Applications e-santé, le contrôle des données personnelles un enjeu majeur pour la protection de la vie privée

Catégorie : spécialisée

Youcef OULD YAHIA[1,2] et Pierre PARADINAS[1],

[1]Conservatoire National des Arts et Métiers, Paris, France
[2] École Polytechnique de Montréal, Canada

youcef.ouldyahia.auditeur@lecnam.net, pierre.paradinas@cnam.fr

Résumé. La protection des données de santé personnelles est devenue un enjeu majeur pour garantir le respect de la vie privée. Et par là, se prémunir de tout risque de monnayage des données, de ciblage ou de discriminations économiques et sociales. Ces risques sont accentués par la prolifération des systèmes d'e-santé intégrant les technologies de l'Internet des Objets et du Cloud. S'ajoute à cet environnement, le risque porté par le degré de confiance à accorder aux fournisseurs de services, en termes de capacité technique à assurer la sécurité des données mais également en termes de responsabilité morale, ceci, même dans un contexte législatif de plus en plus contraignant. L'un des moyens de réduire ces risques est centré sur des processus de protection et du contrôle d'accès aux données centré sur le propriétaire des informations. De nouvelles approches offrent des possibilités prometteuses dans ce sens, notamment le chiffrement par attribut et la « *blockchain* » néanmoins, nous verrons que ces approches font encore face à beaucoup de défis pour arriver à des solutions réalistes.

Mots clés : Vie privée, e-santé, chiffrement par attribut, blockchain, internet des objets, cloud computing, législation.

1 Introduction

De nos jours les systèmes d'information basés sur les nouvelles technologies d'information et de communication sont omniprésents dans notre quotidien, on parle de plus en plus d'informatique ubiquitaire. L'un des secteurs qui bénéficie de ces techniques est le secteur de la santé à travers des systèmes d'e-santé. Ces dernières années, nous assistons à l'émergence de technologies qui rendent le déploiement de tels systèmes de plus en plus facile, à travers notamment le développement du Cloud Computing (qui facilite l'intégration et le traitement d'un grand volume de données) et de l'Internet des Objets (qui facilite la collecte et la restitution des données). Ces technologies offrent la possibilité de déployer de nouvelles applications de santé avec la possibilité de suivre certains paramètres d'un patient (ECG, mouvements, taux de glycémie, etc.),

d'administrer automatiquement des traitements à travers des capteurs connectés, de faciliter la collecte, la gestion et l'exploitation des données médicales du patient par les professionnels de la santé, etc. Néanmoins, la prolifération de telles applications qui manipulent nos données de santé mettent en péril la préservation de notre vie privée. De plus, l'utilisation de l'Internet des Objets introduit des chalenges pour la mise en œuvre d'outils de sécurité et le Cloud pose le problème de confiance, car en délégant la gestion de nos données aux fournisseurs de services de Cloud nous perdons le contrôle sur ces données et nous devons, au final, nous fier à l'honnêteté et à la capacité d'assurer une protection adéquate de nos données par ces fournisseurs, dans un monde où les données de santé sont une ressource monnayable. Un événement récent illustre bien la vulnérabilité des utilisateurs envers les fournisseurs de services. Lors du passage de l'ouragan Irma aux États-Unis, la société Tesla a procédé au débridage, gratuitement et à distance, des capacités des batteries de ses véhicules pour permettre aux habitants d'évacuer les régions menacées. Ce geste « louable » en apparence nous porte à imaginer un scénario où une entreprise devient le décideur principal sur nos données de santé, soumis à son bon vouloir à un moment critique. Ceci nous impose la mise en place de solutions de protection adéquates en réponse aux menaces et risques encourus par la compromission de fournisseurs de service ou leur malhonnêteté éventuelle. Malheureusement, du point de vue de la protection des données et de la vie privée, nous constatons que beaucoup de solutions e-santé proposées dans la littérature, tendent à idéaliser certains composants et acteurs des systèmes au point de s'éloigner de la réalité du monde. À ce sujet, les auteurs dans [1] référencent plusieurs exemples d'applications et de projets de recherche sur l'e-santé où la sécurité présente des lacunes ou bien est laissée comme un élément à développer ultérieurement. Or avec le renforcement de la réglementation [2] et l'introduction du concept de la sécurité et de protection de la vie privée par construction. Une solution e-santé viable ne doit plus laisser comprter de telles lacunes. Nous allons dans la suite de cette communication présenter l'e-santé et la situer dans l'environnement de l'Internet des Objets et du Cloud Computing ainsi que le cadre législatif, nous aborderons les enjeux de la sécurité des données et de la préservation de la vie privée, ainsi qu'une analyse des solutions proposées dans la littérature, en mettant en exergue les défis du monde réel auxquelles elles sont confrontées. Enfin nous terminerons par l'introduction de deux concepts qui sont présentés comme des solutions prometteuses pour la protection des données privées qui sont « l'*Attribute Based Encryption* » et la « *blockchain* » en mettant l'accent sur les difficultés qui restent à surmonter, avant de terminer par une conclusion. Il convient de signaler que ce travail s'inscrit dans le cadre d'une thèse en cours au sein du laboratoire CEDRIC du Conservatoire National des Arts et Métiers en collaboration avec l'École Polytechnique de Montréal. Cette thèse porte sur le développement d'un modèle pour la protection des données et de la vie privée dans un système incluant des objets connectés et le Cloud, avec une implémentation pour le cas du suivi de patients à domicile. Le développement se poursuit avec une expérimentation du chiffrement par attributs sur une plateforme e-santé, construite autour d'une carte Arduino, une modélisation formelle des interactions entre les acteurs du système et une nouvelle approche d'évaluation du risque.

