République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. MIRA-BEJAIA

Faculté des Sciences Exactes

Département d'Informatique

MÈMOIRE

EN VUE DE L'OBTENTION DU DIPLÔME DE MASTER PROFESSIONNEL

Domaine : Mathématiques et Informatique **Filière :** Informatique

Spécialité : Administration et sécurité des réseaux

Présenté par

Mlle.MOHAMMEDI Sara

Mlle.BOUDRIES Lydia

Thème

Proposition d'un protocole de contrôle d'accès au big data dans le contexte de l'Internet des Objets

Devant le jury composé de :

M.	MOHAMMEDI Mohammed	MCB	Univ.de Béjaia	Rapporteur
M.	KACIMI Farid	MAB	Univ.de Béjaia	Examinateur
M.	OUAZINE Kahina	MAB	Univ.de Béjaia	Examinatrice

Année Universitaire : 2019/2020

⁂ *Remerciements* ⁂

Le grand remerciement à Dieu le miséricordieux, qui nous a donné le courage et la patience pour mener à bien ce travail. Nos vifs remerciements sont adressés à toutes les personnes qui ont contribué de manière directe ou indirecte à l'aboutissement de ce travail.

En premier lieu, nos gratitudes à notre encadrant **Dr MOHAMMEDI Mohammed** qui nous a confié ce thème d'actualité. Nous apprécions son enthousiasme, sa gentillesse, ses conseils, ses orientations remarquables, son précieux suivi tout au long de la réalisation de ce travail, l'intérêt qu'il nous a apporté pour l'accomplissement de ce projet de fin de cycle et surtout pour sa grande aide et ses qualités humaines et pédagogiques.

Nous remercions chacun des membres du jury d'avoir consacré une partie de leur temps à la lecture de ce mémoire et pour l'intérêt porté à notre travail en acceptant de l'examiner et de l'enrichir de leurs propositions.

Notre reconnaissance va particulièrement à l'ensemble des enseignants du département d'Informatique pour tout ce qui nous a été transmis tout au long de notre formation.

Notre remerciement les plus chaleureux à nos parents, pour leurs soutiens, les encouragements et leurs sacrifices.

Nous remercions tous nos ami(e)s pour leurs soutiens tout au long de cette année et pour leurs encouragements et conseils notamment dans les moments difficiles.

Enfin, un grand Merci à tous nos proches qui nous ont apporté leur soutien durant l'élaboration de ce travail.

⁕ $\mathcal{D}$*édicaces* ⁕

À mes très chers parents, pour les sacrifices déployés à mon égard, pour leurs soutiens tous les efforts consentis pour mon éducation et ma formation durant toutes les années d'études et sans lesquels je n'aurait jamais réussi. Qu'ils trouvent ici le témoignage de ma reconnaissance, ma profonde affection et mon attachement indéfectible. À ma soeur et mes frères et tous mes ami(e)s qui m'ont soutenu tout au long de ce travail et à toute personne que je porte fort dans mon coeur et qui sauront se reconnaître. À chaque main tendue et pour toute attention témoignée.

M*^{lle} *MOHAMMEDI Sara

⁕ *Dédicaces* ⁕

C'est avec profonde gratitude et sincère mot, que je dédie ce modeste travail :

À mes très chers parents pour leur soutien et encouragement durant toutes nos années d'études et sans lesquels je n'aurais jamais réussi.

À ma très chère sœur « **Yasmine** », au secret du bonheur dans cette vie et au meilleur de ce que Dieu m'a béni dans ce monde pour avoir contribué à la réussite de ce travail d'une manière indirecte, et pour tout le soutien moral....

À mon frère « **Yacine** ».

À ma famille et à tous mes proches grands et petits.

À tous nos enseignants que j'ai eus durant tout mon cursus universitaire et qui m'ont permis de réussir dans nos études.

À tous mes chèrs amis qui étaient présents avec nous.

À toute personne ayant contribué à ce travail de prés ou de loin.

Et je n'oublie pas de dédier ce travail, à mon amie et binôme, qui a participé à le réaliser **« MOHAMMEDI Sara »**.

M*^lle^ *BOUDRIES Lydia

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

LISTE DES ACRONYMES

A	ABAC	Attribute-Based AccessControl.
	ABE	Attribute based Encryption.
	AC	Autorité de confiance.
	API	Application Programming Interface.
C	CP − ABE	Ciphertext Policy-Attribute based Encryption.
	CSP	Cloud Service Provider.
D	DACS − IoT	Device Access Control Scheme-Internet of Thing.
	DME	distance measuring equipment.
E	ECC	Elliptic Curve Cryptography.
	ECDH	Elliptic Curve Diffie-Hellman.
	ETSI	European Telecommunications Standards Institute.
G	G − CP − ABE	Group-Ciphertext Policy- Attribute based Encryption.
	GWN	European Telecommunications Standards Institute.
I	IBE	Identity-Based Encryption.
	IDO	Internet des Objets.
	IoT − FBAC	Internet of Thing-Function-based access control scheme.
	IPv6	Internet Protocol version 6.
	ICP − ABE	Inproved Ciphertext Policy-Attribute based Encryption.
k	KP − ABE	Key Policy-Attribute Based Encryption.
M	M2M	Machine à Machine.
N	NIC	National Intelligence Council.
O	OABACM	Ontology Attribute Based Access Control Model.
P	PPOMACS	Privacy Preserving Outsourced Multi-Authority Access Control Schem.
	PS	Proxy Server.
R	RBAC	Role Based Access Control.
	RFID	Radio Frequence Identification.
	ROR	Real-Or-Random.
	RPL	Routing Protocol for Low-Power and Lossy Networks.
V	VOMAACS	Verifiable Outsourced Multi-Authority Access Control Scheme.
X	XACML	eXtensible Access Control Markup Language.

INTRODUCTION GÉNÉRALE

Internet est un réseau informatique mondial, qui se transforme progressivement en un réseau étendu dit Internet des Objets (IdO), reliant des milliards d'êtres humains et des dizaines de milliards d'objets [28].

L'IdO fait couler beaucoup d'encre actuellement, ce qui marque le début d'une nouvelle ère en matière de connectivité et de mobilité dans des différents domaines de la vie quotidienne telle que : la santé, l'agriculture, le transport, l'industrie, les villes intelligentes, etc. Cependant, à l'instar de toute autre nouvelle technologie, l'Internet des objets n'est pas dénué de difficultés et de défis à relever [26]. Un défi très important reste, sans doute, la protection et la confidentialité des données et la sécurité des objets connectés. Par conséquent, le contrôle de l'accès aux données des utilisateurs étant un moyen de sécuriser et de gérer l'accès à ces données sensibles est un sujet très important dans notre vie quotidienne. En effet, tous les jours, de plus en plus d'appareils sont équipés de capteurs pour recueillir un ensemble de données massives appelé "le big data". À ce fait, le contrôle d'accès à ces données dans l'IdO a fait l'objet de plusieurs recherches durant ces dernières années. Par conséquent, cela est considéré comme l'un des principaux problèmes à résoudre pour promouvoir l'IdO dans monde réel.

La recherche d'un modèle de contrôle d'accès dans un domaine en pleine croissance tel que le "big data" est en émergence grâce à l'Internet des Objets, dont des milliers d'objets dans le monde se voient connecter les uns avec les autres et avec le serveur du Cloud. Donc, assurer le contrôle d'accès et la bonne gestion de ces données massives générées par ces appareils intelligents, aussi celles produites par l'homme sont une question stimulante qui n'est pas encore résolue, dû au volume et à la diversité des données sensées être confidentielles. En outre l'essor des technologies cloud et IdO a accéléré la croissance du système de santé. Les appareils IdO surveillent la santé du patient et téléchargent les données collectées sous forme de dossiers médicaux électroniques dans le cloud pour stockage et partage.

Dans ce contexte, de nombreux travaux de recherche portent de ce fait sur le contrôle d'accès au big data dans l'IdO. Parmi ces solutions, il y a celles qui sont basées sur les rôles (RBAC Role Based Access Control), qui limitent l'accès du système aux utilisateurs autorisés, des rôles sont attribués aux utilisateurs et chaque rôle dispose d'autorisations. D'autres solutions sont basées sur les ontologies. Une ontologie n'est pas un modèle figé, elle doit évoluer pour répondre notamment aux évolutions. Actuellement, la plupart des travaux traitant de l'évolution d'ontologies se préoccupent de la gestion du processus d'évolution afin de vérifier et maintenir la cohérence de l'ontologie modifiée. De plus, on trouve aussi des solutions basées sur le chiffrement à base d'attributs (ABE). Ce type de solution est basé sur le chiffrement à clé publique ou

à clé secrète d'un utilisateur et les données chiffrées dépendent des attributs. D'autres solutions de contrôle d'accès s'ajoutent à cela, ces solutions sont principalement basées sur la cryptographie combinée avec le chiffrement à courbes elliptiques (ECC). Le principal avantage d'ECC est que des clés plus courtes peuvent être utilisées par rapport à d'autres cryptosystèmes. À ce fait, elle est le choix idéal pour implémenter la cryptographie à clé publique dans des appareils à ressources limitées, comme celles trouvées dans les applications envisagées de l'IdO [26].

Il existe plusieurs travaux de recherche liés au contrôle d'accès aux Big Data basés sur l'ABE dans l'IdO, cependant, la plupart de ces solutions n'ont pas donné satisfaction, car elles souffrent des limites de performances, ou bien elles ne sont pas fiables, ou elles sont vulnérables aux attaques et non scalables.

Le travail présenté dans ce mémoire a pour objet le contrôle d'accès au big data dans le contexte de l'IdO. Dans le protocole proposé, nous nous sommes inspirés des solutions existantes et de leurs points forts. Plus exactement, nous proposons un protocole qui assure le contrôle d'accès au big data basé sur la cryptographie à base d'attributs (ABE) en choisissant la variante Ciphertext-Policy Attribute Based Encryption (CP-ABE). Cette dernière, est une technique de cryptage prometteuse qui permet de crypter les données générées par les objets sous les politiques d'accès définis sur quelques attributs de consommateurs de données. De plus, elle permet seulement aux consommateurs de données dont les attributs satisfont les politiques d'accès de décrypter ces données.

Le reste de ce document est structuré comme suit : Le premier chapitre **"Généralités autour de l'Internet des Objets et du big data"** est consacré à l'Internet des Objets et le big data, qui portera sur quelques définitions, ainsi que les domaines d'application et l'architecture, ainsi les vulnérabilités et les menaces relatives à son déploiement, puis nous présenterons quelques défis imposés par big data et la sécurité de l'Internet des Objets. Dans le deuxième chapitre **"Taxonomie sur les protocoles de contrôle d'accès au big data dans l'Internet des objets"**, nous discuterons certains travaux de recherche concernant le contrôle d'accès au big data. Dans le troisième chapitre **"Proposition d'un modèle de contrôle d'accès au big data dans l'Internet des objets"**, nous présenterons en détail l'architecture réseau de notre protocole de contrôle d'accès proposés, ainsi que son principe de fonctionnement, puis nous parlerons sur l'analyse de sécurité réalisée pour prouver l'efficacité du protocole proposé, nous présenterons dans le quatrième chapitre **"Simulation et évaluation de performances"**, les résultats de simulations obtenus suite à l'évaluation de performances du protocole proposé.

Enfin, nous conclurons ce travail par une conclusion générale et quelques perspectives de recherche que nous souhaitons accomplir prochainement.

CHAPITRE 1

GÉNÉRALITÉS AUTOUR DE L'INTERNET DES OBJETS ET DU BIG DATA

1.1 Introduction

L'Internet des Objets (IdO) est un réseau mondial d'objets qui repose sur l'idée que tous les objets peuvent être connectés un jour à Internet, ces objets sont adressables de manière unique. Tout objet, y compris des ordinateurs, des capteurs, des RFID (Radio Frequence Identification) et des téléphones mobiles seront en mesure d'émettre de l'information et éventuellement de recevoir des commandes. L'IdO ouvre la voie vers une multitude de scénarios basés sur l'interconnexion entre le monde physique et le monde virtuel. Cependant, comme d'autres concepts, celui-ci fait face à un nombre de problématiques qui nécessitent d'être étudiées pour permettre à l'Internet des objets d'atteindre son plein potentiel.

Dans ce chapitre, nous présenterons d'abord l'IdO et son architecture, puis ses différents domaines d'application, ainsi que les enjeux et les défis de l'Internet des objets. Ensuite, nous parlerons sur les caractéristiques du big data. Par la suite, nous expliquons brièvement la sécurité dans l'IdO et nous terminerons par une conclusion.

1.2 Internet des objets

1.2.1 Définition

L'Internet des Objets est une infrastructure dynamique d'un réseau global. Ce réseau a des capacités d'auto-configuration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces Intelligentes, et ils sont intégrés aux réseaux d'une façon transparente [28].

1.2.2 Architecture et standarisation

Les racines de l'IdO remontent aux technologies M2M (machine à machine) pour le contrôle des processus à distance. L'IdO qui est aujourd'hui un mélange de plusieurs technologies telles que la RFID,

les capteurs et actionneurs sans fil, le M2M, l'ultrage bande ou 3/4G, IPv6 (Internet Protocol version 6), et RPL (Routing Protocol for Low-Power and Lossy Networks) nécessite la définition d'une architecture et de standards afin de faciliter son développement dans le future. L'ETSI (European Telecommunications Standards Institute) propose une architecture découpée en trois domaines distinct, le domaine du réseau d'objets, le domaine du réseau cœur d'accès et le domaine des applications M2M et applications clients [4].

1.2.3 Domaines d'application

Comme illustré par la figure 1.1, l'IdO couvre un large éventail d'applications et touche à un grand nombre de domaines dans notre vie quotidienne, tels que le domaine d'industrie, les soins de santé, le transport et bien d'autres encore, qui permettra l'émergence des espaces intelligents [15].

