Vers une approche cloud de la protection de la vie privée sur les réseaux sociaux

Youcef Yahiatene

N° Ordre...../FSI/UMBB/2021

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté Des Sciences

Thèse de Doctorat

Présentée par :

Youcef YAHIATENE

En vue de l'obtention du diplôme de **DOCTORAT** en :

Filière : Informatique

Option : Spécifications logiciels et traitement de l'information

---

Vers une approche Cloud de la protection de la vie privée sur les réseaux sociaux

---

Devant le jury composé de :

Mr. MEZGHICHE	Mohamed	Prof	UMBB	Président
Mr. HAMADOUCHE	M'hamed	Prof	UMBB	Examinateur
Mr. BOUDERAH	Brahim	Prof	UMB M'sila	Examinateur
Mr. SENOUCI	Abdelkader	MCA	ESDAT/Réghaia	Examinateur
Mr. RIAHLA	Med Amine	MCA	UMBB	Directeur
Mr. RACHEDI	Abderrezak	Prof	UPEM (France)	Co-Directeur

Année Universitaire 2020/2021

Remerciement

Je tiens à remercier toutes les personnes qui ont contribué et qui m'ont aidé lors de la rédaction de cette thèse.

Je voudrais en premier lieu rendre hommage à notre regretté le Professeur Thouraya Bouabana Tebibel qui nous a quitté trop tôt, elle était une excellente éducatrice. Le Professeur Tebibel était un modèle et une source d'inspiration pour nous tous, elle était mon directeur de thèse. Je rends un hommage particulier à Monsieur Menacer Djamal Eddine, Maître de conférences à l'École Supérieure d'Informatique ESI pour ses précieux conseils et son suivi dans mes travaux de recherche, sa disponibilité, ses précieux conseils et encouragements qui m'ont toujours aidé à avancer et ont grandement contribué l'aboutissement de ce travail.

Je voudrais aussi présenter mes profonds remerciements à mon directeur de thèse Monsieur Riahla Mohamed Amine, Maître de conférences à l'université de Boumerdes, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à améliorer notre recherche.

Je tiens à présenter aussi mes profonds remerciements à mon co-directeur de thèse Monsieur Rachedi Abderrezak Professeur à l'université Paris-Est Marne-la-Vallée (UPEM), il m'a accueilli dans son laboratoire d'informatique Gaspard Monge, il m'a suivi tout le long de mon stage en France. Je le remercie pour sa patience, sa disponibilité et surtout ses judicieux conseils.

Je tiens également à présenter mes profonds remerciements aux membres de jury, qui nous ont honorés en acceptant d'expertiser notre travail. Je remercie Monsieur Mohamed MEZGHICHE, professeur à l'UMBB pour m'avoir fait l'honneur d'accepter de présider mon jury. Je

remercie Monsieur M'hamed HAMADOUCHE, professeur à l'UMBB, Monsieur Brahim BOUDERAH, professeur à l'UMB M'sila et Monsieur Abdelkader SENOUCI, Maître de conférences à ESDAT/Réghaia pour m'avoir fait l'honneur d'examiner mes travaux et d'être membre du jury de ma soutenance.

Que Messieurs les membres du jury trouvent en ces mots l'expression de mon profond respect en espérant que mon travail aura été à la hauteur de leurs exigences scientifiques.

Je voudrais aussi présenter mes remerciements au Professeur TAIRI et Melle.TOUZOUIRT du service des relations extérieures de l'université de Boumerdes qui m'ont donné l'opportunité pour décrocher un séjour scientifique à l'université Paris-EST Marne-la-Vallée.

Durant ces années de thèse et mon travail au sein du département d'informatique à l'UMBB, j'ai eu le plaisir de travailler et collaborer avec des collègues enseignants, doctorant et personnel administratif que je remercie pour leur gentillesse.

J'exprime mes sincères remerciements à tous les enseignants qui m'ont enseigné durant mon cursus universitaire depuis la graduation jusqu'à la post-graduation.

ملخص

يتم تمثيل الشبكات الاجتماعية على الإنترنت "OSN" بمجموعة من الأشخاص يتفاعلون مع بعضهم البعض. تلعب "OSN" دورًا رئيسيًا في الحياة اليومية لمستخدمي الإنترنت. يشارك مستخدمو الإنترنت بيانات ذات طبيعة خاصة أو عامة مثل مقاطع الفيديو والتعليقات والصوتيات والصور والتغريدات وما إلى ذلك.

تجمع "OSN" كل الأنشطة والمعلومات حول المستخدمين بالإضافة إلى جهات الاتصال والعلاقات والآراء الخاصة بهم . لقد ازداد عدد المستخدمين على هذه الشبكات بشكل هائل، مثلFacebook ، الذي قال إنه وصل إلى 2.5 مليار مستخدم نشط شهريًا في الربع الرابع من عام 2019

مع هذا النمو الهائل في المستخدمين، كمية هائلة من البيانات تتم مشاركتها على منصات وسائل التواصل الاجتماعي.
OSN تعرف من هم أصدقاؤنا ، وكيف نبدو ، وأين نحن ، وماذا نفعل ، وأذواقنا ، وما يكرهنا ، وأكثر من ذلك بكثير .لن تتوقف OSN عند هذا الحد ، فهي تحلل بيانات المستخدم ولديها طرق أخرى لتحديد سلوك المستخدم باستخدام العديد من التقنيات مثل تتبع ملفات تعريف الارتباط ،تحليل الإعجابات.

سمحت لنا شعبيةOSN بتضمين الجانب الاجتماعي في الشبكات الحالية مثل شبكات الاستشعار ، وشبكات المركبات ، وما إلى ذلك . دمج الشبكات الاجتماعية في "VANET" يعطي الشبكات الاجتماعية للمركبات VSN

تولد هذه الشبكة الجديدة نوعًا جديدًا من التطبيقات وهي إدارة حركة المرور الذكية التي تساعد المستخدمين على تحسين سلوكهم ، كما تتيح للمستخدمين مشاركة البيانات مثل مقاطع الفيديو والتسجيلات الصوتية وصور الطريق وغيرها من المعلومات من أجهزة الاستشعار المختلفة المدمجة في السيارة

مع مشاركة البيانات في OSNs وVSNs ، يظل جانب الأمان والسرية مصدر قلق كبير.

لذلك، حماية الخصوصية وإخفاء هوية التبادلات , يحتنا للمساهمة في حماية خصوصية المستخدمين.
لقد اقترحنا Framework لـ OSNs يسمى "CloudSN" ، والذي يعتمد على الحوسبة السحابية والتشفير الموزع بناءً على ."ABE" يمكن للمستخدمين تصميم سياسة الوصول الخاصة بهم التي تسمح للأشخاص المصرح لهم فقط بالوصول إلى البيانات

فيما يتعلق بشبكاتVSN ، اقترحنا Frameworkجديدًا يستند إلى مفهومين جديدين هما blockchain والشبكة المعرفة بالبرمجيات ."SDN"هذا الأخير يجعل من الممكن التحكم في الشبكة والتنظيم المركزي والمحاكاة الافتراضية للموارد المتاحة على الشبكة .تم إدخال Blockchain لتصديق المعاملات وسيضمن عدم الكشف عن البيانات و يعمل بطريقة موزعة بالكامل.

Abstract

The online social networks "OSN" are represented by a set of people interacting with each other. The OSN plays a key role in the daily lives of users. They share data that can be private or public such as videos, comments, audios, photos, twittes, etc. An OSN collects all activities and information about users as well as their contacts, relationships, and opinions. The number of users of these OSNs has increased phenomenally. For instance, Facebook declared it had about 2.5 billion monthly active users in the fourth quarter of 2019. With this huge growth of users, a huge amount of data is shared on social media platforms. The OSNs know who are our friends, what we look like, where we are, what we do, our tastes, our dislikes, and much more. The OSNs will not stop there, they analyze user data and they have other means to determine user behavior using several techniques such as tracking cookies, like analysis, etc.

The popularity of The OSNs has allowed us to include the social aspect in existing networks such as sensor networks, vehicular networks, etc. The integration of social networks in the "VANET" gives a new network named Vehicular Social Network "VSN". This new network generates a new type of applications namely intelligent traffic management helping users to improve their behavior. It also allows users to share data such as videos, audios, road pictures, and other information from different sensors integrated into the vehicle.