2 L'e-santé dans la sphère de l'Internet des Objets et du Cloud Computing

Dans cette partie, nous allons présenter les concepts d'e-santé, Cloud Computing et d'Internet des Objets et montrer comment le développement des deux derniers concepts sont en phase de révolutionner le premier. L'e-santé désigne en général l'introduction des technologies du numérique dans la pratique de la médecine au sens large, elle est en phase d'absorber les domaines tels que la télémédecine et les systèmes d'informations médicales traditionnels [3]. Nous pouvons définir l'e-santé comme le fait de mettre à disposition des professionnels de santé mais aussi du grand public des outils, à des coûts raisonnables, permettant de collecter, traiter, stocker, restituer et échanger des données de santé de façon automatisée, pratique et fiable. En d'autres termes, l'e-santé permet d'améliorer la qualité et l'efficacité des soins tout en réduisant les coûts. La particularité de l'e-santé est qu'elle n'est pas réservée exclusivement aux professionnels de la santé, contrairement à la télémédecine par exemple, mais également souhaitée par les patients ou les consommateurs [3]. Les systèmes d'e-santé intègrent dans leur dynamique l'acteur final qui est le patient. Ce dernier n'est plus considéré comme un sujet passif mais plutôt comme un acteur proactif au sein du système [4]. On peut alors parler de systèmes centrés autour de ses utilisateurs finaux [3]. Comme nous allons le voir par la suite, ceci nous amène naturellement à la problématique du contrôle exercé par le propriétaire des données sur ces dernières.

L'e-santé bénéficie largement des services offerts par le Cloud Computing en apportant une réponse viable aux challenges auxquels est confronté l'e-santé, notamment : (i) la croissance du volume de données, qui est accentuée par la prolifération de capteurs et équipements connectés; à ce titre, General Electric Healthcare estime qu'en moyenne, le monitoring d'un patient génère 1,5 GB de données par jour ; (ii) la multiplication des systèmes d'information de santé, dans un contexte qui exige des échanges de plus en plus importants entre structures et organismes de santé ; dans ce sens, les auteurs de [5] soulignent les bénéfices que nous pouvons tirer d'une infrastructure basée sur le Cloud ; (iii) l'utilisation de plus en plus répandue de terminaux mobiles (Smartphones, tablettes, etc.), qui bénéficient du paradigme Mobile Cloud Computing, qui consiste à étendre les capacités limitées, du mobile en délégant l'exécution d'applications lourdes dans le Cloud [6].

S'agissant de l'Internet des Objets, il est admis que Kevin Ashton est le premier à avoir utilisé ce terme en 1999. Selon l'International Data Corporation (IDC), l'Internet des Objets est un réseau de réseaux de terminaux identifiables (ou Objets) qui communiquent sans intervention humaine via la connectivité IP. Les objets connectés couvrent une large gamme d'équipements allant du capteur, peu coûteux, accomplissant une tâche spécifique (mono-tâche) aux smartphones embarquant divers capteurs (GPS, accéléromètre, etc.) et sur lesquels nous pouvons installer des applications variées. Les principales caractéristiques des objets connectés sont leur limitation en matières d'énergie, de capacités de calcul et de mémoire, leur mobilité (pour certains objets), leur capacité de communiquer entre eux et avec Internet.

Pour illustrer l'apport de l'Internet des Objets et du Cloud Computing dans le domaine de l'e-santé, nous pouvons citer : (i) les systèmes de surveillance de l'état de santé des individus (fréquence cardiaque, pression artérielle, mouvements, etc.) dans

l'environnement direct du patient avec des capteurs connectés à Internet ou au mobile via des liaisons de courte portée (Wifi, Bluetooth, ZigBee, 6LoWPAN, etc.), s'affranchissant ainsi de multiples visites aux structures de santé pour effectuer ces mesures ; (ii) les applications grand public pour la surveillance d'indicateurs de santé et inciter ainsi les individus à une certaine hygiène de vie avec la possibilité de suivre et d'analyser notre comportement quotidien (effort physique, alimentation, sommeil, rythme cardiaque, etc.). Plusieurs auteurs proposent une architecture e-santé basée sur l'Internet des Objets et le Mobile Cloud Computing (MCC), qui sont deux technologies convergentes [6]. Une vue générale de cette architecture est donnée par la figure 1, elle est constituée de capteurs connectés, via une liaison sans fil de courte portée (Wi-fi, Bluetooth, NFC, ZigBee, etc.), à un équipement mobile (Smartphone, tablette, etc.) ou station de base, qui joue le rôle d'intermédiaire entre le réseau local et le réseau Internet, et delà aux services du Cloud. Ce type d'architecture permet d'envisager diverses applications eHealth. Doukas et al. [7] ont démonté la facilité de mise en œuvre d'une telle architecture et propose un prototype d'implémentation d'un système e-santé basé sur le Cloud Computing avec le service « Amazon S3 Cloud Storage » et un client mobile sous un OS Android. Dans [8], une architecture similaire est proposée pour la surveillance des personnes prédisposées aux accidents cardiaux-vasculaires avec des capteurs de mouvements et d'accélération, une application sur Smartphone et un service sur le Cloud pour le traitement des données et le stockage. Pour la recherche dans le domaine de la santé publique, les auteurs de [9] proposent une plateforme avec la même architecture pour l'acquisition de données épidémiologiques.

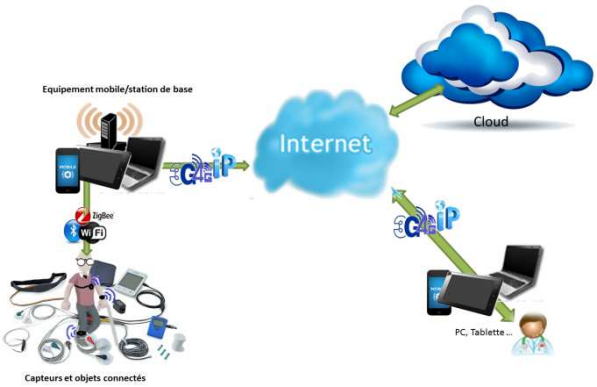

Fig. 1. Architecture e-santé IoT - cloud Computing

La conception d'une plateforme d'e-santé comme son déploiement dans le monde réel doit impérativement prendre en compte tous les aspects sécurité. En effet, au regard des services offerts par l'e-santé, toutes menaces sur ces systèmes (en termes de disponibilité, confidentialité, intégrité des données, respect de la vie privée) peuvent avoir des conséquences éthiques, économiques et juridiques et même vitales, en induisant par exemple une décision thérapeutique fausse. Au final, la multiplication

des incidents va engendrer une désaffection des différents acteurs envers ces systèmes.

