M. Ruiz, R. Rios, R. Roman, and J. Lopez, "Privacidad Contextual en entornos Edge", *VII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2022)*, pp. 122-129, 2022.
NICS Lab. Publications: https://www.nics.uma.es/publications

Privacidad contextual en entornos Edge

Manuel Ruiz, Ruben Rios, Rodrigo Roman, Javier Lopez
NICS Lab, Universidad de Málaga
Campus de Teatinos s/n, 29071, Malaga
{mrr,ruben,roman,jlm}@lcc.uma.es

***Resumen*—La privacidad contextual se refiere a la protección de toda aquella información que puede desprenderse de la interacción entre usuarios y/o servicios, exceptuando los datos que el propio usuario elige transmitir. La localización, el tiempo, los patrones de uso y los diferentes parámetros necesarios para realizar la comunicación son algunos ejemplos. Este tipo de privacidad es extremadamente importante en la computación edge debido al acercamiento de los recursos de la infraestructura a los usuarios. Por ello, el objetivo de este trabajo es ofrecer un análisis y clasificación de las diferentes soluciones propuestas en la literatura respecto a la privacidad contextual en entornos edge, mostrando tanto las capacidades de los mecanismos actuales como los desafíos en este campo.**

***Index Terms*—Privacidad, Computación edge, Privacidad contextual**

Tipo de contribución: *Investigación original*

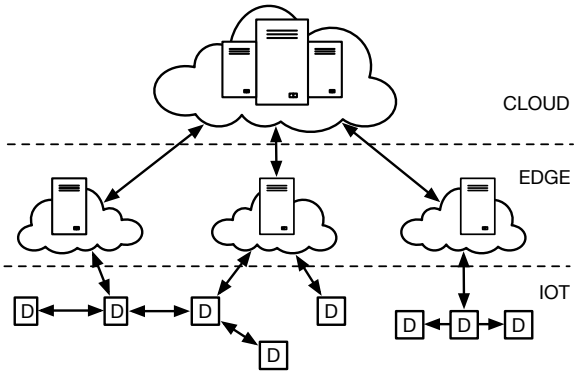

Figura 1. Infraestructura de computación edge

I. Introducción

En los últimos años se ha observado que la computación en la nube no es una solución óptima para muchos de los escenarios de aplicación previstos por la Internet de las Cosas (IoT) [1]. Aplicaciones como las redes vehiculares, la cirugía en remoto o la industria 4.0 simplemente no funcionarán si depende de un sistema remoto y centralizado como la nube. La razón es doble: (1) estas aplicaciones requieren latencias extremadamente bajas para permitir que los dispositivos reaccionen a tiempo a los cambios acontecidos en su entorno, y (2) existe un cuello de botella, en términos de ancho de banda, causado por la transmisión masiva de datos desde multitud de dispositivos en el borde de la red hasta el núcleo – donde se encuentran los servidores de la nube.

La computación en el borde o computación edge (en inglés, *Edge Computing* [2]) es un nuevo paradigma de computación que trata de dar solución a los problemas planteados anteriormente. En este paradigma, los recursos del sistema, principalmente computación y almacenamiento, se distribuyen a lo largo de un continuo que va desde el núcleo de la red hasta los dispositivos del extremo, que son los principales clientes de la infraestructura (ver Figura 1). De esta forma, al no depender directamente de servicios alojados en lugares remotos, se consigue mejorar sustancialmente los tiempos de respuesta de los dispositivos y reducir las necesidades de ancho de banda, entre de otras ventajas.

Además de las evidentes oportunidades que ofrece este nuevo paradigma, también abre la puerta a una serie de importantes retos relacionados con la gestión, coordinación y distribución de recursos. Asimismo, la naturaleza distribuida introduce una serie de importantes retos relacionados con la seguridad y privacidad [3]. Sin los mecanismos de seguridad adecuados, los potenciales beneficios que este paradigma puede aportar se verán empañados por los daños que pueden provocar los atacantes y sus desastrosas consecuencias. Por ejemplo, en un escenario edge dedicado a las redes vehiculares, un atacante puede lanzar ataques de denegación de servicio o incluso destruir físicamente parte de la infraestructura para que los vehículos sean incapaces de tomar decisiones a tiempo en caso de emergencia. Asimismo, la computación edge introduce nuevos retos de privacidad, principalmente debido al acercamiento de elementos de la infraestructura al extremo de la red. Gracias a dicho acercamiento, los operadores de la infraestructura tienen la capacidad de adquirir información que, en entornos basados en el cloud, no estaba a su alcance. De hecho, entre las novedades prometidas por el paradigma edge, se encuentra la capacidad de obtener y aprovechar información sobre el contexto en el que se despliegan los servicios virtualizados para, de esta forma, poder adaptarse a las necesidades o características del entorno y sus clientes.

Por tanto, además de los datos que un usuario puede transmitir desde sus dispositivos a la infraestructura, y que son susceptibles de ser analizados por un proveedor edge, existe también cierta información implícita al contexto que puede desprenderse de estas interacciones. Dicha información, que llamaremos información contextual, podría ser utilizada para fines maliciosos. En este sentido pueden encontrarse diferentes entidades interesadas en este tipo de información sensible. Por un lado, pueden existir proveedores edge que traten de sobrepasar los límites de la legalidad almacenando datos sobre los usuarios y su contexto, como por ejemplo su localización geográfica exacta en diversos instante de tiempo. Por otro lado, pueden existir terceras partes que se aprovechen de la infraestructura y los servicios desplegados para obtener información sensible no sólo sobre los usuarios, sino también sobre la propia infraestructura.