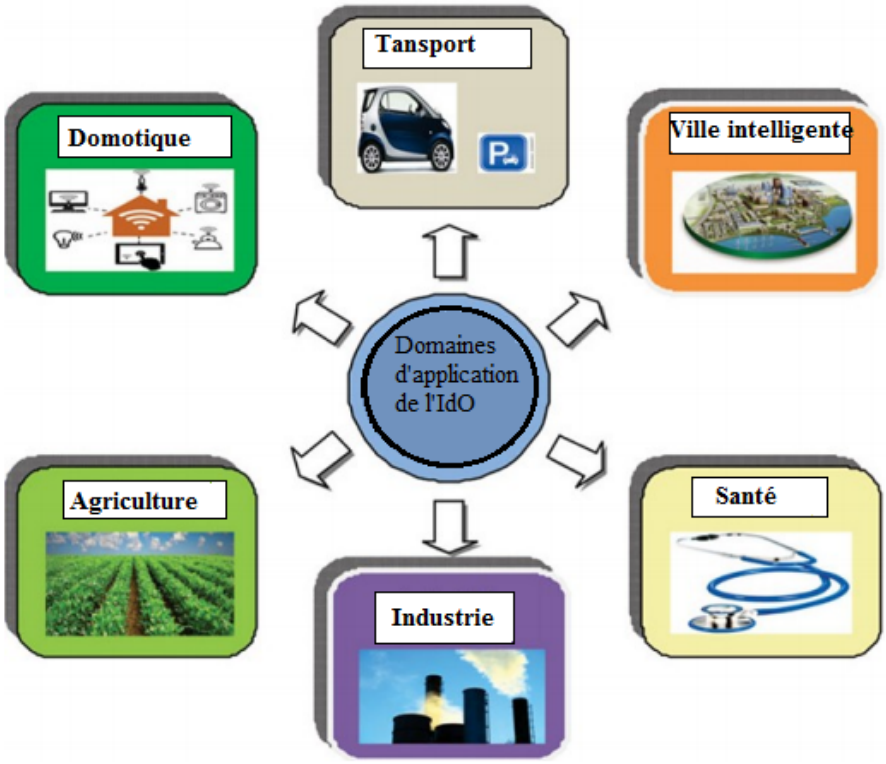


FIGURE 1.1 – Domaines d'application de l'Internet des Objets [15].

1.2.3.1 **Domaine de transport**

Le suivie en temps réel du déplacement des populations, des biens et des moyens de transport dans le monde permettra l'élaboration d'un système de transport intelligent qui a comme objectifs, non seulement le renforcement de la sécurité routière, mais également l'efficacité de la gestion du trafic, l'économie du temps, de l'énergie et le confort des conducteurs.

1.2.3.2 **Domaine de l'industrie**

La technologie IdO permet aux usines d'améliorer l'efficacité de ses opérations, d'optimiser la production, d'améliorer la sécurité des employés, faciliter la lutte contre la contre façon, la fraude et assurer un suivi total des produits.

1.2.3.3 **Domaine de la santé**

Ce domaine de l'IdO assure le suivi des signes cliniques des patients par la mise en place des réseaux personnels de surveillance, ces réseaux seront constitués de biocapteurs posés sur le corps des patients ou dans leurs lieux d'hospitalisation. Cela facilitera la télésurveillance des patients et apportera des solutions pour l'autonomie des personnes à mobilité réduite.

1.2.3.4 **Domaine de l'aérospatial et aviation**

Dans ce domaine, l'IdO vise à porter l'innovation aéronautique pour réduire les coûts de développement et optimiser la performance des avions. De plus, améliorer la sécurité des services, en assurant l'identification des produits et des éléments contrefaits grâce à l'élaboration des pièces critiques des appareils, cela par le bais d'implantation de tag RFID.

1.2.3.5 **Domaine d'énergie**

L'IdO propose des possibilités de gestion en temps réel pour une distribution et une gestion efficace de l'énergie, comme les réseaux électriques intelligents (smart grid). Cela permet d'avoir le contrôle de la consommation d'énergie et la détection des fraudes.

1.2.3.6 **Domaine de la domotique**

Concerne la mise des dispositifs domestiques sur réseau. Cela permet de contrôler les différents équipements d'une maison depuis une même interface (une tablette ou un téléphone par exemple). Mais aussi, il offre la possibilité de contrôler à distance ces équipements via la mise à disposition d'API (Application Programming Interface) sur le web.

1.2.3.7 **Domaine de l'Agriculture**

L'IdO permettra une meilleure aide à la décision en agriculture. L'IdO servira non seulement à optimiser l'eau d'irrigation, mais aussi, cette technologie peut être utilisée pour lutter contre la pollution (l'air et les eaux) et améliorer la qualité de l'environnement en général.

1.2.3.8 **Domaine de villes intelligentes (smart city)**

Les villes intelligentes permettant d'améliorer la qualité de vie de la municipalité en assurant l'optimisation du remplissage des parkings dans la ville grâce à l'identification des places libres en temps réel, l'éclairage publique intelligent qui varie en fonction de l'intensité lumineuse ou des déplacements également. La gestion du trafic est facilitée par une vision fine et en temps réel des flux.

1.2.4 Les enjeux et les défis de l'Internet des Objets

Parmi les principaux défis liés au soutien de ces études, on peut citer les suivants [7] :

- Saisir le grand volume de données hétérogènes produites par divers capteurs IdO (et éventuellement des mesures manuelles), et ce, pour un grand nombre d'activités variées impliquant différentes études et cultures.
- Prise en charge de l'intégration et de l'utilisation de presque tous les appareils IdO, y compris tous les capteurs, caméras, stations météo, etc. disponibles dans le commerce, ce qui permettra de créer un modèle de capteur à emporter.
- Des opérations qui permettront aux agriculteurs, aux producteurs et aux scientifiques de tirer parti de capteurs IdO moins chers/plus performants, ainsi que des préférences et des budgets individuels.
- Intégration de données hétérogènes provenant d'une aussi grande variété de dispositifs IdO, ainsi que des données historiques sur les performances des cultures produites par des études antérieures (ces données et résultats sont généralement disponibles au format CSV).
- Fichiers qui rendent l'utilisation, l'analyse, l'exploration et le partage plus difficiles.
- Fourniture d'un logiciel d'analyse des données sur les performances des cultures et des outils associés pour la recherche, l'analyse et la visualisation autonomes des données collectées dans plusieurs études.

1.3 Le Big data

1.3.1 Définition

Le "Big Data" est un terme générique employé pour désigner les stratégies et technologies mises en œuvre pour rassembler, organiser, traiter et analyser de vastes ensembles de données. Le big Data est l'art de gérer et d'exploiter de gros volumes de données [3].

1.3.2 Caractéristiques du Big Data

Pour décrire le principe du Big data, il est coutumier de résumer ses caractéristiques majeures en utilisant 5 lettres "V" : Volume, Variété, Vélocité, Valorisation, Véracité [2].

- **Volume :** la quantité de données générées est en pleine expansion et suit une loi quasi exponentielle.
- **Variété :** concerne les types de données : données brutes, semi-structurées ou non structurées, provenant de plusieurs sources comme le web, les objets connectés, réseaux, etc.
- **Vélocité :** la rapidité de renouvellement des données dans un monde connecté n'est plus à démontrer.
- **Valorisation :** L'objectif est de créer des valeurs pour les entreprises et les clients en transformant toutes les données en valeurs exploitables.
- **Véracité :** concerne la fiabilité et la crédibilité des données collectées.

1.4 L'Internet des objets et le Big Data

L'Internet des objets et le Big Data sont deux technologies interconnectées et indissociables. De plus en plus d'appareils et d'objets sont connectés à Internet. Ces objets connectés génèrent des données, qui peuvent être analysées pour dégager des tendances et informations à des fins diverses. C'est la raison pour laquelle le Big Data et l'Internet des objets sont étroitement liés [25].

1.5 La sécurité dans l'Internet des objets

La sécurité informatique est l'ensemble des moyens techniques qui visent à empêcher l'utilisation non-autorisée des données. On peut dire aussi que la sécurité informatique est un ensemble de moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles [15].

1.5.1 Vulnérabilités et menaces dans l'Internet des objets

"The National Intelligence Council (NIC)" américain considère que les avancées technologiques combinées à une forte demande des marchés encourageraient une adoption et un déploiement à large échelle de l'IdO. Néanmoins, la plus grande crainte est que les objets du quotidien deviennent des risques potentiels d'attaque de sécurité. Pire encore, la pénétration à large échelle de l'IdO diffuserait ces menaces d'une façon beaucoup plus large que l'Internet d'aujourd'hui. En effet, l'ubiquité de l'IdO amplifiera les menaces classiques de sécurité qui pèsent sur les données et les réseaux. Mais en plus, le rapprochement du monde physique et du monde virtuel à travers l'IdO ouvre la voie à de nouvelles menaces qui pèseront directement sur l'intégrité des objets eux-mêmes, les infrastructures et processus (monde physique), et la vie privée des personnes [2].

1.5.1.1 **Menaces sur les données et les réseaux**

L'omniprésence des objets communicants dépourvus de protection physique et de surveillance, les rendent une proie facile aux attaques matérielles et logicielles. Ces objets peuvent être volés, corrompus et contrefaits. Sans mesure particulière, les données stockées sur ces dispositifs seraient alors accessibles, y compris des données cryptographiques qui permettraient d'accéder à d'autres données sensibles ou jouer des rôles sensibles dans les systèmes complexes les hébergeant. Par ailleurs, les transmissions sans fil, sont à leur tour une proie facile à l'écoute et au dénie de service. Il existe aujourd'hui des solutions cryptographiques pour assurer des services de confidentialité, de contrôle d'intégrité, d'authentification, de non-répudiation, etc. Mais, beaucoup reste à faire pour rendre ces algorithmes efficaces et performants sur des dispositifs embarqués de plus en plus miniaturisés [15].

1.5.1.2 **Menaces sur la vie privée**

Tous les pronostics envisagent le développement d'une informatique ambiante avec potentiellement des dizaines d'objets par personne y compris dans leur sphère privée et intime. Ces objets de l'espace personnel sont géo-localisables, peuvent communiquer avec d'autres objets à travers des réseaux spontanés. Ils peuvent aussi écouter ce que dit la personne, peuvent filmer la personne et/ou son environnement, et peuvent même enregistrer son rythme cardiaque, son rythme respiratoire, la température de son corps, et sa cinématique. Des questions légitimes se posent sur le devenir de cette masse de données personnelles

et parfois intimes. Sans régulation stricte, une protection accrue de la privacy, un degré élevé de contrôle des objets par les usagers, l'adoption de l'IdO serait un échec [15].

1.5.1.3 **Menaces sur les systèmes et l'environnement physique des objets**

L'IdO fera une partie intégrante du monde physique et des systèmes complexes. En conséquence, un disfonctionnement quelconque, un déni de service, ou un comportement byzantin des objets n'entravera plus uniquement l'intégrité du monde virtuel (composé de données et d'informations), mais directement les processus sous leur contrôle en causant des dommages collatéraux importants [15].

1.5.2 Objectifs de la sécurité

La sécurité Informatique d'une manière générale vise à assurer plusieurs objectifs, dont les cinq principaux sont : le contrôle d'accès, l'authentification, la confidentialité, l'intégrité, la disponibilité et la non-répudiation [15].

1.5.2.1 **Confidentialité**

La confidentialité est le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé, permet de garder la communication des données privées entre un émetteur et un destinataire. Le chiffrement des données est la seule solution pour assurer la confidentialité des données.

1.5.2.2 **Intégrité**

L'intégrité permet de garantir que les données sont bien celles que l'on croit être, donc permet de garantir la protection des données contre les modifications et les altérations non autorisées.

1.5.2.3 **Disponibilité**

La disponibilité est un service réseau qui permet de donner une assurance aux entités autorisées d'accéder aux ressources réseaux. L'objectif est d'éviter les attaques du type Denis de service.

1.5.2.4 **Vie privée**

La vie privée est la demande des individus, des groupes ou des institutions de déterminer eux-mêmes quand, comment, et dans quelle mesure l'information leur concernant est communiquée aux autres. Chaque personne a une compréhension différente de ce qu'est la vie privée. On peut la définir comme étant le droit de garder protégées nos données personnelles comme la date de naissance, le numéro de téléphone personnel, la localisation mais, également d'autres données multimédias comme des vidéos et des photos [13].

1.5.2.5 **Authentification**

L'authentification peut être définie comme le processus de prouver une identité revendiquée. Lorsqu'il existe une seule preuve de l'identité (mot de passe) en parle d'authentification simple lorsque cette dernière nécessite plusieurs facteurs on parle alors d'authentification forte.

1.5.2.6 **Non-répudiation**

Non-répudiation permet de garantir qu'une transaction ne peut être niée et qu'un message a bien été envoyé par un émetteur et reçu par un destinataire aucun des deux ne pourra nier l'envoi ou la réception du message.

1.5.2.7 **Contrôle d'accès**

Le contrôle d'accès consiste à associer des droits d'accès et/ou des ressources à une entité (personne, ordinateur), permettant ainsi à l'entité d'accéder à la ressource souhaitée, si elle en a les droits.

1.6 Conclusion

Ces quelques dernières années, l'Internet des objets est devenu l'une des technologies les plus importantes du $21^{ème}$ siècle. Maintenant, que nous pouvons connecter des objets du quotidien (appareils électroménagers, voitures, thermostats, interphones bébés, etc..) à Internet par l'intermédiaire de dispositifs intégrés, des communications sont possibles en toute transparence entre les personnes, les processus et les objets. Grâce à des traitements informatiques peu coûteux, au Cloud, au Big Data, aux analytiques et aux technologies mobiles, les objets physiques peuvent partager et collecter des données avec un minimum d'intervention humaine. Dans ce monde hyper connecté, les systèmes digitaux peuvent enregistrer, surveiller et ajuster chaque interaction entre les objets connectés. Le monde physique rencontre le monde digital, et ils coopèrent. Ce chapitre a été consacré à la présentation de l'IdO, ses domaines d'application ainsi que ses enjeux. Puis, nous avons mis l'accent sur le Big Data et ses caractéristiques. Par la suite, nous avons présenté les notions de base liées à la sécurité dans l'IdO, et cela en définissant les vulnérabilités et menaces dans l'IdO.

Le chapitre suivant sera consacré à un état de l'art sur les mécanismes de contrôle d'accès au big data.

CHAPITRE 2

TAXONOMIE SUR LES PROTOCOLES DE CONTRÔLE D'ACCÈS AU BIG DATA DANS L'INTERNET DES OBJETS

2.1 Introduction

L'Internet des objets (IdO) est une technologie qui a la capacité de révolutionner notre façon de vivre, dans des secteurs allant du transport à la santé, du divertissement à nos interactions avec le gouvernement. Cette fantastique opportunité présente également un certain nombre de défis important. À chaque seconde les objets génèrent une masse importante de données qui s'appelle "big data" ce qui fait que contrôler l'accès à ces données massives est un sujet de préoccupation majeure non encore résolu dû au volume et à la diversité des données sensées être confidentielles.