Dans la suite, pour illustrer nos propos, nous prenons le monitoring à domicile comme scénario d'utilisation. Le choix de cet exemple est motivé par le fait d'intégrer tous les éléments sensibles sur la question de la protection des données personnelles de santé. À savoir, dans l'Internet des Objets, le Cloud Computing où un environnement légal est de plus en plus strict et au sein duquel les opérateurs économiques (ou des entités mal vaillantes) pourraient essayer de tirer profit de données personnelles de santé.

3 Environnement légal

Les applications de surveillance à domicile gèrent des données de santé personnelles, de ce fait, elles doivent se conformer à des réglementations dans de nombreux pays. En Europe, un nouveau règlement sur la protection des personnes physiques en ce qui concerne le traitement des données personnelles a été adopté le 27 avril 2016 et entrera en vigueur le 25 mai 2018 [2], date d'abrogation de la directive 95/46/CE. Cette directive apporte une plus grande harmonisation au niveau européen. Sa caractéristique la plus notable porte sur une nouvelle vision qui n'est pas limitée à la seule sécurisation des données en mettant le propriétaire de ces données au centre de la règlementation. Ces textes définissent clairement les droits et responsabilités des entités en charge des traitements des données. De plus, ce règlement est plus adapté aux exigences technologiques actuelles. En effet, concernant le domaine de la santé, il précise que les données de santé personnelles sont considérées indépendamment de la source, par exemple à partir d'un dispositif médical [2]. Également, pour ce règlement, les données concernant la santé signifient « les données personnelles, y compris la fourniture de services de santé, qui révèlent des informations sur son état de santé… ». Pour notre cas d'étude, l'identité et les attributs d'un professionnel de santé, qui accède aux données, peuvent être utilisés pour déduire des informations sur l'état de santé du propriétaire des données. En outre, ce règlement impose le concept de sécurité par conception, ce qui signifie que les exigences de sécurité doivent être prises en compte lors du processus de conception de la solution. Aux États-Unis, les données personnelles sur la santé sont régies par la loi sur la santé et l'assurance maladie « *Health Insurance Portability and Accountability Act* » (HIPPA) [10]. HIPPA donne des règles de sécurité à tout fournisseur de soins de santé qui traite des informations sur la santé sous format électronique. Par exemple, pour stocker les données de santé personnelles dans le Cloud, ce dernier doit être conforme aux prescriptions du HIPPA. En effet, selon les règles définies par HIPAA, une entité (fournisseurs de soins, de service de santé, etc.) est responsable de la sécurité des données des patients, cela implique qu'une application ou un service qui collecte, traite et stocke les données du patient doit assurer la confidentialité et l'intégrité des données et imposer des restrictions d'accès. À ce titre, pour les services Microsoft Azure, il n'y a pas de certification reconnue pour la conformité à la loi HIPAA, néanmoins Microsoft a publié des recommandations pour le développement et le déploiement d'applications sur sa plateforme pour qu'elle soit conformes à HIPAA [11]. Toutefois, le fournisseur de services de santé reste responsable de son environnement une fois que les services ont

été provisionnés, et le client doit signer un agrément d'association avec la société Microsoft, appelé « *Business Associate Agreement* » (BAA). La même démarche est aussi suivie par Google [12].

Mais comme il a été souligné par [13], les lois sur la protection de la vie privée sont inefficientes s'il n'y a pas de moyens et/ou des mécanismes pour faire appliquer les restrictions au sein des entités qui manipulent des données personnelles. Ceci nous renvoie à la nécessité de prendre en charge la protection de la vie privée avec des solutions techniques adéquates, indépendamment du fournisseur de services et dans certains cas, d'aller au-delà des exigences légales, si ces dernières n'assurent pas une parfaite protection de la vie privée. En effet, une loi, comme la HIPAA, peut exiger des mécanismes de sécurité des données (confidentialité, contrôle d'accès, disponibilité, etc.) alors que des informations sur l'état de santé de l'individu peuvent être obtenues à partir de méta données, sans compromettre la sécurité des données elles-mêmes. Ce genre de fuites d'information doit être interdit [14] car elles constituent une menace pour la vie privée. Ces fuites d'information concernent également la protection des professionnels de santé contre le profilage à des fins commerciales. C'est dans ce sens que l'article L. 4113-7 du code de la santé publique français [15] interdit de constituer des fichiers, à des fins commerciales, composés à partir de données de prescriptions médicales ou personnelles dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur.

4 Sécurité des données personnelles de santé et préservation de la vie privée

Le contrôle des données personnelles de santé est un enjeu majeur. En effet, ces données peuvent entraîner la convoitise d'acteurs malveillants dans le but de générer des profits ou de nuire aux personnes. Une autre menace peut provenir des fournisseurs de services, qui peuvent tirer parti de l'ambiguïté ou du manque de réglementation pour exploiter les données personnelles de santé. De nombreuses entreprises ont des intérêts commerciaux importants dans la collecte de données privées sur la santé [16]. Il existe également un certain risque de confier ses données personnelles aux fournisseurs de services qui ne sont pas complètement exempts d'incidents de sécurité et/ou de fuites d'informations [17]. La perte des propriétés de sécurité (confidentialité, disponibilité, intégrité, non répudiation) risque d'avoir des répercussions néfastes sur le patient et sur les professionnels de santé tant sur le plan médical, légal, éthique ou financier ; à titre non exhaustif :

- fausser la décision du médecin et causer ainsi des erreurs médicales avec de graves conséquences ;
- incapacité d'utiliser ultérieurement les données comme preuve si nous ne pouvons pas garantir l'intégrité et la non répudiation des données ;
- compromettre la vie privée du patient et causer des préjudices moraux et financiers ;
- perte de confiance dans le système d'informations médical d'où une désaffection des utilisateurs envers ces systèmes et une réticence à fournir des informations ;

- faire immerger une discrimination basée sur le profil médical, dans la mesure où des sociétés peuvent conditionner le recrutement ou valoriser leurs services en fonction de l'état de santé de la personne.