A fin de evitar este tipo de problemas, existen en la literatura diversas soluciones que abordan diferentes problemas de

privacidad en entornos edge. Gran parte de estas soluciones se centran en la protección de la privacidad relacionada con el contenido de los mensajes (c.f. [4], [5], [6]). Por otra parte, el número de soluciones que persiguen proporcionar mecanismos para proteger la privacidad contextual es más limitado, aun cuando la información asociada al contexto es igualmente sensible. Es por ello que en este artículo haremos una revisión y análisis de los trabajos relativos a la privacidad contextual en entornos edge, teniendo en cuenta el modelo de atacante al que tratan de hacer frente. Con esto pretendemos ofrecer una visión del estado del arte, así como promover la investigación en algunas áreas que consideramos aún requieren de nuevas soluciones o enfoques.

El resto del artículo se organiza según la estructura descrita a continuación. En primer lugar (sección II) se presentan brevemente trabajos relacionados con el estudio del estado del arte. A continuación, la sección III introduce una taxonomía de los problemas y soluciones de privacidad contextual existentes, que servirá de guía para el resto del artículo. En la sección IV se recogen los diferentes trabajos dedicados a la privacidad de la localización, mientras que en la sección V se aborda el análisis de los trabajos relacionados con la privacidad en las comunicaciones de manera general. En la sección VI, se estudia un conjunto de soluciones que surge para proteger la privacidad en el proceso de asignación de tareas, y posteriormente en la sección VII se analiza el problema de la privacidad temporal. En la sección VIII se ofrece una discusión sobre el estado del arte haciendo énfasis en las posibles líneas de investigación que consideramos más prometedores. Para finalizar, en la sección IX se muestran las conclusiones de este artículo.

II. Trabajo relacionado

Los paradigmas de computación en el borde como elemento vertebrador de un paradigma IoT completamente desarrollado ha provocado un enorme interés tanto en la academia como en la industria. En el ámbito académico se ha puesto mucho empeño en la definición del concepto y los elementos de su arquitectura [7]. Existen numerosos trabajos de investigación dedicados a estudiar las modelos de la computación en el borde (p.ej., [8], [9], [10], [2], [11]). Estos trabajos principalmente cubren aspectos generales de los paradigmas, como las tecnologías y protocolos clave, aplicaciones prometedoras además de problemas abiertos, y oportunidades. Otros autores analizan aspectos más específicos de los paradigmas de la computación edge, como el plano de la comunicación [12], el reparto de la computación [13], o el uso de redes definidas por software [14], entre otros.

También existen muchos trabajos dedicados a analizar el estado del arte de la seguridad en los paradigmas de computación en el borde. La mayoría de estos trabajos (p.ej., [15], [16], [3], [17]) suelen comenzar proporcionando una visión general del estado de los paradigmas edge y, posteriormente, realizan un análisis de las amenazas de seguridad que afectan a los diferentes componentes en estos entornos. Para finalizar, suelen presentar algunos desafíos de seguridad y oportunidades de investigación. La principal diferencia entre estos trabajos se encuentra en la clasificación de las soluciones, así como en el número y el nivel de detalle con que se analizan. Adicionalmente, estos trabajos también consideran y discuten las amenazas relacionadas con la privacidad en los paradigmas edge, pero al ser trabajos de alcance más generalista el análisis de dichas amenazas es limitado.

Existe otros trabajos de investigación que han proporcionado un análisis específico de las amenazas a la privacidad en los paradigmas de computación en el borde. Algunos de estos trabajos [18], [19], [20], [21] tienen un carácter generalista, mientras que otros se centran en aspectos muy específicos de la privacidad. Por ejemplo, Khalid et al. [22] ofrece un estudio sobre privacidad y esquemas de control de acceso, centrándose en el almacenamiento y la recuperación segura de datos. Del mismo modo, Zhang et al. [23] analiza varios métodos para la extracción, computación y la búsqueda segura de datos. En el mismo artículo, también revisan algunos mecanismos para proteger la identidad y la localización. Por último, Tian et al. [24] se centra en explorar y clasificar los retos de privacidad de localización en entornos MEC (Multi-access Edge Computing [25]).

Por lo tanto, como se desprende de los párrafos anteriores, no existen a fecha de hoy trabajos de investigación que proporcionen un estudio específico de la privacidad contextual en entornos edge. En consecuencia este es, hasta donde sabemos, el primer articulo que estudia y analiza el estado del arte de los diferentes retos y soluciones existentes de la privacidad contextual en la computación en el borde.

III. Clasificación de soluciones

En esta sección se proporciona una clasificación de amenazas y soluciones de privacidad contextual, la cual servirá de guía para la exposición de las secciones posteriores. Aunque este tipo de clasificaciones se puede realizar utilizando enfoques muy variados, en este caso nos hemos decantado por considerar en primer lugar el tipo de información a proteger, seguido por los diferentes modelos de atacante que pueden estar interesados en esa información, y, finalmente, por el tipo de soluciones desarrolladas para proteger la información frente a esos modelos de atacante. De esta forma, obtenemos una taxonomía en tres niveles, como se muestra en la Figura 2.

En el primer nivel de la clasificación, relacionado con *el tipo de información que se desea proteger*, se han considerado las siguientes categorías: localización, comunicación, reparto de tareas y registro temporal. Por lo general, la obtención de esta información podría afectar tanto a los clientes como a la propia infraestructura edge. Así pues, un atacante podía estar interesado en determinar la localización de un usuario concreto pero también la localización de servicios o aplicaciones desplegados en la infraestructura. En el segundo caso, el atacante estaría interesado, por ejemplo, en la carga de trabajo del proveedor de servicio en determinadas zonas geográficas, o en el movimiento de tareas entre dispositivos para conocer mejor su modelo de negocio, vulnerando así la privacidad del proveedor edge. Por otra parte, de las comunicaciones también se desprende gran cantidad de información sensible, por ejemplo, la dirección IP que utilizan un dispositivo de usuario es considerada un parámetro identificativo en muchos casos. Como veremos más adelante, estas dos categorías (localización y comunicación) son las que hasta la fecha han recibido una mayor atención por parte de la comunidad investigadora. Cabe mencionarse que existe cierta información contextual relacionada con las anteriores, el reparto de tareas,

