# Context-Aware Enforcement of Privacy Policies in Edge Computing (Cumplimiento de las Políticas de Privacidad según el Contexto en la Computación Perimetral)

**Abstracto:**

La privacidad es una preocupación fundamental que enfrentan los sistemas que manejan datos sensibles. La falta de soluciones robustas para definir y aplicar medidas de privacidad continúa obstaculizando la aceptación general y la adopción de estos sistemas. Edge computing ha sido reconocido como un habilitador clave para aplicaciones mejoradas de privacidad, y ha abierto nuevas oportunidades. En este documento, proponemos un modelo de privacidad novedoso basado en la computación de borde sensible al contexto. Nuestro modelo aprovecha el contexto de los datos para tomar decisiones sobre cómo estos datos deben procesarse y administrarse para lograr la privacidad. Basado en un escenario del dominio de eHealth, mostramos cómo nuestro modelo generalizado puede usarse para implementar y promulgar políticas de privacidad complejas específicas del dominio. Ilustramos nuestro enfoque mediante la construcción de casos de uso del mundo real que involucran un registro de salud electrónico móvil que interactúa con,

**Publicado en:**[Congreso Internacional IEEE 2019 sobre Big Data (BigDataCongress)](https://ieeexplore.ieee.org/xpl/conhome/8805991/proceeding)

**Fecha de la conferencia:** 8-13 de julio de 2019

**Fecha de adición a IEEE *Xplore* :** 29 de agosto de 2019

**Información del ISBN:**

**Información de ISSN:**

**Número de acceso de INSPEC:** 18957654

**DOI:**[10.1109 / BigDataCongress.2019.00014](https://doi.org/10.1109/BigDataCongress.2019.00014)

**Editorial:**IEEE

**Lugar de la conferencia:** Milán, Italia, Italia

**SECCIÓN I.**

## **Introducción**

La computación en la nube y la continua centralización de la computación y la gestión de datos ha causado una creciente preocupación por la privacidad de los datos [1] . La liberación de datos a servicios centralizados es especialmente problemática para los sistemas que manejan datos confidenciales, como los datos de pacientes en sistemas de salud electrónica, ya que esta pérdida de control puede dificultar que los flujos de trabajo de gestión de datos cumplan con las políticas de privacidad [2]o disposiciones de seguridad como HIPPA (Ley de Responsabilidad y Portabilidad del Seguro de Salud). Edge computing ha sido reconocido como una tecnología clave para habilitar aplicaciones de Internet de las cosas (IoT) con privacidad. Sin embargo, la complejidad inherente a las arquitecturas de cómputo de borde hace que sea extremadamente difícil para los desarrolladores de aplicaciones implementar mecanismos que puedan garantizar el cumplimiento de las políticas de privacidad, especialmente en dominios complejos con grandes cantidades de partes interesadas, como eHealth. La investigación actual no proporciona marcos y soluciones concretas para modelar las restricciones de privacidad y promulgar reglas de procesamiento de datos para cumplir con los requisitos de privacidad [3]. La confidencialidad, la integridad y la privacidad de los datos son los conceptos clave para cumplir con esos requisitos. Para evitar la filtración de información, las políticas estrictas de acceso deben garantizar la confidencialidad e integridad de los datos privados, así como el manejo de la localidad de los datos. Esto se realiza comúnmente mediante la definición de roles de acuerdo con diferentes partes interesadas de un sistema, generalmente implementado por técnicas de Control de acceso basado en roles (RBAC) [4]. Sin embargo, otros acuerdos de privacidad de datos (por ejemplo, el intercambio de datos entre las partes interesadas), que también deben definirse, establecerse e implementarse adecuadamente a través de políticas de privacidad, introducen desafíos arquitectónicos, conceptuales y relacionados con el rendimiento adicionales. En este documento, presentamos un modelo novedoso para definir y promulgar políticas de privacidad basadas en cómputo de borde sensible al contexto. Al aprovechar el conocimiento del contexto de las computadoras de borde, permitimos la toma de decisiones en tiempo de ejecución para las aplicaciones sobre cómo aplicar políticas de privacidad durante los flujos de trabajo de datos. En comparación con los enfoques existentes, que se adaptan principalmente a un caso o dominio de uso específico [5] - [6] [7] [8], nuestro modelo se centra en la conciencia del contexto y las acciones correspondientes que deben tomar los dispositivos de borde. De este modo, permitimos flexibilidad en la implementación y ayudamos a los arquitectos o desarrolladores de sistemas a diseñar y construir sistemas descentralizados que puedan hacer uso de datos sensibles a la privacidad, al tiempo que cumplen con las complejas políticas de privacidad de un dominio determinado. Como parte de nuestro modelo de privacidad, definimos niveles de privacidad para incorporar una granularidad de descripción formal más fina. Demostramos nuestro enfoque basado en un escenario del dominio de eHealth, donde la privacidad se considera un requisito crítico. El resto de este trabajo se estructura de la siguiente manera. En la Sección II presentamos un escenario motivacional del dominio de eHealth. La Sección III ofrece una visión general del trabajo relacionado. En la sección IVpresentamos nuestro modelo de privacidad y cómo se toma en cuenta la conciencia de contexto en este modelo. En la Sección V , discutimos la aplicación de políticas de privacidad por nuestro modelo basado en la computación de borde sensible al contexto. Finalmente, la Sección VI concluye el documento y ofrece una perspectiva sobre el trabajo futuro.

