Forensia de Internet de las Cosas (IoT), avances en la investigación

Bibiana Luz Clara, Esteban Rivetti, Alvaro Gamarra,
José Aráoz Fleming, Beatriz Parra de Gallo
IEsIIng – Facultad de Ingeniería, Universidad Católica de Salta, Salta, Argentina,

Abstract
El presente trabajo aborda la problemática generada por Internet de las Cosas (IoT) y los avances logrados por el equipo de investigación del Grupo de Forensia Digital de la UCASAL, respecto de los métodos, estructuras y componentes que resulta necesario definir desde la Forensia Digital. Señalando los principales resultados arribados a la fecha así como los trabajos actuales que desarrolla este equipo, en el marco del proyecto de investigación.

Palabras Clave
Internet de las Cosas, Forensia Digital.

Introducción

Las posibilidades que ha brindado Internet móvil han acercado a millones de personas que de otro modo no podrían haber contado con el servicio, permitiendo una rápida alfabetización digital.

Internet es un mecanismo disruptivo que capacita a los individuos, promueve el desarrollo de la interacción y perfeccionamiento individual y por ende social; es utilizada como el factor de construcción del modelo de transformación, hacia una sociedad inclusiva y sostenible.

Pero, por otro lado, el software malicioso permite ingresar y robar datos o interrumpir el funcionamiento de los sistemas apoderándose de claves y contraseñas, causando daños al comercio y la infraestructura, lo que genera enormes implicancias cuando se depende del correcto funcionamiento en línea de múltiples actividades. Cuando esto puede afectar a objeto que desarrollan funciones conectados a Internet de las Cosas (IoT), y máxime si éstos cumplen tareas vitales o que impliquen alto riesgo, las situaciones de posibles daños se potencian.

Las nuevas tecnologías reemplazan rápidamente a las viejas y esto puede significar el fin de los modelos comerciales anteriores, por la reducción drástica de costos y la aceleración de los tiempos para conquistar nuevos mercados y ofrecer nuevos servicios, reemplazando antiguos modelos de producción por otros disruptivos, que se nutren de la investigación en constante desarrollo.

Estos nuevos desafíos requieren nuevos enfoques, ya que muchos de ellos, producto de la economía colaborativa[1] en expansión, salen al mercado sin marco jurídico que los contenga y en muchos casos es difícil adaptarlos a los moldes establecidos para otras situaciones que se contemplaron en su momento pero que van quedando atrás. Véase por ejemplo el caso de Uber[2], que salió al mercado sin un marco legal acorde y se encuentra funcionando en muchos países, y en otros hasta se ha llegado a prohibir.

Se aplica, por el momento a estas situaciones la normativa general para contrataciones ordinarias civiles y comerciales y la de defensa de los consumidores existente, y se sujetan a la responsabilidad civil, penal y administrativa, que pudiera corresponderles por su accionar.

La participación de todos los sectores, la gobernanza colaborativa, la transparencia, y la búsqueda de consensos son los pilares de este nuevo modelo llamado *multistakeholder*, que lleva a que cada persona tenga influencia sobre otra en la medida en que su comportamiento genere un cambio en el comportamiento de la otra y por ende de muchas más.

---

[1] También denominadas sharing economy, economía p2p, o gig economy, conceptos que la Revista Time incluyo en 2011 en la lista de" 10 ideas para cambiar el mundo. Disponible último ingreso 20/06/2018 en http://content.time.com/time/specials/packages/article/0,28804,2059521_2059717_2059710,00.html

[2] https://get.uber.com

El sistema de economía colaborativa sumado a los IoT, hace de este nuevo modelo un cambio de paradigma, donde la intermediación en la prestación de servicios y compra venta de bienes vaya quedando de lado por encarecer el sistema, máxime en periodos de crisis en las que muchos países se encuentran. Objetos que funcionan en forma autónoma, personas que se conectan con otras para acceder a prestaciones en forma directa, y todo esto esta ocurriendo mientras observamos sin tiempo a reaccionar y sin legislación acorde que le de contención.

Para algunos, el marco legal podría ser un ahogo para dicha economía en crecimiento, por lo cual deberemos ser cuidadosos al momento de elegir las normas que deberán guiar su curso, poniendo el acento en la flexibilidad y neutralidad tecnológica de las mismas, para que puedan mantenerse un tiempo prudencial.

En general la tendencia parece acercarse más a la idea de una corregulación entre países, que tenga en cuenta los códigos de conducta y las buenas prácticas como un complemento a los sistemas legales y jurisdiccionales, para dar mayor amplitud a la seguridad y protección de todos los que operan en las plataformas.

Se requiere un estudio específico en cuanto a los riesgos de la sociedad en línea, por la utilización de las Tics para vigilancia, control social, y maximización de los intereses de unos pocos agentes dominantes frente al colectivo general, por los nuevos mecanismos de contratación mediante contratos inteligentes, y los objetos conectados a la red.

La infraestructura de telecomunicaciones es la piedra angular sobre la que descansa todo el ecosistema digital, y esta ha evolucionado para ser más robusta y llegar a más personas. En este contexto, cobra especial importancia el estudio de IoT, así como la identificación del marco técnico, normativo y legal involucrado. Este es uno de los objetivos del equipo de investigadores que integran el proyecto de "Aplicación de tecnologías semánticas a la Forensia Digital: Estudio y Diseño de una Ontología Semántica aplicada a Sistemas de Interconexión Digital de Objetos Cotidianos (IoT)", que se encuentra en desarrollo en el Instituto de Estudios Interdisciplinarios de Ingeniería (IEs.I.Ing), radicado en la Facultad de Ingeniería de la Universidad Católica de Salta (UCASAL).

Este trabajo cuenta con las siguientes secciones: en la Sección 1 se describe IoT y la seguridad informática, abordando de qué manera ésta está presente en los dispositivos de IoT, en la sección 2 se detalla el marco teórico seleccionado para abordar la investigación; luego la sección 3 aborda los principales aspectos del proyecto de investigación formulado sobre Forensia de IoT; la sección 4 describe los avances logrados a la fecha presentados a la comunidad científica en sucesivas exposiciones y publicaciones, y en la sección 5 se presenta el estado actual de la investigación y por último en la sección 6 se describen las conclusiones.