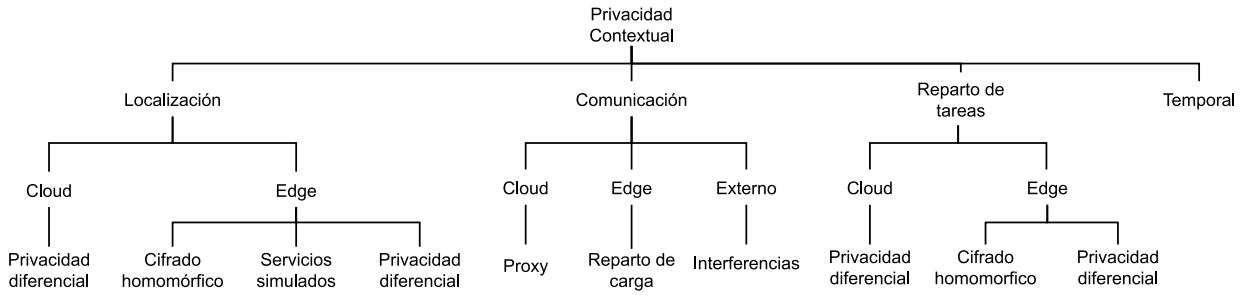

Figura 2. Clasificación de las soluciones encontradas

que hemos decidido considerar como una categoría separada debido al interés suscitado en la literatura sobre la privacidad de este procedimiento. Finalmente, la categoría temporal se refiere a los datos derivados de los patrones de uso y comportamiento. Sin embargo, pese a la importancia de esta información, no se ha encontrado literatura referente a este campo.

En el segundo nivel de la clasificación, relativo al *modelo de atacante*, es posible realizar varias separaciones atendiendo a diversas características. Por ejemplo, podemos distinguir entre atacantes internos o externos, en función de si este tiene o no acceso privilegiado a la infraestructura. Además, en relación a la naturaleza de los ataques realizados, podríamos considerar atacantes pasivos, que son aquellos que se limitan a recoger y analizar información, y atacantes activos, que además de ello se dedican a intervenir en las comunicaciones o alterar componentes del sistema. En este sentido, en la literatura se suele hacer referencia a atacantes semi-honestos (también conocidos como honestos pero curiosos), que son aquellos que no se desvían del comportamiento esperado pero tratan de obtener información a través de su participación en una comunicación o protocolo, y atacantes maliciosos, que se pueden comportar de manera arbitraria desviándose del comportamiento esperado para obtener información adicional.

Sin embargo, en este trabajo se ha decidido enfocar el modelo de atacante desde una perspectiva diferente – aunque complementaria – a las anteriormente presentadas. Esta decisión viene fundamentada por los trabajos encontrados en la literatura, que esencialmente consideran 3 atacantes posibles: (1) el servidor cloud, (2) los servidores edge y (3) atacantes externos. En esencia, esta clasificación considera los privilegios de los atacantes, si son internos o externos, y su ubicación en dentro de la infraestructura. Por lo general, todos estos atacantes se comportarán como entidades semi-honestas o pasivas.

Por último, el tercer nivel de clasificación se dedica a *los mecanismos utilizados por las soluciones propuestas*. Las principales soluciones encontradas se basan en la aplicación de mecanismos basados en privacidad diferencial y en cifrado homomórfico. En esencia, la privacidad diferencial [26] es una técnica de adición de ruido de manera que un atacante no pueda obtener información sensibles a partir del análisis estadístico del conjunto de datos. Por otra parte, el cifrado homomórfico [27] tiene como objetivo permitir la computación sobre datos cifrados, de forma que pueda seguir siendo utilizada por el resto de la infraestructura sin poner en riesgo los datos en sí mismos. También se han encontrado soluciones basadas en otros mecanismos, como la creación de servicios simulados, utilización de servidores proxy o la incorporación de señales de interferencias, que serán explicadas con detenimiento en sus respectivos apartados.

A continuación, se presenta y analiza manera detallada la investigación más relevante desarrollada hasta la fecha en cada una de estas categorías: la privacidad de la localización en la sección IV, la privacidad de la comunicación en la sección V, la privacidad en el reparto de tareas en la sección VI, y la privacidad temporal en la sección VII.

IV. Privacidad de localización

El lugar donde se encuentra un individuo o entidad en un momento determinado es información extremadamente sensible. Por norma general, los individuos son el foco de atención de atacantes aunque la localización de determinados dispositivos o recursos también puede ser de gran interés [28]. La información de localización puede servir a un atacante para identificar a una determinada persona, para crear un perfil sobre esta con sus hábitos, aficiones o gustos, e incluso para hacer un seguimiento o predecir donde estará en el futuro y atentar contra su integridad física o moral. Además, debido al acercamiento de los servicios y la infraestructura edge, esta información puede ser obtenida con más facilidad o precisión, incluso cuando el usuario no ha decidido revelarla libremente. Los mecanismos de privacidad de localización, por tanto, tratan de evitar que esta información se desprenda de las interacciones de los usuarios con el edge.

Si clasificamos las soluciones propuestas desde el punto de vista del atacante, en la literatura encontramos básicamente dos tipos de soluciones – orientadas a un cloud semi-honesto y orientadas a un cloud/edge semi-honesto.

IV-A. Cloud semi-honesto

Un proveedor de servicios cloud semi-honesto es aquel que proporcionan un servicio adecuado pero intentan extraer información de su interacción con el usuario y con los nodos edge. Las soluciones propuestas dentro de este ámbito se aplican en los nodos edge, que se considera confiable. En ambos casos propuestos, se utiliza la privacidad diferencial. En general, el nodo edge recibirá la información exacta de la ubicación del usuario, y ofuscará su contenido antes de enviarla al servidor cloud. De esta forma el proveedor de servicios nunca conocerá la localización exacta.

