la nube como evidencia en un libro de contabilidad digital público similar a Bitcoin. FIF-IoT puede proporcionar confidencialidad, anonimato y no repudio de las pruebas disponibles públicamente. FIF-IoT también puede proporcionar interfaces para la adquisición de evidencia y un esquema para verificar la integridad de la evidencia durante la investigación de un incidente criminal. Presentamos un estudio de caso de un escenario de confrontación. Mostramos que FIF-IoT era a prueba de manipulaciones contra un posible escenario de colusión. También implementamos un prototipo de FIF-IoT y evaluamos el rendimiento.

### AGRADECIMIENTOS

Esta investigación fue apoyada por el National Care Foundation CAREER Award CNS-1351038, ACI-1642078 y SaTC-1723768.