Vers la sécurité dans un environnement opérationnel collaboratif dynamique

Didier Alquié, Nicolas Belloir, Jérémy Buisson, Lionel Touseau

Vers la sécurité dans un environnement opérationnel collaboratif dynamique

Didier Alquié[1], Nicolas Belloir[1,2], Jérémy Buisson[1,2] and Lionel Touseau[1,2]

[1]*Académie Militaire de Saint-Cyr Coëtquidan, 56381 Guer, France*
[2]*IRISA, Campus de Tohannic, 56000 Vannes, France*

Abstract
In this article, we consider systems in which the collaborating systems and their interactions cannot be anticipated at design nor deployment time. Indeed, the systems have to respond to operational environments that are in fact dynamic. An access control must grant communications between systems even if all the systems were not prealably identified, while, at the same time, it must deny any aimless or suspect access. Namely, access control must take into account the operational context when decisions are made. In this paper, we aim at outlining how the current state of the art addresses this challenge, as well as emphasizing some of the research questions that remain open.

Keywords
Chiffrement basé attributs, contrôle d'accès basé attributs, système collaboratif, collaboration non anticipée

Résumé
Dans cet article, nous considérons un environnement opérationnel dynamique, tel que les collaborations entre les systèmes ne peuvent être pleinement anticipées dès la conception et le déploiement du système. Il convient donc, tout en permettant des interactions entre des systèmes pas forcément pré-identifiées, d'empêcher d'éventuels intrus d'accéder illégitimement aux systèmes participant à l'opération. Pour ce faire, nous envisageons d'étudier comment le contrôle d'accès peut contextualiser les requêtes, au regard de la situation opérationnelle, afin d'automatiser le droit et le besoin d'en connaître. Dans cet article, nous présentons une introduction au chiffrement basé attributs et l'ébauche des travaux que nous projetons.

1. Introduction

En France, l'IGI 1300 [1] décrit les règles pour assurer la protection du secret de la défense nationale. Dans ses principes généraux, ces règles reposent sur trois concepts. Une information protégée se voit attribuer un niveau de *classification*, au plus juste, pour concilier la circulation de l'information nécessaire à l'efficacité opérationnelle tout en empêchant une divulgation excessive potentiellement nuisible qui donnerait à l'adversaire l'opportunité d'empêcher l'opération. Pour accéder à une information, une personne doit être *habilitée* au niveau de classification

C&ESAR'22: Computer & Electronics Security Application Rendezvous, Nov. 15-16, 2022, Rennes, France
didier.alquie@st-cyr.terre-net.defense.gouv.fr (D. Alquié); nicolas.belloir@st-cyr.terre-net.defense.gouv.fr (N. Belloir); jeremy.buisson@st-cyr.terre-net.defense.gouv.fr (J. Buisson); lionel.touseau@st-cyr.terre-net.defense.gouv.fr (L. Touseau)

de l'information, attestant la confiance accordée à cette personne. Le *besoin d'en connaître* conceptualise par ailleurs que l'accès à une information classifiée est motivé par l'exercice de la fonction ou l'accomplissement d'une mission. En complément de l'habilitation, le besoin d'en connaître contextualise donc les demandes au regard du besoin opérationnel pour décider d'accorder ou non l'accès. Se pose donc la problématique d'automatiser la manière de prendre ainsi en compte ce contexte opérationnel lors des décisions d'accorder ou non l'accès.

Dans cet article, nous proposons une introduction au contrôle d'accès et au chiffrement basé attributs, dans la perspective de supporter, voire d'automatiser les décisions de contrôle d'accès dans des scénarios semblables à l'IGI 1300. La section 2 présente des scénarios que nous identifions et qui partagent cette problématique. La section 3 synthétise comment prendre en compte ce problème de contrôle d'accès, et plus particulièrement l'approche de contrôle d'accès basé attributs (ABAC [2]). La section 4 présente le chiffrement basé attributs (ABE [3]), une technologie qui utilise des mécanismes cryptographiques pour établir la confiance lors de la mise en œuvre du contrôle d'accès basé attributs. Avant de conclure à la section 6, la section 5 présente une première mise en œuvre architecturale du contrôle d'accès basé attributs.