Dans ce chapitre, nous commencerons tout d'abord par présenter les critères d'analyse, suivi par une classification des solutions étudiées, puis nous présenterons et discuterons chaque solution. Enfin, nous conclurons ce chapitre par une synthèse et comparaison des travaux analysés.

2.2 Critères d'évaluation des protocoles existants

Pour une meilleure évaluation des travaux de recherche étudiés, nous avons établi certains critères jugés pertinents, en tenant compte des besoins et contraintes liés aux big data, nous avons établi une liste de critères d'évaluation. Notre liste comprend les éléments suivants [24] :

2.2.1 Résistance aux attaques

En raison des données sensibles échangées par les utilisateurs, un mécanisme de sécurité développé pour le protocole de contrôle d'accès doit être résistant aux attaques et répondre aux principales exigences de sécurité.

2.2.2 Scalabilité

Elle fait référence à la capacité d'être extensible en termes de nombre d'utilisateurs et de nœuds physiques sans affecter négativement la qualité des services fournis par le système IdO. La mise en œuvre de cette exigence implique un moyen efficace pour gérer les nœuds physiques au sein du système IdO. La gestion des nœuds comprend des aspects tels que l'enregistrement et l'identification des nœuds, ainsi que le stockage et le traitement d'un énorme volume de données générées par les nœuds physiques.

2.2.3 Interopérabilité

Est une exigence importante pour toutes les applications IdO. Les systèmes IdO sont généralement constitués de dispositifs, services et applications hétérogènes de différents fournisseurs et prestataires de services qui utilisent différentes technologies et formats de communication pour l'échange de données.

2.2.4 Fiabilité

La fiabilité fait référence au bon fonctionnement d'un écosystème IdO. La détection, la transmission et le traitement des données doivent être fiables en ce sens que même en cas de panne ou de dysfonctionnement, l'écosystème IdO doit toujours garantir la prestation de services. La fiabilité implique la disponibilité de la détection, de la communication et du traitement des données, ainsi que des services et applications qui consomment les données.

2.2.5 Utilisabilité

L'utilisabilité est une exigence primordiale dans les applications IdO qui se caractérisent par une forte implication des utilisateurs et par l'utilisation d'appareils portables comme dans les maisons intelligentes et l'IdO de santé. Les appareils portables ont souvent de très petits écrans, ce qui rend l'interaction de l'utilisateur et la détermination des informations à afficher un facteur délicat, mais important. Les interfaces des appareils doivent également être facilement personnalisables par les utilisateurs et faciliter la gestion et l'administration de l'appareil lui-même.

2.2.6 Performance

Les systèmes IdO sont souvent constitués d'appareils à ressources limitées qui ont des capacités de stockage, de mise en réseau et de traitement limitées. Par conséquent, les protocoles de contrôle d'accès dans l'IdO doivent être légers, ce qui signifie que les coûts de communication et du calcul doivent être aussi faibles que possibles du côté de l'appareil. Les performances peuvent également être affectées par la latence du transfert de données entre les nœuds en raison du réseau sous-jacent et de l'infrastructure middleware. Les retards dans la transmission et le traitement des données devraient être minimaux.

2.3 Classification des travaux examinés

Protéger la vie privée relative aux utilisateurs d'Internet est d'une importance capitale dans l'IdO. Afin de réaliser un mécanisme de sécurité qui répond aux exigences des objets connectés, plusieurs recherches ont été menées. Nous avons choisi de faire une classification qui englobe quelques protocoles de contrôle

d'accès au big data dans l'IdO en les regroupant en trois grandes catégories. La première catégorie contient les protocoles basés sur la cryptographie, la deuxième regroupe les protocoles basés sur les rôles et la troisième comporte ceux qui sont basés sur l'ontologie.

La figure 2.1, représente notre classification des différentes solutions pour le problème du contrôle d'accès aux big data.

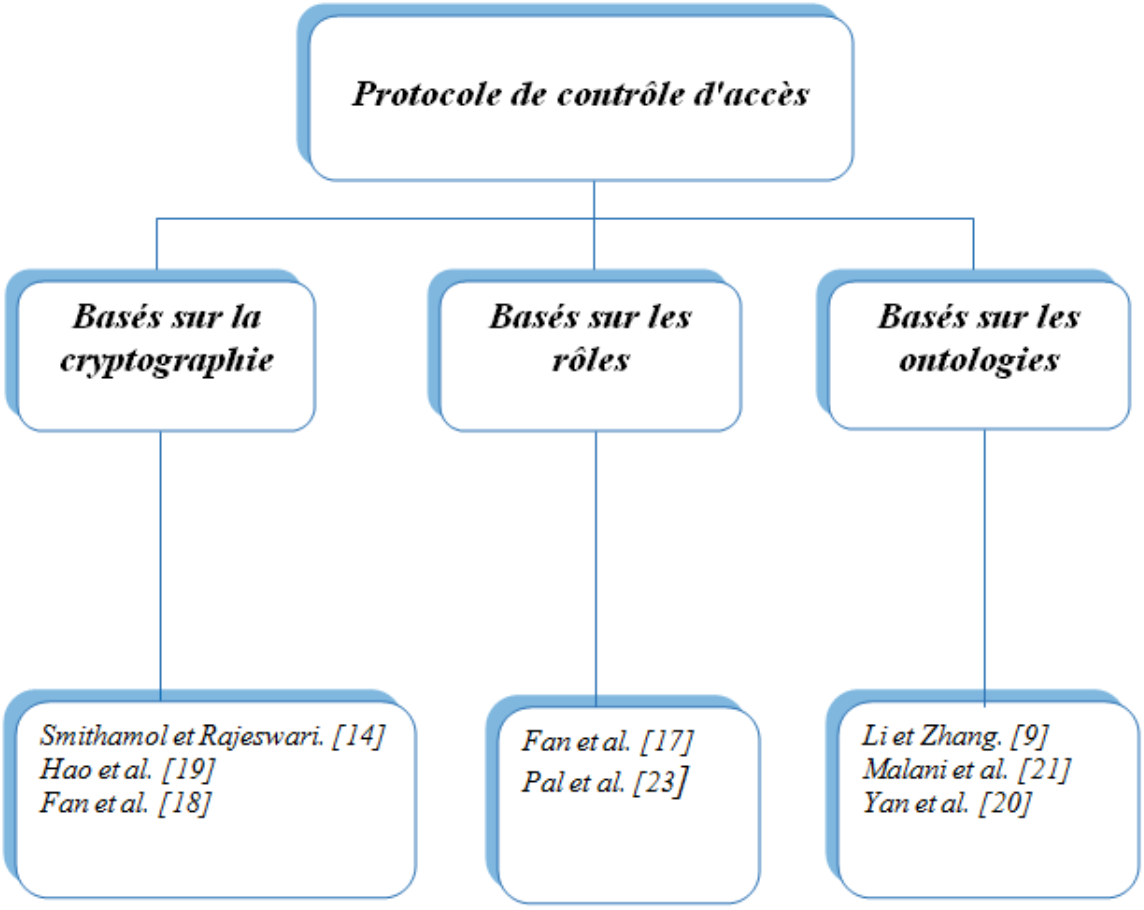


FIGURE 2.1 – Classification des travaux étudiés.

2.4 Revue de la littérature sur quelques protocoles de contrôle d'accès au big data

2.4.1 Solutions basées sur la cryptographie

- **Hybrid Solution for Privacy-Preserving Access Control for Healthcare Data**
  Smithamol et Rajeswari [14], ont proposé un modèle de contrôle d'accès nommé ABE (Attribute-Based Encryption) qui a été amélioré en proposant deux nouvelles variantes à savoir l'ABE de politique clé KP-ABE (Key-Policy Attribute Based Encryption) et l'ABE de cryptographie-politique CP-ABE (Ciphertext-Policy Attribute based Encryption), mais, c'est cette dernière qui est extrêmement utile dans le système DME (Distance Measuring Equipment) car elle permet de contrôler

l'accès aux données de santé hébergé dans le cloud. Et après quelques études de plus, une nouvelle méthode a été proposé pour créer une structure basée sur un groupe à l'aide de P-O-S-E-T qui met en œuvre une nouvelle architecture de sécurité appelée G-CP-ABE (Group-Ciphertext-Policy Attribute based Encryption) son principale avantage réside dans les combinaisons bilinéaires minimales par rapport à celles des travaux existants. Enfin Smithamol et Rajeswari [14] ont choisi la dernière architecture dans le partage des dossiers médicaux dans divers établissements de santé parce qu'elle permet de surveiller les problèmes de santé même à partir d'un appareil IdO limité de ressources. 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.

- **Fine-grained data access control with attribute-hiding policy for cloud-based IoT**
  Hao et al. [19], ont proposé une amélioration au système de contrôle d'accès qui se focalise sur la technique CP-ABE (Ciphertext Policy-Attribute based Encryption) pour résoudre le problème de fuite de confidentialité causé par la stratégie d'accès public. Ils ont proposé un schéma de contrôle d'accès aux données à grain fin prenant en charge la politique d'accès expressif avec une politique de masquage d'attributs pour l'IoT basé sur le cloud. Spécifiquement, les informations d'attribut sont entièrement cachées dans la politique d'accès en utilisant une technique aléatoire. De plus, pour aider le décodage de données ils ont pu concevoir un mécanisme de positionnement d'attribut flou basé sur un filtre de Bloom tronqué, pour aider les destinataires autorisés à localiser leurs attributs dans la matrice d'accès, et à déchiffrer le texte chiffré avec succès. Le système proposé permet d'assurer une préservation de la confidentialité des stratégies. Malgré cette préservation du système, mais, il n'a pas réduit le nombre de tests de déchiffrement pour les destinataires autorisés, l'adversaire est autorisé à interroger un numéro de ligne pour chaque attribut de son ensemble d'attributs. De plus, l'adversaire peut vérifier tous les attributs du système.
- **Efficient and privacy preserving access control scheme for fog-enabled IoT**
  Fan et al. [18], ont proposé un système de contrôle d'accès multi-autorité externalisée efficace et préservant la vie privée, appelé PPO MACS (Privacy Preserving Outsourced Multi-Authority Access Control Scheme). Tous les attributs des utilisateurs finaux sont transformés pour être anonymes et authentifiable afin de préserver la confidentialité des politiques des textes chiffrés. De plus, il adopte une méthode de décryptage externalisée pour réduire les frais de calcul du côté de l'utilisateur final. En outre, Fan et al. [18] ont fourni un système de révocation des utilisateurs pour garantir la flexibilité du système, le CSP (Cloud Service Provider) et les PS (Proxy Server) ne peuvent pas obtenir la clé secrète de l'utilisateur, ils ne peuvent donc pas décrypter complètement le texte chiffré pour récupérer le message. De plus, les utilisateurs révoqués ne peuvent pas obtenir le texte chiffré partiellement déchiffré correct car leurs clés proxy ont été supprimées. Enfin, le résultat de l'analyse de sécurité et de la simulation montre que ce protocole est performant. Mais, d'un autre côté ce modèle n'est pas scalable parce qu'il y a un seul administrateur.

2.4.2 Solutions basées sur les rôles

- **Policy-based access control for constrained healthcare resources in the context of the Internet of Things**
  Pal et al. [23], ont proposé un modèle de contrôle d'accès basé sur des attributs, des rôles et des

capacités pour la conception d'autorisation. Dans ce modèle, les attributs sont appliqués pour l'attribution d'appartenance à un rôle et dans l'évaluation des autorisations, cette appartenance à des rôles qui accorde des capacités qui peuvent être paramétrées sur la base d'autres attributs de l'utilisateur et sont ensuite utilisées pour accéder à des services spécifiques fournis par des dispositifs IdO. Le protocole proposé est piloté par XACML (eXtensible Access Control Markup Language). Pal et al. [23] ont implémenté un prototype de preuve de concept et fourni une analyse détaillée des performances de l'implémentation. Les résultats de l'évaluation montrent que cette approche nécessite un minimum de frais supplémentaires par rapport à d'autres propositions utilisant des capacités de contrôle d'accès dans l'IdO. Mais, la notion d'intéropérabilité n'est pas satisfaite et aussi il n'est pas fiable.

- **A secure and verifiable outsourced access control scheme in fog-cloud computing**
  Fan et al. [17], ont proposé un système de contrôle d'accès nommé VOMAACS (Verifiable Outsourced Multi-Authority Access Control Scheme) multi-autorité externalisée et vérifiable. Dans cette construction, la plupart des calculs de chiffrement et de déchiffrement sont externalisés, les dispositifs anti-fog et les résultats des calculs peuvent être vérifié à l'aide de la méthode de vérification externalisés. C'est-à-dire si un cloud renvoie des résultats incorrects, les utilisateurs peuvent le remarquer immédiatement en exécutant le programme. Pendant ce temps, pour résoudre le problème de révocation, ils ont conçu une méthode de révocation des utilisateurs et des attributs pour cela. En général, une couche de fog est ajoutée entre le serveur cloud et les terminaux afin que certains calculs sur le serveur cloud puissent être délégués aux périphériques du brouillard qui sont plus proches des terminaux. Ainsi, les différentes tâches de différentes régions peuvent être exécutées par les dispositifs de fog correspondants. Dans ce modèle, le contrôle d'accès est sécurisé contre les attaques de collusion mais, d'un autre côté ce modèle n'est pas scalable car il contient un seul administrateur central qui gère les différents accés.

2.4.3 Solution basée sur les ontologies

- **An ontology-based approach to improve access policy administration of attribute-based access control**
  Li et Zhang. [9], ont proposé un modèle de contrôle d'accès appelé ABAC (Attribute-Based Access Control) basé sur une ontologie O-A-BACM (Ontology-Attribute-Based Access Control Model), c'est un modèle qui est basé sur les attributs. L'accès à une ressource dans ce protocole est déterminé par une collection de plusieurs attributs. Il prend en compte les attributs d'utilisateur (attributs de sujet), les attributs de ressource (attributs d'objet) et les attributs environnementaux. Les attributs sont les caractéristiques des utilisateurs, des ressources et de l'environnement. Ce protocole contient trois types de relations entre les objets ABAC, y compris l'équivalence, l'inclusion et la disjonction, sont identifiés et décrits dans celui-ci. En outre, la représentation de la politique et le mécanisme de raisonnement sont discutés au sein de l'OABACM, s'il est équipé de raisonneurs appropriés. L'OABACM peut afficher naturellement certaines propriétés logiques inhérentes qui permettent de gérer la redondance et la cohérence des stratégies. Des différents scénarios expérimentaux sont testés pour démontrer l'efficacité de l'OABACM dans le traitement de la redondance des politiques et des conflits.
  L'avantage d'OABACM est qu'il permet de représenter les relations entre différentes classes afin

d'établir une hiérarchie, ce qui rendra les règles d'accès plus concises et plus claires. Mais, la notion d'alerte n'est pas satisfaite, c'est pourquoi le modèle est vulnérable aux attaques.