With the data shared in OSNs and VSNs, the aspect of security and confidentiality remains a major concern. Therefore, the protection of privacy and the anonymity of exchanges motivate our research to contribute in the protection of users' privacy. We have proposed a framework for OSNs called "CloudSN", which is based on cloud computing and distributed encryption based on "ABE" attributes. Users can design their own policy which allows only authorized persons to have access to the data.

Regarding the VSNs, we proposed a new framework based on two main concepts the blockchain and the Software-Defined Network "SDN". The SDN makes to have a control over the network and centralized orchestration and virtualization of resources available on the network. The blockchain has been introduced to allow certification of transactions and will guarantee the anonymity of data in a fully distributed manner.

Résumé

Les réseaux sociaux en ligne "OSN" sont représentés par un ensemble de personnes ou de groupe de personnes interagissant les uns avec les autres. Les OSNs jouent un rôle clé dans la vie quotidienne des internautes. Ces derniers partagent des données à caractère privée ou publique telles que les vidéos, les commentaires, les audios, les photos, les twittes, etc. Un OSN collecte toutes les activités et les informations sur les utilisateurs ainsi que leurs contacts, relations et opinions. Le nombre d'utilisateurs de ces OSN a augmenté d'une manière phénoménale, par exemple Facebook a déclaré qu'il avait 2,5 milliards d'utilisateurs actifs mensuels au quatrième trimestre 2019.

Avec cette croissance pharamineuse des utilisateurs, une quantité énorme de données est partagée sur les plateformes des réseaux sociaux. Les OSNs savent qui sont nos amis, à quoi nous ressemblons, où sommes-nous, ce que nous faisons, nos goûts, nos aversions et bien plus encore. Les OSNs ne s'arrêteront pas là, ils analysent les données des utilisateurs et ils ont d'autres moyens pour déterminer leurs comportements en utilisant plusieurs techniques telles que le tracking cookies et l'analyse des j'aimes "likes".

La popularité des OSNs nous a permis d'inclure l'aspect social dans des réseaux existants tels que les réseaux de capteurs, les réseaux véhiculaires, etc. L'intégration des réseaux sociaux dans les "VANET" engendre un autre type de réseaux à savoir les réseaux sociaux véhiculaire "Vehicular Social Network VSN". Ce nouveau réseau suscite un nouveau type d'application à savoir la gestion intelligente du trafic aidant les utilisateurs à améliorer leurs comportements, il permet aussi aux usages de partager des données telles que des vidéos, des audios, des photos de route et d'autres informations provenant de différents capteurs intégrés dans un véhicule.

Avec les données partagées dans les OSNs et les VSNs, l'aspect de la sécurité et de la confidentialité reste une préoccupation majeure. De ce fait, la protection de la vie privée et l'anonymat des échanges motivent nos recherches pour contribuer dans la protection de la vie privée des utilisateurs. Nous avons proposé un framework pour les OSNs appelé "CloudSN", ce dernier est basé sur le cloud computing et le chiffrement distribué basé sur les attributs "ABE". Les utilisateurs peuvent concevoir leur propre politique qui permet uniquement aux personnes autorisées d'avoir accès aux données.

Concernant les VSNs, nous avons proposé un nouveau framework basé sur deux nouveaux concepts à savoir la blockchain et le Software-Defined Network "SDN". Ce dernier permet d'avoir un contrôle sur le réseau et une orchestration centralisée et une virtualisation des ressources disponibles en réseau. La blockchain a été introduite pour

permettre la certification des transactions et garantir l'anonymat des données d'une manière entièrement distribuée.

Table des matières

1 Contexte général : Réseaux sociaux **5**

1.1 Introduction 6

1.2 Classifications des solutions de protection de la vie privée dans OSN . . . 7

1.2.1 Les solutions basées sur la plateforme de OSN 7

1.2.2 Les solutions non basées sur la plateforme de OSN 9

1.2.2.1 Stockage de données sensibles sur la machine locale de l'utilisateur 9

1.2.2.2 Stockage de données sensibles indépendamment de la machine locale de l'utilisateur 10

1.3 Conclusion 11

2 Le chiffrement à base d'attributs Attribute-Based Encryption "ABE" 12

2.1 Introduction 13

2.2 La cryptographie 13

2.2.1 Le fonctionnement de la cryptographie 14

2.2.1.1 La cryptographie symétrique 14

2.2.1.2 La cryptographie asymétrique 15

2.2.1.3 L'authentification 16

2.3 Infrastructure à clés publiques "Public Key Infrastructure" 17

2.3.1 Les composants d'une PKI 18

2.3.2 La PKI et la hiérarchie de confiance 19

2.3.3 L'autorité de certification 21

2.3.4 Le certificat électronique 21

2.3.5 La structure d'un certificat 22

2.4 Le chiffrement à base d'attributs "ABE" 24

2.5 La classification des solutions ABE 25

2.5.1 Le schéma CP-ABE Ciphertext Policy Attribut Based Encryption 26

2.5.2 Le schéma KP-ABE Key-Policy Attribut Based Encryption 27
2.5.3 Les solutions ABE avec une formule d'accès monotonic 29
2.5.4 Les solutions ABE avec une formule d'accès non-monotonic . . . 29
2.5.5 Les solutions ABE Hiérarchique 30
2.5.6 Le schéma ABE distribué 30
2.6 Le cloud computing 32
2.6.1 Les caractéristiques du cloud computing 32
2.6.2 Les modèles de déploiement du cloud 33
2.6.2.1 Le cloud privé 33
2.6.2.2 Le cloud publique 33
2.6.2.3 Le cloud hybride 33
2.6.3 Les différents services du cloud 33
2.6.3.1 L'infrastructure comme un service "IaaS" 34
2.6.3.2 La plateforme comme un service "PaaS" 34
2.6.3.3 Le logiciel comme un service "SaaS" 35
2.6.3.4 Le stockage comme un service "STaaS" 35
2.6.3.5 Les avantages d'utilisation d'une solution cloud 36
2.7 Conclusion 37

3 Vers une approche ABE distribuée pour la protection de la vie privée dans les réseaux sociaux en ligne 38
3.1 Introduction 39
3.2 Les menaces liées aux réseaux sociaux en ligne 40
3.2.1 Les menaces liées aux fournisseurs de services 40
3.2.2 Les menaces liées aux applications tierces 41
3.2.3 Les menaces liées aux utilisateurs 42
3.2.3.1 Les attaques classiques 42
3.2.3.2 Les attaques modernes 45
3.3 Le CloudSN framework 49
3.3.1 La gestion de la sécurité dans CloudSN 50
3.3.1.1 Les mécanismes cryptographiques 50
3.3.1.2 La sécurité basée sur le contrôle d'accès 51
3.3.2 Une vue globale de CloudSN 51
3.4 Évaluation des performances 56
3.4.1 Setup 56

3.4.2 L'analyse des performances . . . 57
3.5 L'analyse de la sécurité . . . 59
3.5.1 l'analyse de la robustesse . . . 59
3.5.2 Résistance aux attaques . . . 60
3.5.2.1 La résistance à la coalition d'attributs : . . . 63
3.6 Conclusion . . . 65

4 Les réseaux sociaux véhiculaires 66
4.1 Introduction . . . 67
4.2 Définition des réseaux sociaux véhiculaires . . . 69
4.3 Architecture des réseaux sociaux véhiculaires . . . 69
4.3.1 Architecture centralisée . . . 69
4.3.2 Architecture distribuée ou décentralisée . . . 70
4.3.3 Architecture hybride . . . 70
4.4 Applications des réseaux sociaux véhiculaires . . . 70
4.4.1 Les applications de sécurité . . . 71
4.4.2 Les applications basées sur la commodité . . . 71
4.4.3 Les applications basées sur le confort . . . 71
4.4.4 Les applications basées sur le divertissement . . . 71
4.5 Conclusion . . . 72

5 Applications de la Blockchain pour l'IoT "Internet Of Things" 73
5.1 Une vue globale sur la Blockchain . . . 74
5.2 Applications de la Blockchain dans l'IoT . . . 75
5.2.1 Internet des objets dans la santé "Internet of healthcare things" . . . 75
5.2.2 Fog computing . . . 76
5.2.3 IoT pour devices . . . 77
5.2.4 Software-defined networking . . . 77
5.2.5 Internet des véhicules IoV . . . 78
5.3 Conclusion . . . 81

6 Vers une approche basée sur la Blockchain et "Software-Defined Vehicular Networks" pour sécuriser les réseaux sociaux véhiculaires 82
6.1 Introduction . . . 83
6.2 Un framework basé sur l'architecture de la Blockchain . . . 84
6.2.1 Présentation de l'architecture . . . 85