2. Scénarios pour un contrôle d'accès dépendant du contexte opérationnel

En France, la création de « Mon espace santé » [4] permet le partage d'informations entre les professionnels de santé, afin d'améliorer la coordination et de permettre aux soignants d'éclairer leurs décision sur la base d'une connaissance partagée des antécédents du patient et traitements en cours. Ce service adopte la vision française concernant la confidentialité des données de santé, qui font l'objet de règles spécifiques au sein de la protection des données personnelles. Le patient peut, à sa discrétion, autoriser ou non l'accès des professionnels de santé aux documents, et bloquer l'accès pour des professionnels spécifiques ou des documents spécifiques. Cependant, la politique de contrôle d'accès reconnaît qu'un patient peut souhaiter, lorsque la situation l'exige par exemple en cas d'urgence, assouplir les restrictions d'accès. Ainsi, un professionnel de santé peut temporairement passer outre les blocages et accéder à des documents auxquels l'accès lui est normalement refusé, lorsqu'il intervient dans le contexte opérationnel d'une situation d'urgence du patient.

Gupta et al. [5] présentent un scénario prospectif dans le contexte des transports et villes intelligents. Il s'agit, en particulier, d'envisager que les véhicules se connectent à l'infrastructure urbaine pour offrir des services, par exemple d'amélioration du trafic en présence d'événements pertubateurs. Avec le même objectif d'amélioration du trafic, pour favoriser le covoiturage, l'infrastructure urbaine propose également de mettre en relation des demandeurs piétons et des automobilistes. Un demandeur peut toutefois refuser que ses informations (localisation et destination) soient visibles par un automobiliste localisé ou se rendant dans un quartier trop éloigné de la demande. Un demandeur peut également restreindre l'accès à ses informations pour les automobilistes ayant des caractéristiques spécifiques, par exemple ceux qui sont engagés dans une activité incompatible avec le covoiturage au moment de la demande, ou bien ceux qui ont de trop mauvaises évaluations. Il en est de même pour un automobiliste vis-à-vis des demandeurs de covoiturage. Pour autant, lorsqu'un automobiliste se fait voler sa voiture, celui-ci

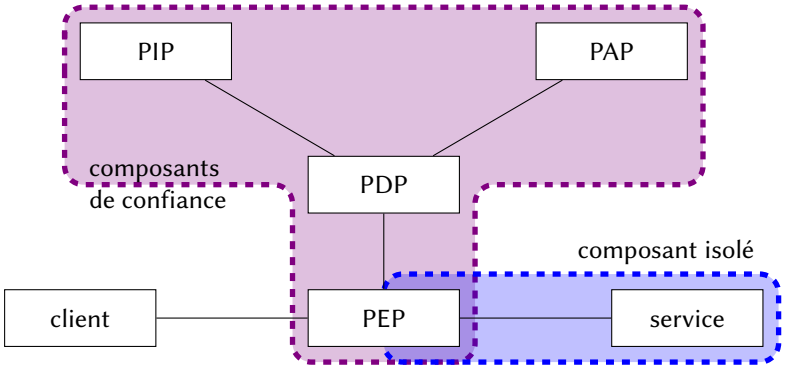

Figure 1: Architecture fonctionnelle typique pour mettre en œuvre le contrôle d'accès basé attributs.

peut solliciter les autres acteurs en leur demandant d'accepter, à titre exceptionnel, de partager leur localisation lorsqu'ils aperçoivent la voiture volée. Les règles de contrôle d'accès sont donc conditionnées par la situation opérationnelle des acteurs.

Dans ces deux scénarios comme pour l'IGI 1300, la décision d'accorder ou non l'accès n'est pas seulement prise selon le sujet (et ses habilitations), l'action et l'objet (et sa classification) – c'est-à-dire selon une matrice de contrôle d'accès traditionnelle, mais également selon la situation opérationnelle et le contexte dans lesquels l'accès est demandé. Cette situation et ce contexte sont dynamiques, et incluent (la nature) des activités dans lesquelles les acteurs sont engagés au moment de la demande d'accès. Cette situation et ce contexte doivent être réévalués à chaque demande d'accès, lors de l'application de la politique de contrôle d'accès.