**SECCION II.**

## **Escenario motivacional**

El Comité Nacional de Estadísticas Vitales y de Salud (NCVHS), un comité asesor clave del Departamento de Salud y Servicios Humanos de EE. UU., Define la privacidad en el contexto de la información de salud como " *el derecho de un individuo a controlar la adquisición, uso o divulgación de su o sus datos de salud identificables* " [9] . Por lo tanto, otorgar a los pacientes control sobre sus registros médicos, incluso si los datos son propiedad de otra parte (como es común en los registros de salud electrónicos) es fundamental para permitir la privacidad. El concepto de mHealth [10]puede facilitar esto aprovechando plataformas móviles para monitorear, procesar y almacenar datos médicos en los llamados registros de salud electrónicos móviles (mEHR). Sin embargo, esta descentralización aumenta la complejidad de los flujos de trabajo de gestión de datos, en particular cuando las políticas de privacidad deben ser promulgadas por el sistema automáticamente en tiempo de ejecución. Consideramos un escenario típico del dominio médico, donde un paciente ingresa a un hospital en busca de consulta médica y posteriormente es examinado por un médico. El paciente tiene un mEHR como aplicación instalada en su teléfono inteligente. Este registro comprende campos de datos personales como nombre, dirección o género; y campos de datos médicos organizados en secciones como diagnósticos, recetas o terapias. Múltiples partes interesadas también están involucradas en pasos adicionales en este escenario. Por ejemplo, considere a un farmacéutico que reparte medicamentos recetados, o un especialista en biotecnología (que, por ejemplo, es consultado por implantes artificiales especializados). Estas partes interesadas también pueden ser otras máquinas, como dispensadores de medicamentos o dispositivos inteligentes de imágenes médicas. Además, en este escenario, los diagnósticos también se pueden realizar de forma remota, lo que requiere que un sistema esté interconectado a través de diferentes redes. Todos estos ejemplos requieren el intercambio o el procesamiento de datos confidenciales en diferentes contextos entre diferentes partes interesadas. Un sistema que admita este tipo de escenario complejo requiere no solo mecanismos de control de acceso estándar basados ​​en roles para garantizar la privacidad, sino que debe Estas partes interesadas también pueden ser otras máquinas, como dispensadores de medicamentos o dispositivos inteligentes de imágenes médicas. Además, en este escenario, los diagnósticos también se pueden realizar de forma remota, lo que requiere que un sistema esté interconectado a través de diferentes redes. Todos estos ejemplos requieren el intercambio o el procesamiento de datos confidenciales en diferentes contextos entre diferentes partes interesadas. Un sistema que admita este tipo de escenario complejo requiere no solo mecanismos de control de acceso estándar basados ​​en roles para garantizar la privacidad, sino que debe Estas partes interesadas también pueden ser otras máquinas, como dispensadores de medicamentos o dispositivos inteligentes de imágenes médicas. Además, en este escenario, los diagnósticos también se pueden realizar de forma remota, lo que requiere que un sistema esté interconectado a través de diferentes redes. Todos estos ejemplos requieren el intercambio o el procesamiento de datos confidenciales en diferentes contextos entre diferentes partes interesadas. Un sistema que admita este tipo de escenario complejo requiere no solo mecanismos de control de acceso estándar basados ​​en roles para garantizar la privacidad, sino que debe*reaccionar y adaptarse* a diferentes cambios en el contexto ambiental. Dichas reacciones son operaciones o procesos que aseguran que la privacidad de los datos se conserva y se lleva a cabo de una manera que se ajuste a la política correspondiente.