6.2.1.1 Le module de contrôle 85
6.2.1.2 Le module de données 87
6.2.1.3 Le module Cloud et le Fog computing 87
6.2.2 Module de la sécurité et de la confidentialité 88
6.2.3 Modèle de confiance 89
6.2.3.1 Valeur de la confiance directe 90
6.2.3.2 La livraison du modèle de confiance 91
6.2.3.3 Mise à jour de la confiance 92
6.2.3.4 La décision de confiance 93
6.3 La sélection des mineurs basée sur l'algorithme CDS 95
6.4 Analyse des performances 99
6.4.1 La configuration de la simulation 99
6.4.2 Analyse des résultats de la simulation 101
6.5 Analyse de sécurité 105
6.5.1 Résistance aux attaques 105
6.5.1.1 La métrique de confiance distribuée 106
6.5.1.2 Les attaques dans un réseau social véhiculaire 107
6.6 Conclusion 110

7 Conclusion générale & perspectives **112**
7.1 Conclusion générale & perspectives 113
7.2 Conclusions 113
7.3 Orientations de nos travaux futurs 115

Bibliography **116**

Table des figures

1.1 Différentes approches utilisées dans les solutions existantes 7

2.1 Le processus du chiffrement et déchiffrement 13
2.2 Le chiffrement à base de clé symétrique 15
2.3 Le chiffrement asymétrique 15
2.4 PKI : cycle de génération d'un certificat 19
2.5 La hiérarchies de l'autorité de certification 20
2.6 La structure d'un certificat X.509 22
2.7 La classification de ABE 25
2.8 Le schéma de CP-ABE "Ciphertext Policy Attribut Based Encryption" . 26
2.9 Le schéma de KP-ABE "Key Policy Attribut Based Encryption" 28
2.10 La politique d'accès sous forme d'arbre "Tree" 29
2.11 Les différents services proposés par le cloud 34
2.12 La gestion des service Iaas, Paas et Saas par le fournisseur du cloud [1] . 35

3.1 Les Menaces des utilisateurs dans OSN 41
3.2 L'attaque de phishing 43
3.3 L'attaque de cross-site scripting "XSS" 44
3.4 L'attaque de clickjacking 45
3.5 Le processus de classification des données de l'utilisateur 49
3.6 Gestion de la sécurité dans CloudSN. 50
3.7 Une vue globale sur l'architecture. 52
3.8 Temps de chiffrement en fonction du nombre d'attributs 58
3.9 Temps de déchiffrement en fonction du nombre d'attributs 59
3.10 MA-CP-ABE résistance aux coalitions 64

5.1 Architecture de la Blockchain. 74
5.2 Applications de la Blockchain dans IoT. 76

6.1 Présentation de l'architecture 85
6.2 Interaction entre différents modules de l'architecture 86
6.3 Processus de selection des mineurs 89
6.4 L'organigramme de la décision de confiance 94
6.5 L'organigramme du processus de sélection des mineurs 96
6.6 Processus de sélection des mineurs la phase de compétition 97
6.7 Processus de sélection des mineurs la phase de décision 98
6.8 Le nombre de nœuds mineurs en fonction de la densité de nœuds. 101
6.9 Le nombre de nœuds mineurs en fonction de la portée radio. 102
6.10 Le nombre de mineurs en fonction de noeuds qui se retire du réseau. . . . 103
6.11 Le nombre de mineurs en fonction de l'adhésion des noeuds au réseau. . . 103
6.12 Le nombre de mineurs selon la métrique de confiance. 104
6.13 Comparison entre DM-CDS et DSP-CDS algorithmes. 105
6.14 Classification des attaques dans un réseau social véhiculaire. 106
6.15 L'attaque par wormhole. 109
6.16 L'attaque injection de fausses données. 109

Liste des tableaux

3.1 Comparaison de CloudSN avec des solutions existantes 64

4.1 La comparaison entre les réseaux MANET, VANET et VSN 68

5.1 Comparaison des travaux existants liés à la sélection des mineurs 79

6.1 Paramètres de simulation de l'algorithme DM-CDS. 101
6.2 La variation de la métrique de confiance 104

Les acronymes

VSN	Vehicular Social Network.
SDVN	Software-Defined Vehicular-Networks.
PC	Principal controller.
RSU	Road Side Units.
DM-CDS	Distributed Miners Connected Dominating Set algorithm.
OBU	On-Board Unit.
Tm	Trsut metric.
Deg	connectivity Degree.
LQI	the average Link Quality Indicator.
CDS	Connected Dominating Sets algorithm.
IoT	Internet of Things.
V-to-V	Vehicle to Vehicle.
V-to-I	Vehicle to Infrastructure.
PAPA	Privacy Accuracy Property and Accessibility.
SPRING	Social-based PRivacy-preserving packet forwardING.
IBC	Identity Based Cryptography.
EVSE	Efficient Vehicle Social Evaluation.
SES	social evaluation server.
SDN	Software-Defined Networks.
VANET	Vehicular Adhoc Network.
DSP-CDS	Distributed Single-Phase algorithm for constructing a Connected Dominating Set .
SM	Security Managers.
P2P	peer-to-peer.
PHEVs	Plug-in Hybrid Electric Vehicles.
LAGs	Local AGgregator.
ECC	Elliptic curve cryptography.
EVs	Electric vehicles.
EMRs	Electronic Medical Records.
EHRs	Electronic Health Records.
MA-ABS	Multiple Authorities Attribute-Based Signature.
CB-MDEE	Consortium Blockchain for Malware Detection and Evidence Extraction.
EVCE	Vehicles Cloud and Edge Computing.
QoS	Quality of Services.
MPD	Markov Decision process.
Saas	Software as a service .
MEC	Multi-access Edge Computing.
RNC	Radio Network Controller.
ACK	ACKnowledgement.
Sim	Similarity.
TPM	Trust Platform Module.

Introduction générale

De nos jours, les réseaux sociaux en ligne "Online Social Network OSN" ont changé la vie des utilisateurs, c'est la technologie la plus remarquable du 21 eme siècle, le nombre d'utilisateurs a augmenté d'une manière phénoménale. Le réseau le plus utilisé et le plus actif sur la toile est Facebook avec 2,5 milliards d'utilisateurs actifs mensuellement au quatrième trimestre 2019 [2], la société a déclaré que 2,9 milliards de personnes utilisaient au moins l'une des principales applications de la société Facebook à savoir WhatsApp, Instagram ou Messenger chaque mois.

Avec cette croissance pharamineuse des utilisateurs, une quantité énorme de données est partagée sur les plateformes des réseaux sociaux. Les statistiques sur les données partagées sont de quatre millions de likes chaque minute, 350 millions de photos téléchargées chaque jour. Facebook génère quatre nouveaux péta-octets de données par jour et 100 millions d'heures de visionnage vidéo par jour [3]. Cette quantité de données est stockée dans des data-centers qui sont au nombre de 15 situés dans le monde entier [4].

Facebook est en possession d'une mine d'or, il collecte de grandes quantités de données personnelles de plusieurs façons innovantes. Avec les données partagées, le géant du web est en mesure de savoir qui sont nos amis, à quoi nous ressemblons, où nous sommes, ce que nous faisons, nos goûts, nos aversions et bien plus encore. Facebook ne s'arrête pas là, il analyse les données des utilisateurs et il a d'autres moyens de déterminer le comportement des utilisateurs en utilisant plusieurs techniques telles que le tracking cookies, l'analyse des likes, etc.

En s'appuyant sur la popularité croissante des réseaux sociaux, des travaux traitent la manière d'inclure les aspects sociaux dans des réseaux existants, tels que les réseaux de capteurs et les réseaux véhiculaires "VANET". L'intégration des réseaux sociaux dans les "VANET" donne les réseaux sociaux véhiculaire "Vehicular Social Network VSN". Ce nouveau réseau fournit de nouveaux types d'applications à savoir la gestion intelligente du trafic aidant les utilisateurs à améliorer leurs comportements, ou à aménager leurs horaires de déplacement. Grâce aux données spatio-temporelle, il est possible de générer une carte du trafic indiquant les niveaux de trafic à différents endroits dans les routes.

Le VSN prend en charge un large éventail d'applications, il ne se limite pas à la gestion du trafic et à la sécurité routière, il permet également aux voyageurs de partager des données telles que des vidéos, des audios, des photos de routes et d'autres informations provenant de différents capteurs intégrés. L'aspect de communication ne se limite

pas aux conducteurs, mais se généralise aux passagers, Véhicule-2-Véhicule, Véhicule-2-infrastructure ou bien avec n'importe quel support de communication Véhicule-2-X.