Aussi, à la lumière des menaces qui pèsent sur les données de santé personnelles, toute proposition pour la protection de la vie privée doit prévoir un contrôle renforcé du propriétaire des données sur le processus de chiffrement et de contrôle d'accès à ses données [18]. Également, il est important d'éviter la fuite d'informations personnelles qui est induite par certaines métadonnées non protégées et disponibles pour un attaquant [8].

5 Analyse des solutions proposées dans la littérature

L'Internet des Objet et le Cloud sont des environnements hétérogènes, qui rendent difficilement réalisable le développement de solutions, de bout en bout, pour sécuriser les données et protéger la vie privée tout en assurant les fonctionnalités de collecte, stockage, traitement et partage des données. En effet, dans le Cloud, les ressources sont relativement illimitées néanmoins nous sommes souvent confrontés à un niveau de confiance limité, car le Cloud est généralement géré par un tiers [17]. Par contre du côté de l'IoT nous avons un niveau de confiance relatif, qui peut être maîtrisable notamment en ayant un contrôle physique sur les équipements. Cependant, le manque de ressources, qui caractérise les objets connectés, limite le déploiement des solutions de sécurité traditionnelles. L'analyse des solutions proposées dans la littérature montre qu'elles sont confrontées à ce problème. Par exemple, les auteurs de [17] et [19] donnent une solution intéressante pour le contrôle d'accès dans l'environnement Cloud, mais elle ne prend pas en charge les contraintes de l'Internet des Objets. Par contre, les auteurs [20] et [21] proposent de sécuriser les données et de protéger la vie privée dans l'environnement IoT sans pour autant proposer de solutions pour le partage des données et le contrôle d'accès dans le Cloud. Ces exemples sont une bonne illustration de la difficulté engendrée par l'environnement IoT-Cloud pour développer une solution de sécurité générale et viable. Dans ce contexte, l'adaptation de solutions existantes avec un minimum d'innovation, à des cas d'utilisation précis, est plus rentable que de chercher à concevoir une solution innovante de bout en bout, en imposant des hypothèses fortes sur l'environnement au risque de s'éloigner du monde réel. C'est dans ce contexte que les auteurs de [22] proposent une construction dans l'environnement IoT-Cloud qui peut être implémentée pour le contexte de la santé. Dans cette proposition, la sécurité de la transmission desDatagram Transport Layer Security (DTLS), néanmoins pour la sécurité du stockage des données et le contrôle d'accès, il est nécessaire d'avoir un Cloud privé totalement sécurisé. Le même type de solutions est proposé par OBJOBJOBJOBJ.

Nous remarquons des solutions précédentes que le problème du contrôle d'accès se pose au niveau du cloud qui doit être de confiance, d'autres solutions se proposent de résoudre ce problème. L'approche proposée dans [19] est basée sur Attribute Based Encryption (ABE) pour contrôler l'accès aux données de santé hébergées dans le Cloud. Cette solution a la particularité de renforcer la protection de la vie privée en réduisant les privilèges de l'hébergeur des données. Ce type de contrôle d'accès est

centré sur le patient, contrairement aux approches traditionnelles. Cependant, la solution proposée n'élimine pas complètement l'autorité de confiance pour la gestion du contrôle d'accès et ne prend pas en charge les ressources limitées des objets connectés. En effet, l'implémentation d'ABE, en l'état actuel, nécessite de disposer d'importante ressources [25]. La solution à ce problème est d'externaliser les calculs lourds, tels que proposés par de nombreux auteurs comme [26], [27]. Mais toutes les propositions basées sur ce principe introduisent un tiers de confiance et nécessitent une connexion Internet lors de l'utilisation du Cloud pour externaliser les calculs avec des mécanismes complexes de gestion de session.

En résumé, les approches proposées dans la littérature pour assurer la confidentialité des données de santé dans un environnement IoT-Cloud sont confrontées à la difficulté d'une forte protection de la vie privée dans l'écosystème Cloud et à surmonter le manque de ressources du paradigme Internet des Objets. Malheureusement, une solution réaliste doit fournir une réponse viable qui prend en compte ces deux contraintes. En outre, toutes les solutions proposées se concentrent sur la protection des données ou leur partage, alors qu'il n'y a pas d'efforts significatifs pour interdire aux fournisseurs de services de collecter des informations privées qui peuvent être déduites de la mise en œuvre du système.

Dans la suite du document nous présentons deux concepts innovants pour assurer la protection de la vie privée en fournissant des mécanismes de partage de données centrés sur leur propriétaire mais qui font face en l'état actuel à certaines difficultés qui restent à surmonter et que nous étudions dans le cadre de nos travaux.

6 Le Chiffrement par attributs (*Attribute Based Encryption*)

Traditionnellement, un schéma de chiffrement comme RSA et AES fournit une transmission et un stockage de données sécurisées dans un environnement Cloud mais l'inconvénient de ces schémas est la difficulté de mettre en place un contrôle d'accès avec une granularité fine pour le partage des données, en particulier dans le cas où nous ne connaissons pas l'identité des utilisateurs au préalable. Se pose également le problème des mécanismes de révocation. Une solution à ces problèmes est donnée par le chiffrement par attributs ou « *Attribute Based Encryption* » (ABE) [28], qui incorpore un processus de génération des clés de chiffrement et de déchiffrement et la notion de politique d'accès basée sur des attributs, offrant des fonctionnalités de chiffrement et de contrôle d'accès [29]. Le chiffrement par attributs (ABE) est un schéma de chiffrement à clé publique du type *un-à-plusieurs*, c'est-à-dire qu'on chiffre avec une seule clé et on a la possibilité de générer de plusieurs clés pour déchiffrer. Un avantage évident de cette technique est que chaque utilisateur à une clé dédiée, en cas de révocation d'une clé, il n'est pas nécessaire de refaire le chiffrement des données. Les données peuvent être chiffrées à la source et entreposées tel quel, et à aucun moment le fournisseur de service n'accède au clair même que ce soit pour le processus de partage ou de révocation de droit. L'idée initiale a été énoncée par les auteurs de [30]. En plus de sécuriser la transmission et le stockage des données, ABE fournit un contrôle d'accès à forte granularité, une gestion des clés évolutives et une distribution de données flexible [29], [31], [19], [32]. Il permet de chiffrer les données et d'assurer le

partage sur la base d'attributs descriptifs, sans aucune connaissance préalable de l'identité des destinataires.