Par ailleurs, dans ces scénarios, les seules actions sont la mise à disposition d'une donnée protégée, et la consultation d'une donnée lorsque la politique de contrôle d'accès l'autorise.

3. Contrôle d'accès basé attributs

La préoccupation de contextualiser le contrôle d'accès n'est pas spécifique aux exemples simples de la section 2. Les modèles de contrôle d'accès OrBAC [6] (*organization-based access control*) et ABAC [2, 7] (*attribute-based access control*) ont été proposés pour spécifiquement prendre en compte le contexte et sa dynamicité. Pour ce faire, il s'agit d'une part de caractériser la situation par une base de faits maintenue dynamiquement, et utilisée pour évaluer la politique de contrôle d'accès par exemple en utilisant la logique du premier ordre comme sémantique. Le contenu de la matrice de contrôle d'accès est déduit à la volée par le système déductif. XACML [8] est un exemple de langage concret standardisé pour exprimer des politiques de contrôle d'accès basées attributs.

La figure 1 présente une architecture fonctionnelle en support de ces langages de politique de contrôle d'accès. Il s'agit d'une simplification du patron *policy-based access control* [9], qu'on retrouve également dans l'architecture de référence *zero-trust* [10] par exemple. Dans cette architecture, les clients ne peuvent accéder directement aux services qui sont isolés, par exemple en utilisant des mécanismes réseau ou système selon l'échelle du déploiement. Il s'agit de garantir qu'un *policy enforcement point* (PEP) intercepte toutes les requêtes des clients pour

mettre en œuvre le contrôle d'accès. À chaque requête, le PEP interroge un *policy decision point* (PDP) chargé d'évaluer la politique de contrôle d'accès que lui fournit un *policy administration point* (PAP). L'évaluation utilise les informations fournies par le *policy information point* (PIP).

C'est lorsque le PEP, le PDP et le PIP opèrent à la volée que le contexte opérationnel est pris en compte dynamiquement, au moment des demandes d'accès. Plus spécifiquement, c'est le PIP qui calcule le contexte opérationnel.

Les composants PEP, PDP, PIP et PAP doivent être des composants de confiance. L'architecture repose aussi sur l'incapacité du client à contourner le PEP, et donc sur le mécanisme d'isolation du service.

4. Chiffrement basé sur les attributs

Le chiffrement basé sur les attributs (*Attribute-Based Encryption*, ABE [3]) est une forme de chiffrement asymétrique dont le déchiffrement est conditionné par la nature du profil du destinataire, à savoir le fait qu'il possède - ou pas - un certain nombre de caractéristiques - les attributs. Par construction, les mécanismes d'ABE interdisent la collusion : deux clients distincts, qui ne peuvent pas individuellement déchiffrer un message, ne peuvent pas non plus le déchiffrer "ensemble" en mettant en commun leurs clés respectives.

Les outils mathématiques utilisés dans la spécification des chiffrements basés sur les attributs sont essentiellement l'utilisation des couplages et l'utilisation des réseaux euclidiens.

- Un couplage est une application bilinéaire non dégénérée entre deux groupes commutatifs. L'intérêt de leur utilisation en cryptographie est son lien de parenté avec des problèmes algorithmiques difficiles, comme l'extraction d'un logarithme discret ou le problème décisionnel Diffie-Hellman. Ils ont été utilisés notamment pour la spécification de chiffrement basés sur l'identité [11, 12], une forme "primitive" si l'on peut dire des chiffrements basés sur les attributs, ou pour le protocole de Diffie-Hellman tripartite [13], une très élégante généralisation du protocole de Diffie-Hellman.
- Les réseaux euclidiens sont des sous-groupes discrets de $\mathbb{R}^n$ (ou des $\mathbb{Z}$-modules libres de rang n). Concrètement, il s'agit de généralisations à un espace euclidien de dimension quelconque d'un quadrillage bidimensionnel ou d'un maillage tridmensionnel. La spécificité et l'intérêt des réseaux en cryptographie tient dans ce qu'ils ne sont pas forcément orthonormés, et qu'alors il existe deux problèmes réputés difficiles sur lesquels on peut s'appuyer pour définir des chiffrements asymétriques "ordinaires": le problème du plus court vecteur (*shortest vector problem*, SVP), et le problème du vecteur le plus proche d'un vecteur donné de l'espace (*closest vector problem*, CVP). Ils ont notamment dejà servi à définir des cryptosystèmes à clé publique de chiffrement et de signature [14]. Ils connaissent aujourd'hui un regain d'intérêt majeur pour la cryptographie post quantique (*post quantum cryptography*, PQC), car on pense que les problèmes difficiles reliés sont immunes à l'ordinateur quantique, contrairement aux problèmes de la factorisation et du logarithme discret.