**SECCION III.**

## **Trabajo relacionado**

Asegurar la integridad y el intercambio de información es un requisito crítico en sistemas distribuidos complejos que manejan datos confidenciales. El cifrado de datos es una herramienta común para impedir que un usuario no intencionado infiera información de datos almacenados o transferidos. En [11] se presenta una visión general de diferentes enfoques y técnicas de cifrado bien investigados . Para proteger los datos de la alteración, modificación o eliminación en un sistema distribuido, se han desarrollado y establecido varias estrategias de integridad de datos. Estos incluyen Posesión de datos comprobables (PDP) [12] , Prueba de recuperación (PoR) [13] y Auditoría de terceros (TPA) [14]. Hoy en día, los dispositivos periféricos interconectados como teléfonos inteligentes, sensores, etiquetas de identificación por radiofrecuencia (RFID) o dispositivos domésticos inteligentes están produciendo una gran cantidad de datos. A medida que estos dispositivos se integran cada vez más en nuestra vida diaria, afectan y cambian significativamente nuestra forma de vida, comportamiento social y estilo de vida [3] . Estos datos se utilizan para generar información contextual (por ejemplo, el seguimiento de la duración del viaje desde el hogar de una persona a su lugar de trabajo) [15]. En este documento nos enfocamos en la privacidad de los datos per se, que trata con la protección de la información personal. Por ejemplo, los datos privados de los pacientes, los diagnósticos o los planes de terapia pueden ser mal utilizados por, por ejemplo, las compañías de seguros para adaptar las tarifas y, por lo tanto, deben estar bien protegidos. El cumplimiento de la privacidad en los sistemas de software se ha abordado principalmente mediante la incorporación de técnicas RBAC. Estándares como XACML [16]puede usarse para definir políticas y manejar el acceso a datos, pero no tiene en cuenta los diferentes contextos ambientales ni describe cómo y dónde deberían habilitarse estas políticas. Además, la mayoría de esos mecanismos se basan en una arquitectura centralizada con una compleja constelación de roles y los datos confidenciales a menudo se duplican o distribuyen. Nuestro modelo describe cómo estos enfoques RBAC bien establecidos podrían extenderse, incorporando técnicas informáticas de vanguardia, para facilitar el desarrollo de sistemas descentralizados de preservación de la privacidad.