Dans ABE, les données sont chiffrées et déchiffrées en fonction d'attributs et de politique d'accès. Seules les entités avec des attributs qui satisfont une politique d'accès aux données peuvent déchiffrer un texte. Les deux principales variantes sont « *Ciphertext-Policy Attribute Based Encryption* » (CP-ABE) proposée pour la première fois par les auteurs de [33], dans CP-ABE, la politique d'accès est intégrée dans le texte chiffré et les clés secrètes sont générées avec un ensemble d'attributs décrivant l'utilisateur légitime qui pourra déchiffrer ce texte. Seule la clé secrète avec un ensemble d'attributs qui satisfait la politique d'accès précédente peut récupérer le texte clair. La deuxième variante est « *Key-Policy Attribute Based Encryption* » (KP-ABE) [34]. Pour KP-ABE, la politique d'accès est intégrée dans la clé secrète, en d'autres termes, on décide pour chaque utilisateur quels sont les objets auxquels il aura accès. On attache à chaque texte chiffré un ensemble d'attributs. Une clé secrète donnée, avec une politique d'accès donnée, ne peut déchiffrer que le texte chiffré ayant les attributs qui satisfont sa politique d'accès. Comme mentionné dans [32], un système basé sur ABE permet en théorie de fournir globalement les fonctionnalités suivantes : (i) la confidentialité des données, (ii) un contrôle d'accès avec une fine granularité, (iii) le passage à l'échelle, (iv) la révocation d'utilisateurs et (v) la résistance à la collusion entre utilisateurs.

Concernant les cas d'utilisation typiques, CP-ABE peut être est implémenté pour permettre au propriétaire des données de définir la politique d'accès pour ses données, sans avoir à spécifier explicitement l'identité des utilisateurs au préalable. Alors que KP-ABE est utilisé par exemple pour partager les informations du journal d'audit. La figure 2 illustre un exemple de partage de données avec la variante KP-ABE. Chaque enregistrement de données peut être lié à un attribut et une clé de déchiffrement sera liée quant à elle à une politique d'accès P_i qui, pour chaque utilisateur, détermine quels enregistrements peuvent être déchiffrés. Une revue d'applications possibles pour ABE est donnée par [35].

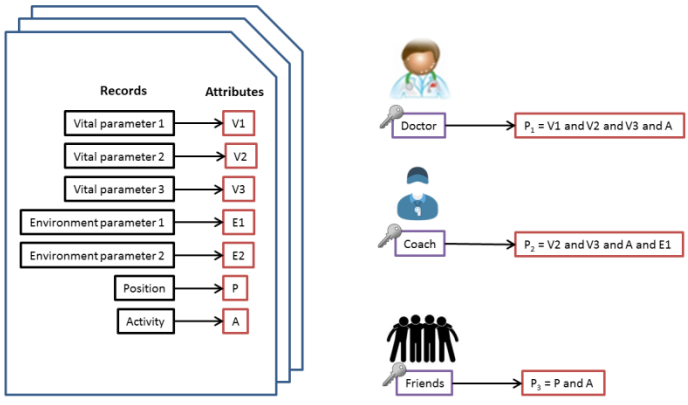

Fig. 2. Partage de données avec KP-ABE

Le système ABE est constitué de quatre algorithmes, donnés ci-après. Pour KP-ABE et CP-ABE, les algorithmes *KeyGen, Encryption, Decryption* sont légèrement différents vu que la politique d'accès est liée à la clé secrète de déchiffrement et les attributs au chiffré dans le cas de KP-ABE et réciproquement pour CP-ABE :

Setup: *Entrée* : un paramètre de sécurité l.
Sortie: une clé publique de chiffrement Pk et une clé secrète principale MSk qui servira à générer les clés secrètes de déchiffrement.

Encryption : *Entrée* : message m, la clé publique Pk et un ensemble d'attributs a_i dans le cas de KP-ABE ou une politique d'accès P dans le cas de CP-ABE.
Sortie : le chiffré « c ».

KeyGen: *Entrée* : la clé secrète principale MSk et un ensemble d'attributs a_i dans le cas de CP-ABE ou une politique d'accès P dans le cas de KP-ABE.
Sortie : une clé de déchiffrement Sk. Liée à un ensemble d'attributs a_i dans le cas de CP-ABE ou à une politique d'accès P dans le cas de KP-ABE.

Decryption : *Entrée* : le chiffré « c » et une clé de déchiffrement Sk.
Sortie : si l'ensemble d'attributs a_i satisfont la politique P alors sortie m sinon $\perp$.

Un aspect de la sécurité du schéma ABE est la résistance aux collusions [33]. En effet, une bonne construction d'ABE ne doit pas permettre à deux utilisateurs de combiner leurs clés privées pour déchiffrer une donnée pour laquelle ils n'ont pas d'accès individuel, en d'autres termes, deux utilisateurs ne doivent pas pouvoir combiner leurs attributs pour pouvoir avoir des droits d'accès supérieurs à ceux qu'ils ont individuellement.