Les aspects de sécurité et de confidentialité qui restent encore l'une des préoccupations les plus importantes des réseaux sociaux véhiculaires.
Les problèmes susmentionnés ont été très peu étudiés et demandent plus d'efforts de la part de la communauté des chercheurs afin de proposer de nouvelles techniques permettant de diminuer l'impact de ces problèmes sur les "VSN". Plusieurs challenges ont été soulevés dans les réseaux sociaux en ligne et les réseaux sociaux véhiculaires à savoir :

— **La protection de la vie privée**.
— La détection et la classification de la population des réseaux sociaux.
— L'identification de la source de données.
— La confidentialité, l'intégrité et la non répudiation des données.
— Le traitement des données vu la quantité énorme de données partagées.
— L'anonymat des échanges et modèle de confiance.

Motivations et contributions

Ces tendances émergentes motivent nos recherches pour contribuer dans **la protection de la vie privée des utilisateurs**, cette dernière représente un souci majeur dans les réseaux sociaux vu les quantités pharamineuses des données partagées.
Les travaux de cette thèse se concentrent sur le développement d'un ensemble de solutions pour la protection de la vie privée qui représente un défis majeur dans les réseaux sociaux en ligne et leurs applications (telle que les VSN). Nous proposons dans ce mémoire un ensemble de contributions que nous classons en deux parties :

1. **Un Framework CloudSN** : Pour atténuer les problèmes de la vie privée et la confidentialité des données partagées sur les plateformes des réseaux sociaux en ligne, nous avons proposé un nouveau framework basé sur deux principaux concepts : le cloud computing et le chiffrement basé sur les attributs "Attribut Based Encryption" ABE, plus précisément nous avons utilisé le chiffrement par attributs distribués. Ce type de chiffrement permet d'instaurer un contrôle d'accès basé sur le rôle. Les utilisateurs peuvent concevoir leur propre politique qui permet uniquement aux personnes autorisées d'avoir accès à leurs données. Ce schéma réduit le risque de point de défaillance unique "Single point of failure". De plus, le framework proposé permet aux utilisateurs de partager leurs profils en deux parties : publique et privée. La partie publique restera dans le réseau social et concernant la partie privée, l'utilisateur sélectionne les personnes et crée

la politique d'accès. Après cela, les données seront cryptées et envoyées vers le cloud computing. Nous avons analysé la robustesse du framework proposé en analysant différentes familles de menaces : les menaces des fournisseurs de services, les menaces des applications tierces, ainsi que les menaces sur les utilisateurs qui peuvent être classées en deux catégories : les attaques classiques et les attaques modernes. Les résultats de ce travail ont donné lieu à une publication dans la conférence IEEE Wireless Communications and Networking Conference 15-19 April 2019 Marrakech, Morocco [5].

2. **Un Framework basé sur la blockchain pour sécuriser les réseaux sociaux véhiculaires** Nous avons proposé un nouveau framework basé sur deux nouveaux concepts à savoir la blockchain et le Software-Defined Network "SDN". En se basant sur le SDN qui est une approche d'architecture réseau permettant une gestion intelligente et centralisée d'un réseau, le SDN offre un contrôle centralisé des ressources réseau, une orchestration centralisée et une virtualisation des ressources disponibles en réseau. Cependant, l'utilisation de SDN crée également une vulnérabilité bien connue qui est le point de défaillance unique. Par conséquent, nous proposons d'introduire le paradigme de la blockchain qui permettra la certification des transactions et garantira l'anonymat des données d'une manière entièrement "distribuée". A cette fin, trois niveaux de contrôleurs sont nécessaires : un contrôleur principal "PC", des unités routières "RSU" et un contrôleur local. Afin de sélectionner dynamiquement les mineurs, un algorithme "Distributed Miners Connected Dominating Set DM-CDS" a été proposé. Le "DM-CDS" est un algorithme distribué monophasé qui prend en charge une topologie dynamique basée sur un modèle de confiance et certains autres paramètres de réseau, tels que le degré de connectivité, l'indicateur de qualité de liaison moyenne et le rang. La performance du DM-CDS proposé a été évalué avec plusieurs scénarios à l'aide de différents paramètres, tels que la métrique de confiance, la densité du nœud, la mobilité du nœud et la portée radio. Les résultats obtenus mettent en évidence l'importance d'une telle architecture, notamment en termes de nombre de mineurs requis. Les résultats de ce travail ont donné lieu à deux publications : la conférence IEEE Conference on Standards for Communications and Networking 29-31 October 2018 – Paris, France [6]. et le journal Transactions on Emerging Telecommunications Technologies [7].

Organisation de la thèse

La suite de cette thèse est structurée en cinq chapitres. Le premier chapitre est introductif dans lequel nous avons présenté le contexte général des réseaux sociaux et leurs applications. Le deuxième chapitre rappelle les différentes techniques de chiffrement, ainsi une présentation sur le cloud computing a été introduite. Le troisième chapitre est consacré à la présentation de l'approche "ABE" distribuée pour la protection de la vie privée dans les réseaux sociaux en ligne. Le chapitre quatre a été dédie pour présenter les réseaux sociaux véhiculaires qui sera suivi par le chapitre cinq qui a été consacré aux applications de la Blockchain pour l'IoT "Internet Of Things". Par la suite, nous avons présenté l'approche basée sur la Blockchain et "Software-Defined Vehicular Networks" pour sécuriser les réseaux sociaux véhiculaires dans le chapitre six. Enfin, les conclusions et les futurs directions de recherche sont décrites dans la dernière partie.

Chapitre 1

CONTEXTE GÉNÉRAL : RÉSEAUX SOCIAUX

Sommaire

1.1 Introduction 6

1.2 Classifications des solutions de protection de la vie privée dans OSN 7

1.2.1 Les solutions basées sur la plateforme de OSN 7

1.2.2 Les solutions non basées sur la plateforme de OSN 9

1.3 Conclusion 11

1.1 Introduction

De nos jours, les réseaux sociaux en ligne "Online Social Network OSN" jouent un rôle clé dans la vie quotidienne des utilisateurs. Une grande quantité d'informations est partagée sur le Web : publications, actualités, commentaires, vidéos, etc. L'OSN collecte toutes les activités et les informations sur les utilisateurs. Il recueille des informations sur les contacts, les relations et leurs opinions [8].
Ces données peuvent être utilisées à des fins publicitaires, commerciales et politiques [9]. L'OSN permet aux utilisateurs de présenter leurs profils de manière très détaillée [10]. Même avec les paramètres de confidentialité, les utilisateurs ne connaissent pas toujours leurs paramètres, ils ont tendance à utiliser les paramètres par défaut, ce qui peut nuire à leurs vies privées. Le problème de la confidentialité dans l'OSN peut être classé en trois catégories :

- La confidentialité sociale : c'est une intrusion induite par une personne exploitant une mauvaise configuration des paramètres de confidentialité, afin de nuire à la réputation de l'utilisateur.
- La confidentialité institutionnelle : les données personnelles de l'utilisateur sont utilisées par des institutions publiques ou privées. Ils collectent et stockent des données lorsqu'un utilisateur clique sur des publicités.
- La confidentialité gouvernementale : cela se produit lorsque les données privées d'un utilisateur sont transmises aux gouvernements par l'OSN sans son consentement pour une enquête [9].

Une fois que les données sont partagées par les utilisateurs sur les plateformes de OSN, elles sont accessibles à tout moment et n'importe où. Par conséquent, l'utilisateur n'aura aucun contrôle sur elles et la confidentialité de ses données est menacée. Pour garantir une meilleure accessibilité, l'OSN réplique les données de l'utilisateur sur ses centres de données, par conséquent, l'utilisateur ne peut pas trouver où se situent ses données, donc un problème de localisation des données peut survenir. Un autre problème rencontré dans un OSN est l'utilisation d'APIs "Application Programming Interfaces", qui sont un ensemble de règles, d'instructions et de fonctions permettant un accès aux services d'une application.