**SECCION IV.**

## **Modelo de privacidad en Edge Computing**

El modelo de privacidad que proponemos describe las circunstancias bajo las cuales una entidad puede acceder a partes específicas de datos confidenciales. La definición de un modelo coherente permite una definición coherente de las políticas que garantizan la privacidad de los datos, y también maneja la localidad de los datos. Nuestro modelo de privacidad combina y correlaciona ciertos niveles de privacidad (por ejemplo, restricciones de visibilidad en conjuntos de datos específicos) con un contexto dado. La determinación de un contexto específico se maneja mejor más cerca del entorno correspondiente. Por lo tanto, la computación perimetral es adecuada para esta tarea, donde cada dispositivo perimetral está expuesto a un contexto determinado y específico.

### A. Políticas de privacidad

Una forma común de habilitar y hacer cumplir la privacidad en la computación perimetral es definir políticas que especifiquen el manejo de datos confidenciales [17] , [18]. Un caso de uso puede ser la necesidad de políticas para manejar correctamente la recopilación, el intercambio y la divulgación de datos del paciente (por ejemplo, en escenarios de consulta médica). Retener la calidad de los datos y la accesibilidad requerida para el procesamiento médico, respetando al mismo tiempo los aspectos de privacidad de todas las personas involucradas, es uno de los desafíos clave al definir las políticas de privacidad en eHealth. Una implementación simple y concreta de dicha política podría describir qué campos de datos de un conjunto determinado de información personal deberían persistir y qué campos de datos deberían manejarse de manera transitoria. La desventaja de tales políticas es que a menudo se adaptan a casos de uso específicos y, por lo tanto, carecen de flexibilidad y generalidad. En este artículo distinguimos entre dos tipos diferentes de políticas. Primero, hay políticas que definen las modalidades de persistencia de datos de datos privados, y segundo, políticas que describen cómo y dónde se modifican los datos (p. ej., anonimizados o encriptados) para su transporte e inspección u otros cálculos. Por lo tanto, distinguimos entre límites de privacidad lógicos y físicos. Mientras que los límites lógicos tratan con restricciones basadas en roles, restricciones legales, etc., los límites físicos comprenden restricciones basadas en la ubicación, restricciones de red u otros dispositivos involucrados.

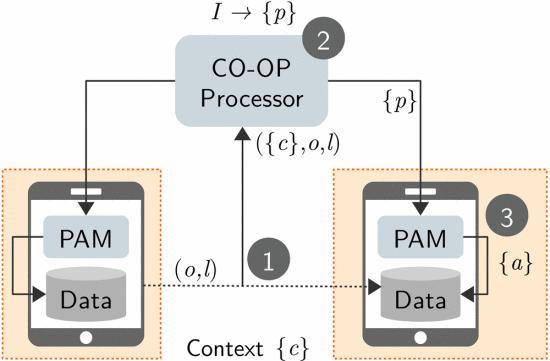
Una vez que se definen las políticas, solo un subconjunto de ellas debe implementarse y almacenarse en dispositivos perimetrales relevantes, basándose en el supuesto de que no todas las políticas son aplicables en cada contexto.

### B. Niveles de privacidad

Para incorporar más granularidad en las políticas, sugerimos definir diferentes niveles de privacidad. Con respecto a nuestro escenario de ejemplo, dividimos los datos relacionados con la privacidad en (i) datos específicos del dominio, como datos de anamnesis, diagnósticos médicos, recetas farmacéuticas, etc., y (ii) datos personales como el nombre completo, la dirección y otros datos de dominio personal. Un ejemplo de una política de privacidad en el dominio de eHealth podría obligar a un dispositivo o sistema a decidir entre los niveles de visibilidad de los datos del paciente. Un nivel podría definir que todos los datos son visibles (por ejemplo, para uso personal), mientras que un médico o farmacéutico solo debe tener acceso a secciones de datos específicos, como recetas abiertas o diagnósticos médicos. Si un médico busca consulta, otro nivel podría indicar que toda la información personal es invisible y que solo los datos médicos son visibles. Al final, el nivel más restrictivo sería que todos los datos son invisibles para cualquiera, por ejemplo, estar encriptados para su transmisión. Nuestro modelo propuesto presupone que para cada nivel diferente se incorpora información contextual. Además, estos niveles deben definirse en un nivel más granular dependiendo de las dependencias del sistema dado, como restricciones de dominio específicas, políticas, legales o arquitectónicas, y operar en conjuntos de datos holísticos, secciones de datos o campos de datos únicos.