En [29] se propone un nuevo entorno de trabajo de privacidad diferencial llamado Pri-ENV, que permite proteger la ubicación exacta del usuario sin limitar la calidad del servicio prestado por los proveedores de servicios. Este entorno de

trabajo está compuesto por dos elementos: (1) El mecanismo de privacidad diferencial Pri-LBS y (2) un módulo PLA diseñado para permitir a los vehículos solicitar información útil basada en la localización enviada sin revelar su privacidad. Este módulo será el responsable de identificar el equilibrio entre la privacidad y la calidad del servicio mediante un nivel de privacidad ajustable. Ambos elementos se encuentran en los nodos edge de la red, que serán los encargados de aplicar las medidas de privacidad diferencial a la información. Los resultados obtenidos muestran que al aumentar el nivel de privacidad la calidad del servicio no baja drásticamente, lo que permite a los usuarios encontrar un equilibrio personalizado.

Miao et al. [30] proponen también un sistema basado en privacidad diferencial. En este caso se presenta un marco de trabajo denominado MEPA. Dentro de este marco de trabajo se muestra un algoritmo de privacidad diferencial y transmisión de peticiones denominado "Quadtree Differential Privacy" basado en "Hilbert curve division" (QTDP-H). Gracias a esta división de curvas se puede transformar un espacio de dos dimensiones en un espacio de una dimensión manteniendo poca pérdida de información, lo que permite disminuir el coste computacional que conlleva este tipo de técnicas. Comparado con los métodos tradicionales, se reducen tanto el tiempo medio de ejecución como el error medio relativo. Sin embargo, es necesario mencionar que el algoritmo propuesto no maneja bien la inconsistencia de los datos, lo que se propone en el artículo como línea de trabajo futuro.

IV-B. Cloud y edge semi-honesto

En ocasiones, el usuario no confiará en ningún elemento de la infraestructura. Así pues, en esta categoría encontramos las soluciones que también consideran a los nodos edge como atacantes semi-honestos. En este caso, es el dispositivo del propio usuario quien se encargará de proteger la privacidad de los datos de localización. Dentro de esta categoría encontramos varios enfoques. El primero estaría centrado en la utilización de cifrado homomórfico, y el segundo basado en la creación de servicios simulados que distraigan al atacante. Para finalizar, también se describe una solución basada en privacidad diferencial, similar a las anteriores.

En el caso del cifrado homomórfico, Jiang et al. [31] proponen dos protocolos de localización de la ubicación de sensores, los cuales permiten mantener su privacidad haciendo uso del cifrado homomórfico Paillier. La localización de los sensores se consigue a través del envío de la distancia del usuario con respecto a 3 estaciones base. Así, cuando el sensor quiere conocer su posición, solicita el cálculo de la distancia a las estaciones base. Éstas envían la información cifrada a los usuarios a través de los nodos edge – lo cuales no pueden extraer dicha información.

De esta forma, la información cifrada de las coordenadas del sensor pueden ser calculadas a partir de la información cifrada de la distancia obtenida con las 3 estaciones base. En todas estas comunicaciones la información se transmite cifrada, por lo que la privacidad está basada en la seguridad del esquema de cifrado. No obstante, cabe mencionarse que en ambos protocolos propuestos la clave pública del sensor y la localización de las estaciones base son públicas, por lo que un atacante externo puede elegir una localización y simular una interacción legítima.

Otro enfoque es el utilizado por He et al. [32], quienes consideran el uso de servicios simulados dentro de la red para dificultar las escuchas externas por parte de un atacante. El atacante intentará observar la trayectoria de los servicios mientras migran por los distintos nodos edge. Los servicios creados serían instancias independientes del mismo servicio que el usuario está utilizando, indistinguible del servicio original. Adicionalmente, respecto al patrón de movimiento de estos servicios, se estudian distintas estrategias basadas tanto en la imitación del comportamiento de los usuarios en la red como en la utilización de movimientos optimizados para minimizar la detección o el seguimiento del usuario real.

Así, una de las estrategias de optimización propuestas consigue llevar la precisión del seguimiento del atacante a cero cuando la movilidad del usuario real es lo suficientemente aleatoria. Asimismo, si el usuario real siempre permanece conectado al mismo nodo edge, es más apropiado utilizar la estrategia de la imitación de usuarios reales. No obstante, estos enfoques basado en el uso de servicios simulados presentan varios problemas. El inconveniente principal es el aumento del uso de recursos de la red. Además, si el atacante conoce las estrategias utilizadas por dichos servicios simulados, la utilidad de los mismos puede reducirse al mínimo.

Finalmente, Kaur et al. [33] plantean otra solución basada en privacidad diferencial para el caso de los datos de localización. El enfoque es similar a las soluciones vistas en la sección anterior, excepto por la incorporación de un nuevo elemento: el Secure Service Offloader (SSO). El SSO consiste en una nueva capa de nodos entre los nodos edge y el dispositivo, que sería la encargada de aplicar la privacidad diferencial a los datos que recoge de los dispositivos, evitando así la información sin ofuscar sea transmitida a los nodos Edge.

V. Privacidad en la comunicación

Del análisis de las comunicaciones, aunque estas estén protegidas mediante técnicas criptográficas seguras, se desprende también gran cantidad de información de información sensible, como las entidades que se comunican, la frecuencia con que lo hacen, el volumen de estas comunicaciones, etcétera. Precisamente por ello, se ha dedicado un gran esfuerzo de investigación a proporcionar soluciones capaces de proteger frente a atacantes con diversas capacidades de análisis de tráfico. Aunque la mayor parte de soluciones está enfocada a las comunicaciones en Internet, también se han estudiado estos problemas y desarrollado soluciones en otros entornos especializados, como las redes de sensores o entornos edge, que mostraremos a continuación.