- **Certificate-based anonymous device access control scheme for IoT environment**
  Malani et al [21], ont proposé un système de contrôle d'accès aux appareils léger basé sur des certificats qui sont chargés dans les appareils intelligents avant leur déploiement dans l'environnement IoT, appelé DACS-IoT (Device Access Control Scheme-Internet of Thing). Les certificats pour les appareils intelligents sont uniquement crées par la clé privée du GWN de confiance. Le protocole proposé prend également en charge l'ajout d'un nouveau déploiement de dispositifs IdO après le déploiement initial dans un environnement IdO. Le DACS-IoT comprend quatre phases, à savoir la configuration, l'inscription des périphériques, le contrôle d'accès aux périphériques et l'ajout dynamique de périphériques. Pour analyser la sécurité du DACS-IoT, ils ont utilisés une analyse de sécurité formelle à l'aide du modèle ROR (Real-Or-Random) largement accepté, et une vérification de sécurité formelle basée sur la validation automatisée largement acceptée des protocoles et applications de sécurité Internet. L'objectif de protocole DACS-IoT est d'empêcher les appareils intelligents malveillants, qui peuvent être directement déployés sur le réseau ou qui peuvent être d'anciens appareils manipulés par un adversaire, de participer à l'environnement IdO. Mais, d'un autre coté l'interopérabilité n'est pas réalisée car le système ne peut pas fonctionner avec d'autres systèmes existants.
- **IoT-FBAC : Function-based access control scheme using identity-based encryption in IoT**
  Yan et al. [30], ont proposé un protocole de contrôle d'accès basé sur les fonctions utilisant le schéma IBE (Identity-Based Encryption), qui prend en charge un accès aux fonctions indépendant des appareils, appelé IoT-FBAC (Function-based access control scheme using identity-based encryption in IoT) afin d'empêcher l'accès à des privilèges excessifs. Ce protocole utilise une méthode de chiffrement basé sur l'identité (IBE) pour crypter les données générées par les appareils, qui est une primitive importante de la cryptographie à chiffrement à clé public. Dans la méthode IBE, la clé publique d'un utilisateur est l'information unique telle que l'identité. Le système lancera et générera des clés secrètes pour chaque utilisateur. Lorsqu'un expéditeur envoie un message à un destinataire, il crypte le message en utilisant l'identité du destinataire. Le destinataire obtiendra le message en utilisant la clé secrète. En utilisant le chiffrement IBE pour chiffrer les données avant de les télécharger sur le serveur cloud, ce qui garantit la confidentialité des données. Le protocole proposé empêche l'application d'accéder à des fonctions non autorisées telle que lorsqu'une application est installée sur le téléphone d'un utilisateur, l'utilisateur doit définir le privilège d'accès de cette application. Il ne peut accéder aux données de la fonction que si la fonction de l'appareil est autorisée, sinon il ne peut pas réussir. Enfin, l'analyse et les résultats démontrent que la confidentialité des données dans ce système est sécurisée. Mais, malgré la sécurité du système, le protocole n'est pas scalable car il contient un seul administrateur central qui gère les différents accés.

2.5 Synthèse et comparaison entre les solutions étudiées

Plusieurs protocoles ont été proposés pour contrôler l'accès au big data dans le contexte de l'Internet des objets. Notre étude des travaux existants nous a permis de classifier ces travaux selon le problème

traité : protocoles basés sur les rôles, protocoles basés sur les ontologies et protocoles basés sur la cryptographie, ce dernier nous a permis de les classifier en deux catégories telles que la certification et le chiffrement à base d'ABE. Cependant, chaque protocole se caractérise par un ensemble de points forts et de points faibles. En d'autres termes, nous avons remarqué que certains protocoles sont plus performants que d'autres, mais requièrent plus de ressources. Notre étude des travaux basés sur les certificats montre que les solutions proposées présentent l'avantage du contrôle d'accès mais, s'avèrent de faible efficacité du point de vue que la capacité de calcul des objets est très limité et ils ne peuvent pas utiliser les algorithmes complexes. Ce qui influence négativement sur les décisions d'accès qu'elles génèrent et fait que cette solution n'est pas la mieux adaptée pour le contrôle d'accès au big data dans l'IdO [11]. La plupart des travaux de recherche existants basés sur l'ABE sont appliqués pour le contrôle d'accès dans le cloud computing car ABE est flexible et évolutif pour appliquer les politiques à un grand nombre d'utilisateurs inconnus. Ainsi, qu'à assurer la confidentialité de données sur la base du chiffrement d'attribut. Celui-ci permet à tout utilisateur de déchiffrer le texte chiffré tant qu'il possède les attributs satisfaisant une politique d'accès. Cette fonctionnalité fait d'ABE une très populaire solution pour assurer la transmission, le stockage et le partage de données sécurisées dans l'environnement tel que l'IdO. De plus, 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. Seules les entités avec des attributs qui satisfont une politique d'accès aux données peuvent déchiffrer un texte selon que la clé privée ou le texte chiffré est associé à la politique de contrôle d'accès, le concept d'ABE est amélioré en proposant deux variantes, à savoir l'ABE de politique clé (KP-ABE) et l'ABE de texte chiffré (CP-ABE). La principale différence est que dans CP-ABE, la politique d'accès est incluse dans le chiffré et les attributs sont inclus dans la clé de déchiffrement, alors que dans KP-ABE, c'est exactement l'inverse [29]. Dans ce travail, nous proposons un protocole qui assure le contrôle d'accès au big data basé sur la cryptographie à base d'attributs (ABE) en choisissant la variante Ciphertext-Policy Attribute Based Encryption (CP-ABE), combiné avec le chiffrement à courbe elliptique (ECC) pour résoudre les problèmes de sécurité dans l'IdO. ECC est conçu pour faire le chiffrement/déchiffrement. Celle-ci reposant sur des clés de taille réduite, des temps de traitement raisonnables et des capacités de stockage moins importantes. Celui-ci est un moyen puissant de chiffrer des données personnelles. En revanche, les systèmes asymétriques utilisent deux clés, une pour chiffrer et une autre pour déchiffrer. RSA et ECC assurent le même niveau de sécurité mais, l'avantage du ECC c'est qu'il utilise des clés de taille réduite [1]. Par exemple, une clé ECC de 256 bits équivaut à des clés RSA de 3072 bits, qui sont alors 50% plus longues que les clés de 2048 bits couramment utilisées à l'heure actuelle.

Afin de mieux comprendre la diversité des protocoles étudiés dans ce chapitre et traitant le problème du contrôle d'accès, nous illustrons une étude comparative que nous avons menée sur les protocoles étudiés dans le tableau 2.1 :

		Résistance aux attaques	**Scalabilité**	**Intéropérabilité**	**Fiabilité**	**Utilisabilité**	**Performance**
Basés sur la cryptographie	Smithamol et Rajeswari. [14]	✗	✓	✗	✓	✗	✗
	Hao et al. [19]	✗	✓	✗	✓	✗	✓
	Fan et al. [18]	✓	✗	✗	✓	✗	✓
Basés sur les rôles	Fan et al. [17]	✓	✗	✗	✗	✓	✓
	Pal et al. [23]	✓	✗	✗	✗	✗	✓
Basés sur les ontologies	Li et Zhang. [9]	✗	✓	✓	✓	✗	✓
	Malani et al. [21]	✓	✓	✗	✗	✓	✓
	Yan et al. [30]	✓	✗	✓	✓	✗	✓

TABLE 2.1 – Comparaison des protocoles de contrôle d'accès aux big data

2.6 Conclusion

La sécurité dans l'Internet des objets est un domaine important, et un grand nombre de problèmes restent encore à être surmontés. Beaucoup de travaux ont été effectués afin d'avoir un modèle de contrôle d'accès performant qui assure un niveau élevé de sécurité. Dans ce chapitre, nous avons établi un état de l'art sur quelques protocoles de contrôle d'accès au big data dans l'Internet des objets. Pour ce faire, nous avons proposé une classification des solutions selon l'approche suivie. Ensuite, nous avons brièvement décrit chaque solution étudiée suivie d'une discussion des points forts et des points faibles. Enfin, nous les avons comparées selon les différents critères retenus.

Le chapitre suivant sera consacré à la description détaillée de notre modèle de contrôle d'accès au big data dans le contexte de l'IdO.

CHAPITRE 3

PRIVACY-PRESERVING ACCESS CONTROL SCHEME FOR BIG DATA IN IOT

3.1 Introduction

Au cours des dernières années, nous avons été témoins de l'excitation de l'Internet des objets, comprenant de nombreux appareils et applications physiques connectés. Bien que les appareils IdO disposent de ressources informatiques limitées notamment en termes du stockage, ils peuvent tirer parti des puissantes capacités et ressources du cloud pour faire face à ses contraintes technologiques. Avec des ressources informatiques sensiblement illimitées, une capacité de stockage à la demande à faible coût et des ressources disponibles de n'importe où, le cloud est une solution rentable et pratique pour compenser les contraintes technologiques de l'IdO. Cependant, le cloud offre un stockage flexible et rentable pour le big data, mais le défi majeur est le contrôle d'accès au big data. Celui-ci est un moyen important pour sécuriser les données et d'empêcher des fuites d'informations, chaque accès aux données doit être contrôlé et bien évidemment tous les accès non autorisés doivent être impérativement bloqués.

Dans ce chapitre, nous parlerons en premier lieu de ce qui nous a motivé à réaliser ce travail, puis nous décrirons l'architecture réseau détaillée de notre modèle de contrôle d'accès. Par la suite, nous présenterons le principe de notre protocole, puis nous terminerons par une analyse de sécurité du protocole proposé et une conclusion.

3.2 Motivation

Le "big data" est en pleine croissance grâce à l'Internet des objets, dont des milliers d'objets dans le monde se voient connecter les uns avec les autres en partageant des données avec les serveurs du Cloud. Le contrôle d'accès est l'un des principaux défis du big data à relever tant que les données collectées sont sensibles et doivent être confidentielles, pour cela nous avons choisi de proposer un modèle de contrôle d'accès qui permet d'empêcher l'accès des intrus et préserver l'intégrité des données. En effet, nous nous somme intéressées aux protocoles basés sur le chiffrement à base d'attributs (ABE), plus exactement CP-ABE (Ciphertext Policy Attribute Based Encryption). Cette technique est meilleure en termes de

sécurité que les autres techniques et prometteuse pour contrôler l'accès aux données massives [6]. Elle permet de crypter les données générées par les objets sous la politique d'accès définie sur quelques attributs de consommateurs de données. En outre, pour sécuriser la transmission et le stockage des données, CP-ABE fournit un contrôle d'accès détaillé et un partage flexible de données. D'autre part, nous nous somme focalisées sur le principe de courbes elliptiques. L'utilisation de ces dernières permet d'améliorer les primitives cryptographiques existantes, par exemple en construire de nouvelles primitives cryptographiques qui n'étaient pas connues auparavant. D'autre part les systèmes cryptographiques basés sur les courbes elliptiques permettent d'obtenir un gain en efficacité dans la gestion de clés. En effet, de tels crypto-systèmes utilisent des clés de taille beaucoup plus modeste, ce qui représente un avantage pour les systèmes utilisant des dispositifs à faibles ressources et dont l'espace mémoire est très limité. De plus, les algorithmes de calculs liés aux courbes elliptiques sont plus rapides, et ont donc un débit de génération et d'échange de clés beaucoup plus rapide [8].

3.3 Modèle de système

La figure 3.1, illustre le modèle de système pris en compte dans notre travail. Le système que nous proposons comprend cinq éléments essentiels, à savoir : (1) **Propriétaire de données :** pour économiser les coûts de stockage et les calculs locaux, les propriétaires de données externalisent leurs données, qui sont générées par les appareils IdO, vers le fog d'une manière sécurisée. Puis ils les envoient au serveur du Cloud pour stocker ses données privées, c'est le seul à avoir le droit de donner accès à ses données, (2) **Nœud fog :** dans notre architecture le fog est utilisé comme intermédiaire entre les propriétaires de données et le serveur du Cloud où les objets de l'IdO vont envoyer leurs données au fog au lieu de les envoyer au serveur Cloud, (3) **Fournisseur de services cloud :** est en charge du stockage de données massives cryptées, de la liste des attributs anonymes et de la liste des clés proxy appartenant aux consommateurs de données. Il gère également les demandes d'accès aux données des patients et effectue une opération d'attribution et de mise à jour des utilisateurs pour l'utilisateur révoqué, (4) **Consommateur de données :** chaque utilisateur de données a une liste d'attributs pour décrire son droit. Les informations d'attribut sont implicitement incluses dans la clé secrète. Le consommateur de données effectue une recherche par mot-clé sur les données chiffrées avec les étapes suivantes : Tout d'abord, le consommateur de données obtient la clé secrète de l'autorité de confiance. Deuxièmement, étant donné un mot-clé, le consommateur de données génère une requête valide et la soumet au serveur cloud. Seuls les consommateurs de données dont l'ensemble d'attributs satisfait la stratégie d'accès spécifiée peuvent générer une requête valide. Dans la phase de recherche, le serveur cloud effectue une recherche par mot-clé sur les données chiffrées et récupère les informations correspondantes, (5) **Autorité de confiance (AC) :** est responsable de la génération et de la distribution des paramètres publics et des clés privées pour tous les utilisateurs du cloud en ce qui concerne leurs informations d'identification associées. elle est responsable aussi de l'émission d'attributs correspondant aux caractéristiques des consommateurs de données, la fourniture d'une identité unique correspondant aux attributs de chaque utilisateur et la génération d'une clé secrète et publique correspondante à chaque attribut. De plus, AC maintient la liste des attributs correspondant à chaque consommateur de données.