Les APIs permettent à un tiers d'accéder aux données personnelles de l'utilisateur, ce qui menace la confidentialité de ce dernier. Parmi les solutions existantes qui protègent la vie privée d'un utilisateur on trouve "Scramble" [11] et "Persona" [12]. La solution "Scramble" est basée sur la cryptographie asymétrique. Lorsqu'un utilisateur souhaite

partager un contenu, il doit être en possession de toutes les clés publiques de ses utilisateurs, qui seront par la suite stockées dans la machine de l'utilisateur. Le problème avec "Scramble" se situe dans le stockage local des clés des utilisateurs. La solution "Persona" [12] est une application basée sur Facebook, ce dernier à le pouvoir de la supprimée de sa plateforme. Par conséquent, la solution "Persona" ne pourra pas être utilisée par les utilisateurs de Facebook. Cette solution utilise une architecture centralisée qui mènera vers le problème de point de défaillance unique "single point of failure", ce qui est potentiellement un obstacle à une utilisation généralisée dans OSN. Le détail de ces solutions et d'autres seront décrits dans la section suivante.

1.2 Classifications des solutions de protection de la vie privée dans OSN

Dans cette section, nous présentons les travaux existants liés à la sécurité et à la confidentialité dans OSN basés sur Facebook, car il s'agit du réseau social en ligne le plus répandu. De plus, nous classons les solutions en différentes catégories comme présentés dans la Figure 1.1.

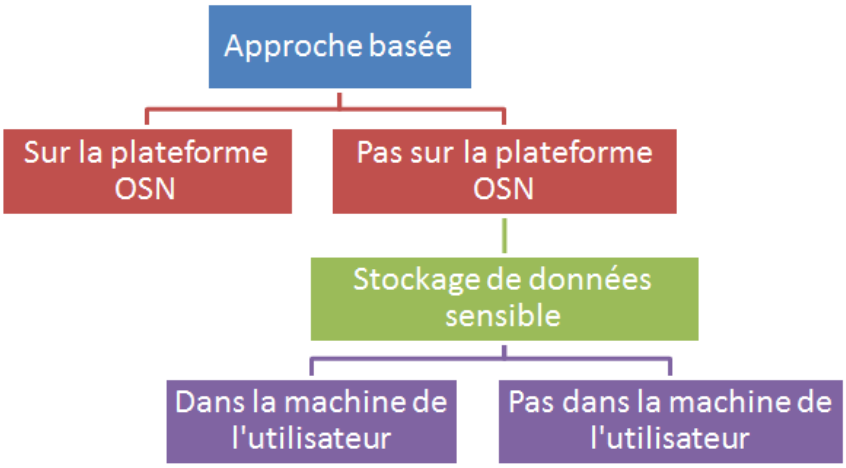

FIGURE 1.1 – Différentes approches utilisées dans les solutions existantes

1.2.1 Les solutions basées sur la plateforme de OSN

Plusieurs solutions et architectures ont été proposées pour protéger la confidentialité d'un utilisateur dans OSN. La solution "FlyByNight" est proposée par Lucas et al[13]. Il

s'agit d'une application Facebook qui facilite la communication sécurisée des messages un à un et un à plusieurs entre les utilisateurs. Chaque utilisateur génère une paire de clé publique / privée et fournit un mot de passe. Le mot de passe est utilisé pour crypter la clé privée. Cette clé cryptée est stockée dans une base de données sur le serveur "FlyByNight". Ces opérations sont effectuées en "JavaScript" côté client. L'utilisateur crypte un message avec la clé publique avant de le stocker dans une base de données sur le serveur "FlyByNight" en passant par le serveur de Facebook. Le "FlyByNight" utilise la plate-forme de ce dernier, ce qui peut compromettre la confidentialité de l'utilisateur en remplaçant le "JavaScript" côté client ou en remplaçant les clés publiques des amis de l'utilisateur.

Baden et al[12] ont proposé "Persona", qui est une application Facebook utilisant des règles de confidentialité, ces règles permettant aux utilisateurs de maintenir la liste de contrôle d'accès ACL "Access Control List" aux données et aux ressources, le propriétaire des données peut modifier l'ACL et administrer à un groupe spécifique différents niveaux d'accès aux données. "Persona" possède une application appelée "Storage", qui permet à un utilisateur de partager des données avec d'autres utilisateurs. Le service stockage utilise des primitives cryptographiques qui incluent le chiffrement basé sur les attributs "ABE"[14].

Chaque utilisateur génère une paire de clés asymétriques et distribue la clé publique aux utilisateurs avec lesquels il partage des données. "Persona" permet à l'utilisateur de créer des groupes et de gérer l'accès aux ressources en combinant "ABE" et la cryptographie traditionnelle. Dans "ABE", chaque chiffrement doit spécifier une structure d'accès et une expression logique sur les attributs. "ABE" génère pour chaque utilisateur la clé publique d'ABE appelé "APK" et la clé principale d'ABE "AMSK", puis l'utilisateur peut générer pour chaque ami une "ASK" (une clé secrète ABE) avec un ensemble d'attributs qui définit l'ami qui peut accéder aux données. L'utilisateur crypte cette clé à l'aide de la clé publique des utilisateurs cibles et la stocke sur le service de "Storage". L'utilisateur stocke les données cryptées sous le service "Storage" et met une référence à ces données dans une application "Doc-wall" (modèle pour stocker et formater les méta-données avec des références aux contenus cryptés). Par la suite tout utilisateur peut récupérer les données cryptées de l'application "Doc-wall" mais il ne pourra pas les décrypter s'il n'a pas le droit d'accès.
Cette solution utilise un schéma "ABE" centralisé qui souffre du problème "single point of failure". La solution dépend de la plateforme de Facebook, donc elle pourra être supprimée par Facebook au niveau du répertoire des applications.

1.2.2 Les solutions non basées sur la plateforme de OSN

Cette sous-section décrit les solutions qui ne sont pas basées sur la plateforme Facebook. Nous distinguons deux types de solutions : celles qui proposent un stockage de données au niveau de la machine de l'utilisateur et d'autres qui ne dépendent pas du stockage de la machine de l'utilisateur.

1.2.2.1 Stockage de données sensibles sur la machine locale de l'utilisateur

Parmi les solutions existantes dont les données sensibles dépendent de la machine de l'utilisateur, nous pouvons citer : Virtual Private Social Networks, c'est une approche proposée par Mauro et al [15], elle intègre le concept du "VPN : Virtual Private Network" au niveau du réseau social. L'idée est de construire un réseau social privé "VPSN" entre les utilisateurs
"VPSN" permet aux utilisateurs de modifier leurs informations d'origine par des pseudos-informations via une extension "Firefox" qui seront stockées sur le réseau social, tandis que les informations d'origines sont envoyées et stockées dans la machine d'un ami qui est autorisé à les voir au format XML. Dans cette solution, l'utilisateur perd le contrôle d'accès sur ses informations, car elles seront stockées dans les machines de ses amis.

Une autre solution appelée "FaceCloak" est proposée dans [16]. Il s'agit d'une extension du navigateur "Firefox" pour la plateforme Facebook, elle accomplit la confidentialité en trois étapes :

1. la phase de configuration.
2. la phase de cryptage.
3. la phase de décryptage.

Dans la phase de configuration, "FaceCloak" génère des clés pour crypter les informations publiées par l'utilisateur.
Dans l'étape de cryptage, l'utilisateur soumet un texte qu'il veut crypter, "FaceCloak" le remplace par un faux texte aléatoire de Wikipedia, le vrai texte sera crypté et envoyé à un serveur tiers.
Dans l'étape de décryptage, "FaceCloak" utilise les clés distribuées dans la première phase pour vérifier si l'utilisateur est autorisé à décrypter le contenu. Le texte aléatoire agit comme un index des données chiffrées sur le serveur. Le problème avec cette solution est que tous les fichiers liés au compte Facebook (liste des amis, clés, etc.) sont stockés dans le répertoire de la machine locale de "Firefox", par-conséquent si l'utilisateur

change de machine, il perdra tous ses fichiers. Un autre problème avec "FaceCloak" est que l'utilisation de texte provenant de "Wikipedia" peut entraîner des conflits sociaux.

Une autre solution appelée "Scramble" est proposée dans [11]. Cette solution est basée sur la cryptographie asymétrique, chaque utilisateur a une clé publique et secrète "PKu, SKu", seule la clé publique "PKu" est connue par toutes les relations de l'utilisateur. L'échange de "PKu" se fait lorsqu'une relation d'amitié s'établit. "Scramble" permet à l'utilisateur de contrôler ses données et de spécifier qui peut y accéder. Si un utilisateur "A" souhaite partager un contenu avec un ensemble d'utilisateurs, il doit être en possession de toutes leurs clés publiques. Cette solution utilise le chiffrement hybride, le contenu est chiffré par une clé secrète "k" générée de façon aléatoire (clé de session) avec un algorithme symétrique, puis cette clé est chiffrée à l'aide de la clé publique de chaque utilisateur. L'intégrité du contenu est assurée en se basant sur la signature avant le chiffrement.
Le module principal de "Scramble" est une extension "Firefox" développée principalement en "JavaScript", la gestion des clés est gérée par "Scramble". Les utilisateurs échangent leurs clés publiques via "OpenPGP" [17], les clés "OpenPGP" de tous les utilisateurs sont stockées dans la machine des utilisateurs (utilisateur qui souhaite partager des données avec un ensemble d'utilisateurs).
Le deuxième module est "Tiny LinkServer", ce serveur a été développé pour éviter la limitation de la taille du contenu crypté imposée par les réseaux sociaux. Le serveur stocke des données cryptées et renvoie une courte URL qui est publiée sur le réseau social.