Al igual que en el apartado anterior, volvemos a clasificar los trabajos de investigación según su consideración respecto a los atacantes.

V-A. Cloud semi-honesto

Suponiendo únicamente un servidor cloud honesto pero curioso, tenemos el trabajo de Zhang et al. [34], [35]. En él se presenta un sistema escalable basado en MEC, llamado Mobility Support System (MSS), que permite ocultar el tráfico y la localización de red del usuario móvil a los nodos de la red. El sistema se basa en crear un proxy de red dinámico y distribuido por cada usuario para conseguir minimizar la sobrecarga del tráfico y el coste computacional. El proxy

manejará el tráfico entrante y saliente del usuario. Los nodos objetivo serán los nodos al que se encuentra dirigido el tráfico, que pueden ser desde un servidor web a otro nodo móvil con un agente MSS. Además, dentro de este sistema se añade un nuevo elemento: el proveedor de servicio de movilidad (MSP). Este elemento manejará una flota de servidores, llamados routers virtuales (VR), que serán distribuidos dinámicamente desde los servidores centrales. Estos VR serán capaces de almacenar varios proxys.

Cuando un usuario quiere conectarse a otro nodo, el agente MSS en el host solicitará un proxy al MSP. Este proxy se asignará a una ubicación de red lo más cercana posible al nodo objetivo, y se conectará directamente a él. El tráfico entre el usuario y el nodo objetivo se envía a través del proxy utilizando una conexión entre el usuario y el proxy basada en su identidad. A continuación, la dirección del proxy será la expuesta a la red y no cambiará sin importar la ubicación del usuario. Por lo tanto, la dirección de red real del usuario y su movimiento se encuentran completamente ocultos del nodo objetivo. Cuando el nodo objetivo es un servidor estándar de internet y la conexión está vinculada a una dirección IP, MSS otorga un soporte adicional a la movilidad que permite a los protocolos de red tradicionales funcionar sin interrupción incluso si el usuario se encuentra desconectado temporalmente.

V-B. Edge semi-honesto

El trabajo de He et al. [36] trata únicamente la relación del dispositivo del usuario con el nodo edge, por lo que es este último el que se supone semi honesto. En esta investigación también se menciona la localización del usuario como elemento clave, pero además añade el patrón de uso de la red en la comunicación con los usuarios. El servidor edge puede ser capaz de extraer información estadística e incluso patrones del uso de la red de cada dispositivo basado en su historial de repartición de tareas y utilizar dicho patrón como huella para identificar la presencia de cierto usuario. Además, también podría determinar el servicio que esta ejecutándose en el lado del usuario, según el patrón de las tareas generadas por el servicio.

Para solucionar estos problemas, se propone un algoritmo de reparto de tareas basado en un proceso de decisión de Markov (CMDP) que tiene en cuenta la privacidad del usuario. Desde el punto de vista de envío de comunicación con la red, este algoritmo optimiza el retraso y rendimiento de consumo mientras que se mantiene un nivel de privacidad establecido con anterioridad.

Con el uso de este algoritmo, el dispositivo transmitirá algunas tareas – probablemente falsas – cuando las condiciones del canal sean inestables. Esto servirá para proteger su ubicación y patrón de uso. Sin embargo, como efecto secundario, este nivel de privacidad más elevado también conllevaría un mayor retraso y consumo de energía.

V-C. Atacante externo

Dentro de esta sección cabe destacar los conceptos mostrados en [37], donde se explora la seguridad a nivel físico. Se cree que este tipo de métodos basados en la teoría de la información proporcionan una mayor noción de privacidad que la criptografía y conllevan una menor carga computacional. Por lo tanto, pueden ser más apropiados para defenderse de atacantes externos en los entornos edge. Aprovechando la naturaleza inalámbrica del paradigma, se propone que el servidor edge envíe señales falsas para crear interferencia e impedir la escucha de atacantes externos, actuando sobre la privacidad general así como en la contextual. Estas señales de interferencia se generarán a la hora de la comunicación con los dispositivos finales, por lo que también se diseña un algoritmo de distribución de carga capaz de optimizar la combinación de las interferencias con las señales reales. Adicionalmente, se presenta un algoritmo para calcular la potencia óptima de las señales de interferencia. Finalmente, se presentan dos modos de operación basados en dos problemas de optimización, uno referente a la energía consumida y otro al retraso de ejecución.

Sin embargo, cabe mencionar que el trabajo habla únicamente de la comunicación de un nodo edge con un dispositivo. La inclusión de más antenas se menciona como futuras líneas de investigación, así como el estudio de nuevas técnicas de privacidad basadas en la capa física.

VI. Privacidad en el reparto de tareas

El reparto de tareas es una interesante aplicación que surge en entornos MEC con sensores móviles. En este tipo de aplicación, cobra mucha importancia la localización tanto de las tareas como del usuario que las emite y el que las recibe. Es por ello que muchos trabajos de investigación se centran únicamente en la privacidad dentro de este ámbito, en lugar de proporcionar un enfoque más genérico.

VI-A. Cloud semi-honesto

La solución propuesta por Shen et al [38], [39] se basa en el uso de técnicas de ofuscación para proteger el reparto de tareas de un servidor central semi-honesto ubicado en el cloud. El entorno propuesto se compone únicamente del servidor central, los servidores edge, y los usuarios móviles. Así, la protección de la privacidad recae sobre el servidor edge, basado principalmente en la ofuscación de información a través de un algoritmo genético.