Dans l'état de l'art, il existe deux manières de contrôler le déchiffrement dans un chiffrement basé sur les attributs. Elles sont illustrées par les deux architectures de référence de la figure 2:

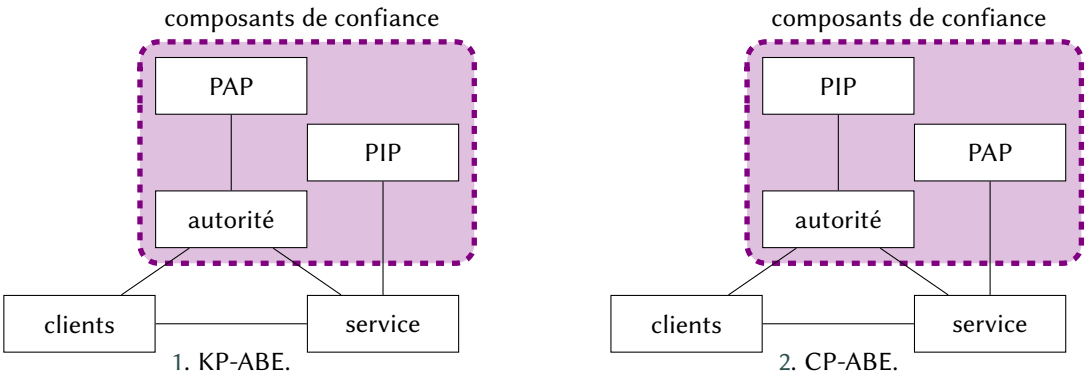

Figure 2: Architectures fonctionnelles de base pour le chiffrement basé attributs.

1. La politique d'accès peut être embarquée dans les clés de déchiffrement (*Key Policy Attribute-Based Encryption*, KP-ABE [15]). L'autorité génère et conserve une clé maître. Elle diffuse au service la clé publique associée. Le service utilise cette clé publique et l'ensemble des attributs calculé par le PIP pour chiffrer le message. Le chiffré est diffusé aux clients. En utilisant la clé maître et la politique donnée par le PAP, l'autorité génère une clé de déchiffrement pour chaque client. Chaque clé embarque une politique de contrôle d'accès, et ne peut déchiffrer que si le chiffré a été produit avec un ensemble d'attributs accepté par la politique embarquée dans la clé de déchiffrement. Avec KP-ABE, l'autorité impose donc la politique de contrôle d'accès, et laisse le service librement fixer les attributs dans le chiffré.
2. La politique d'accès peut être embarquée dans le chiffré (*Ciphertext Policy Attribute-Based Encryption*, CP-ABE [16, 17]). L'autorité génère et conserve une clé maître. Elle diffuse au service la clé publique associée. Le service utilise cette clé publique et la politique donnée par le PAP pour chiffrer le message. Le chiffré est diffusé aux clients. En utilisant la clé maître et l'ensemble d'attributs calculé par le PIP, l'autorité génère une clé de déchiffrement pour chaque client. Chaque clé embarque l'ensemble d'attributs calculé par le PIP, et ne peut déchiffrer que si cet ensemble d'attributs est accepté par la politique embarquée dans le chiffré. Avec CP-ABE, l'autorité certifie donc les attributs possédés par chaque client, et laisse le service librement décider la politique de contrôle d'accès.

OpenABE[1] est une implémentation de ces deux stratégies.