1. Internet de las Cosas (IoT) y la seguridad informática

A partir de los conceptos de comunicación ubicua y comunicación máquina a máquina, Internet de las Cosas (IoT) se define como "…*un conjunto de tecnologías enfocadas a permitir la conexión de objetos heterogéneos a través de diferentes redes y métodos de comunicación; su principal objetivo es posicionar dispositivos inteligentes en diferentes lugares para capturar, guardar y administrar información para que ésta sea accesible a las personas desde cualquier parte del mundo*…"[1].

Por su parte, [2]señalan que Internet de las cosas, no es más que la combinación en la red de varios objetos físicos con electrónica, software y conectividad de red, que permite a estos objetos físicos recolectar e intercambiar datos entre varias fuentes y destinos. La idea básica o fundamental detrás de este concepto es la presencia omnipresente a nuestro alrededor de una variedad de cosas u objetos - tales como

etiquetas de identificación de radiofrecuencia (RFID), sensores, actuadores, teléfonos móviles, etc que son capaces de interactuar entre sí y cooperar con sus vecinos para alcanzar objetivos comunes. Desde el punto de vista del usuario individual, uno de los efectos más prominentes del IoT será su *visibilidad* tanto en el ámbito laboral como en el doméstico. En los Estados Unidos de América, el Consejo Nacional de Inteligencia (NIC) predice que para 2025 los nodos de Internet pueden ocuparse en las cosas cotidianas. Muchos países desarrollados como los Estados Unidos de América, Europa y algunos países de Asia como India, China y Japón, ahora están considerando Internet de las cosas (IoT) como un área de innovación y crecimiento. Por lo tanto, para desarrollar este sistema, se está realizando una extensa investigación en varias universidades y en muchas organizaciones de investigación en todo el mundo.

Uno de los puntos más preocupantes referentes al tema IoT es la *seguridad y privacidad de la información,* entendiendo que –inicialmente- el contexto de internet de las cosas se presenta como un escenario vulnerable y proclive a la invasión de la vida íntima de las personas.

Desde el punto de vista de la privacidad de la información, IOT involucra a múltiples partes interesadas: individuos (el sujeto de la recolección de datos), organizaciones (que son responsables de procesar los datos recolectados de los individuos) y terceros (por ejemplo, usuarios que se benefician o usan los datos recogidos o procesados). IOT promete múltiples beneficios a todos estos interesados. Para los individuos, le proporcionaría valor tales como beneficios de salud y bienestar. Para organizaciones y terceros, proporcionaría información para ofrecer mejores servicios a las personas y a la sociedad en general. Sin embargo, teniendo en cuenta la creciente tendencia a recopilar datos cada vez más individuales y personalizados, las prácticas de recolección, manipulación y procesamiento de datos de IOT plantean muchas cuestiones relativas al impacto en la privacidad de una persona desde una perspectiva jurídica [3].

Focalizados en este punto -la privacía de los datos- [4] ya advierte sobre la necesidad de que los países líderes definan políticas pertinentes y planes dirigidos a la protección de los usuarios y sus datos personales, como fundamento de la sociedad hiperconectada.

Y avanzando más en este sentido, se observa también el uso de IoT en la consumación de delitos. Es decir, el contexto de ubicuidad y omnipresencia resulta atractivo para la comisión de transgresiones contra la ley, a partir de la interconectividad de componentes de diferentes fuentes y destinos (celulares, GPS, sensores, cámaras de CCTV, alarmas, etc.).

El contexto legal sobre el que se avanzará se definirá en función de la realidad local y regional actual, tomando como premisa lo dicho por la Comisión Asesora sobre Evaluación del Personal Científico y Tecnológico del MINCYT en el documento denominado “Políticas de Investigación Aplicada y Desarrollo Tecnológico en Ingeniería” [5] acerca de que resulta necesario volcar los esfuerzos de investigación hacia el medio productivo local y regional de manera que el impacto de la investigación sea inmediato, contribuyendo a la solución de problemas concretos o demandas específicas nacionales, regionales o locales de carácter social o productivo.

Dada la característica geopolítica de la provincia de Salta, que se encuentra expuesta a situaciones de delitos internacionales por su ubicación estratégica en el centro del NOA Argentino, resulta de interés social particularizar esta investigación tomando como base los organismos públicos de investigación de delitos, tal como el Ministerio Público de la Provincia de Salta. El Ministerio Público es un órgano autónomo e independiente de los demás Poderes del Estado, que integra el sistema de administración de Justicia. En cuanto a su estructura, está dividido en tres grandes ramas: a) Ministerio Público Fiscal, ejerce la acción penal pública y acciona en

defensa de la legalidad, intereses generales, difusos y medio ambiente; b) Ministerio Público de la Defensa, tiene a su cargo el asesoramiento y la representación judicial de personas de escasos recursos y de quienes estuviesen ausentes; y c) Ministerio Público Tutelar, vela por los derechos y bienes de los menores e incapaces de hecho. Esta institución cuenta con un área de Informática Forense y en la que es posible trabajar para tipificar la evidencia digital que se trabaja en los distintos casos en los que actuó, de manera de identificar el tipo de delito que sería más conducente de abordar, desde esta visión de impacto de la i+d en el contexto local y regional.

2. Marco teórico para estudiar Internet de las Cosas (IoT) desde la Forensia Digital

La bibliografía sobre IoT es abundante, y cada vez más detallada. Las investigaciones avanzan en varios sentidos: la constitución de IoT, el uso de IoT, la seguridad y vulnerabilidad, el impacto social, entre otros.

Desde un punto de vista conceptual, el IoT tiene como soporte la capacidad de un objeto inteligente de ser notable, comunicarse e interactuar entre sí, y diseñar redes de varios objetos interconectados. Esta *inteligencia* de los objetos es la capacidad de estar asociados a un nombre (descripción legible para los humanos que permite la individualización del objeto) y una dirección IP (cadena legible para las máquinas y que permite la comunicación entre los objetos). Por último, los objetos inteligentes deben ser capaces de realizar algunos cálculos fundamentales básicos.

La Internet de las Cosas puede ser vista como un sistema de red altamente dinámico, que consiste en un gran número de objetos inteligentes o "Cosas" que producen y consumen información desde una vista o observación a nivel de sistema. La capacidad de interactuar con la Área o zona física se logra mediante la presencia de dispositivos capaces de detectar fenómenos físicos y traducirlos en una corriente de información o datos, así como a través de la presencia de dispositivos capaces de activar acciones que tengan un impacto o colisión en la zona o área física. Esta capacidad de actuación con el entorno, de hacerse "autoreconocibles" y la inteligencia de cada objeto les permiten acceder a información que ha sido agregada por otras cosas, o pueden ser componentes de *servicios web*[3] complejos.