1.2.2.2 Stockage de données sensibles indépendamment de la machine locale de l'utilisateur

Tootoonchian et al [18] ont proposé "imageLock", c'est une autre solution basée sur une extension "Firefox". La solution publie une fausse image sur le réseau social et stocke l'image réelle ailleurs. L'image réelle est stockée sur un serveur tiers en format non crypté et une fausse image est téléchargée sur le réseau social avec quelques informations supplémentaires telles que id de l'image et "URL". Le problème avec cette solution est que les images sont stockées au format non crypté sur un serveur tiers et cette approche ne convient qu'aux images.

Guha et al [19] ont proposé une solution basée sur le chiffrement par substitution aléatoire pour protéger la confidentialité des utilisateurs appelée "NOYB None Of Your

Business". Les informations des utilisateurs sont divisées en atomes (morceaux de données, exemple, nom, genre, etc.). "NOYB" remplace les données de l'utilisateur "A" par un atome provenant d'un autre utilisateur qui utilise "NOYB", par-exemple si on a des utilisateurs "B", "C" et "D". L'utilisateur "A" est en possession des atomes nom "A", genre "A", adresse "A", ils sont remplacés par nom "B", genre "C", adresse "D" des utilisateurs "B", "C" et "D" respectivement. Ainsi, seul l'utilisateur "A" et ses amis peuvent inverser le processus et reconstruire le profil de chaque utilisateur. La technique "NOYB" possède certaines limites, elle n'est appliquée qu'au profil de l'utilisateur. Les données publiées sur le mur ou l'actualité dans l'application Facebook ne sont pas protégées. L'efficacité de "NOYB" dépend du nombre d'utilisateurs et l'anonymat est meilleur lorsque le nombre d'utilisateurs augmente. Un autre problème concerne les vieux amis, ils ne peuvent pas rester en contact à moins d'avoir suffisamment des données pour retrouver le profil.

1.3 Conclusion

Dans cette partie nous avons traité les réseaux sociaux en ligne "Online Social Network OSN" comme Facebook et leurs impacts dans la vie quotidienne des utilisateurs. Avec la grande quantité d'informations qui est partagée sur le web, les "OSNs" collectent toutes les activités et les informations sur les utilisateurs. Nous avons proposé une classification des solutions qui traitent la protection de la vie privée des utilisateurs. Nous les avons classées selon la dépendance par rapport aux plateformes "OSN", et selon l'emplacement du stockage des données sensibles des utilisateurs.
Le chapitre suivant sera dédie au fonctionnement de la cryptographie ainsi qu'une classification des solutions d'attributs "ABE" a été abordée. Par la suite, nous avons abordé le cloud computing en tant que service qui sera utilisé pour externaliser les données crypté par "ABE".

Chapitre 2

LE CHIFFREMENT À BASE D'ATTRIBUTS ATTRIBUTE-BASED ENCRYPTION "ABE"

Sommaire

2.1 Introduction 13
2.2 La cryptographie 13
2.2.1 Le fonctionnement de la cryptographie 14
2.3 Infrastructure à clés publiques "Public Key Infrastructure" 17
2.3.1 Les composants d'une PKI 18
2.3.2 La PKI et la hiérarchie de confiance 19
2.3.3 L'autorité de certification 21
2.3.4 Le certificat électronique 21
2.3.5 La structure d'un certificat 22
2.4 Le chiffrement à base d'attributs "ABE" 24
2.5 La classification des solutions ABE 25
2.5.1 Le schéma CP-ABE Ciphertext Policy Attribut Based Encryption 26
2.5.2 Le schéma KP-ABE Key-Policy Attribut Based Encryption . 27
2.5.3 Les solutions ABE avec une formule d'accès monotonic . . . 29
2.5.4 Les solutions ABE avec une formule d'accès non-monotonic . 29
2.5.5 Les solutions ABE Hiérarchique 30
2.5.6 Le schéma ABE distribué 30
2.6 Le cloud computing 32
2.6.1 Les caractéristiques du cloud computing 32
2.6.2 Les modèles de déploiement du cloud 33
2.6.3 Les différents services du cloud 33
2.7 Conclusion 37

2.1 Introduction

Le chiffrement ou connu sous l'acronyme "le cryptage" est une technique qui consiste à dissimuler une donnée claire et la rendre non compréhensible. Le déchiffrement ou "le décryptage" est le procédé inverse qui permet de restituer la donnée d'origine.
Le cryptage de la donnée produit une donnée illisible appelée "donnée chiffrée" ou "cryptogramme". L'utilisation du chiffrement garantit que la donnée restera inaccessible à tous ceux qu'ils n'auront pas le droit d'y accéder.

Plusieurs techniques de chiffrement existent à savoir le chiffrement symétrique, le chiffrement asymétrique et le chiffrement à base d'attributs. Le chiffrement symétrique consiste en l'utilisation d'une seule clé pour le cryptage des données, tandis que le chiffrement asymétrique utilise deux clés différentes pour le cryptage et le décryptage des données respectivement. Le chiffrement par attributs est une nouvelle technique qui consiste en l'utilisation des attributs pour crypter une donnée, ce type de chiffrement fait partie du cryptage asymétrique

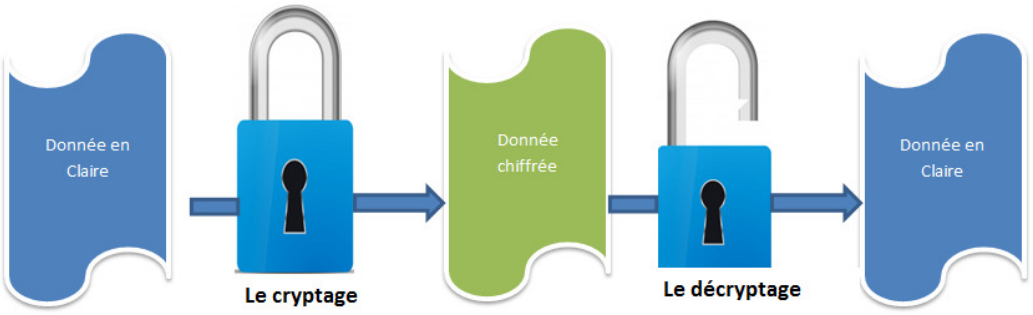

FIGURE 2.1 – Le processus du chiffrement et déchiffrement

2.2 La cryptographie

La cryptographie est la science qui utilise les mathématiques pour crypter et décrypter les données, les termes cryptés et chiffrés ainsi que décryptés et déchiffrés sont utilisés d'une manière interchangeable. La cryptographie moderne apporte des solutions à des problèmes tels que :

1. L'identification de la source.
2. L'authentification de l'origine de données.
3. La confidentialité des données.

4. L'intégrité des données.
5. La non-répudiation.
6. L'anonymat des communicants.

L'utilisation de la cryptographie permet d'envoyer des données sensibles sur un réseau non sécurisé et l'accès aux données cryptées n'est pas permis qu'aux personnes autorisées La cryptographie est le processus de sécurisation de l'information et la cryptanalyse est le processus inverse de la cryptographie, elle combine plusieurs outils d'applications mathématiques et de raisonnements analytiques pour casser la cryptographie.

2.2.1 Le fonctionnement de la cryptographie

La robustesse du chiffrement des données dépend de deux paramètres à savoir : l'algorithme de chiffrement et la clé secrète. L'algorithme de chiffrement est une fonction mathématique utilisée dans la phase du cryptage. Son fonctionnement est associé avec une "clé" en forme de nombre, un mot ou une chaîne de caractère. Deux types de chiffrement sont disponibles à savoir :

1. La cryptographie conventionnelle ou "la cryptographie à clé secrète " ou bien à clé symétrique.
2. La cryptographie à clé publique ou bien à clé asymétrique.