Des fonctions additionnelles ont été proposées pour compléter le chiffrement basé attributs de base. Par exemple, Yu et al. [18] ont proposé un mécanisme de re-chiffrement par proxy (proxy re-encryption [19]) pour CP-ABE pour permettre la révocation d'attributs. Li et al. [17], par exemple, propose une approche pour encoder des attributs à valeur entière. Zhang et al. [20] complètent l'étude de l'état de l'art, dans le cas particulier de CP-ABE, pour permettre les univers d'attributs larges, d'autres stratégies pour la révocation d'attributs, la traçabilité, le masquage ou la modification de politique d'accès, les organisations multi-autorités.

[1] https://github.com/zeutro/openabe

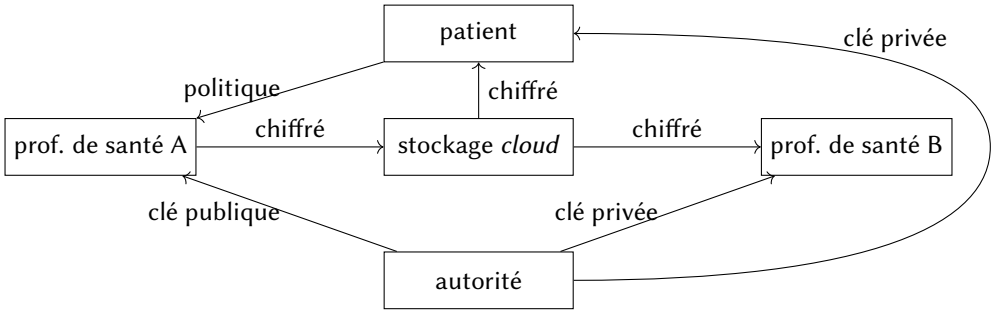

Figure 3: Une architecture possible pour le dossier médical.

5. Utilisation opérationnelle du chiffrement basé attributs

Dans le cas particulier des services qui consistent à produire des données protégées, ce qui est le cas de l'IGI 1300 et des scénarios de la section 2, une stratégie possible, pour mettre en œuvre l'architecture de la figure 1 est d'utiliser le chiffrement basé sur les attributs. Intuitivement, il s'agit de faire coïncider la capacité à déchiffrer la donnée protégée avec la décision d'autoriser la consultation de cette donnée, et d'aligner les architectures en conséquences.

Plus spécifiquement, l'IGI 1300 et « Mon espace santé » sont deux scénarios consistant à produire et stocker des documents pour les mettre à disposition, à l'image des fournisseurs de services de stockage dans le *cloud*. L'état de l'art réalisé par Zhang et al. [20] pour le cas spécifique de CP-ABE se place dans cette situation. Le producteur d'un document chiffre ce document – le chiffreur joue le rôle du PEP. De par CP-ABE, le chiffré embarque la politique de déchiffrement, c'est-à-dire les règles indiquant quels sujets peuvent déchiffrer le document et donc le consulter, en fonction des attributs: le fournisseur de service de stockage peut diffuser largement le chiffré indépendamment de cette politique. Comme indiqué dans la figure 2, une autorité génère des clés pour les sujets, selon les attributs de chacun de ces sujets.

La figure 3 présente une architecture possible, simplifiée pour « Mon espace santé » en utilisant CP-ABE. Le patient communique la politique qu'il souhaite au professionnel de santé A qui produit le document, afin que ce dernier chiffre le document produit avec la clé publique fournie par l'autorité. Le chiffré est envoyé au service de stockage pour persistance, indexation et diffusion. Le patient comme les professionnels de santé B obtiennent de l'autorité des clés privées de déchiffrement, qui attestent de leurs attributs, utilisés pour évaluer la politique embarquée dans le chiffré. Cette architecture soulève notamment deux questions concernant le chiffrement basé attributs:

- Lorsque le professionnel de santé B obtient une clé privée en situation d'urgence, il faut ultérieurement révoquer cet attribut pour ce professionnel de santé une fois la situation situation d'urgence terminée. Par exemple, Yu et al. [18] ont proposé un mécanisme de re-chiffrement par proxy (proxy re-encryption [19]) pour CP-ABE pour la révocation d'attributs, qui consiste à générer une clé permettant au service de stockage de re-chiffrer le document sans le déchiffrer, et en faisant confiance au service de stockage pour ne pas conserver le chiffré précédent.