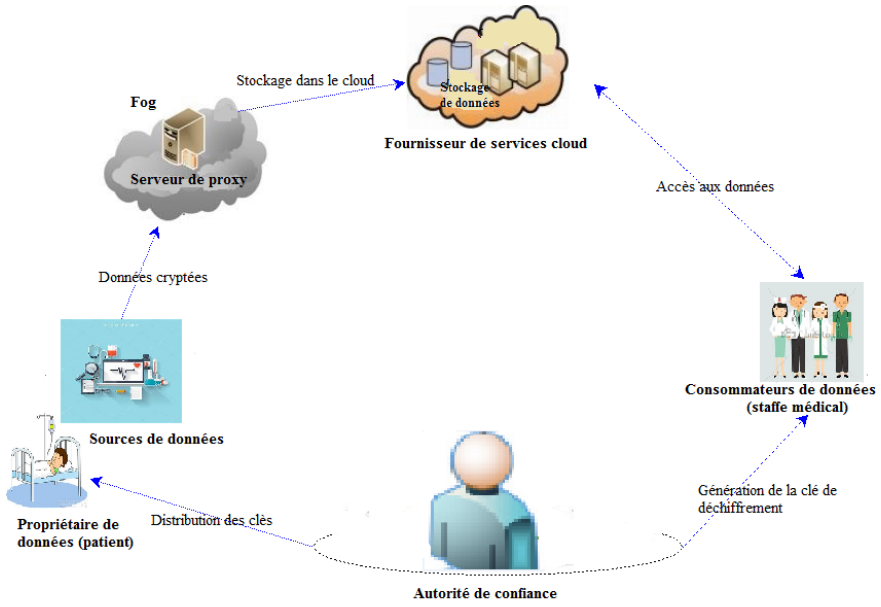


FIGURE 3.1 – Notre modèle de système.

3.4 Modèle de menace

Afin de mieux sécuriser notre modèle de système, nous avons dressé un inventaire des menaces qui pourraient affecter son bon fonctionnement, nous les résumons comme suit :

L'analyse de notre modèle système nous a permis de dégager une première menace induite par le canal de communication. Souvent on utilise des communications sans fil, qui peuvent être facilement interceptables. En outre, un attaquant peut écouter, supprimer, et modifier un message, dans lequel il peut être la cible d'entités malveillantes. Il peut également faire l'objet d'une fuite d'informations personnelles par inadvertance. Nous pouvons aussi dégager une autre menace qui est l'attaque de collision, c'est une attaque sur une fonction de hachage cryptographique tel que l'attaquant tente de trouver deux entrées de cette fonction qui produisent le même résultat (appelé valeur de hachage), c'est-à-dire qui résultent en une collision.

3.5 Notions préliminaires

Dans cette section, nous rappelons quelques définitions de base pour comprendre le protocole proposé :

A. Structure formelle du CP-ABE

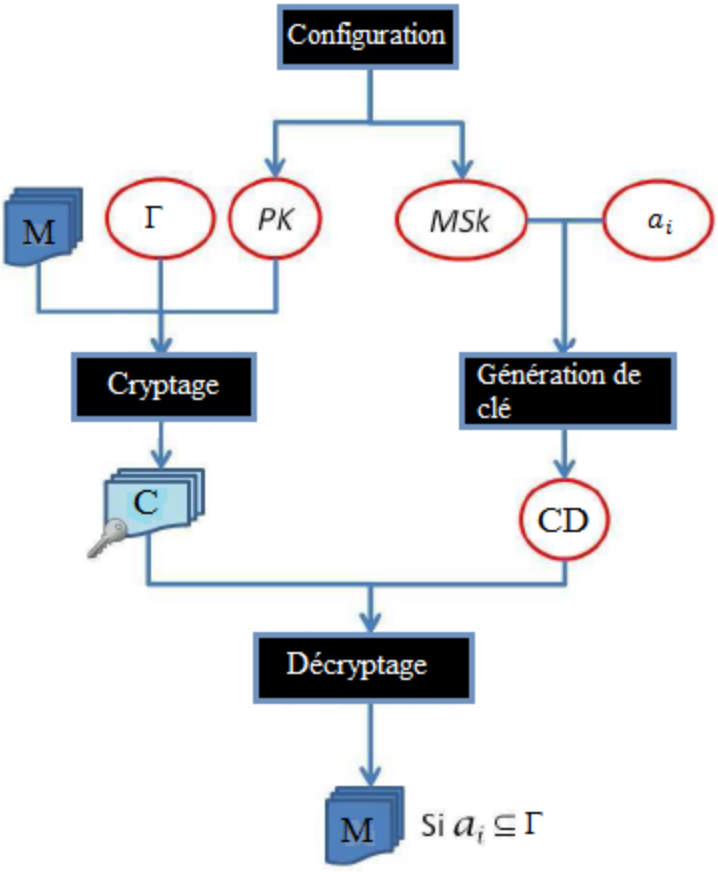
CP-ABE proposée pour la première fois par Bethencourt et al. [6] en 2007, dans laquelle la politique d'accès est intégrée dans le texte chiffré et les clés secrètes sont générées avec un ensemble d'attributs décrivant l'utilisateur légitime qui pourra déchiffrer ce texte. Seules les clés secrètes avec un ensemble d'attributs peuvent récupérer le texte en clair [29]. Comme illustré dans la figure 3.2, le schéma CP-ABE comprend quatre algorithmes suivants [12] :

1. **Configuration :** cet algorithme ne prend aucune entrée autre que les paramètres implicites de sécurité. Il donne en sortie : la clé publique PK et la clé secrète principale MSK.

2. **Cryptage :** cet algorithme prend en entrée la clé publique PK, un message à chiffrer M, et un arbre d'accès Γ qui définit tous les ensembles d'attributs possibles qui vont permettre le déchiffrement et l'accès au message M. Il donne en résultat le chiffrement du message M, l'arbre d'accès Γ, et d'autres informations nécessaires au déchiffrement de la donnée.

3. **Génération de clé :** cet algorithme prend comme entrée la clé secrète principale MSK, et un ensemble d'attributs a_i qui définit un utilisateur. Il donne en sortie une clé de déchiffrement CD.

4. **Décryptage :** cet algorithme prend en entrée la clé publique PK, le message chiffré C et d'autres informations telles que l'arbre d'accès Γ et une clé de déchiffrement CD, qui est spécifique à un certain ensemble d'attributs a_i. Si ce dernier satisfait l'arbre d'accès Γ, l'algorithme va être capable de déchiffrer le message.



:

FIGURE 3.2 – Schéma fonctionnel du CP-ABE [29].

B. Cryptographie à courbe elliptique

La cryptographie à base des courbes elliptiques (ECC) s'est finalement avérée être une construction mathématique intéressante dans un cryptosystème à clé publique bien établi. Ce genre de cryptographie est déjà inclus dans de nombreuses normes. En fait, ECC est maintenant une technique usuelle, qui a pu résister à de longues séries d'attaques, ce qui la marque comme un cryptosystème mûr et robuste. La cryptographie par courbe elliptique est une approche de cryptographie à clé publique, basée sur la structure algébrique des courbes elliptiques à corps finis. L'utilisation de ces courbes dans la cryptographie a été suggérée la première fois par S. Miller en 1985 [22]. ECC a un certain nombre d'avantages par rapport à d'autres cryptosystèmes à clé publique telle que RSA. En particulier, pour un niveau indiqué de sécurité, la taille des clés cryptographiques et les opérandes impliqués dans le calcul des cryptosystèmes à courbes elliptiques sont normalement beaucoup plus courts que dans d'autres crypto-systèmes. Ceci est dû à la puissance informatique disponible pour la cryptanalyse qui grandit et cette différence devient de plus en plus apparente. C'est un état avantageux particulièrement pour des applications où les ressources telles que la mémoire et/ou la puissance de calcul sont limitées [20].

Une courbe elliptique E est définie sur un corps fini F_p, où p est le cardinal du corps, par l'équation suivante :

$$y^2 \bmod p = x^3 + ax + b \bmod p, \tag{3.1}$$

Où, a et b sont des nombres entiers répondant à la condition suivante :

$$4\ a^3 + 27\ b^2 \bmod p \neq 0. \tag{3.2}$$

Les constantes a et b ainsi qu'un point générateur G appartenant à la courbe, constituent en grande partie les paramètres du domaine de la cryptographie par les courbes elliptiques [16].

Les différents protocoles de chiffrement se basent sur des problèmes algorithmiques dit difficiles. La difficulté à résoudre nous renvoie à la définition de la sécurité calculatoire asymptotique, dans le contexte de la cryptographie. En effet, ce sont des problèmes algorithmiques qui supposent qu'aucun algorithme s'exécutant en un temps polynomial ne peut résoudre ce problème avec une probabilité non négligeable (à un niveau asymptotique) [29], et parmi les problèmes de calcul existant sur le groupe de courbes elliptiques on trouve [10] :

- **Définition** 1 **:** Problème du logarithme discret de courbe elliptique (ECDLP) étant donné un tuple $(P, Q) \in_{G_p}$, il est difficile à calculer par un algorithme limité dans le temps polynomial de trouver un entier $k \in [1, n-1]$ tel que $Q = k \cdot P$[28, 35, 36].
- **Définition** 2 **:** Problème de calcul Diffie-Hellman (CDHP) étant donné un tuple $(P, a \cdot P, b \cdot P) \in_{G_p}$ pour toute $a, b \in [1, n-1]$, le calcul de $a \cdot b \cdot P$ est difficile par un algorithme limité dans le temps $\mathtt{polynomial}$[28, 35, 36].
- **Définition** 3 **:** Problème de factorisation de courbe elliptique (ECFP) étant donné un tuple $(P, Q) \in_{G_p}$, où $Q = a \cdot P + b \cdot P$ et $a, b \in [1, n-1]$. Le calcul de $a \cdot P$ et $b \cdot P$ est difficile par un algorithme limité dans le temps $\mathtt{polynomial}$[28].

C. Structure d'accès dans le contexte d'ABE

- **Définition**

  Soit $\{A_1, A_2, ..., A_n\}$ un ensemble d'attributs. Une collection $A \subseteq 2^{\{A_1, A_2, ..., A_n\}}$ est dit monotone, si $\forall$ B, C, si nous avons B $\in$ A et B $\subseteq$ C alors, C $\in$ A. Une structure d'accès (ou-bien, une structure d'accès monotone) contient une collection (respectivement, une collection monotone) de A, sous-ensemble non vide de $\{A_1, A_2, ..., A_n\}$.

  L'ensemble A est appelé l'ensemble des éléments autorisés et les éléments qui ne sont pas dans A sont appelés les éléments non-autorisés.

  Dans la définition originale de Beimel [5], l'ensemble d'attributs est désigné par un ensemble de parties. Dans notre cas, la structure d'accès A est appelée structure d'accès monotone si elle ne contient pas la négation des attributs. Si c'est le cas, on l'appelle structure d'accès non monotone. Dans la suite de ce mémoire, nous considérerons uniquement les structures d'accès monotones.

  Dans la littérature relative à ABE, la structure d'accès prend généralement la forme d'un arbre d'accès, noté τ. La Figure 3.3, illustre un tel arbre pour un exemple de politique d'accès simple : $P = Att_1$ OR $((Att_2$ AND $Att_3)$ OR $(Att_4$ AND $Att_5))$. Chaque feuille représente un attribut et chaque nœud interne est une porte logique (AND, OR) [29].

  Pour définir l'arborescence d'accès, les notations suivantes sont présentées :

  1) **parent(x) :** parent du nœud x, par exemple : OR ;

  2) **attr(x) :** attribut associé au nœud x, par exemple : utilisateur 1 : Att5, Att4 ;

  3) **num(x) :** nombre d'enfants du nœud x, par exemple : AND : 2 enfants ;

  4) **index(x) :** nombre associé au nœud x (ce nombre correspond à l'ordre des enfants de chaque nœud dans l'arbre), par exemple : Att4 : 2 ;

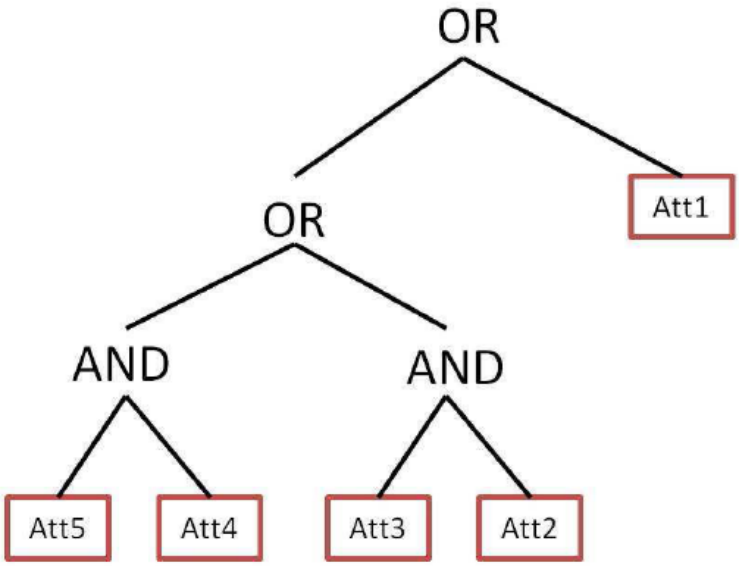


FIGURE 3.3 – Arbre d'accès pour un exemple de politique simple.

3.6 Notre contribution

Dans cette section, nous donnons un bref aperçu sur notre politique d'accès aux signes vitaux du patient, puis nous donnons la description détaillée de notre protocole.

3.6.1 Notre politique d'accès aux informations médicales d'un patient

Comme le montre la figure 3.4, notre politique s'adapte à la structure expressive de la spécification de politique qui contient les rôles (médecin, infirmier, aide soignant), les attributs et les privilèges de chaque rôle. Cette politique se présente sous forme d'un arbre d'accès composé de portes "AND" et "OR" et d'attributs. Chaque nœud interne de l'arbre d'accès est une porte logique (porte and, porte OR) et le nœud feuille contient un attribut. Seuls les individus possédant des attributs qui satisfont l'arbre d'accès sont en mesure de déchiffrer le contenu. Ainsi, pour accéder aux informations médicales, en accord avec l'arbre d'accès de la figure 3.4, la personne doit être médecin, infirmier ou aide-soignant, et remplir l'une des deux conditions au choix : faire partie de CHU de Bejaia et du service de pneumologie ou de CHU de Sétif et du service de pneumologie. Le fait de contrôler l'accès à un document par chiffrement permet d'assouplir les conditions de stockage (dans un cloud par exemple), l'hébergeur n'ayant pas accès aux contenus en clair. L'autre avantage du schéma est directement lié à l'utilisation de l'arbre d'accès qui offre beaucoup de flexibilité dans la formulation de la politique d'accès et une meilleure protection des données personnelles car, même en cas de déchiffrement d'un document, il est impossible de déduire précisément la liste des attributs détenus par l'individu.