Les fonctionnalités d'ABE semblent être intéressantes pour une solution assurant la protection de la vie privée [25], notamment en implémentant un système de sécurité centré sur le propriétaire des données [17] [19] où même dans le Cloud, le fournisseur de services, ne pourra avoir accès aux données en clair car le chiffrement des données se fait par et sous le contrôle du propriétaire des données tout en assurant le partage de ces dernières. Aussi, le chiffrement par attribut commence à être assez mature pour être incorporé comme module fonctionnel d'une solution de sécurité [29]. Cependant, ABE est une méthode de chiffrement coûteuse en termes de capacité de calcul, si elle ne pose pas de problèmes particuliers pour une utilisation dans le Cloud, ceci n'est pas le cas pour une implémentation sur les dispositifs ayant des contraintes de ressources [36]. Cet état de fait illustre parfaitement la problématique de la protection des données personnelles de santé et de la préservation de la vie privée dans un environnement Internet des Objets et Cloud. Néanmoins, l'approche ABE fait l'objet d'actifs travaux de recherche, les principaux axes de développement sont l'externalisation des calculs lourds ou l'optimisation de ces derniers pour une implémentation dans des dispositifs à ressources réduites.

7 La blockchain

Une nouvelle approche prometteuse pour le contrôle d'accès est basée sur la blockchain. Motivé par l'intérêt récent de la communauté scientifique d'utiliser la blockchain pour améliorer la vie privée, nous examinerons si ce paradigme peut être utile

dans le domaine de la santé déployé dans l'environnement de l'IoT et du Cloud Computing. La technologie de la blockchain nous promet de se passer des tiers de confiance pour interagir de manière sécurisée dans un réseau pair à pair. La première description d'une blockchain se trouve dans un article écrit sous le pseudonyme de Satoshi Nakamoto [37], qui a donné naissance à la monnaie cryptographique Bitcoin. La blockchain est une sorte de registre publique infalsifiable et indestructible, disponible dans un réseau pair à pair où chaque nœud peut s'ériger en une sorte de garant des informations enregistrées dans la blockchain, en effectuant un travail particulier et rémunéré. Ces nœuds sont appelés *mineurs*. Dans la blockchain Bitcoin, chaque compte est caractérisé par une paire de clés publique/privée et identifié par une adresse dérivée de sa clé publique. Pour comprendre le fonctionnement de la blockchain, nous allons prendre l'exemple d'Alice qui veut transférer un montant de x Bitcoin à partir de l'un de ses comptes vers un compte appartenant à Bob. Alice va générer une transaction, qu'elle va signer avec la clé privé de son compte et qui contient comme information : les adresses des comptes source et destination, le montant du transfert et une référence à une ou plusieurs transactions précédentes qui ont servi à créditer le compte d'Alice (on n'a pas le droit au découvert). Cette transaction est partagée sur le réseau pair à pair où elle est récupérée par les nœuds qui jouent le rôle de mineur. Ces derniers rassemblent plusieurs transactions pour constituer un bloc qu'ils valident mathématiquement avant de le chainer à la blockchain à travers un processus de consensus spécifique entre les mineurs. Dans le cas de Bitcoin, ce processus est appelé preuve de travail. Une fois la transaction enregistrée dans la blockchain, elle devient publique, infalsifiable, irrévocable et indestructible et ceci est garanti par la communauté du réseau et non par une autorité centrale de confiance. Voir [38], [39] pour une compréhension plus approfondie des principes de la blockchain, également le livre [40] offre une bonne lecture pour les possibilités offertes par la blockchain. Une évolution de la blockchain est constituée par les contrats intelligents « *smart contract* », qui sont des applications autonomes programmées pour l'exécution d'actions, si des conditions, convenues par les parties impliquées dans la transaction, sont satisfaites. Ces contrats sont enregistrés sous forme de script dans une blockchain [39]. Ethereum, qui utilise l'Ether comme une crypto-monnaie, est une plate-forme prometteuse pour le développement de telles applications [41].

La résilience de la blockchain, son intégrité et l'absence d'autorité centrale de confiance ont inspiré plusieurs travaux dans le domaine de la confidentialité et le contrôle d'accès [42], [43] notamment dans l'environnement IoT et Cloud [44] [45]. Les auteurs de [42] proposent une solution qui gère le contrôle d'accès aux données de santé personnelles stockées dans différentes bases de données à travers des contrats intelligents embarqués dans une blockchain. Quant à [44], les auteurs proposent une solution, basée sur la blockchain, qui permet de gérer, par leur propriétaire, l'accès aux données produites par les objets connectés. Le schéma général des solutions proposées est l'utilisation de blockchain pour la gestion du contrôle d'accès, alors que les données elles-mêmes sont manipulées en hors-chaîne. Ceci est une évidence vue que l'un des principes de la blockchain est que chaque nœud du réseau peut avoir localement une copie de la blockchain. En résumé, la blockchain est utilisée comme une sorte de base de données distribuée, persistante et infalsifiable pour le contrôle d'accès. Aussi, l'un des avantages de l'utilisation de la blockchain est de fournir un outil

élégant pour la révocation du droit d'accès, le tout en s'affranchissant d'une autorité centrale de confiance.

Ceci étant, dans le monde réel, une attention particulière doit être accordée à certains aspects de déploiement des blockchains. D'abord le passage à l'échelle, par exemple dans [44] il est fait état d'une solution qui s'adapte à de grandes échelles en termes de nombre d'objet connectés, mais comme le souligne [46] l'une des faiblesses actuelles de la blockchain est le nombre de transactions possibles par unité de temps, qui est estimé à 7 transactions par seconde. Un autre aspect à prendre en compte est la préservation de la vie privée en évitant les fuites d'informations à travers la blockchain. En effet, étant par essence un registre publique, les transactions doivent être construites de façon à rendre impossible la déduction d'informations sur l'état de santé de l'individu à travers l'observation de l'utilisation qui est faite des données. Se pose également le problème de l'anonymat dans les blockchains, car même si en principe les utilisateurs ont la possibilité de se cacher derrière autant d'adresses blockchain qu'ils peuvent générer de clés, des méthodes existent pour mettre à mal cet anonymat [46], [47]. Un autre défi dans le cadre de ce type d'applications est de trouver un modèle de rétribution des nœuds travaillant sur la validation de la blockchain (les mineurs), qui est une condition nécessaire si on veut se passer d'un tiers de confiance à moins d'avoir une blockchain privée avec un serveur de confiance pour effectuer le travail des mineurs, mais avec cette approche on s'éloigne de l'esprit de la blockchain. L'un des rares travaux qui proposent une solution de protection de la vie privée dans l'écosystème de la santé, à l'aide de blockchain tout en décrivant un modèle de rétribution des mineurs est donnée par [42]. Les auteurs proposent aux nœuds désirant participer au réseau en tant que mineur deux modèles incitatifs, un pour le fournisseur de prestations de santé et le second pour les chercheurs et les autorités de santé, tous deux sont basés sur Ether (la devise pour Ethereum).