El método de trabajo es el siguiente. Primero el servidor central publica la localización de las tareas a los servidores edge pertinentes. Después, los usuarios dentro del área designada envían su localización real a los nodos edge. Los servidores edge, tras recibir la información, ofuscan la localización de los usuarios y reparten las tareas en función de la localización ofuscada. A continuación, los usuarios que quieran participar en las tareas informarán al servidor edge, y realizarán la tarea. Tras recibir los resultados, el servidor edge enviará únicamente al servidor central los resultados y la localización ofuscada de los usuarios que han participado en completar las tareas.

VI-B. Cloud y edge semi-honesto

Dentro de la privacidad en el reparto de tareas, existen trabajos que consideran semi-honestos tanto al cloud como a los servidores edge. Uno de ellos, Ding et al. [40], propone un sistema de distribución de tareas para entornos edge basados en sensores móviles que tiene en cuenta la privacidad, y cuya característica principal es el uso del cifrado homomórfico para la localización del usuario, junto con la colaboración de varios

servidores edge para el reparto de la tarea cifrada. El esquema de comportamiento es similar a [38], [39], pero dando más peso a los solicitantes de tareas.

Primero, los solicitantes envían sus tareas al servidor central y se genera un par de claves para cada tarea. Después, el servidor central entrega las claves públicas a un servidor edge que se encuentre en la región solicitada, y entrega las claves privadas al servidor edge más cercano al primero. El primer servidor edge publica las tareas junto con sus claves públicas a los usuarios. A continuación, los usuarios solicitarán las tareas en las que se encuentren interesados mediante el envío al servidor edge de la distancia a las tareas, cifrada con la clave pública correspondiente. El servidor edge seleccionará los ganadores y los usuarios se desplazarán a la localización de la tarea, donde la completarán y subirán los datos cifrados al primer servidor edge. Después, el servidor edge cargará los datos recibidos en el servidor central junto con la distancia cifrada ofuscada. El servidor central pagará al servidor del edge y a los participantes, y por último, el servidor central es cifra y agrega los datos solicitados, y los devuelve al solicitante. Con este sistema, gracias al cifrado homomórfico, ni el servidor central ni el servidor edge pueden obtener la localización real de los usuarios durante el proceso.

En otro enfoque, Wu et al. [41] proponen añadir un elemento más a la mezcla: el centro de autorización (CA). Éste será el responsable de registrar todas las entidades del sistema y distribuir las claves necesarias. Todos los elementos del sistema son considerados semi-honestos excepto el CA, que es considerado totalmente honorable durante el desarrollo del protocolo.

El procedimiento sería el siguiente. Primero, el CA registra todas las entidades asignando los pares de claves correspondientes. Cada solicitador de tareas (TO) envía de forma anónima la tarea al servidor central. El servidor central reparte las tareas entre los servidores edge dependiendo de la localización. Estos últimos publicitan las tareas a los usuarios. Si un usuario quiere participar en alguna tarea, interactúa con el servidor edge para obtener los secretos correspondientes que además sirven como credenciales para la autorización de la tarea. Mientras tanto, el servidor central no puede saber que secretos ha solicitado el usuario. Finalmente los datos recogidos se ofuscan con un número aleatorio y se cifran con su clave pública antes de ser enviados. El servidor edge comprueba la integridad de todos los datos recogidos y calculan en colaboración con el servidor central la agregación de los mismos.

Respecto a la seguridad de los TOs, el sistema es capaz de mantener la privacidad de la identidad, de las tareas y de los resultados. Respecto a la privacidad de los participantes, el servidor central no conoce la relación entre las tareas y los participantes. Además, los nodos edge u otros usuarios no pueden identificar la información enviada de un usuario.

VII. Privacidad temporal

La privacidad temporal es otro de los aspectos a tener en cuenta dentro del paradigma de computación edge. La información temporal de conexión a la red puede ayudar a la predicción de comportamiento de individuo. Además, combinado con la localización, puede fomentar la creación de perfiles individuales.

No obstante, no se han encontrado estudios de investigación que traten en detalle el problema específico de la privacidad temporal dentro de los entornos de computación edge. Cabe mencionarse que si existen dichos estudios aplicados a otros paradigmas similares. Por ejemplo, en el entorno de las redes de sensores, se encuentran trabajos como el de Chakraborty et al. [42], que proponen mantener la privacidad temporal retrasando los envíos de algunos paquetes en algunos puntos de la ruta entre el sensor que detecta el evento y la estación base para que el atacante no pueda deducir el tiempo en el que tiene lugar dicho evento.

VIII. Desafíos Futuros

Tras una exhaustiva revisión de la literatura relativa a la privacidad contextual en entornos edge, se han detectado y analizado múltiples soluciones, que resumimos en la Tabla I.

A tenor de los resultados de este artículo, podemos afirmar que la investigación sobre privacidad contextual en entornos edge está aún en una fase de desarrollo muy temprana. Si bien existen áreas concretas donde hay ya un corpus de soluciones relativamente amplio, existen otras aún inexploradas. Como se puede observar en la Tabla I, hasta la fecha la mayor parte de soluciones se ha centrado en desarrollar soluciones relativas a la protección de información de localización y al reparto de tareas, siendo este último problema una versión especializada del primero. Otras áreas, en cambio, ha recibido poca o ninguna atención. En el ámbito de la privacidad en las comunicaciones existen pocas soluciones, aunque novedosas y variadas, pero presentan inconvenientes y/o son incapaces de dar una solución completa a los desafíos planteados. Por último, cabe destacar la ausencia absoluta de soluciones dedicadas a la protección de la privacidad temporal. En este sentido, consideramos que puede resultar de enorme interés analizar soluciones que haya surgido en otras áreas de investigación afines y estudiar si sería posible adaptar las soluciones propuestas en ellas a los entornos edge.