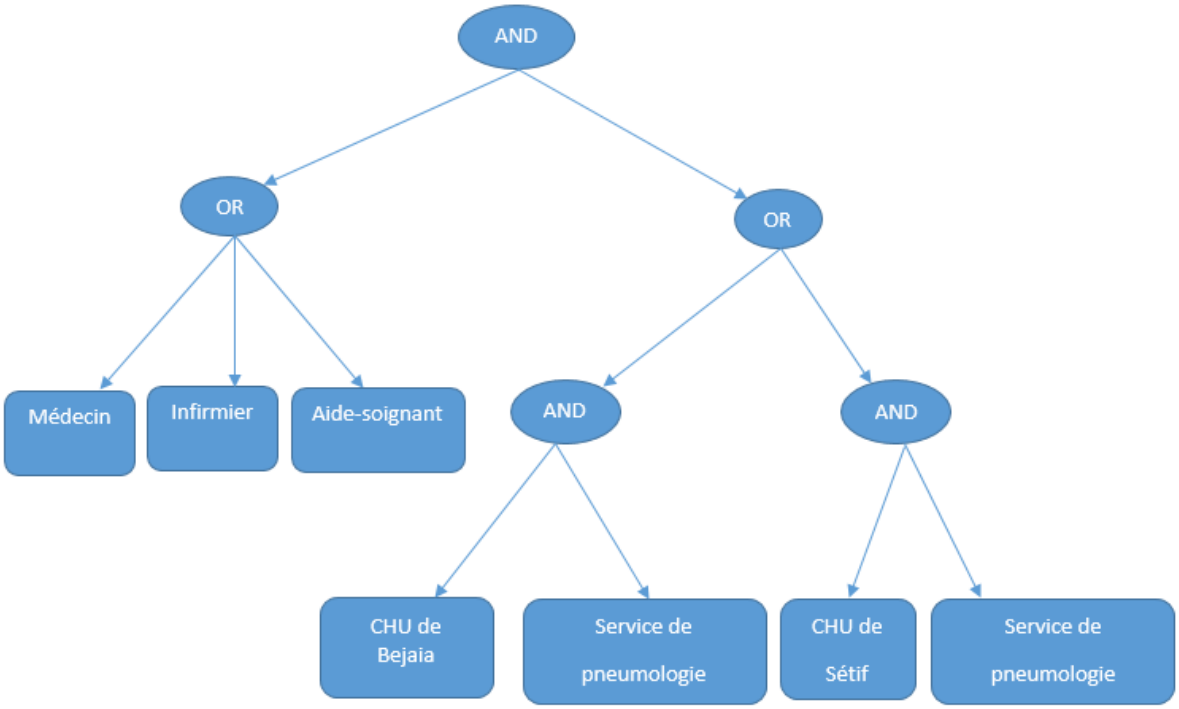


FIGURE 3.4 – Notre politique d'accès aux informations médicales d'un patient.

3.6.2 Description détaillée de notre protocole

Dans cette section, nous présentons notre protocole de contrôle d'accès au big data. Il se dévise en trois phases distinctes à savoir : phase d'initialisation du système, phase d'enregistrement de données, et phase d'autorisation d'accès. Une explication détaillée de ces trois phases, un organigramme ainsi qu'un tableau de notations utilisées dans notre protocole sont présentées dans ce qui suit :

Symbole	**Signification**
Con_i	Consommateur de données
M	Message en clair
C	Message chiffré
a_i	Ensemble d'attributs du consommateur de données i
PK	Clé publique principale de AC
MSK	Clé secrète principale de AC
PKA_i	Clé publique de consommateur de données
SKA_i	Clé secrète de consommateur de données
PKB_i	Clé publique de l'objet IdO
SKB_i	Clé secrète de l'objet IdO
P	Politique d'accès
Γ	Arbre d'accès
QSK_i	Clé symétrique partagée entre l'objet i et le fog
SK_i	Clé symétrique partagée entre le consommateur de données i et AC
AC	Autorité de Confiance
CD	Clé de déchiffrement
$E(a, b)$	Courbe elliptique
n	Grand nombre
F_p	Corps fini de cardinal p
G	Point de base
m_c	Mot clé
id_i	Identifiant du consommateur de données i
Q	Point dans la courbe elliptique
(A, R)	Matrice d'accès
$h(.)$	Fonction de hachage à sens unique sécurisée
T_1/T_2	Estampille à deux instants différents
ΔT	Intérvalle du temps valide
$(+, -, \cdot)$	Opérations d'addition, soustraction, multiplication dans les courbes élliptiques.

TABLE 3.1 – Notations utilisées dans le protocole proposé

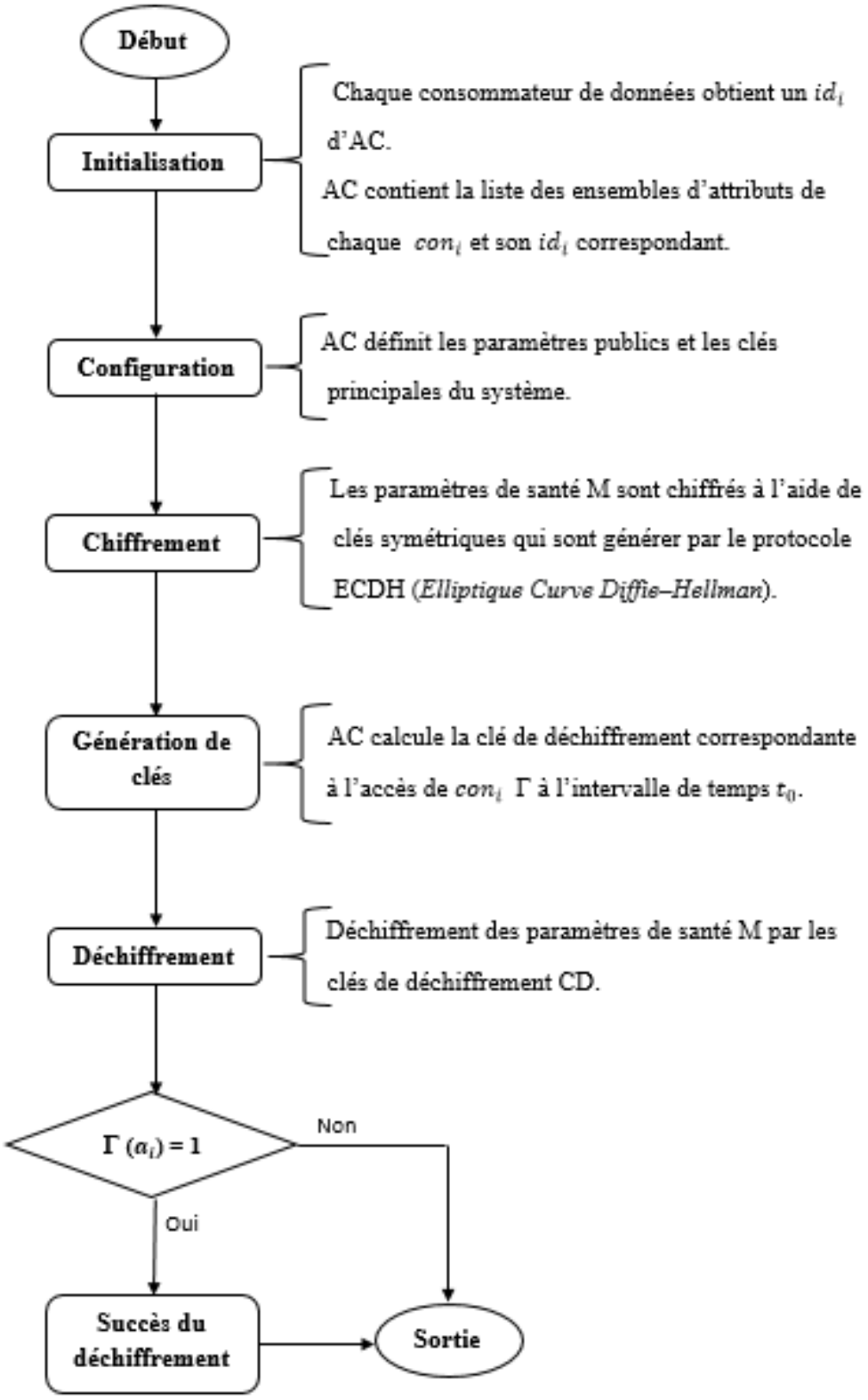


FIGURE 3.5 – Organigramme du protocole proposé CP-ABE.

— **Phase 1, Initialisation du système :**
Cette première phase est primordiale pour le déroulement correct de notre protocole. Elle permet entre autre, de s'entendre sur une courbe elliptique et de générer les clés privées de chaque objet, AC est la responsable de la génération et de la distribution des paramètres publics et des clés privées pour tous les consommateurs de données.
Dans notre protocole, chaque consommateur de données Con_i possède un ou plusieurs attributs qui sont gérés par l'autorité de confiance. Cette dernière définit les attributs pour chaque consommateur de données et génère une paire de clés pour chaque attribut.
Initialement, les objets IdO se mettant publiquement d'accord sur une courbe elliptique E(a,b) définie sur l'intervalle $[1, n-1]$, et ils se mettent aussi d'accord sur un point générateur G, une fois la courbe définie et le point générateur choisi, le protocole Diffie-Hellman basé sur les courbes elliptiques (ECDH) stipule qu' AC génère deux clés symétriques, QSK_i partagée entre l'objet IdO et le fog et SK_i partagée entre l'autorité de confiance et le consommateur de données i. En outre, AC génère sa paire de clés (PK, MSK) en choisissant un nombre atléatoire dans l'intervalle $[1, n-1]$ comme clé privée MSK, elle en dérive ensuite sa clé publique $PK = (MSK, G)$ où $PK = MSK \cdot G$. Puis, en suivant les mêmes étapes AC génère une paire de clés (PKA_i, SKA_i) pour le consommateur de données en choisissant un nombre aléatoire dans l'intervalle $[1, n-1]$ comme clé privée SKA_i, elle en dérive ensuite sa clé publique $PKA_i = (SKA_i, G)$ où $PKA_i = SKA_i \cdot G$, et de la même façon elle génère une paire de clé (PKB_i, SKB_i) pour l'objet IdO.
Après la génération des clés l'autorité de confiance distribue les clés pour tous les utilisateurs.

— **Phase 2, Enregistrement de données :** lors de cette phase, les objets IdO ont la capacité de mesurer les paramètres de santé sur le corps du patient à savoir : la température, la pression artérielle, le taux d'oxygène dans le sang, ECG, EMG, etc. Avant qu'un objet IdO_i envoie les paramètres de santé qu'il a collectée au fog, il les chiffre avec la clé symétrique QSk_i puis il envoie la requête $< M_{QSk_i}, T_1 >$ au fog. À la réception du message $< M_{QSK_i}, T_1 >$, le fog compare T_1 reçu avec son estampille T_2 actuel comme suit : $|T_2 - T_1| \leqslant \Delta T$, ou ΔT est l'intervalle de temps valide pour un délai de transmission, si ce n'est pas vérifié, il rejette la demande d'œverture de session. Sinon, il déchiffre les données envoyées avec la même clé symétrique QSk_i. Ensuite, ce dernier chiffre le message M en utilisant l'algorithme de chiffrement 1 chiff $(M, (A, R), PK_i, \Gamma)$ puis il envoie le résultat obtenu $<C>$ au cloud.
À la réception de ce message chiffré C, le cloud vérifie sa fraîcheur puis il le stocke.

Algorithm 1 chiff

Entrées: M, (A, R), PK, Γ ;
Sorties: C ;

1: Le fog choisit $s \in [1, n-1]$;
2: Le fog calcule $C_0 = Q + S \cdot P$;
3: Le fog choisit un vecteur $v \in [1, n-1]^l$;
4: Le fog calcule $\lambda_x = A_x \cdot v$;
5: Le fog choisit un vecteur $u \in [1, n-1]^l$;
6: Le fog calcule $w_x = A_x \cdot u$;
7: Le fog calcule $C_{1,x} = \lambda_x \cdot G + w_x \cdot Pk_{R(x)}$, $C_{2,x} = w_x \cdot G, \forall x$;
8: **Return** C ;

— **Phase 3, Autorisation d'accès :** lorsqu'un consommateur de données Con_i souhaite accéder aux données stockées dans le cloud, il envoie une requête $< m_c, id_i, P_{SK_i}, T_3 >$ à l'autorité de confiance AC pour lui générer une clé de déchiffrement CD. À la réception de la requête $< m_c, id_i, P_{SK_i}, T_3 >$, AC vérifie sa fraîcheur en comparant T_3 reçu avec son estampille T_4 actuel comme suit : $|T_4 - T_3| \leqslant \Delta T$, si cette condition n'est pas vérifié AC rejette la demande d'œverture de session, sinon elle vérifie si ce consommateur de données Con_i ouvre droit d'accéder aux données stockées dans le cloud. Dans le cas positif, elle sollicite l'algorithme 2 keygen (MSK, a_i, id) pour générer une clé de déchiffrement au Con_i. Ensuite, AC envoie la clé de déchiffrement généré sous la requête $< P, CD_{SK_i}, T_5 >$.

À la réception de cette requête le consommateur de données Con_i vérifie sa fraîcheur en comparant T_5 reçu avec son estampille T_6 actuel comme suit : $|T_6 - T_5| \leqslant \Delta T$, si cette condition n'est pas vérifié Con_i rejette la demande d'œverture de session, sinon il déchiffre la clé de déchiffrement CD avec sa clé symétrique SK_i.

Après avoir récupéré la clé de déchiffrement CD, le consommateur de données envoie au cloud une requête $<m_c, id_i>$, une fois le cloud a reçu cette demande il effectue une recherche par mot-clé sur les données chiffrées et récupère les informations correspondantes, puis il les envoie au consommateur de données mais elles sont toujours chiffrées, ce dernier exécute l'algorithme 3 de déchiffrement (C, $CD_{i,id}$) pour déchiffrer et accéder aux données du patient.