2.2.1.1 La cryptographie symétrique

Dans la cryptographie symétrique, une seule clé est utilisée à la fois pour le chiffrement et le déchiffrement de la donnée comme illustré dans la Figure 2.2. Un exemple des algorithmes à clé symétrique est "Triple DES" (3DES) "Data Encryption Standard" [20]. C'est un algorithme de chiffrement symétrique par bloc, il a été développé par Walter Tuchman d'IBM (chef de projet de "DES" Data Encryption Standard). Le fonctionnement de cet algorithme est basé sur le mode "EDE" "Encryption, Decryption et Encryption", ce qui le rend compatible avec le "DES". LE "3 DES" utilise une taille du bloc de 64 bits et une longueur de clé qui varie entre 112 et 168 bit. On trouve aussi le "AES Advanced Encryption Standard ", qui est plus récent développé par le "NSA National Security Agency", il devint le standard de chiffrement pour les organisations du gouvernement des États-Unis [21].

Le chiffrement symétrique a des avantages à savoir la rapidité de chiffrement en utilisant une clé unique pour le cryptage et le décryptage des données. Cependant, ce type de chiffrement pour la transmission des données sécurisées peut-être assez pénible

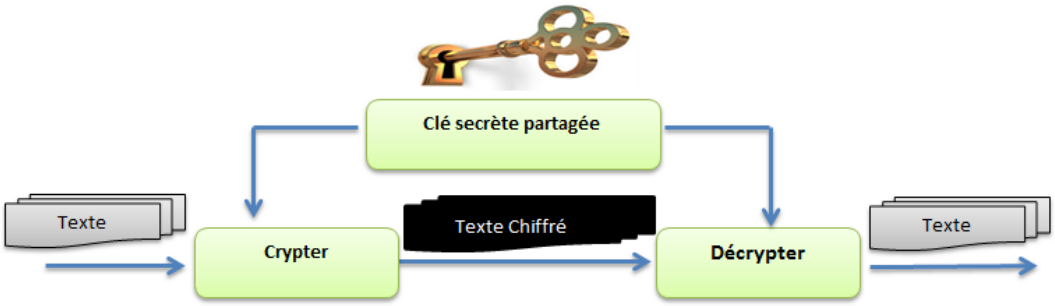

FIGURE 2.2 – Le chiffrement à base de clé symétrique

en raison des difficultés rencontrées dans la distribution sécurisée de la clé secrète. Donc le défi avec le chiffrement symétrique est la "distribution de la clé (clé de session)".

2.2.1.2 La cryptographie asymétrique

La cryptographie asymétrique ou connue comme la cryptographie à clé publique est venue pour la résolution du problème de la distribution des clés dans le chiffrement symétrique. Le concept fut inventé par les deux auteurs "Whitfield Diffie et Martin Hellman" [22]. La cryptographie asymétrique se repose sur un schéma utilisant une paire de clés pour le cryptage : une clé publique permettant le chiffrement des données et une clé privée servant comme une clé de déchiffrement comme illustré dans la Figure 2.3. La clé privée n'est jamais transmise à quiconque, alors que la clé publique est transmissible sans restriction.

FIGURE 2.3 – Le chiffrement asymétrique

Un système reposant sur la cryptographie à clé publique nous permet de :

1. Crypter la donnée permet de garantir la confidentialité de cette dernière en utilisant la clé publique pour la chiffrer et la clé privée du destinataire pour la déchiffrer
2. L'authenticité de l'expéditeur, ce dernier envoie un message chiffré avec sa clé privée au destinataire, celui-ci utilise la clé publique de l'expéditeur afin de déchiffrer le message reçu pour authentifier l'auteur du message.

La déduction de la clé privée depuis la clé publique est mathématiquement impossible. Une personne en possession de la clé publique a la possibilité de chiffrer un message mais elle ne peut pas le déchiffrer. Seule la personne en possession de la clé privée est en mesure de déchiffrer le message. La nécessité pour que les deux interlocuteurs puissent partager des clés privées via un canal de transmission fiable est éliminée. La cryptographie asymétrique est basée sur une fonction mathématique à sens unique dont il est extrêmement difficile de retrouver la donnée d'origine ainsi que la clé secrète. supposons que deux interlocuteurs dénommés "Alice" et "Bob" veulent communiquer sur un canal peu fiable susceptible d'être écouté par une personne malveillante "Eve" :

1. Alice envoie à Bob sa clé publique et garde pour elle la clé secrète.
2. Bob utilise la clé publique d'Alice pour chiffrer son message.
3. Alice reçoit le message chiffré ensuite le déchiffre à l'aide de sa clé privée.
4. Si un utilisateur malveillant est en écoute sur le canal de communication et il intercepte le message chiffré, il ne pourra pas le déchiffrer, car il n'est pas en possession de la clé privée.

Parmi les exemples des cryptosystèmes asymétriques nous trouvons "Elgamal" (au nom de son inventeur, Taher Elgamal[23], RSA au nom de ses inventeurs, Ron Rivest, Adi Shamir, et Leonard Aldeman[24].

2.2.1.3 L'authentification

Un autre problème qui peut surgir dans la cryptographie asymétrique est le fait que la clé publique est distribuée à toutes les personnes. De ce fait, lorsqu'une personne est en possession de sa clé privée, elle n'a pas les moyens pour vérifier la source de provenance des messages qui lui sont adressés, nous parlons de problèmes d'authentification. La résolution de ce problème est l'utilisation d'un mécanisme d'authentification afin de garantir la source des données chiffrées :

1. L'expéditeur Bob va créer une paire de clés asymétriques publique/privé, la clé publique est diffusée librement.

2. Le destinataire Alice va opter pour la même opération.
3. Bob effectuera un hachage sur son message à l'aide d'une fonction de hachage [25], après il crypte ce dernier avec sa clé privée.
4. Bob chiffre le tout avec la clé publique d'Alice et il lui envoie le message chiffré.
5. Alice va recevoir le message chiffré sur un canal de communication peur fiable, donc quelqu'un d'autre pourra l'intercepter.
6. Alice déchiffre le message avec sa clé privée et obtiendra le message crypté avec la clé privée de Bob sous forme de Hachage.
7. Alice utilisera la clé publique de Bob afin de s'assurer que le message provient de Bob, dans le cas contraire, le message ne peut pas être déchiffré et elle peut en déduire que le message a été altéré par une personne malveillante.

Cette technique d'authentification est basée sur les spécificités de la cryptographie asymétrique : nous pouvons chiffrer une donnée avec la clé publique du destinataire et assurait l'authenticité du message grâce au chiffrement avec la clé privée de l'expéditeur.

2.3 Infrastructure à clés publiques "Public Key Infrastructure"

Les infrastructures à clés publiques ou "PKI Public Key Infrastructure" sont constituées d'un ensemble d'équipements physiques et de logiciels cryptographiques permettant de gérer les certificats électroniques des utilisateurs [26].
La "PKI" permet de faire la liaison entre la clé publique et son propriétaire, elle représente une garantie de confiance sur la validité de la clé publique. Le rôle d'une infrastructure à clés publiques consiste en la délivrance des certificats électroniques ou numériques contenant la clé publique de l'utilisateur. Les certificats électroniques sont utilisés dans le chiffrement et les signatures numériques des données, l'utilisation des certificats électroniques permet de :

1. Garantir la confidentialité des données, seul l'utilisateur en possession de la clé privée pourra déchiffrer les données.
2. Garantir l'authentification de l'expéditeur des données.
3. Garantir l'intégrité, elle permet de garantir que les données n'ont pas été altérées pendant la transmission.

4. La non-répudiation, elle permet d'assurer que l'expéditeur ne renie pas l'action entreprise.

Plusieurs modèles d'infrastructure à clés publiques existent, parmi ces modèles nous citons :

1. Les autorités de certification "CA" Certificate Autority.
2. La toile de confiance c'est un concept répandu dans les systèmes décentralisés tels que "PGP Pretty Good Privacy" [27].

2.3.1 Les composants d'une PKI

La PKI est composée de plusieurs entités, chaque entité est responsable d'une tâche particulière à savoir :

— L'autorité de certification :
  — Émetteur de certificats.
  — Émetteur de la liste de révocation.
— L'autorité d'enregistrement "RA Registration Authority".
— L'annuaire de publication.
— Les administrateurs.