Por lo general, una amplia gama de servicios son proporcionados por Internet de las cosas (IoT) a los fabricantes, empresas y diversas industrias. En muchas industrias productivas (tales como: monitoreo ambiental, inventario, manejo de productos, etc.) la tecnología IOT encontrará mucha aplicabilidad.

IoT será categorizado por una gran heterogeneidad en términos de dispositivos que participan en el sistema de tecnología y se espera que presenten capacidades muy diferentes desde el punto de vista computacional y de comunicación. En la tecnología IoT el nivel de escalabilidad surge en diferentes niveles. Esto incluye la comunicación de datos y la creación de redes (o redes de computadoras) debido al número muy alto de interconexiones entre un gran número de entidades u organizaciones.

En Internet de las Cosas (IoT), la tecnología o sistemas de comunicación inalámbrica jugarán un papel vital y están permitiendo que los objetos inteligentes o "Cosas" estén conectados en red. La asunción universal de los sistemas de comunicación inalámbrica para el intercambio de datos o información creará varias cuestiones en términos de disponibilidad de espectro de frecuencia y

[3] Servicios web: designa una tecnología que permite que las aplicaciones se comuniquen en una forma que no depende de la plataforma ni del lenguaje de programación. Un servicio web es una interfaz de software que describe un conjunto de operaciones a las cuales se puede acceder por la red a través de mensajería XML estandarizada. Usa protocolos basados en el lenguaje XML con el objetivo de describir una operación para ejecutar o datos para intercambiar con otro servicio web.
Extraído de https://www.ibm.com/developerworks/ssa/webservices/newto/service.html [Consultado el 08/07/2017]

que impulsará hacia la asunción de sistemas de radio inteligente [6].

La tecnología IoT no es nada más que el intercambio de información de un dispositivo a otro dispositivo y también la capacidad para analizar la enorme cantidad de datos que se generan. Por lo tanto, con el fin de convertirlos en información muy útil y también para garantizar la interoperabilidad entre dos o más aplicaciones, es muy importante proporcionar suficientes datos con formatos especificados y lenguajes bien definidos. La seguridad para el sistema IoT debe ser una propiedad clave y debe ser tomado muy en cuenta, al igual que el diseño de la arquitectura lógica.

En la siguiente figura, [2] describen y clasifican las tecnologías, conceptos y estándares de los sistemas IoT que se destacan.

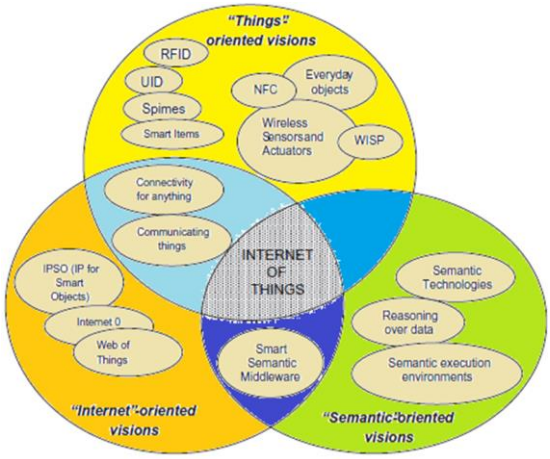

Figura 1: Diagrama de Arquitectura de IoT (Fte: [2])

En el área identificada como "Visiones orientadas a las cosas" (*Things Oriented Visions)* se mencionan las identificaciones de radiofrecuencia o RFID [4], y otros componentes básicos para enlazar los componentes digitales (tecnología inalámbrica de corto alcance o NFC [5], sensores y actuadores de red, entre otros). En particular interesa la acción de los sensores con capacidades cada vez mayor en cuanto a captura, resguardo y transmisión de datos, y que se incorporan en objetos de la más amplia diversidad, dependiendo de la variable que se quiere medir. Así, existen sensores de contacto, ópticos, térmicos, de humedad, magnéticos, infrarrojos, que se colocan en ropa, muebles, vehículos, animales, personas, etc.

En el área identificada como "Visiones orientadas a internet" (*Internet Oriented Visions)* se incluyen las características o componentes de la red referidas principalmente a la capacidad de identificación de los objetos por su IP. Se menciona IPSO (*Internet Protocol of Smart Objets)* para apoyar el gran número de aplicaciones emergentes para objetos inteligentes, en el que la tecnología de internet subyacente debe ser inherentemente escalable, interoperable y tener una sólida base de estandarización para apoyar la innovación futura como IoT [7], mediante la simplificación del Protocolo de Internet para cambiarlo a cualquier objeto y también hacer que los objetos sean direccionables y accesibles desde cualquier tipo de ubicación.

En el área identificada como "Visión orientada a la Semántica" (*Semantic Oriented Visions)*, el autor de esta investigación describe el trabajo desafiante que insumirá la comprensión, identificación y análisis vinculante de todas las formas de recopilación de información, interconexión, búsqueda y comunicación de IoT, por lo que entiende que las tecnologías de la web semántica podrán ser de utilidad para conocer como interactúa IoT.

En particular, se menciona un área común entre estos tres conceptos enunciados, denominada *Smart Semantic Middleware*. Respecto de este término [8] indica en su

[4] RFID: La identificación por radiofrecuencia o RFID por sus siglas en inglés (radio frequency identification), es una tecnología de identificación remota e inalámbrica en la cual un dispositivo lector o **reader** vinculado a un equipo de computo, se comunica a través de una antena con un **transponder** (también conocido como tag o etiqueta) mediante ondas de radio. *Extraído de* http://www.egomexico.com/tecnologia_rfid.htm, [Consultado el 08/07/2017]

[5] NFC: son las siglas de *Near Field Communication*, La tecnología NFC permite interacciones bidireccionales simples y seguras entre dispositivos electrónicos, permitiendo a los consumidores realizar transacciones sin contacto, acceder a contenido digital y conectar dispositivos electrónicos con un solo toque. *Extraído de* http://nfc-forum.org/what-is-nfc/about-the-technology/ [Consultado el 08/07/2017]

trabajo que a medida que los sistemas ubicuos se vuelven cada vez más complejos, las soluciones tradicionales para administrarlos se limitan y se plantea una necesidad de auto-gestión. Además, la heterogeneidad de los componentes omnipresentes, los estándares, diversidad de formatos de datos, etc., crea importantes obstáculos para la interoperabilidad en sistemas tan complejos. Por ello, es prometedor abordar estos problemas desde las tecnologías semánticas para generar un *espacio de intermediación para los objetos inteligentes basado en las tecnologías semánticas.*

El diccionario de la Real Academia Española define a la ontología como "*Parte de la metafísica que trata del ser en general y de sus propiedades trascendentales"*[6].