Nous avons vu que le concept blockchain implique plusieurs choix à faire : la nature de la blockchain (publique ou privée), les mécanismes utilisés pour le consensus, l'incitation des mineurs, etc. Ces choix dépendent fortement de l'utilisation qui sera faite des blockchains et de la fonctionnalité attendue. Pour le cas de la surveillance à domicile, la blockchain peut être utilisée pour renforcer la préservation de la vie privée en supprimant les tiers de confiance tout en créant un système de contrôle d'accès aux données centré sur l'utilisateur. Mais nous devons prendre en compte les considérations du déploiement et au besoin de masquer certaines informations, comme les identités et les services fournis. La blockchain est un concept relativement nouveau, on commence juste à entrevoir les possibilités offertes notamment pour la sécurisation du partage des données personnelles. Cependant, concernant la préservation de la vie privée au sens large et sans avoir recours à des autorités de confiance, la mise en place d'une blockchain doit être accompagnée de mesures visant à protéger également l'activité des utilisateurs sur cette blockchain.

8 Conclusion.

Dans ce document nous avons montré que le problème de la protection des données personnelles et la préservation de la vie privée dans le domaine de l'e-santé ne se résument pas à proposer des solutions aux traditionnelles exigences de sécurité (confi-

dentialité, intégrité, etc.) et aux problèmes de contrôle d'accès aux données. En effet, en sus de la conformité à la réglementation en vigueur, le processus de développement d'un système assurant la protection de la vie privée doit fournir un contrôle effectif sur les données par leur propriétaire. Par ailleurs, il doit prendre en considération les contraintes de l'environnement de déploiement, notamment en termes de degré de confiance à accorder aux fournisseurs de services. Il doit également faire la distinction entre données personnelles et informations personnelles. Ces dernières peuvent être déduites en observant le fonctionnement correct du système sans avoir à violer les exigences de sécurité des données personnelles. Enfin, de nouvelles techniques prometteuses comme le chiffrement par attribut permettent de construire des solutions de protection de la vie privée, centrées autour du propriétaire de la donnée. Néanmoins, la consommation de ressources reste un défi pour son déploiement. Même si l'externalisation vers des dispositifs particuliers des fonctionnalités lourdes en terme calcul pour le chiffrement par attribut est une solution viable, il restera le problème de l'évaluation dynamique de la confiance à accorder à ces dispositifs. Ce dernier point fait aussi l'objet de développement dans le cadre des travaux de thèse avec une nouvelle approche d'évaluation des risques.

Références bibliographiques

1. P. Gope and T. Hwang, ‘BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network’, *IEEE Sens. J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.
2. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016.
3. V. D. Mea, ‘What is e-Health (2): The death of telemedicine?’, *J. Med. Internet Res.*, vol. 3, no. 2, p. e22, 2001.
4. D. Gachet, M. de Buenaga, F. Aparicio, and V. Padrón, ‘Integrating Internet of Things and cloud Computing for Health Services Provisioning: The Virtual cloud Carer Project’, in *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2012, pp. 918–921.
5. R. Zhang and L. Liu, ‘Security Models and Requirements for Healthcare Application clouds’, in *2010 IEEE 3rd International Conference on cloud Computing*, 2010, pp. 268–275.
6. S. Bouzefrane and L. V. Thinh, ‘Trusted Platforms to Secure Mobile cloud Computing’, in *2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC,CSS,ICESS)*, 2014, pp. 1068–1075.
7. C. Doukas, T. Pliakas, and I. Maglogiannis, ‘Mobile healthcare information management utilizing cloud Computing and Android OS’, *Conf. Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. IEEE Eng. Med. Biol. Soc. Annu. Conf.*, vol. 2010, pp. 1037–1040, 2010.
8. M. S. Karunarathne, S. A. Jones, S. W. Ekanayake, and P. N. Pathirana, ‘Remote Monitoring System Enabling cloud Technology upon Smart Phones and Inertial Sensors for Human Kinematics’, in *2014 IEEE Fourth International Conference on Big Data and cloud Computing (Bdcloud)*, 2014, pp. 137–142.