### C. Toma de decisiones conscientes del contexto

Para lograr un mayor grado de flexibilidad en la implementación de políticas de privacidad, proponemos un proceso de toma de decisiones consciente del contexto para adaptarse dinámicamente a las situaciones cambiantes del entorno en el borde. El contexto en la informática puede interpretarse de muchas maneras diferentes. En el enfoque de este artículo, usamos el término *contexto*como información ambiental reconocible por dispositivos de borde. Puede tratarse de información sobre la red y su topología, dispositivos conectados, información espacial, proximidad, ubicación u hora. Un sistema sensible al contexto puede interpretar los cambios en el entorno y reaccionar ante ellos de una manera predefinida. Una forma de decirle al sistema cómo reaccionar ante ciertos cambios de contexto es mediante la definición de políticas mencionadas anteriormente y mejorarlas con parámetros contextuales. Con respecto a la privacidad, tales sistemas conscientes del contexto son, por un lado, capaces de anticipar riesgos potenciales y proporcionar recomendaciones, por ejemplo, a un usuario, qué acciones tomar, y, por otro lado, automatizan ciertas adaptaciones en la gestión y el procesamiento de datos. Sin embargo, en escenarios del mundo real, tales sistemas no cuentan con información holística del entorno todo el tiempo, y a veces tienen que tomar decisiones basadas en datos incompletos. Esto debe tenerse en cuenta al implementar políticas de privacidad siguiendo una estrategia conservadora, es decir, deshabilitar controles u ocultar datos confidenciales en una interfaz de usuario, o una estrategia de toma de decisiones optimista como permitir el acceso de lectura en datos parcialmente ofuscados. Un enfoque más sofisticado podría ser la implementación de técnicas de aprendizaje automático, que infieren automáticamente decisiones futuras basadas en información histórica.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8805991/8818170/8818192/277200a001-fig-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8805991/8818170/8818192/277200a001-fig-1-source-large.gif)

**Figura 1.** Interacción de componentes del modelo y dispositivos de borde que operan en diferentes contextos.

**SECCION V.**

## **Aplicación de políticas conscientes del contexto en el borde**

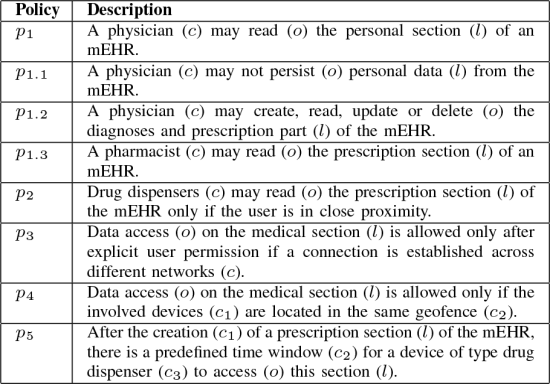
Al apegarnos a nuestro ejemplo motivador, ilustramos cómo se definen las políticas de privacidad conscientes del contexto y describimos los procesos de decisión correspondientes que habilitan / hacen cumplir aquellos que reciben un determinado contexto utilizando nuestro modelo. El modelo consta de tres partes encapsuladas esenciales que funcionan juntas de manera coherente pero que también pueden implementarse por separado (por ejemplo, utilizando estándares existentes) si es necesario. La primera parte describe el proceso de cómo definir políticas de privacidad sensibles al contexto para un determinado sistema y cómo describirlas utilizando nuestro modelo de privacidad. La segunda parte define un mecanismo de inferencia para obtener una o más políticas (dependiendo del grado de granularidad de las definiciones de políticas) y la tercera parte describe un mecanismo que determina las acciones resultantes después de que se identificaron una o más políticas.