Algorithm 2 keygen

Entrées: MSK ; id ;
Sorties: CD_i ;

1: Pour $i = 1 \cdots n$;
2: AC choisit un entier $K \in [1, n-1]$;
3: AC calcule $CD_{i,id} = K_i + H(id) \cdot MSK$;
4: **Return** $CD(i, id)$;

Algorithm 3 Déchiffrement

Entrées: C ; $CD_{i,id}$;
Sorties: M ;

1: Con_i choisit A_x de A tel que $(1, 0, 0, \cdots, 0) \in A_x$;
2: Si AC possèdent ces attributs en fonction de a_i ;
3: Pour chaque $(C_{2,x,R(x)})$, AC calcule $\Sigma C_{2,x} \cdot CD_{R(x),id} = \Sigma(w_x \cdot G(k_{R(x)} + H(id) \cdot MSK$
$= \Sigma(w_x \cdot k_{R(x)} \cdot G + w_x \cdot H(id) \cdot MSK \cdot G$;
4: Con_i calcule $\Sigma C_{1,x} - \Sigma C_{2,x} \cdot CD_{R(x),id} = \Sigma(\lambda_x \cdot G + w_x \cdot Pk_{R(x)}) - \Sigma(w_x \cdot k_{R(x)} \cdot G + w_x \cdot H(id) \cdot MSK \cdot G)$
$= \Sigma(\lambda_x \cdot G - w_x \cdot H(id) \cdot MSK \cdot G)\ \forall\ x$;
5: Con_i sélectionne les constantes $c_x \in [1, n-1]$ tel que $\Sigma_x c_x \cdot A_x = (1, 0, \cdots, 0)$;
6: Con_i Calcule $\Sigma_x c_x(\lambda_x \cdot G - w_x \cdot H(id) \cdot MSk \cdot G) = s \cdot G$ Où, $v \cdot (1, 0, \cdots, 0) = s$ et $u \cdot (1, 0, \cdots, 0) = 0$;
7: Con_i Calcule $C_0 - s \cdot G = M$;
8: **Return** M ;

3.7 Analyse de sécurité

Dans cette section, nous passons à l'analyse des propriétés de sécurité de la solution proposée afin de montrer qu'elle est résistante aux types d'attaques suivantes :

3.7.1 Attaque de rejeu (Replay attack)

L'attaque par rejeu est une action offensive par laquelle un adversaire peut jouer le rôle d'un patient légitime en réutilisant une information obtenue à partir d'un processus précédent du protocole.

Dans notre protocole le message $< M_{QSk_i}, T_1 >$ envoyé au fog est déchiffré par la clé symétrique partagée entre le fog et les capteurs IdO, donc le message ne peut être déchiffré que par le fog. Si un adversaire veut modifier un ancien message il ne peut modifier le paramètre de temps inclus dans ce message, ce qui fait le fog détecte facilement qu'il s'agit d'une attaque par rejeu car $|T_2 - T_1| > \Delta T$.

3.7.2 Attaque de l'homme au milieu (Man in the middle attack)

Dans l'attaque de l'homme du milieu, un intrus malveillant s'interpose entre deux entités communicantes, se faisant passer pour l'une et l'autre à leur insu, et obtient l'accès aux informations que les deux parties s'échangent. Dans notre protocole, lors de l'émission d'une quelconque requête, cette dernière est accompagnée d'une clé, ce qui permet une authentification directe du demandeur de service. même si un attaquant essaie de s'interposer entre les deux parties, il n'aura aucun moyen de se faire passer pour l'une comme pour l'autre. Par exemple, si un attaquant essaie de s'interposer entre les deux parties communicantes, il n'aura aucun moyen de se faire passer pour l'une comme pour l'autre, car une authentification est effectuée entre chaque objet et l'utilisateur qui veut accéder.

3.7.3 Résistance aux collisions

Une attaque de collisions est une attaque sur une fonction de hachage cryptographique qui tente de trouver deux entrées de cette fonction qui produisent le même résultat. Dans notre protocole, il n'est pas possible pour les différents consommateurs de données de combiner leurs ensembles d'attributs afin d'accéder aux données médicales. Même si les adversaires utilisent un attribut ayant le même nom et la même valeur de l'autorité de confiance, ils ne peuvent pas collaborer avec l'utilisateur légal dans l'autorité partagée des données cibles. Ceci est dû au fait que chaque attribut possède sa propre clé publique, son identifiant unique. En outre, la liste d'attributs et l'ensemble de clés secrètes d'attributs sont échangées via un canal sécurisé. Cela empêche l'attaque de collision des adversaires.

3.8 Conclusion

La gestion du contrôle d'accès au big data est un problème difficile à résoudre dans l'Internet des Objets, dû à la vitesse d'envoi, le volume et la variété de données. La recherche d'un modèle de contrôle d'accès dans un domaine en pleine croissance telle que le "big data" est en émergence grâce à l'Internet des Objets, dont des milliers d'objets dans le monde se voient connecter les uns avec les autres et avec le serveur du Cloud. Donc, assurer le contrôle d'accès et la bonne gestion de ces données massives générées par ces appareils intelligents, aussi celles produites par l'homme sont une question stimulante qui n'est pas

encore résolue, dû au volume et à la diversité de données sensées être confidentielles. Dans ce chapitre, nous avons présenté en détail le principe de notre approche. En résumé, notre solution consiste à combiner la cryptographie à courbe elliptique avec le protocole CP-ABE permettant de garantir la confidentialité des échanges entre les différents points d'accès du réseau. Cette dernière représente un des éléments pouvant masquer les informations d'identité de l'utilisateur afin de préserver la confidentialité de l'utilisateur ou de l'organisation. Il peut protéger les informations de l'utilisateur contre les abus de la part d'un attaquant, mais également protéger contre les attaques malveillantes.

Le chapitre suivant sera consacré à l'évaluation de performances du protocole proposé.

CHAPITRE 4

SIMULATION ET ÉVALUATION DE PERFORMANCES

4.1 Introduction

Après avoir décrit les différentes phases de notre architecture dans le chapitre précédent, une évaluation des performances s'impose afin de démontrer par une expérimentation et à travers des simulations la performance de notre protocole.

Ce chapitre est consacré à l'évaluation des performances du protocole de contrôle d'accès que nous avons proposé. Nous présenterons en premier lieu l'environnement et les paramètres de simulation considérés pour l'évaluation. Nous décrirons par la suite le critère et les métriques de simulation utilisés. Les résultats obtenus à l'issue de ces simulations seront finalement interprétés et comparés avec un protocole récent étudié dans le chapitre de l'état de l'art.

4.2 Environnement de simulation

Dans cette section, nous présentons au préalable les paramètres de simulation, puis nous décrivons le critère et les métriques de simulation utilisés.

4.2.1 Paramètres de simulation

Notre protocole de contrôle d'accès a été simulé sous le langage de programmation Java. Il s'exécute en trois phases, dans chaque phase un ensemble d'opérations est effectué. Dans la phase d'initialisation nous avons appliqué les opérations de multiplication d'ECC (Elliptic Curve Cryptography) pour générer les paires de clés des utilisateurs. Dans la phase d'enregistrement de données nous avons chiffré les paramètres de santé collectée avec une clé symétrique pour les envoyés au fog puis on chiffre le message avec ECC. Puis, dans la phase d'autorisation d'accès, nous avons déchiffré les paramètres de santé collectés avec une clé de déchiffrement en appliquant les opérations d'ECC afin de récupérer les données chiffrées pour avoir les données en clair.

Pour évaluer les performances de notre protocole, ainsi que celles du protocole de comparaison, nous avons utilisé la taille de la clé générée par les courbes elliptiques à 224 bits. Puis, nous avons constaté

l'évolution de temps de chiffrement et de déchiffrement de chacune des opérations utilisées.

4.2.2 Critère et métriques de simulation

Dans cette section, nous présentons le critère et les métriques de simulation que nous avons utilisé pour l'évaluation des performances de notre protocole.

4.2.2.1 Critère de simulation

Le critère de simulation utilisé pour l'évaluation de performances de notre protocole est le nombre d'attributs. Dans l'IdO, le nombre d'objets est très grand. Le nombre d'attributs connectés se trouve être un paramètre important à prendre en compte vu son influence sur les temps de chiffrement, et le temps de déchiffrement.

4.2.2.2 Métriques de simulation

Afin d'évaluer les performances de notre protocole, nous utilisons les métriques de simulation suivantes : temps de chiffrement, et temps de déchiffrement.

- **Temps de chiffrement :** le temps de chiffrement est une métrique importante à mesurer dans notre protocole. En effet, elle représente la durée nécessaire pour que les données générées par les objets arrivent à l'utilisateur d'une manière sécurisée c'est-à-dire chiffrées en effectuant les différents algorithmes de chiffrements possibles.
- **Temps de déchiffrement :** le temps de déchiffrement c'est le temps de récupération des données en clair, il représente le temps nécessaire pour que la requête d'accès des consommateurs de données soit satisfaite auprès du serveur du Cloud, c'est-à-dire le temps qu'il faut pour télécharger les données chiffrées et les déchiffrer.

4.3 Résultats et discussion

Dans cette section, nous nous sommes intéressés à comparer les performances d'un protocole étudié dans le chapitre de l'état de l'art avec celles de notre proposition. Dans ce qui suit, nous présentons les résultats sous forme de graphiques puis nous les interprétons.

La figure 4.1 illustre la variation de temps de chiffrement en fonction du nombre d'attributs pour notre protocole et celui d'Hao et al. [19].

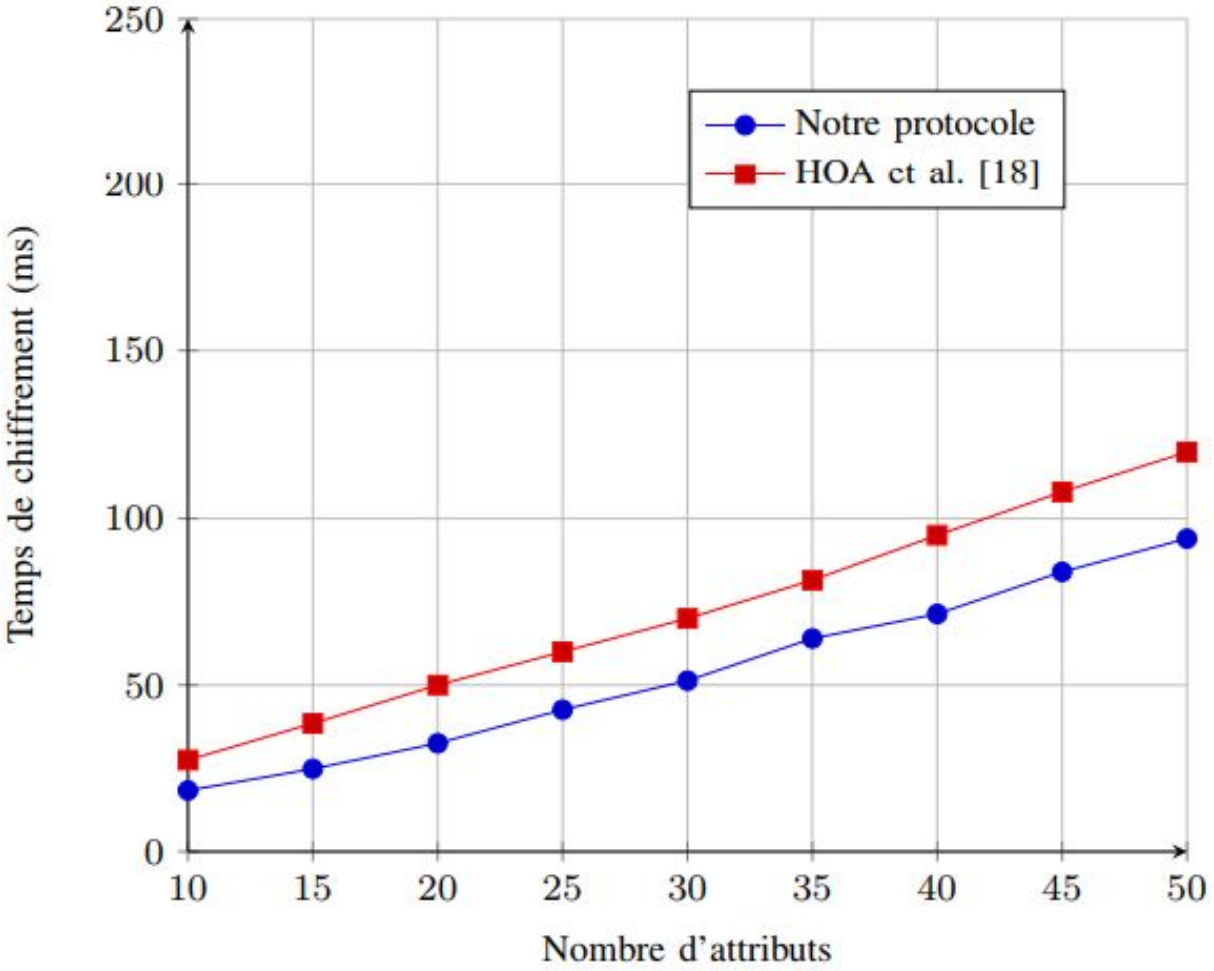


FIGURE 4.1 – Temps de chiffrement en fonction du nombre d'attributs.

La figure 4.2 illustre la variation de temps de déchiffrement en fonction de nombre d'attributs pour notre protocole et celui d'Hao et al. [19].