En el ámbito de la computación, el concepto fue incorporado rápidamente como una herramienta para formular la representación del conocimiento, con una fuerte asociación a la *semántica* del objeto que se está trabajando. Lassila propone incluso una "*ontology spectrum"* para indicar la diversidad de aplicaciones o significados con que se asume el término [9].

Siendo tan diversa la aplicación de esta tecnología, resulta muy difícil acordar una única postura respecto de "qué" representar y "como" hacerlo. Así, las ontologías se estudian desde sus más diversas cualidades y componentes: tipos de ontologías, lenguajes de desarrollo, vinculación con la web semántica, concluyendo todo ello en lo que se conoce como "ingeniería ontológica".

La aplicación de las tecnologías semánticas es de lo más variada. En su relación con la web semántica se han producido implementaciones en todos los órdenes. Sin ser excluyente ni exhaustiva, la siguiente lista menciona los campos de aplicación tradicionales para la web semántica:

- Comercio electrónico
- Gestión del conocimiento corporativo
- Búsqueda de información en la web
- Procesamiento del lenguaje natural
- Enseñanza
- Librerías digitales
- Turismo
- Patrimonio cultura

En la bibliografía se encuentran algunas contribuciones que comienzan utilizar ontologías y tecnologías semánticas en la Forensia Digital. Los siguientes estudios muestran la variedad de temáticas abordadas:

- IoT-Lite, una instanciación de la ontología de la red de sensores semánticos (SSN) para describir los conceptos clave de IoT que permiten la interoperabilidad y el descubrimiento de datos sensoriales en plataformas IoT heterogéneas mediante una semántica ligera [10].
- Relación entre "Internet de las Cosas" (IoT) y "Web de las Cosas"(WoT) mediante la combinación de la web semántica para la anotación semántica y razonamiento en los datos para construir aplicaciones interoperables de IoT / WoT. [11]

3. Aspectos Distintivos del Proyecto de Investigación

El Grupo de Investigación de FORENSIA DIGITAL, constituido en la Facultad de Ingeniería de la Universidad Católica de Salta (UCASAL), está abocado ahora a trabajar en este proyecto, constituyendo un equipo de trabajo de 6 (seis) personas: 2 profesionales del área del Derecho y 4 profesionales del ámbito de la Informática.

El proyecto, subvencionado por la UCASAL según RR 1582/17, se ha formulado metodológicamente de la siguiente manera.

Como actividad indispensable para el inicio de la investigación se deberá realizar una revisión bibliográfica para profundizar el conocimiento en el área de investigación en la que se desarrollará el proyecto, así como las tecnologías y las diferentes propuestas existentes.

En cuanto a las actividades de investigación, el trabajo inicial consistirá en profundizar el análisis del dominio de la forensia digital,

[6] http://www.rae.es/

sus requerimientos de información y estudiar los casos vinculados con Sistemas de Interconexión Digital de Objetos Cotidianos (IoT).

En primer término se identificará delitos de interés social en los que se encuentren involucrados este tipo de sistemas, tomando como organismo público de investigación de delitos de referencia al Ministerio Público de la Provincia de Salta. A partir de los requerimientos identificados, se formalizarán las debilidades de las arquitecturas y modelos desarrollados hasta el presente y las razones de las mismas, y se comenzará en el diseño de la ontología que represente el conocimiento requerido en el caso seleccionado.

Para la definición de las ontologías se seguirá la propuesta de Methontology. Esta metodología ha sido desarrollada por el Grupo de Ingeniería Ontológica de la Universidad Politécnica de Madrid [12], permite construir ontologías en el nivel de conocimientos, y tiene sus raíces en las actividades identificadas por el proceso de desarrollo de software propuesto por la IEEE y en otras metodologías de ingeniería de conocimientos. ODE y WebODE se construyeron para dar soporte tecnológico a METHONTOLOGY.

Esta metodología propone guías de actividades para la especificación, conceptualización, formalización, implementación y mantenimiento de la ontología a construir, bajo un esquema de procesos iterativos que ayudan en el ajuste del modelo a construir. A continuación se sintetizan estas fases:

- La actividad de ***especificación*** permite determinar por qué se construye la ontología, cuál será su uso, y quiénes serán sus usuarios finales.
- La actividad de ***conceptualización*** se encarga de organizar y convertir una percepción informal del dominio en una especificación semi-formal, para lo cual utiliza un conjunto de representaciones intermedias (RRII), basadas en notaciones tabulares y gráficas, que pueden ser fácilmente comprendidas por los expertos de dominio y los desarrolladores de ontologías. El resultado de esta actividad es el modelo conceptual de la ontología.
- La actividad de ***formalización*** se encarga de la transformación de dicho modelo conceptual en un modelo formal o semicomputable.
- La actividad de ***implementación*** construye modelos computables en un lenguaje de ontologías (Ontolingua, RDF Schema, OWL, etc.). La mayor parte de las herramientas de ontologías permiten llevar a cabo esta actividad de manera automática. Por ejemplo, WebODE puede importar y exportar ontologías desde y a los siguientes lenguajes: XML, RDF(S), OIL, DAML+OIL, OWL, CARIN, FLogic, Jess y Prolog.
- La actividad de ***mantenimiento*** se encarga de la actualización y/o corrección de la ontología, en caso necesario.

METHONTOLOGY también identifica actividades de gestión (planificación, control y aseguramiento de la calidad), y de soporte (adquisición de conocimientos, integración, evaluación, documentación y gestión de la configuración).

Es importante destacar que estas etapas no son totalmente secuenciales, el desarrollo de ontologías es un proceso iterativo e incremental. Si alguna debilidad y/o necesidad se detecta durante la ejecución de una etapa, es posible volver a la etapa previa para realizar modificaciones y/o refinamientos.