Figure 1 illustrates the general principle of our model and how the distinct components work together in three basic steps. First, a device requests access to (private) data on another device. Context, Operation and Privacy Levels are transmitted to a Context Operations (CO-OP) Processor. Second, the CO-OP Processor returns inferred policies to the Policy Application Manager (PAM) implemented on each device. Third, the PAM triggers certain actions performed on corresponding data records to enforce the policies returned by the CO-OP Processor. Each of those elements will be discussed in detail in the following.

### A. Policy Definition

Policies should be defined at an early stage during the system design phase, and comprise fine-grained domains-specific parameters as it reduces ambiguity in implementation details. The structural elements of our model are i) privacy levels, ii) data management operations, and iii) context. The first thing to ascertain is the characteristic of either logical or physical types of different contexts in the system. A typical example for a logical form of context is the *role* of a user or device. A physical form of context could be the current *location* of a user or the proximity of a device to an edge node. We describe these types of contexts in more detail in Section V-C. Después de identificar diferentes tipos de contextos, sus manifestaciones deben asignarse a ciertas operaciones de gestión de datos (como las operaciones CRUD clásicas o las restricciones de persistencia) que respetan los niveles de privacidad predefinidos.

**Tabla I** Ejemplo de políticas de privacidad de datos de una aplicación de salud basada en parámetros de contexto específicos del dominio, operaciones de administración de datos y niveles de privacidad



La Tabla VA muestra políticas de privacidad ejemplares definidas en el contexto de nuestro escenario motivacional. Estas políticas se basan en casos de uso típicos en el dominio de eHealth. En las descripciones textuales de la política, destacamos los elementos estructurales definidos por nuestro modelo. Una política define uno o más contextos.C2, un nivel de privacidad ly una operación de datos o.

### B. Procesador CO-OP

Después de definir varias políticas de privacidad, un dispositivo periférico necesita saber si una determinada política debe aplicarse y cuándo. Esta tarea es implementada por un procesador de operación de contexto (procesador CO-OP) que infiere una o más políticas dados los parámetros de contexto específicos del dominio, niveles de privacidad y un conjunto de operaciones de datos. La función de inferencia correspondienteyo puede expresarse formalmente como:

yo: Cnorte× O × L → Pmetro(1)

Ver fuenteRight-click on figure for MathML and additional features.dónde C es el conjunto de parámetros de contexto específicos del dominio { c1, c 2, ... } y O es una operación específica (como CRUD o persistir), y Les el nivel de privacidad correspondiente en el que se debe operar. El resultado es una o más políticasp ∈ Peso necesita ser promulgado. El procesador CO-OP debe implementarse directamente en un dispositivo de borde.

### C. Gerente de aplicación de políticas

La determinación de una determinada política por parte del procesador CO-OP implica acciones específicas para que se ejecute un dispositivo. Policy Application Manager toma una o más de dichas políticasp ∈ P como argumento y devuelve una o más acciones a ∈ Aque deben tomarse para promulgar la política de privacidad. Esta funciónUNAF se puede definir formalmente como:

UNAF: Pnorte→ Ametro(2)

Ver fuenteRight-click on figure for MathML and additional features.dónde F es el conjunto de políticas determinado por yoy UNA es el conjunto de posibles acciones.

Las acciones devueltas incluyen operaciones básicas de creación, lectura, actualización o eliminación (CRUD) o tareas de persistencia, así como acciones más complejas como desencadenar otro proceso de decisión delegado en el procesador CO-OP o transferir, descifrar o computar datos adicionales. Formalmente descrita, una acción opera dentro del modelo de privacidad de una política dada que cumple con el cumplimiento de su propósito. El PAM debe implementarse por dispositivo o por nodos de borde, porque las acciones disparadas pueden diferir, por ejemplo, entre los tipos de dispositivos. La delegación de acciones a los dispositivos correspondientes también es realizada por el PAM. Los siguientes escenarios ilustran la aplicación práctica de nuestro modelo al cubrir varios ejemplos de manifestaciones de contexto, tareas de administración de datos, la inferencia resultante de las políticas de privacidad correspondientes y su aplicación práctica.