9. K. K. F. Tsoi, Y. H. Kuo, and H. M. Meng, ‘A Data Capturing Platform in the cloud for Behavioral Analysis among Smokers: An Application Platform for Public Health Research’, in *2015 IEEE International Congress on Big Data*, 2015, pp. 737–740.
10. O. for C. R. (OCR), ‘Summary of the HIPAA Privacy Rule’, *HHS.gov*, 07-May-2008, http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
11. ‘Microsoft Trust Center | HIPAA and the HITECH Act’, https://www.microsoft.com/en-us/trustcenter/Compliance/HIPAA.
12. ‘HIPAA Compliance with G Suite - G Suite Administrator Help’, https://support.google.com/a/answer/3407054?hl=en.
13. E. B. Fernandez, ‘Security in Data Intensive Computing Systems’, in *Handbook of Data Intensive Computing*, B. Furht and A. Escalante, Eds. Springer New York, 2011, pp. 447–466.
14. A. L. Ferrara, G. Fachsbauer, B. Liu, and B. Warinschi, ‘Policy Privacy in Cryptographic Access Control’, in *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*, 2015, pp. 46–60.
15. *Code de la santé publique - Article L4113-7*, vol. L4113-7. .
16. H. Lin, J. Shao, C. Zhang, and Y. Fang, ‘CAM: cloud-Assisted Privacy Preserving Mobile Health Monitoring’, *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 6, pp. 985–997, Jun. 2013.
17. H. S. G. Pussewalage and V. Oleshchuk, ‘A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using cloud Computing’, in *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, 2016, pp. 46–53.
18. W. T. Tang, C. M. Hu, and C. Y. Hsu, ‘A mobile phone based homecare management system on the cloud’, in *2010 3rd International Conference on Biomedical Engineering and Informatics*, 2010, vol. 6, pp. 2442–2445.
19. M. Li, S. Yu, K. Ren, and W. Lou, ‘Securing Personal Health Records in cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings’, in *Security and Privacy in Communication Networks*, S. Jajodia and J. Zhou, Eds. Springer Berlin Heidelberg, 2010, pp. 89–106.
20. T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, ‘A Medical Healthcare System for Privacy Protection Based on IoT’, in *2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, 2015, pp. 217–222.
21. H. Khemissa and D. Tandjaoui, ‘A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things’, in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015, pp. 90–95.
22. A. Sharma, T. Goyal, E. S. Pilli, A. P. Mazumdar, M. C. Govil, and R. C. Joshi, ‘A Secure Hybrid cloud Enabled architecture for Internet of Things’, in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 274–279.
23. J. H. Abawajy and M. M. Hassan, ‘Federated Internet of Things and cloud Computing Pervasive Patient Health Monitoring System’, *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 48–53, Jan. 2017.
24. M. R. Abdmeziem and D. Tandjaoui, ‘An End-to-end Secure Key Management Protocol for e-Health Applications’, *Comput Electr Eng*, vol. 44, no. C, pp. 184–197, mai 2015.
25. X. Wang, J. Zhang, E. M. Schooler, and M. Ion, ‘Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT’, in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 725–730.

26. J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, 'Securely Outsourcing Attribute-Based Encryption with Checkability', *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2201–2210, août 2014.
27. X. A. Wang, J. Ma, and F. Xhafa, 'Outsourcing Decryption of Attribute Based Encryption with Energy Efficiency', in *2015 10th International Conference on P2P, Parallel, Grid, cloud and Internet Computing (3PGCIC)*, 2015, pp. 444–448.
28. O. Kocabas, T. Soyata, and M. K. Aktas, 'Emerging Security Mechanisms for Medical Cyber Physical Systems', *IEEEACM Trans. Comput. Biol. Bioinforma. IEEE ACM*, vol. 13, no. 3, pp. 401–416, Jun. 2016.
29. N. Oualha and K. T. Nguyen, 'Lightweight Attribute-Based Encryption for the Internet of Things', in *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, 2016, pp. 1–6.
30. A. Sahai and B. Waters, 'Fuzzy Identity-Based Encryption', in *SpringerLink*, 2005, pp. 457–473.
31. S. R. Hemalatha and Manickachezian, 'Security Strength of RSA and Attribute Based Encryption for Data Security in cloud Computing', *International Journal of Innovative Research in Computer and Communication Engineering*, 2014.
32. C.-C. Lee, P.-S. Chung, and M.-S. Hwang, 'A survey on attribute-based encryption schemes of access control in cloud environments', *Int. J. Netw. Secur.*, vol. 15, pp. 231–240, Jan. 2013.
33. J. Bethencourt, A. Sahai, and B. Waters, 'Ciphertext-Policy Attribute-Based Encryption', in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, Washington, DC, USA, 2007, pp. 321–334.
34. V. Goyal, O. Pandey, A. Sahai, and B. Waters, 'Attribute-based Encryption for Fine-grained Access Control of Encrypted Data', in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, New York, NY, USA, 2006, pp. 89–98.
35. B. Balamurugan and P. Krishna, 'Extensive survey on usage of attribute based encryption in cloud', *J. Emerg. Technol. Web Intell.*, vol. 6, pp. 263–272, Jan. 2014.
36. M. Ambrosin, M. Conti, and T. Dargahi, 'On the Feasibility of Attribute-Based Encryption on Smartphone Devices', in *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*, New York, NY, USA, 2015, pp. 49–54.
37. 'bitcoin.pdf', https://bitcoin.org/bitcoin.pdf.
38. J.-P. Delahaye, 'Les blockchains, clefs d'un nouveau monde', *Pour Sci.*, no. 449, pp. 80–85, Mar. 2015.
39. K. Christidis and M. Devetsikiotis, 'blockchains and Smart Contracts for the Internet of Things', *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
40. blockchain France, Paris, *La blockchain décryptée. Les clefs d'une révolution*. Observatoire Netexplo, 2016.
41. *Ethereum France*, https://www.ethereum-france.com.
42. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, 'MedRec: Using blockchain for Medical Data Access and Permission Management', in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, pp. 25–30.
43. G. Zyskind, O. Nathan, and A. Pentland, 'Decentralizing Privacy: Using blockchain to Protect Personal Data', in *2015 IEEE Security and Privacy Workshops*, 2015, pp. 180–184.
44. S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, 'World of Empowered IoT Users', in *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2016, pp. 13–24.
45. A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, 'Towards a Novel Privacy-Preserving Access Control Model Based on blockchain Technology in IoT', in *Europe and MENA*

Cooperation Advances in Information and Communication Technologies, Springer, Cham, 2017, pp. 523–533.
46. J. Herrera-Joancomartí and C. Pérez-Solà, 'Privacy in Bitcoin Transactions: New Challenges from blockchain Scalability Solutions', in *Modeling Decisions for Artificial Intelligence*, 2016, pp. 26–44.
47. P. Koshy, D. Koshy, and P. McDaniel, 'An Analysis of Anonymity in Bitcoin Using P2P Network Traffic', in *Financial Cryptography and Data Security*, 2014, pp. 469–485.