Los principios de coherencia, exactitud, inteligibilidad, adaptabilidad, mínimo compromiso ontológico y eficiencia guiarán el desarrollo de la ontología. Sin embargo, algunos de estos principios compiten entre sí, por lo cual deberá encontrarse un equilibrio entre los mismo. El principio de coherencia requiere, entre otras cosas, axiomatizar tantas definiciones como sea posible. Sin embargo, si una ontología está demasiado restringida por axiomas, puede violar el principio de mínimo compromiso

ontológico.
La fase de evaluación de ontologías comprende tres aspectos: i) validación, (ii) verificación y (iii) evaluación. Los dos primeros aspectos están asociados con un juzgamiento técnico del contenido de la ontología respecto a un marco de referencia, que puede estar dado por la especificación de requerimientos, las preguntas de competencia planteadas en la fase de especificación y/o el mundo real. La validación trata de determinar cuánto se ajustan al dominio las definiciones de la ontología. La verificación trata de probar que la ontología cumple con los requerimientos especificados y que es posible responder a las preguntas de competencia a partir de las definiciones de la ontología. Por su parte, la evaluación se enfoca en juzgar el contenido de la ontología desde el punto de vista del usuario. El resultado de utilizar las ontologías en diferentes tipos de aplicaciones y en distintos dominios será utilizado para evaluar la ontología según este último aspecto.
Para dar cumplimiento a los objetivos definidos como "Estudiar y analizar la jurisprudencia y la normativa legal nacional e internacional aplicable a este tipo de Sistemas de Interconexión Digital de Objetos Cotidianos (IoT)" y "Estudiar y desarrollar protocolos de actuación pericial para el análisis forense de Sistemas de Interconexión Digital de Objetos Cotidianos (IoT)", la metodología indicada se nutrirá de actividades paralelas que conlleven al desarrollo de los siguientes componentes también de utilidad para la investigación:

- Búsqueda bibliográfica y estado del arte respecto de la normativa legal nacional e internacional de interés para el proyecto
- Definición del Contexto de aplicación y experimentación
- Definición de protocolos de actuación propios para los sistemas en estudio
- Elaboración de informes y propuestas de normas para la legislación de este tipo de sistemas IoT.

4. Avances logrados a la fecha

Los resultados logrados a la fecha se formalizaron en sendos trabajos de investigación, que se expusieron y publicaron en eventos científicos de la materia. Se resumen a continuación los resultados más destacados.
Se realizó un estudio acerca del ***estado de situación*** de las pericias informáticas en el contexto judicial argentino [13]. En principio se estudió el ámbito juridico en general, arribando a la conclusión de que cada día son más los casos en que se requiere la presentación de evidencia digital, particularmente en el ámbito penal y laboral. Se subraya que, por el tipo de relaciones que se mantienen en la actualidad, una gran cantidad de evidencias, proceden del ámbito informático siendo esta una disciplina transversal a casi todo lo que hacemos, pues la mayoría de nuestras actividades hoy convergen hacia Internet.
También se analizó el estado actual del sistema judicial, los ámbitos civil y comercial, laboral y penal, y las pericias que los mismos, necesariamente y cada día con mayor asiduidad, requieren.
Se observó que los servicios que se prestan sobre Internet así como lo que se conoce como "Internet de las Cosas" (IoT), nos llevarán a otra nueva estadio sobre las implicancias que esto puede traer al momento de suscitarse conflictos y tener que obtener pruebas válidas para el ámbito judicial.
En cuanto a los actores del proceso judicial, que no son del ámbito informático o tecnológico, se observó que los jueces están abandonando sus compartimentos estancos, a la vez que los peritos informáticos van adentrándose en lo jurídico, quienes hacen las normas van comprendiendo que deben avanzar en crear el marco adecuado, surgen guías de actuación judicial propiciadas por las fuerzas de seguridad, la doctrina estudia y coadyuva en esta dirección.
Finalmente, se observó la necesidad de utilización de un lenguaje uniforme que permita reglas de actuación claras, en un lenguaje sencillo y accesible tanto para el

tribunal como para los justiciables, permitiendo mejorar la comunicación entre todos.

Luego, el grupo de investigación avanzó sobre la ***vulnerabilidad de IoT*** [14].,En paralelo con el amplio desarrollo de IoT y su incidencia en las áreas locales y regionales productivas, se consideró de interés abordar el marco legal existente, así como los distintos problemas que se vislumbran, cuando las pruebas digitales a obtener se generan en el contexto de IoT. Y se planteó analizar las normativas nacionales e internacionales existentes y su aplicación concreta en un caso de estudio real en el que ocurrieron graves infracciones a la seguridad de los datos, proponiendo un conjunto de criterios base para abordar un curso de acción tendiente a enfrentar esta problemática.

Considerando un caso real de un ataque de denegación de servicios de internet sin precedentes, ocurrido el 21 de octubre de 2016, y que dejó inaccesibles a grandes plataformas de Internet principalmente en Norteamérica y Europa, pero que tuvo un alcance global, se estudió el impacto producido como consecuencia de esas acciones; planteando el análisis de las consecuencias técnicas y legales implicadas en tal situación. Así, observando el contexto tecnológico-legal disponible hoy para el análisis forense de un caso como el esbozado (y suponiendo que algún usuario afectado por esta situación quisiera iniciar acciones legales contra un tercero), se identificaron las fortalezas y debilidades de dicho contexto y propusieron mejoras para una respuesta más adecuada cuando se requiere la actuación de la forensia digital.

El estudio realizado destacó fundadamente que el ataque puso de manifiesto la vulnerabilidad de los sistemas IoT y desde el punto de vista del derecho mostró la indefensión de los usuarios. Sin pretender formular una solución concreta y única al problema planteado, se señaló una serie de interrogantes coadyuvantes a definir el marco legal e identificar ciertos criterios o elementos técnicos y legales tendientes a definir el camino a seguir. Incursionando por último en algunas consideraciones particulares para la forensia IoT.

La investigación realizada concluye afirmando que IoT propone un contexto totalmente diferente al conocido hasta hoy, estableciendo una nueva forma de relacionarnos con la tecnología, que hoy se vive en una situación de cambio permanente en este aspecto y que, por ello, es necesario reconocer la situación, adaptarse a ella y nunca dejar de aprender; siendo esta la característica imprescindible en estos tiempos. Todo esto en un contexto de apertura y flexibilidad y, en donde, la legislación debería acompañar este proceso de cambio a fin de lograr hacer de nuestro mundo un sistema colaborativo e integrador, donde se puedan desarrollar soluciones agiles y acordes al entorno digital en el que estamos inmersos, bajo premisas de convivencia que nos permita ser mejores personas.