En lo relativo al modelo de atacante ocurre algo similar. En general, la mayoría de artículos se centran en atacantes alojados bien en el cloud o que comprenden toda la infraestructura cloud-edge. Sólo uno de los trabajos encontrados considera un modelo de atacante diferente, en concreto un atacante externo. Además, todos estos trabajos consideran un modelo de atacante semi-honesto, que trata de obtener información sensible sin excederse de sus funciones. Por tanto, el estudio de diferentes modelos de atacantes, especialmente aquellos activos o maliciosos, es un problema abierto que necesita de soluciones.

Por último, en el plano de las técnicas utilizadas para la protección de diferentes tipos de información, observamos que gran parte de ellas se sustentan en el uso de privacidad diferencial y cifrado homomórfico. Así pues, es necesario investigar otros mecanismos y técnicas que puedan ser aplicadas en entornos de computación edge y que se ajusten a su propia naturaleza. Sin duda, hay espacio para nuevas soluciones con enfoques innovadores.

IX. Conclusión

Las características de la computación edge, como la distribución y la limitación de recursos, provocan tanto la aparición de nuevos problemas de privacidad como la agravación de

Tabla I
MEDIDAS DE PRIVACIDAD SEGÚN LOS TRABAJOS DE INVESTIGACIÓN ESTUDIADOS

Referencia	Información contextual	Atacante		Técnica de protección
[29]	Localización	Cloud	Semi-honesto	Privacidad diferencial
[30]	Localización	Cloud	Semi-honesto	Privacidad diferencial
[31]	Localización	Cloud y Edge	Semi-honesto	Cifrado homomórfico
[32]	Localización	Cloud y Edge	Semi-honesto	Servicios Simulados
[33]	Localización	Cloud y Edge	Semi-honesto	Privacidad diferencial
[34], [35]	Comunicación	Cloud	Semi-honesto	Proxy
[36]	Comunicación	Edge	Semi-honesto	Algoritmo de reparto de carga
[37]	Comunicación	Externo	Pasivo	Señales de interferencia
[38], [39]	Reparto de tareas	Cloud	Semi-honesto	Privacidad diferencial
[40]	Reparto de tareas	Cloud y Edge	Semi-honesto	Cifrado homomórfico
[41]	Reparto de tareas	Cloud y Edge	Semi-honesto	Privacidad diferencial

otros existentes, en comparación con otros paradigmas afines como el paradigma cloud. Algunas de las medidas de privacidad efectivas en entornos cloud no pueden ser aplicadas directamente en la computación edge debido a dichas características. Por tanto, sería necesario adaptarlas al nuevo entorno o innovar para mitigar los problemas emergentes.

Este artículo ha revisado y analizado la literatura relativa a los problemas de privacidad contextual en entornos edge. Los aspectos más cubiertos por la literatura existente son la privacidad de la localización y la privacidad durante el reparto de tareas en la computación edge. El estado de esta investigación es bastante significativa, considerando la novedad de este paradigma y su desarrollo concurrente. Sin embargo, existen varios aspectos como la privacidad en el contexto de las comunicaciones y en el aspecto temporal, que carecen de soluciones suficientes, sobre todo si lo comparamos con otros paradigmas similares. Esto es, sin lugar a dudas, una oportunidad para investigadores interesados en dicho ámbito que pueden aportar soluciones tempranas y novedosas dentro del paradigma.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia e Innovación a través del proyecto SecureEDGE (PID2019-110565RB-I00), la Consejería de Economía, Conocimiento, Empresas y Universidad de la Junta de Andalucía a través del proyecto SAVE (P18-TP-3724) y el proyecto BIG$^{\text{Priv}}$DATA (UMA20-FEDERJA-082) del Programa Operativo FEDER Andalucía 2014-2020.

REFERENCIAS

[1] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, ser. MCC '12. New York, NY, USA: ACM, 2012, pp. 13–16.

[2] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Generation Computer Systems*, vol. 97, pp. 219–235, aug 2019.

[3] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, Part 2, pp. 680–698, jan 2018.

[4] S. Gupta, R. Garg, N. Gupta, W. S. Alnumay, U. Ghosh, and P. K. Sharma, "Energy-efficient dynamic homomorphic security scheme for fog computing in IoT networks," *Journal of Information Security and Applications*, vol. 58, p. 102768, 5 2021. [Online]. Available: https://abdn.pure.elsevier.com/en/publications/energy-efficient-dynamic-homomorphic-security-scheme-for-fog-comp

[5] J. N. Liu, J. Weng, A. Yang, Y. Chen, and X. Lin, "Enabling efficient and privacy-preserving aggregation communication and function query for fog computing-based smart grid," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 247–257, 1 2020.

[6] F. Yildirim Okay, S. Ozdemir, and Y. Xiao, "Fog computing-based privacy preserving data aggregation protocols," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 4, 4 2020.

[7] Z. Mahmood, Ed., *Fog Computing: Concepts, Frameworks and Technologies*. Springer International Publishing, 2018.

[8] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 416–464, 2018.

[9] M. Mukherjee, L. Shu, and D. Wang, "Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1826–1857, 2018.

[10] P. Bellavista, J. Berrocal, A. Corradi, S. K. Das, L. Foschini, and A. Zanni, "A survey on fog computing for the Internet of Things," *Pervasive and Mobile Computing*, vol. 52, pp. 71–99, jan 2019.

[11] F. Liu, G. Tang, Y. Li, Z. Cai, X. Zhang, and T. Zhou, "A Survey on Edge Computing Systems and Tools," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1537–1562, aug 2019.

[12] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A Survey on Mobile Edge Computing: The Communication Perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[13] P. Mach and Z. Becvar, "Mobile Edge Computing: A Survey on Architecture and Computation Offloading," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1628–1656, 2017.

[14] A. C. Baktir, A. Ozgovde, and C. Ersoy, "How Can Edge Computing Benefit From Software-Defined Networking: A Survey, Use Cases, and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2359–2391, 2017.

[15] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in Fog computing: A survey," *Future Generation Computer Systems*, vol. 88, pp. 16–27, nov 2018.