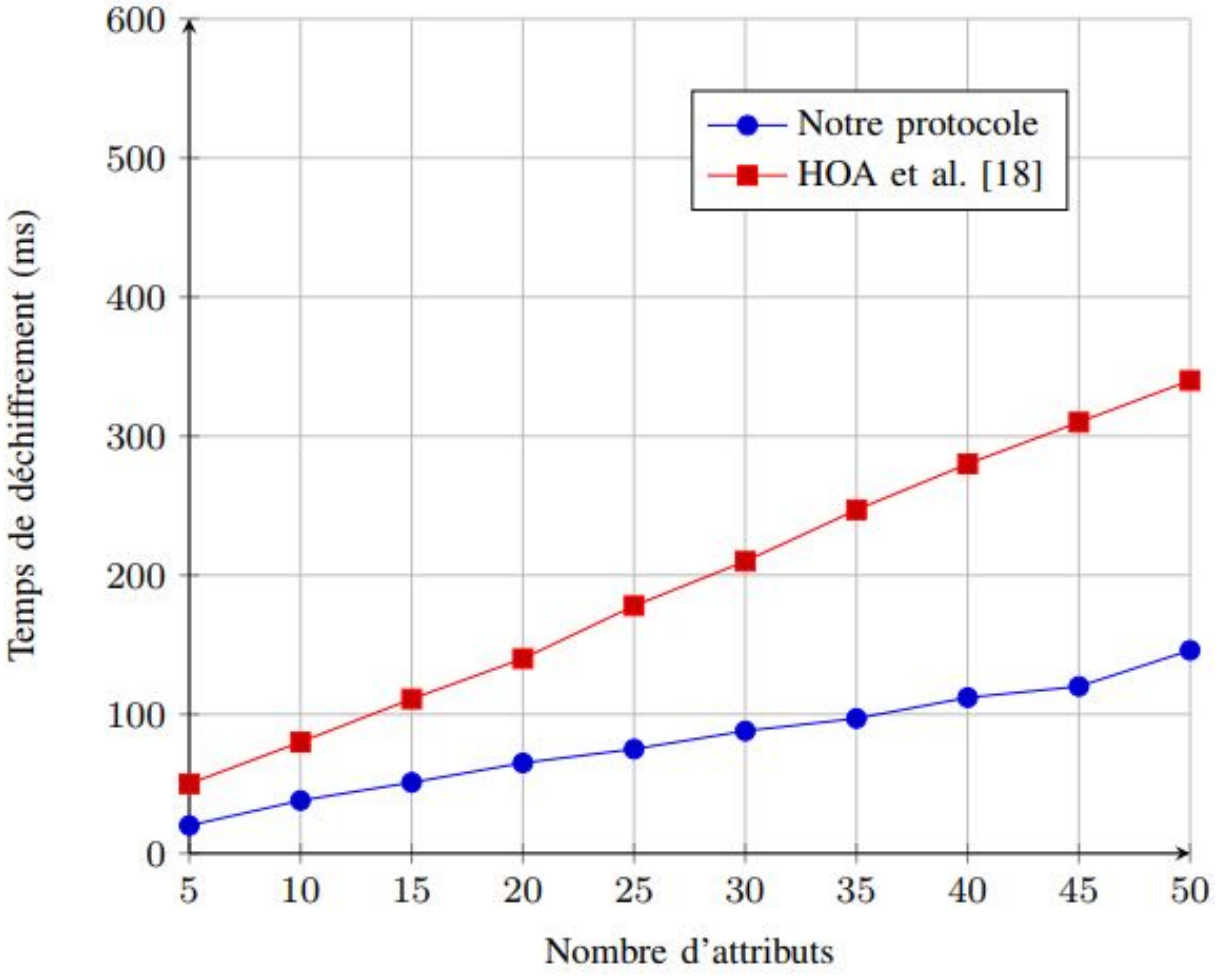


FIGURE 4.2 – Temps de déchiffrement en fonction du nombre d'attributs.

L'analyse des graphiques précédents montre que l'augmentation du nombre d'attributs entraîne l'accroissement des deux métriques mesurées.

Concernant le temps de chiffrement et de déchiffrement, Les performances de notre protocole sont néanmoins meilleures puisqu'elle consomme moins de temps de chiffrement et de déchiffrement comparé au protocole concurrent. Ceci revient au fait d'utiliser le protocole CP-ABE. En effet, dans notre protocole, l'utilisation de CP-ABE a permis de réduire le temps de chiffrement et de déchiffrement. Parallèlement, dans le protocole d'Hao et al. [19], le temps de chiffrement de déchiffrement augmente considérablement.

4.4 Conclusion

Nous avons conclu dans ce dernier chapitre notre travail avec une simulation et une évaluation des performances de notre protocole. Nous avons comparé les résultats obtenus avec celle d'un autre protocole de contrôle d'accès existant dans la littérature. Pour ce faire, nous avons varié le nombre d'attributs afin d'étudier son impact sur le temps de chiffrement et le temps de déchiffrement des données. Les résultats obtenus montrent que notre protocole présente une haute performance en terme de temps de chiffrement

et de temps de déchiffrement des données par rapport au protocole étudié dans le chapitre de l'état de l'art.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

Au cours de ces dernières années, la notion d'Internet des Objets (IdO) a évolué à une vitesse très exceptionnelle. L'IdO est apparus comme une technologie ayant le potentiel pour révolutionner divers domaines de notre vie quotidienne. Des milliards d'objets intelligents et autonomes, à travers le monde sont connectés et communiquent entre eux. Toutefois, le big data et l'Internet des objets sont encore au stade précoce de leur développement, et plusieurs défis de recherche doivent être surmontés afin qu'ils puissent être largement déployés. Le contrôle d'accès est l'un des principaux défis du big data à relever tant que les données collectées sont sensibles et doivent être confidentielles.

L'objectif visé par ce travail était de s'intéresser à la problématique de la sécurité de données stockées afin de pouvoir les partager avec les utilisateurs autorisés tout en préservant la confidentialité et leurs vies privées. Pour atteindre cet objectif, nous avons fait une étude bibliographique sur le problème du contrôle d'accès au big data dans le contexte de l'Internet des objets.

Notre protocole se base sur la cryptographie à base d'attributs (ABE) qui est une technique prometteuse pour contrôler l'accès aux données massives en se basant sur la variante Ciphertext Policy-Attribute Based Encryption (CP-ABE). Le principe de cette dernière est que les clés privées de l'utilisateur sont spécifiées par un ensemble d'attributs et les données chiffrées ne peuvent être déchiffrées que par les utilisateurs autorisés par une politique d'accès à base de ces attributs. Cette approche permet de cacher l'identité de l'utilisateur pour préserver sa vie privée lorsqu'il accède au cloud pour stocker ou télécharger les données chiffrées. Elle protège les informations de l'utilisateur des l'abus par un agresseur et des vulnérabilités aux attaques malveillantes. Cette solution permet de fournir un niveau de sécurité élevé et de préserver la vie privée de l'utilisateur. Pour une bonne manipulation des données, nous avons opté à combiner entre CP-ABE et les courbes elliptiques (ECC). Le principal avantage d'ECC est que des clés plus courtes peuvent être utilisées par rapport à d'autres cryptosystèmes. De plus, ECC est un outil efficace dans la cryptographie à clé publique en raison des forces de calcul, de communication et de sécurité. À ce fait, elle est le choix idéal pour implémenter la cryptographie à clé publique dans des appareils IdO.

Pour la validation de notre proposition nous avons simulé notre proposition en la comparant avec un protocole récent parmi ceux étudiés. Les résultats obtenus sont satisfaisants et montrent l'avantage de notre approche en termes de temps de chiffrement et de temps de déchiffrement des données.

Comme perspectives, nous envisageons de comparer le protocole proposé à d'autres protocoles concurrents de la littérature, en se basant sur d'autres critères. En outre, pour résoudre le problème de mise à jour d'une clé de consommateur de données sans affecter les autres, nous prévoyons d'intégrer de manière

efficace la révocation d'attribut/clé dans le protocole proposé. Enfin, nous souhaitons implémenter le protocole proposé sur une plateforme réelle.

BIBLIOGRAPHIE

[1] https://openclassrooms.com/fr/courses/1362801-la-cryptographie-asymetrique-rsa/1362859-rsa-quest-ce-donc/, (consulté le 09 mai 2020).

[2] http://www.piloter.org/business-intelligence/big-data-definition.htm, (consulté le 17 octobre 2019).

[3] https://www.custup.com/big-data-introduction/, (consulté le 17 octobre 2019).

[4] http://blog.octo.com/modeles-architectures-internet-des-objets/, (consulté le 19 octobre 2019).

[5] A. BEIMEL. Secure schemes for secret sharing and key distribution. thèse de doctorat, israel institute of technology, technion, haifa, israel, 1996.

[6] J. BETHENCOURT, A. SAHAI, and B. WATERS. Ciphertext-policy attribute- based encryption. *IEEE Computer Society.*, pages pages 321–334,, 2007.

[7] Zahra Dafri. Réalisation d'un système basé sur internet des objets pour le contrôle des serres intelligentes. mémoire de fin d'études master, université de 8 mai 1945 – guelma, Juillet 2019.

[8] W. AIT ABDELMALEK et A. MANSOURI. L'authentification à base d'empreinte digitale dans les réseaux à faibles ressources. mémoire de fin de cycle, université a/mira de béjaia, 2015.

[9] J. LI et B. ZHANG. An ontology-based approach to improve access policy administration of attribute-based access control. *Information and Computer Security*, Vol. 11, 2019.

[10] S. ISLAM et G. BISWAS. Dynamic id-based remote user mutual authentication scheme with smartcard using elliptic curve cryptography. *Journal of electronics (China)*, Vol. 31 No. 5, 2014.

[11] S. FUGKEAW et H. SATO. Privacy-preserving access control model for big data cloud. *Journal IEEE*, 2015.

[12] S. ATRAM et N. BORKAR. A review paper on attribute-based encryption scheme in cloud computing. *A Monthly Journal of Computer Science and Information Technology*, Vol. 6, No. 5 :260–266, 2017.

[13] N. BOUSSAID et R. BRAHAMI. Privacy dans l'internet des objets. cas d'étude : la localisation. mémoire de master recherche, université a/mira de béjaia, 2017.

[14] M. SMITHAMOL et S. RAJESWARI. Hybrid solution for privacy-preserving access control for healthcare data. *Advances in Electrical and Computer Engineering*, Vol. 17, 2017.

[15] L. CHALAL et S. SIROUAKNE. Gestion des clés dans l'internet desobjets. mémoire de master recherche, université a/mira de béjaia, 2017.

[16] F. CHERIFI et S. ZEBBOUDJ. Authentification biométrique dans les systèmes mobiles de soins et de santé. mémoire de master recherche, université a/mira de béjaia, 2016.

[17] K. FAN, X. WANG J. WANG, H. LI, and Y. YANG. A secure and verifiable outsourced access control scheme in fog-cloud computing. *Sensors*, Vol. 17, 2017.

[18] K. FAN, H. XU, L. GAO, H. LI, and Y. YANG. Efficient and privacy preserving access control scheme for fog-enabled iot. *Future Generation Computer Systems*, pages 134–142, 2019.

[19] J. HAO, C. HUANG, J. NIB, H. RONG, M. XIAN, and X. SHEN. Fine-grained data access control with attribute-hiding policy for cloud-based iot. *Computer Networks*, 2019.

[20] S. KHALI. Dévelopement d'une technique de distribustion de clés de cryptage pour les applications multicast sur les réseaux sans fil adhoc. mémoire présenté à l'université du québec à trois-riviéres, 2008.

[21] S. MALANI, J. SRINIAS, A. KUMAR, K. SRINATHAN, and M. JO. Certificate-based anonymous device access control scheme for iot environment. *journal IEEE*, 2019.

[22] VICTOR S. MILLER. Use of elliptic curves in cryptography. *In Advances in Cryptology - CRYPTO'85 Proceedings*, page 417–426, 1985.

[23] S. PAL, M. HITCHENS, V. VARADHARAJAN, and T. RABEHAJA. Policy-based access control for constrained healthcare resources in the context of the internet of things. *Journal of Network and Computer Applications*, pages 57–74, 2019.

[24] S. RAVIDAS, A. LEKIDIS, F. PACI, and N. ZANNONE. Access control in internet-of-things. *Journal of Network and Computer Applications*, pages 79–101, 2019.

[25] D. ROMAIN. Iot and big data : understanding the relationship between these two technologies. *Journal IEEE*, 2018.

[26] I. SALEH. Internet des objets (ido) : Concepts, enjeux, défis et perspectives. 2017.

[27] K. SOWJANYA, M. DASGUPTA, S. RAY, and S. MOHAMMAD. An efficient elliptic curve cryptography-based without pairing kpabe for internet of things. *Journal IEEE*, 2019.

[28] H. SUNDMAEKER, P. GUILLEMIN, P. FRIESS, and S. WOELFFLe. Vision and challenges for the internet of things. *Cluster of European Research Projects on the Internet of Things*, 2010.

[29] Y. OULD YAHIA. Proposition d'un modèle de sécurité pour la protection de données personnelles dans les systèmes basés sur l'internet des objets. thèse de doctorat. ecole doctorale informatique , télécommunications et electronique (paris), 2019.

[30] H. YAN, Y. WANG, C. JIA, J.LI, Y. XIANG, and W. PEDRYCZ. Iot-fbac : Function-based access control scheme using identity-based encryption in iot. *Future Generation Computer Systems*, page 344–353, 2019.

[31] 0. YAO, Z. CHEN, and Y. TIAN. A lightweight attribute-based encryption scheme for the internet of things. *Future Generation Computer Systems*, pages 104–112, 2015.

RÉSUMÉ

L'Internet des Objets (IdO) est un écosystème composé, entre autres, de divers capteurs et actionneurs en réseau, réalisant principalement des progrès liés à la réduction des coûts de production et à la flexibilité du flux de travail. L'extension de l'internet touche actuellement différentes entités du monde physique. La démocratisation de cette technologie fait ressurgir beaucoup de problèmes associés à la sécurité des données transmises. Utiliser un protocole de contrôle d'accès sécurisé est l'une des solutions qui s'adaptent au modèle d'internet des objets. L'introduction du contrôle d'accès au big data de tels environnements est considéré comme difficile, principalement en raison de la variété des technologies et des protocoles dans les dispositifs et les réseaux IdO. Dans ce mémoire, nous avons proposé un protocole capable d'assurer le contrôle d'accès au big data dans l'IdO en utilisant un modèle basé sur la méthode de chiffrement à base d'attributs (ABE), plus exactement CP-ABE (Ciphertext-Policy Attribute Based Encryption). Cette technique est prometteuse pour contrôler le big data. Les résultats des simulations de notre protocole et une comparaison avec un autre protocole existant dans la littérature ont mis en relief les avantages de notre protocole, en terme de temps de cryptage et de décryptage.

Mots clés : Internet des Objets, ABE, Big data, CP-ABE, Contrôle d'accès, ECC.

ABSTRACT

The Internet of Things (IoT) is an ecosystem made up of, among other things, various networked sensors and actuators, primarily achieving progress related to lower production costs and flexible workflow. The spread of the internet is affecting different parts of the physical world today. The democratization of this technology brings back many problems associated with the security of transmitted data. Using a secure access control protocol is one of the solutions that fits the Internet of Things model. The introduction of big data access control in such environments is considered difficult, mainly due to the variety of technologies and protocols in IoT devices and networks. In this memory, we have proposed a protocol capable of ensuring access control to big data in the IoT using a model based on the attribute-based encryption method (ABE), more exactly CP-ABE (Ciphertext-Policy Attribute Based Encryption). This technique is promising for controlling big data. The results of the simulations of our protocol and a comparison with another protocol existing in the literature have highlighted the advantages of our protocol, in terms of encryption, and decryption time.

Keywords : Internet of Things, ABE, Big data, CP-ABE, Access control, ECC.