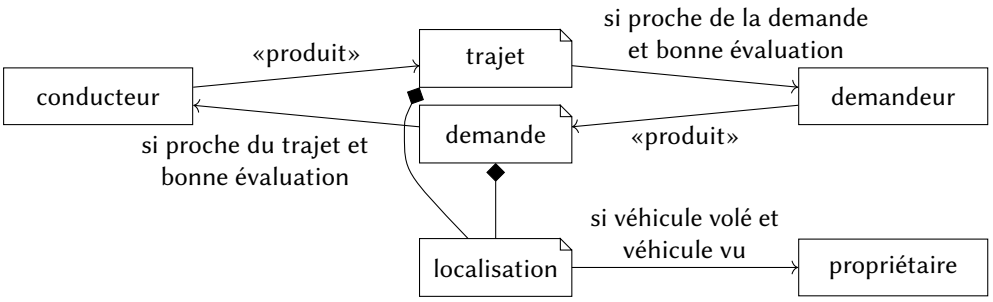

Figure 4: Une architecture possible pour le service de mise en relation dans le système de transport intégré à un système urbain.

- Comme la politique est embarquée dans les chiffrés stockés, alors chaque modification que le patient souhaite apporter à la politique nécessite de mettre à jour les chiffrés stockés. Une solution a par exemple été proposée par Zhang et al. [21], un schéma inspiré du re-chiffrement par proxy qui permet au service de stockage de réaliser cela.

La figure 4 montre l'architecture du cas du service de mise en relation entre conducteurs et piétons demandeurs dans un système de transport intégré à un système urbain, et qui prévoit la transmission de la localisation aux propriétaires dont le véhicule a été volé. Dans cette figure 4, nous avons centré la description sur les documents et les politiques d'accès à ces documents par les acteurs du système. Un conducteur offre son trajet aux potentiels demandeurs, et un demandeur publie sa demande aux potentiels conducteurs, dans les deux cas sous réserve de proximité avec l'attente (respectivement demande ou trajet) de l'autre acteur et de sa bonne évaluation. Les trajets et demandes contiennent notamment la localisation du conducteur et du demandeur (respectivement). Si le véhicule d'un propriétaire est volé et si l'acteur (conducteur ou demandeur) voit le véhicule volé, alors le propriétaire peut accéder à la localisation de l'acteur. Cette architecture soulève les questions suivantes:

- Dans une version décentralisée du système, l'absence d'autorité soulève la question de la distribution des clés de déchiffrement et de la confiance dans la valeur des attributs. Les schémas de chiffrement basé attributs multi-autorités ou à autorités hiérarchiques [20] ne semblent pas répondre à cette problématique.
- L'attribut de véhicule volé, pour le propriétaire doit pouvoir être révoqué, comme dans le scénario de la figure 3. Cet attribut ne donne accès qu'à une partie des documents produits par les acteurs. Enfin, la localisation (tout comme les trajets et demandes) ont une durée de vie limitée avant obsolescence.

6. Conclusion

Nous avons présenté deux scénarios dans lesquels la décision de contrôle d'accès repose sur la situation opérationnelle, au moment de la demande d'accès. Dans l'état de l'art, le contrôle d'accès basé attributs (ABAC [2, 7]) offre un canevas pour exprimer de telles politiques de contrôle d'accès. Et le chiffrement basé attributs (ABE [3, 15, 16]), raffiné en deux stratégies,

offre un mécanisme cryptographique qui peut être utilisé pour mettre en œuvre un ABAC. Les deux stratégies correspondent à deux alternatives pour répartir les responsabilités de certifier les attributs et les politiques de contrôle d'accès, entre l'autorité et le service qui chiffre la donnée.

Dans nos prochains travaux, nous expérimenterons l'utilisation de l'ABE, en l'état actuel des connaissances, pour mettre en œuvre les scénarios que nous avons présentés, en particulier dans un environnement décentralisé ou de collaborations opportunistes, soulevant donc les questions de la confiance dans la mesure des attributs et de la présence de l'autorité pour la distribution des clés, en particulier lorsque l'univers des attributs est dynamique. Ces travaux futurs supposeront de développer des méthodes et langages pour modéliser l'architecture de ces systèmes, comme nous avons commencé à l'ébaucher dans cet article.