La tercera acción destacable del grupo de investigación de Forensia de IoT de la UCASAL, consistió en el ***análisis de las herramientas para protección de datos personales*** [15]**.** Esta vez se trabajó sobre el análisis de herramientas que promueven la protección de los datos personales de los usuarios de internet. La mayoría de proveedores de servicios en internet han sido desarrollados con un modelo de negocio basado en los datos de sus usuarios, sin pensar demasiado en su privacidad y haciendo un uso indebido de la confianza que estos le han otorgado. El modelo tradicional de aceptar los *Términos y Condiciones de Uso* ha caído en desuso ante los avances de la tecnología, y resultan difíciles y casi imposibles de entender para un usuario común. Las opciones que los usuarios tienen son dos: aceptar las condiciones o quedarse excluidos de los servicios. Además, en muchos casos, ni siquiera tienen la opción de elegir, ya que su privacidad se ve afectada por las decisiones de otras personas con las que establece ciertas relaciones. En este se discutieron algunas de las herramientas orientadas a la

protección de la privacidad de los datos, destacando la urgente necesidad de abordar este aspecto de la seguridad informática desde la perspectiva del propio usuario.

En la actualidad, cuando un usuario desea utilizar un servicio o un dispositivo electrónico, en la mayoría de los casos se requiere que éste inicie sesión de alguna manera en el sistema del fabricante. Por lo general, al iniciar sesión el usuario debe elegir entre continuar y aceptar los Términos y Condiciones (TC), o simplemente no aceptarlos y cancelar el proceso, quedándose excluido del uso total o parcial del servicio y/o dispositivo electrónico [16].

Los TC suelen incluir cláusulas que requieren el consentimiento de los usuarios para el intercambio de datos con fines comerciales. El típico *"He leído y acepto los términos y condiciones de uso"* es inadecuado, ya que estas cláusulas son muy largas y complicadas de entender para un usuario típico. Teniendo en cuenta que en términos técnicos y legales, consentir es autorizar, las personas muchas veces desconocen las consecuencias y simplemente optan por aceptar dichos TC, otorgándoles a distintas empresas información diversa y sumamente precisa. Además, muchos TC contemplan la posibilidad de ser actualizados sin previo aviso, lo que implica que los usuarios deben revisarlos constantemente para mantenerse informados.

El advenimiento del Internet de las Cosas (IoT) y los más variados dispositivos IoT que se esperan a futuro, los cuales estarán provistos de distintos sensores capaces de recolectar datos de nuestro entorno, nos plantea el problema de la privacidad. Y es que, ante los avances de la tecnología, el modelo actual se ha quedado por detrás y es necesario un nuevo planteo que tenga en cuenta los tiempos modernos. Los usuarios desconocen muchas veces el destino que les será conferido a sus datos, además de no contar con la posibilidad de solicitar la eliminación de estos, aunque las leyes lo prevean.

Las Redes Sociales En Línea (OSN, del inglés *Online Social Networks*) son plataformas que agrupan a los usuarios de manera que pueden establecer amistades e interactuar unos con otros sobre sus actividades rutinarias [17]. Las OSN se han extendido de las redes convencionales debido a la evolución de Internet, de manera que estamos brindando gran parte de nuestros datos personales[7] a unas pocas OSN que no han sido diseñadas, desde su concepción, teniendo en cuenta la privacidad de sus usuarios.

Como conclusión de este estudio, se observa que se ha ingresado en la era de las Tecnologías que Invaden la Privacidad (PiTs, del inglés *Privacy-invading Techonologies*) y distintas investigaciones se han llevado a cabo tanto en los aspectos legales como en las tecnologías que ayudan a proteger la privacidad (PETs, del inglés *Privacy-Enhancing Technologies*). Estas últimas son diseñadas desde el comienzo teniendo en cuenta la privacidad del usuario, lo que se conoce como Privacidad por Diseño (PbD, del inglés *Privacy by Design*).

5. Estado actual de la investigación

A la fecha, el equipo de investigadores se encuentra abocado al estudio de diversos *Modelos o Metodologías Forenses en Entornos de IoT*. El objetivo es estudiar cual es el contexto de seguridad informática que está disponible en los componentes de IoT, a partir del análisis de distintos modelos forenses, considerando un conjunto de características que hagan comparable los distintos modelos en análisis.

Sin agotar el tema, se han seleccionado para iniciar el estudio 3 modelos: *Profit*[18], *Probe-IoT* [19] *y FAIoT* [20].

El modelo *PRoFIT* consiste en la cooperación de los dispositivos del entorno, con lo cual redefine las fases del modelo forense tradicional como se conoce actualmente. Las fases de este modelo se

[7] Según el Artículo 4 de GDPR (http://www.privacy-regulation.eu/es/4.htm): Dato personal es toda información que pueda determinar, en particular mediante un identificador, la identidad de una persona física. Por ejemplo: nombre, número de identificación, datos de localización, estado físico, fisiológico, etc.

definen como:

- Preparación
- Recolección basada en el contexto
- Análisis de datos y correlación
- Compartición de la información
- Presentación
- Revisión

Si bien no vamos a entrar en detalle de cada fase, lo nuevo de este modelo es que integra requisitos de privacidad durante todo el ciclo de vida de la norma ISO/IEC 29100:2011. A medida que se lleva a cabo la investigación, cada fase debe ir cumpliendo con los principios de esta norma.

Propone integrar ciertos principios de privacidad, lo cual lo hace aplicable siempre que se trate en un marco de investigación ideal, esto significa que bajo otras circunstancias es muy difícil que se aplique o que se logre cumplimentar todas las fases de la metodología ya que no siempre se logra el consentimiento de todas las partes involucradas. Hoy en día ante el avasallamiento de dispositivos IoT en el que estamos rodeados es muy difícil si se saca del contexto propuesto por este modelo.

En la práctica, este modelo requiere de un software que es necesario instalar en los dispositivos para recabar información, este se puede preconfigurar en el entorno IoT, lo cual se hace antes de que ocurran los hechos a investigar.