#### 1) Contexto basado en roles

Para realizar tareas específicas en un mEHR, se definen políticas que describen *quién* puede realizar estas tareas de administración de datos. Nuestra política predefinida P1.2 establece que *un médico* puede crear, actualizar o eliminar diagnósticos y partes de prescripción del mEHR y P1 que solo puede leer campos de datos personales. En un momento especial durante el proceso de consulta, un médico (por ejemplo, a través de su PC) quiere establecer una conexión con el teléfono inteligente del paciente para acceder al mEHR. Envía una solicitud al procesador CO-OP en el borde, proporcionando el contexto en forma de su *rol* , la operación, en nuestro caso *leído* , así como el nivel de privacidad *personal y la sección de diagnósticos*del mEHR. El procesador CO-OP devuelve los ID de política P1, P1.1 y P1.2 que luego serán procesados ​​por el Administrador de aplicaciones de políticas. Debido a P1.1, los datos personales no se conservarán en la PC del médico, por lo tanto, se tratarán como datos transitorios siempre que se establezca la conexión (si una política no establece lo contrario). Por otro lado, el mEHR del paciente registra una solicitud de conexión realizada por *un médico*y, por lo tanto, también solicita políticas del nodo de borde correspondiente. Luego aplica la política correspondiente que permite establecer la conexión y que el médico acceda a los datos de los pacientes. Por el contrario, si un farmacéutico quisiera hacer lo mismo, ninguna política definida le permitiría hacerlo (P1.3 solo permite el acceso de lectura en la sección de recetas). Esta estrategia RBAC es la base de nuestro modelo. Se han realizado exhaustivas investigaciones sobre este tema y, por lo tanto, podrían facilitar la implementación básica de nuestro modelo.

#### 2) Contexto relacionado con la proximidad

Siguiendo nuestro ejemplo motivador, asumimos que el médico le recetó al paciente un medicamento determinado. El paciente luego conecta su mEHR a un dispensador de drogas especial [19] . La aplicación mEHR del paciente reconoce el dispensador de medicamentos como un *tipo de dispositivo especial* e infiere una política correspondiente (P2) que permite que cualquier dispositivo de este tipo lea la parte de datos de prescripción del mEHR. Además, el dispositivo que ejecuta el mEHR debe estar muy cerca del dispensador de drogas. Si bien un dispositivo específico también podría modelarse como un rol, la proximidad debe ser *detectada* y procesada por un dispositivo de borde cercano. Si se cumplen ambas restricciones, el dispensador de medicamentos lee los campos de datos relacionados con la prescripción y entrega al paciente su medicamento.

#### 3) Contexto relacionado con la red

Otra política de privacidad (P3) define que las conexiones entrantes solo se manejan automáticamente si el dispositivo de conexión (por ejemplo, PC de médicos) se encuentra en la misma red que el dispositivo con la aplicación mEHR instalada. Mientras este sea el caso, las acciones resultantes se basan en decisiones tomadas por políticas definidas como se describió anteriormente. Sin embargo, si, por ejemplo, el paciente está en casa y un médico intenta acceder al mEHR desde la red del hospital, un nodo de borde reconoce que el mEHR no está conectado a su red y, por lo tanto, envía una notificación al usuario que indica que alguien o algo está tratando de acceder a su mEHR. Mediante un diálogo de permiso o un mecanismo de GUI similar, el paciente puede permitir o denegar la conexión entrante y el procesamiento de datos.