References

[1] SGDSN, Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale, 2021. URL: https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-generale-interministerielle-n-1300-sur-la-protection-du-secret-de-la-defense-nationale/.

[2] L. Wang, D. Wijesekera, S. Jajodia, A logic-based framework for attribute based access control, in: Proceedings of the 2004 ACM workshop on Formal methods in security engineering, FMSE '04, 2004, pp. 45–55. doi:10.1145/1029133.1029140.

[3] A. Sahai, B. Waters, Fuzzy Identity-Based Encryption, in: Advances in Cryptology – EUROCRYPT 2005, Lecture Notes in Computer Science, 2005, pp. 457–473. doi:10.1007/11426639_27.

[4] JORF, Décret n° 2021-1048 du 4 août 2021 relatif à la mise en œuvre de l'espace numérique de santé, 2021.

[5] M. Gupta, J. Benson, F. Patwa, R. Sandhu, Dynamic Groups and Attribute-Based Access Control for Next-Generation Smart Cars, in: Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, 2019, pp. 61–72. doi:10.1145/3292006.3300048.

[6] A. A. El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel, G. Trouessin, Organization based access control, in: Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks, 2003, pp. 120–131. doi:10.1109/POLICY.2003.1206966.

[7] V. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, Technical Report NIST Special Publication (SP) 800-162, National Institute of Standards and Technology, 2019. URL: https://csrc.nist.gov/publications/detail/sp/800-162/final. doi:10.6028/NIST.SP.800-162.

[8] OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0, 2013. URL: https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[9] E. Fernandez-Buglioni, Security Patterns in Practice: Designing Secure Architectures Using Software Patterns, 2013.

[10] S. W. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero Trust Architecture, Technical Report SP800-207, NIST, 2020. URL: https://www.nist.gov/publications/zero-trust-architecture.

[11] A. Shamir, Identity-based cryptosystems and signature schemes, in: Advances in Cryptology, Proceedings of CRYPTO, Springer, volume 196 of *Lecture Notes in Computer Science*, 1984, p. 47–53. doi:10.1007/3-540-39568-7_5.

[12] M. Boneh, Dan; Franklin, Identity-based encryption from the weil pairing, SIAM Journal on Computing. 32 (3) (2003) 586–615. doi:10.1137/S0097539701398521.

[13] A. Joux, A one round protocol for tripartite Diffie-Hellman, in: Proceedings of the ANTS-IV workshop, ANTS, 2000.

[14] J. Hoffstein, J. Pipher, J. H. Silverman, NTRU: A ring-based public key cryptosystem, in: Algorithmic Number Theory, Lecture Notes in Computer Science, 1998, pp. 267–288. doi:10.1007/BFb0054868.

[15] V. Goyal, O. Pandey, A. Sahai, 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, CCS '06, 2006, pp. 89–98. doi:10.1145/1180405.1180418.

[16] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-Policy Attribute-Based Encryption, in: 2007 IEEE Symposium on Security and Privacy (SP '07), 2007, pp. 321–334. doi:10.1109/SP.2007.11, iSSN: 2375-1207.

[17] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin, G. Srivastava, An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things, IEEE Journal of Biomedical and Health Informatics (2021). doi:10.1109/JBHI.2021.3075995.

[18] S. Yu, C. Wang, K. Ren, W. Lou, Attribute based data sharing with attribute revocation, in: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS '10, 2010, pp. 261–270. doi:10.1145/1755688.1755720.

[19] M. Blaze, G. Bleumer, M. Strauss, Divertible protocols and atomic proxy cryptography, in: Advances in Cryptology — EUROCRYPT'98, Lecture Notes in Computer Science, 1998, pp. 127–144. doi:10.1007/BFb0054122.

[20] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li, D. Zheng, Attribute-based Encryption for Cloud Computing Access Control: A Survey, ACM Computing Surveys 53 (2020) 83:1–83:41. doi:10.1145/3398036.

[21] Y. Zhang, J. Li, X. Chen, H. Li, Anonymous attribute-based proxy re-encryption for access control in cloud computing, Security and Communication Networks 9 (2016) 2397–2411. doi:10.1002/sec.1509.