El modelo *Probe-IoT* consiste en almacenar todas las interacciones de los dispositivos IoT en la nube utilizando *Blockchain* [8]. Todas las interacciones son almacenadas en un libro distribuido el cual es público y pueden acceder las partes interesadas. Toda la información es almacenada en una transacción la cual es cifrada mediante una clave pública y con el cifrado correspondiente. Al usar claves públicas, existe una entidad de administración la cual posee la identidad de las entidades. En una investigación, se deberá solicitar al administrador de claves para poder validar la información y poder proceder con el análisis de la información almacenada en un bloque.

Este modelo al utilizar blockchain hace uso de las virtudes de esta forma de almacenar información, plantea que todos los dispositivos deben emitir todas las interacciones para poder almacenrlas en internet. El inconveniente que se presenta es con los dispositivos que generan datos no estructurados y no indica como los dispositivos IoT informaran las interacciones, o sea a través de que medio o utilizando algún software o algún tipo de interfaz a que lleve al dispositivo a generar datos para subir a la nube. Otro problema es que puede haber información a nivel local del dispositivo que puede ser muy importante para una investigación, por lo cual en este modelo no se tiene en cuenta.

El modelo *FAIoT* propone que los dispositivos IoT informen a la nube toda la información que generan, para ello existe un repositorio de evidencias donde se almacenan todos los datos brindados por los dispositivos. Para ello se debe registrar los dispositivos indicando los datos del propietario con lo cual se puede separar o filtrar por propietario. Utiliza el sistema de cifrado mediante clave pública para preservar la evidencia y la privacidad de la información. De este modo solo los investigadores podrán acceder a la información.

Mediante una aplicación que solo los investigadores o entidades autorizadas tendrán acceso, podrán conectarse a este repositorio de evidencia y gestionar la información que necesita en una investigación.

Como en el modelo anterior, cierta información que se almacena en la memoria local puede ser útil en una investigación, la cual en este modelo no es tenida en cuenta.

El registro de los dispositivos y el propietario, al crecer exponencialmente en nuestras vidas, es el punto mas complicado que se pueda cumplir. No informa sobre qué tipo de información se va a almacenar, si el

[8] BLockChain: es una estructura de datos distribuida y segura (con cifrado) que se puede aplicar a todo tipo de transacciones. Evita el uso de bases de datos localizadas en un único servidor o equipo, ya que los distintos componentes de esta estructura se distribuyen en diferentes espacio de la internet.

propietario puede restringir o indicar el alcance de hasta donde esta dispuesto a divulgar sobre su vida privada.
Considerando un conjunto de características distintivas, se ha elaborado un cuadro comparativo (Tabla 1) que señala el cumplimiento o nó de estas características en cada uno de los 3 modelos señalados.

Tabla 1: Cuadro Comparativo de los Modelos Analizados

	PRoFIT	PROBE-IoT	FAIoT
Privacidad de los datos	SI	SI	SI
El propietario define el alcance de la información	SI	NO	NO
Utiliza Software	SI	NO	NO
Se tiene en cuenta el análisis a nivel local	SI	NO	NO
Propone técnica forense de extracción	NO	NO	NO
Herramienta forense	NO	NO	NO
Tipo de almacenamiento	BD LOCAL	NUBE	NUBE
Utiliza Blockchain	NO	SI	NO
Tipo de acceso	SOFTWARE	NO	API

El gran crecimiento de dispositivos de Internet de las Cosas (IoT) aparece con nuevos problemas para el análisis forense digital. Como nuevo desafío en esta área, el volumen de dispositivos que requieren ser analizados, examinados y preservados así también como la diversidad en los formatos de almacenamiento hacen que la tarea sea más ardua. Suponiendo un caso típico de IoT, como lo es un sistema de CCTV (Circuito Cerrado de Televisión), que consta de un equipo central y cierta cantidad de cámaras de video de diversas tecnologías, marcas y características, veamos que se espera encontrar, si se aplica alguno de los modelos analizados.
La implementación del modelo *PRoFIT* implica la instalación de un software en los dispositivos para que recabe información lo cual no se considera factible para este caso, ya que las cámaras en muchos casos no cuentan con los requerimientos básicos para el funcionamiento de un software adicional (memoria, procesador, etc.).
Si se aplicara la metodología que propone *Probe-IoT* se plantea la necesidad de que todos los dispositivos intervinientes tengan la habilidad de emitir sus interacciones y estas ser almacenadas en una blockchain a través de Internet lo cual no necesariamente se realiza en los sistemas de CCTV. Tampoco contempla el análisis de información almacenada a nivel local en los dispositivos
FAIoT propone la necesidad de almacenar toda la información que generan los dispositivos IoT en la nube. Este hecho generalmente no ocurre, principalmente con la información en formato video generada por estos dispositivos la cual es almacenada localmente y su análisis no es tenido en cuenta por este modelo de manera similar al modelo anterior.
De lo dicho se observa que el solo hecho de seguir un modelo específico a menudo no suele ser suficiente como para adaptarse a las necesidades de los distintos casos que se plantean ante la ley.
Este ejemplo, sirve para identificar los inconvenientes que puede haber al intentar aplicar alguna metodología forense demasiado *generalista*. Este primer estudio permite observar la necesidad de definir *primero* el objeto de estudio, y luego aprovechar las metodologías forenses existentes o propuestas, para elaborar una propuesta propia, de caracter viable, y que se ajuste a las características de la funcionalidad de IoT.
Hasta aquí una primera aproximación al tema. Desde el equipo de investigación se pretende continuar con las siguientes acciones:

- Identificar un objeto de estudio, definiéndolo desde sus características técnicas y funcionalidades. Puede ser un sistema de CCTV, o algún electrodoméstico hogareño o dispositivos de control automático de señales, entre otros objetos que se pueden considerar en IoT.
- Estudiar y analizar las políticas, normas y disposiciones sobre seguridad informática vinculadas a dicho objeto de estudio. Enfocando este estudio tanto desde el ámbito del Derecho como de la Informática.

- Formular una metodología de análisis forense para el objeto de estudio, identificando los componentes, funcionalidades, estructuras y demás características que permitan generalizar el método mediante sucesivas pruebas piloto.