[16] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018.

[17] M. Yahuza, M. Y. I. B. Idris, A. W. B. A. Wahab, A. T. S. Ho, S. Khan, S. N. B. Musa, and A. Z. B. Taha, "Systematic Review on Security and Privacy Requirements in Edge Computing: State of the Art and Future Research Opportunities," *IEEE Access*, vol. 8, pp. 76 541–76 567, 2020.

[18] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 2, pp. 1078–1124, 4 2021.

[19] B. Ali, M. A. Gregory, and S. Li, "Multi-access edge computing architecture, data security and privacy: A review," *IEEE Access*, vol. 9, pp. 18 706–18 721, 2021.

[20] T. Khalid, M. A. K. Abbasi, M. Zuraiz, A. N. Khan, M. Ali, R. W. Ahmad, J. J. Rodrigues, and M. Aslam, "A survey on privacy and access control schemes in fog computing," *International Journal of Communication Systems*, vol. 34, no. 2, 1 2021.

[21] Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al-Ahmad, "Fog computing security and privacy for the Internet of Thing applications: State-of-the-art," *Security and Privacy*, vol. 4, no. 2, p. e145, 3 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.145https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.145https://onlinelibrary.wiley.com/doi/10.1002/spy2.145

[22] T. Khalid, M. A. K. Abbasi, M. Zuraiz, A. N. Khan, M. Ali, R. W. Ahmad, J. J. Rodrigues, and M. Aslam, "A survey on privacy and access control schemes in fog computing," *International Journal of Communication Systems*, p. e4181, oct 2019.

[23] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18 209–18 237, 2018.

[24] Z. Tian, Y. Wang, Y. Sun, and J. Qiu, "Location privacy challenges in mobile edge computing: Classification and exploration," *IEEE Network*, vol. 34, no. 2, pp. 52–56, mar 2020.

[25] IBM News Release. Ibm and nokia siemens networks announce world's first mobile edge computing platform. [Online]. Available: https://www-03.ibm.com/press/us/en/pressrelease/40490.wss

[26] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy." *Found. Trends Theor. Comput. Sci.*, vol. 9, no. 3-4, pp. 211–407, 2014.

[27] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys (Csur)*, vol. 51, no. 4, pp. 1–35, 2018.

[28] R. Rios, J. Lopez, and J. Cuellar, *Location Privacy in Wireless Sensor Networks*, ser. CRC Series in Security, Privacy and Trust. Taylor & Francis, 2016. [Online]. Available: https://www.crcpress.com/Location-Privacy-in-Wireless-Sensor-Networks/Rios-Lopez-Cuellar/p/book/9781498776332

[29] L. Zhou, L. Yu, S. Du, H. Zhu, and C. Chen, "Achieving differentially private location privacy in edge-assistant connected vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4472–4481, 6 2019.

[30] Q. Miao, W. Jing, and H. Song, "Differential privacy–based location privacy enhancing in edge computing," in *Concurrency and Computation: Practice and Experience*, vol. 31, no. 8. John Wiley and Sons Ltd, 4 2019.

[31] H. Jiang, H. Wang, Z. Zheng, and Q. Xu, "Privacy preserved wireless sensor location protocols based on mobile edge computing," *Computers and Security*, vol. 84, pp. 393–401, 7 2019.

[32] T. He, E. N. Ciftcioglu, S. Wang, and K. S. Chan, "Location privacy in mobile edge clouds: A chaff-based approach," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2625–2636, 11 2017.

[33] J. Kaur, A. Agrawal, and R. A. Khan, "Encryfuscation: A model for preserving data and location privacy in fog based IoT scenario," *Journal of King Saud University - Computer and Information Sciences*, 3 2022. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S131915782200074X

[34] P. Zhang, M. Durresi, and A. Durresi, "Network Location Privacy Protection with Multi-access Edge Computing," in *Advances in Intelligent Systems and Computing*, vol. 926. Springer Verlag, 2020, pp. 1342–1352.

[35] ——, "Multi-access edge computing aided mobility for privacy protection in Internet of Things," *Computing*, vol. 101, no. 7, pp. 729–742, 7 2019.

[36] X. He, J. Liu, R. Jin, and H. Dai, "Privacy-Aware Offloading in Mobile-Edge Computing," *2017 IEEE Global Communications Conference, GLOBECOM 2017 - Proceedings*, vol. 2018-January, pp. 1–6, 7 2017.

[37] X. He, R. Jin, and H. Dai, "Physical-Layer Assisted Privacy-Preserving Offloading in Mobile-Edge Computing," *IEEE International Conference on Communications*, vol. 2019-May, 5 2019.

[38] H. Shen, G. Bai, Y. Hu, and T. Wang, "P2TA: Privacy-preserving task allocation for edge computing enhanced mobile crowdsensing," *Journal of Systems Architecture*, vol. 97, pp. 130–141, 8 2019.

[39] Y. Hu, H. Shen, G. Bai, and T. Wang, "Privacy-preserving task allocation for edge computing enhanced mobile crowdsensing," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11337 LNCS. Springer Verlag, 2018, pp. 431–446.

[40] X. Ding, R. Lv, X. Pang, J. Hu, Z. Wang, X. Yang, and X. Li, "Privacy-preserving task allocation for edge computing-based mobile crowdsensing," *Computers & Electrical Engineering*, vol. 97, p. 107528, 1 2022.

[41] H. Wu, L. Wang, and G. Xue, "Privacy-Aware Task Allocation and Data Aggregation in Fog-Assisted Spatial Crowdsourcing," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 589–602, 1 2020.

[42] B. Chakraborty, S. Verma, and K. P. Singh, "Temporal Differential Privacy in Wireless Sensor Networks," *Journal of Network and Computer Applications*, vol. 155, p. 102548, 4 2020.