#### 4) Contexto basado en la ubicación

Determinar la ubicación física del dispositivo del paciente es una tarea común en la informática móvil y especialmente en los teléfonos inteligentes. Ciertas políticas podrían aplicarse en función de la ubicación actual del paciente. Como ejemplo, ampliamos nuestro caso de uso y nos referimos a la política P4, que impone la *presencia* (por ejemplo, al menos dentro del hospital) del paciente cerca de un dispositivo específico, similar al contexto basado en la proximidad. Esto podría realizarse definiendo las llamadas geofences, que describen un perímetro virtual basado en datos de GPS [20] . Esto podría volverse relevante, por ejemplo, para tareas de gestión como la asignación dinámica de camas realizada por el personal de enfermería, si los pacientes no tienen restricciones para permanecer en su habitación u hospital de forma permanente.

#### 5) Contexto basado en estado

El último ejemplo de toma de decisiones conscientes del contexto utiliza un *estado* inferido basado en acciones previas que se ejecutaron en los pacientes mEHR. Por ejemplo, es razonable que después de que el médico le recete al paciente un medicamento, el siguiente paso lógico para el paciente sería llegar al dispensador de medicamentos y recoger su medicamento recetado. Una de nuestras políticas predefinidas (P5) define que, después de que se modifica la parte de prescripción de un mEHR, hay una ventana de tiempo (por ejemplo, 72h) para que el teléfono inteligente del paciente establezca una conexión con un dispensador de medicamentos. Sin embargo, el procesamiento del contexto basado en el estado podría conducir a un sistema que incorpore muchas condiciones de excepción.

**SECCION VI.**

## **Conclusión y perspectivas**

El Internet de las cosas (IoT) con todos sus dispositivos de borde genera, procesa y almacena una gran cantidad de datos. Muchos de estos datos incluyen información sensible a la privacidad y pueden usarse para inferir patrones de comportamiento específicos del usuario o, en el peor de los casos, comprometer a un usuario. Los enfoques holísticos se enfrentan a desafíos arquitectónicos, conceptuales y relacionados con el rendimiento. Por lo tanto, proponemos un modelo que aproveche las técnicas informáticas de vanguardia donde el flujo de datos confidenciales se maneja más cerca del usuario, ya que garantizar la privacidad no es solo una cuestión de autenticación y autorización, sino una tarea más compleja que debe tener en cuenta el contexto ambiental en el que se manejan los datos. cuenta. Armados con una variedad de sensores potentes que se considera que reconocen la información ambiental relevante, estos nodos de borde eliminan la carga de trabajo de la centralizada tradicional, enfoques basados ​​en la nube al tiempo que ayuda a las tareas de localización de datos sensibles. Nuestro modelo puede ayudar a los arquitectos y desarrolladores a identificar estos contextos a los que se enfrenta un sistema. Al definir políticas en un punto temprano del diseño del sistema, las preocupaciones de privacidad se pueden mitigar o incluso erradicar. Los dispositivos de borde involucrados deben poder*sentido*cierto contexto y los desarrolladores deben implementar las funciones de inferencia correspondientes para hacer cumplir una determinada política. Por lo tanto, las políticas de privacidad deben estar vinculadas a varios contextos en forma de definiciones detalladas. Sugerimos que esto se puede lograr mediante el enriquecimiento de políticas basadas en características RBAC bien establecidas con información contextual. Por lo tanto, la aplicación de dichas políticas no se limita a ejecutarse solo después de solicitudes específicas de un dispositivo a un nodo de borde correspondiente. Los dispositivos de borde, conscientes del contexto, podrían anticipar riesgos potenciales de antemano y automatizar ciertas adaptaciones en la gestión y el procesamiento de datos. Parte de nuestro trabajo futuro será una mayor investigación en el campo de la aplicación de la privacidad sensible al contexto y las implementaciones prototípicas de técnicas de aplicación de políticas para diferentes tipos de dispositivos de borde.