6. Conclusiones

Es importante reconocer el avance del tema, no solo por la tecnología que se expande con mucha rapidez, sino principalmente por la universalidad del ámbito en que se propaga. Debe tenerse presente lo dicho por [24] en cuanto a los *desafíos* que plantea IoT a la Forensia Digital, entre los cuales se enuncian:

- Las herramientas y tecnologías forense generalmente no son medios aptos para identificar y analizar la infraestructura de IoT, es necesario desarrollar nuevas herramientas y protocolos de actuación pericial.
- El proceso de análisis forense tradicional se verá afectado. Los dispositivos IoT producen una gran cantidad de datos, que se siguen generando al momento mismo de la investigación forense, requiriendo más tiempo para la identificación de la información relevante, su resguardo y preservación. Estos dos últimos pasos son los más críticos debido a que usualmente los dispositivos de IoT no se pueden desconectar para aislarlos y preservar la prueba digital.
- El proceso de extracción de pruebas también se podría complicar ya que los dispositivos IoT cuentan con formatos de datos heterogéneos, protocolos e Interfaces físicas involucradas. Se destaca particularmente la diversidad de dispositivos, con sistemas operativos propietarios, y la creciente capacidad inteligente de los sensores y actuadores.

Estos aspectos destacados, se suman a la problemática que en sí ya tiene la Forensia Digital, como ser: rigurosidad en la cadena de custodia, capacitación de los analistas forenses en estas nuevas tecnologías, normalización y estandarización de los registros (logs) de eventos, normativa legal y jurisprudencia sobre el tema.

Se debe aceptar que en este nuevo orden, las tecnologías informáticas que encuentran su máxima expresión en Internet de las Cosas, resulta un ámbito muy adecuado para el desarrollo del delito, considerando además que no se trata solo de dispositivos y redes, sino que también se ha profesionalizado el uso de las TICs en el campo delictivo.

Por otra parte, y ya desde el equipo de trabajo abocado a este proyecto, cabe mencionar que se ha logrado establecer una simbiosis entre los profesionales de las distintas disciplinas – derecho e informática- con beneficio para todos, particularmente porque los investigadores más experimentados se ocupan de enseñar a los investigadores noveles, quienes agregan al equipo el entusiasmo y la dinámica necesaria para el logro de los objetivos.

Referencias

[1] D. Betancourt, G. Gómez, and J. I. Rodríguez, “Introducción a la internet de las cosas,” *Tecnogestión: Una Mirada Al Ambiente*, 2016.

[2] G. Misra, V. Kumar, A. Agarwal, and K. Agarwal, “Internet of Things (IoT) – A Technological Analysis and Survey on Vision , Concepts , Challenges , Innovation Directions , Technologies , and Applications (An Upcoming or Future Generation Computer Communication System Technology),” *Am. J. Electr. Electron. Eng.*, vol. 4, no. 1, pp. 23–32, 2016.

[3] X. Caron, R. Bosua, S. B. Maynard, and A. Ahmad, “The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective,” *Comput. Law Secur. Rev.*, vol. 32, no. 1, pp. 4–15, 2016.

[4] A. C. Raul, *The Privacy , Data Protection and Cybersecurity Law Review*. 2014.

[5] C. A. sobre E. del Personal and C. y Tecnológico, “Documento I - Comisión Asesora de Evaluación Personal CyT,” pp. 1–11, 2012.

[6] S. Haykin, “Cognitive Radio : Brain-Empowered,” *Ieee J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, 2005.

[7] A. Dunkels, “The Internet of Things : IP for Smart,” *Science (80-.).*, 2008.

[8] A. Katasonov, O. Kaykova, O. Khriyenko, S. Nikitin, and V. Terziyan, “Smart Semantic Middleware for the Internet of Things,” 2006.

[9] O. Lassila and D. L. McGuinness, “The Role of Frame-Based Representation on the Semantic Web,” *Rev. Account. Stud.*, vol. 12, no. 3, p. 369, 2001.

[10] M. Bermudez-Edo, T. Elsaleh, P. Barnaghi, and K. Taylor, “IoT-Lite: a lightweight semantic model for the internet of things and its use with dynamic semantics,” *Pers. Ubiquitous Comput.*, vol. 21, no. 3, pp. 475–487, 2017.

[11] P. Patel, A. Gyrard, S. K. Datta, and M. I. Ali, “Swotsuite: A toolkit for prototyping end-to-end semantic web of things applications,” *26th Int. World Wide Web Conf. 2017, WWW 2017 Companion*, pp. 263–267, 2019.

[12] O. Corcho, M. Fernandez, A. Gomez, and A. Lopez-Cima, “Construcción de ontologías legales con la metodología METHONTOLOGY y la herramienta WebODE,” *Law Semant. Web Leg. Ontol. Methodol. Leg. Inf. Retrieval, Appl.*, pp. 142–157, 2005.

[13] J. Araoz Fleming, B. Luz Clara, and H. B. Parra de Gallo, “La importancia de las pericias informáticas en el ámbito del Derecho,” in *FODERTICS 7.0 Estudios sobre Derecho Digital*, 2018, pp. 217–226.

[14] B. Luz Clara, J. D. Aráoz Fleming, E. Rivetti, A. Gamarra, and H. B. Parra de Gallo, “PROPUESTA DE CRITERIOS TÉCNICOS Y LEGALES PARA RESPONDER A LA VULNERABILIDAD DE INTERNET DE LAS COSAS,” in *XXII Congreso Iberoamericadno de Derecho e Informática*, 2018.

[15] E. Notario, B. L. Clara, and B. P. De Gallo, “Análisis de herramientas para protección de datos personales,” in *6to CONGRESO NACIONAL DE INGENIERÍA EN INFORMÁTICA/SISTEMAS DE INFORMACIÓN*, 2018, pp. 4–9.

[16] L. Belli, M. Schwartz, and L. Louzada, “Selling your soul while negotiating the conditions: from notice and consent to data control by design,” *Health Technol. (Berl).*, vol. 7, no. 4, pp. 453–467, 2017.

[17] F. Li and T. C. Du, “The effectiveness of word of mouth in offline and online social networks,” *Expert Syst. Appl.*, vol. 88, pp. 338–351, 2017.

[18] A. Nieto, R. Rios, and J. Lopez, “PRoFIT: Modelo forense-IoT con integración de requisitos de privacidad,” no. Jitel, pp. 302–309, 2017.

[19] M. Hossain, R. Hasan, and S. Zawoad, “Probe-IoT: A public digital ledger based forensic investigation framework for IoT,” *INFOCOM 2018 - IEEE Conf. Comput. Commun. Work.*, pp. 1–2, 2018.

[20] S. Zawoad and R. Hasan, “FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things,” *Proc. - 2015 IEEE Int. Conf. Serv. Comput. SCC 2015*, no. June, pp. 279–284, 2015.