La PKI est responsable sur les certificats délivrés, elle est présente pour suivre le cycle de génération d'un certificat électronique comme illustré dans la Figure 2.4. Les différentes phases du cycle de génération d'un certificat électronique peuvent être illustrées dans ces étapes :

1. L'autorité d'enregistrement : son rôle consiste en l'enregistrement des demandes des certificats et la vérification des informations des demandeurs.
2. L'autorité de certification : elle crée et distribue les certificats.
3. L'autorité de validation : son rôle consiste à vérifier la validité des certificats.
4. La révocation des certificats non valides par CRL "Certificate Revocation List"
5. Annuaire des certificats : un dépôt pour publier les certificats ainsi que les certificats révoqués, en utilisant par exemple le standard LDAP "Lightweight Directory Access Protocol".

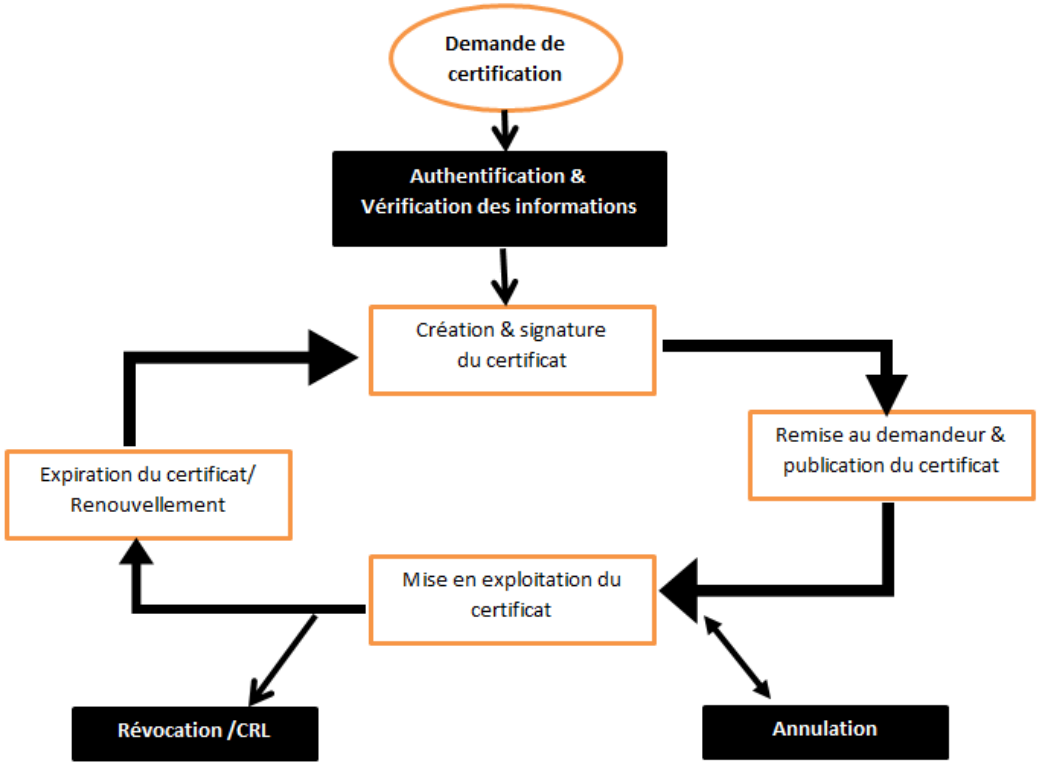

FIGURE 2.4 – PKI : cycle de génération d'un certificat

2.3.2 La PKI et la hiérarchie de confiance

Au départ, La "CA" pour générer et signer des certificats électroniques pour des applications d'utilisateurs, elle doit signer son propre certificat pour prouver son identité. Ce type de "CA" est appelé Autorité de Certification racine "rootCA". Une autorité de certification peut être constituée de plusieurs autres autorités de certifications, par exemple "Globalsign"[28], elle représente une "CA" publique exploitant plusieurs "CA" sous forme hiérarchique, cette disposition permet de créer une chaîne de confiance.

Chaque autorité de certification est en possession de son propre certificat pour prouver son identité. Ce certificat est signé par l'autorité hiérarchiquement supérieure et ainsi de suite jusqu'à l'autorité racine comme illustré dans la Figure 2.5. L'intérêt principal de cette hiérarchie est d'étendre le domaine de sécurité. Le but de cette hiérarchie et de ce concept c'est de créer un large domaine de confiance sur des réseaux peu sécurisés comme internet. Le nombre de niveaux entre le "RootCA" certificat racine et le certificat d'utilisateur final et la complexité de la hiérarchie varient en fonction de l'environnement du travail IoT, l'industrie, etc.

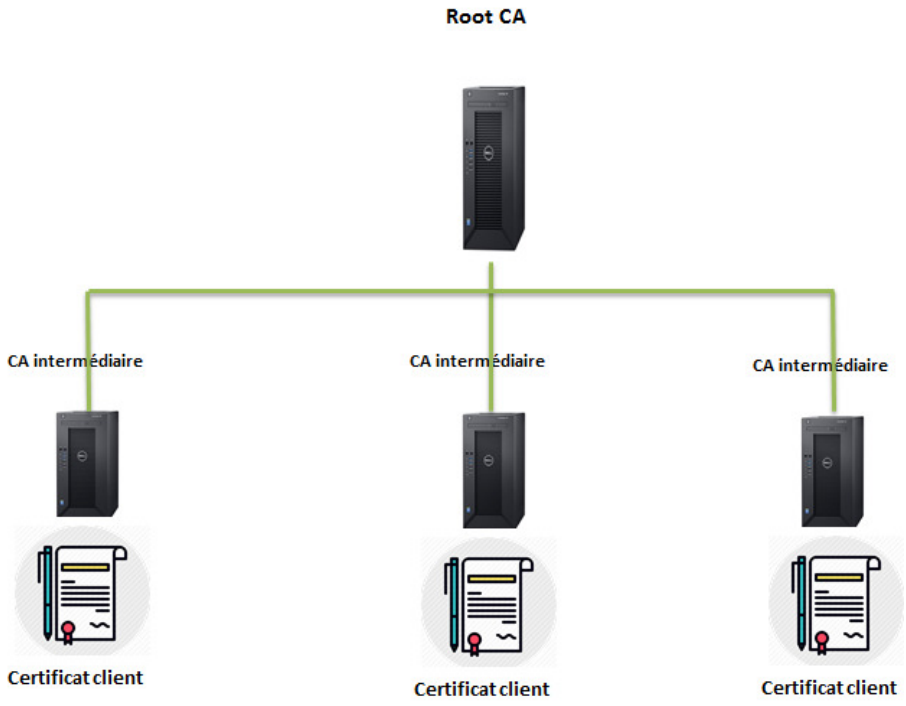

FIGURE 2.5 – La hiérarchies de l'autorité de certification

La hiérarchie de l'autorité de certification comporte principalement trois éléments clés à savoir :

- **La "RootCA"** : c'est l'autorité de certification racine située au niveau le plus élevé de la hiérarchie. Elle représente l'autorité de confiance à laquelle les "CAs" intermédiaire et les entités finales sont reliées. La "RootCA" est isolée de l'accès réseau et souvent maintenu dans un état de "offline" pour conserver sa sécurité et la protéger contre "key escrow". Un compromet des clés de l'autorité root rendraient la racine et tous les certificats qui sont émis par elle non fiables. Le rôle de la "RootCA" consiste en la création de la "CA intermédiaire".
- **La "CA intermédiaire"** : elle se situe entre le "RootCA" et les certificats d'entités finales. Son rôle consiste en l'émission, la distribution et la révocation des certificats électroniques sans l'action directe de la "RootCA".
- **Les certificats d'entités finales** : elles représentent les certificats qui seront installés au niveau des serveurs des utilisateurs. Exemple les certificats "SSL/TLS" pour chiffrer les communications en utilisant le HTTPS, le "S/MIME" utilisé pour chiffrer les émails.

2.3.3 L'autorité de certification

Une autorité de certification "Certificate Authority" CA est un tiers de confiance enregistré et certifié par les autorités publiques. Son rôle principal consiste à délivrer des certificats électroniques pour des personnes morales ou physiques tout en mettant en place des moyens de vérification de la validité des certificats délivrés. Un certificat électronique respecte un standard qui spécifie son contenu. Les deux formats les plus utilisés sont :

1. X.509 définit par RFC 5280 [29].
2. OpenPGP, défini par RFC 4880 [30].

Le certificat X.509 est basé sur un seul identifiant et ne peut être signé que par une seule autorité de certification. Par contre, le certificat "OpenPGP" peut avoir plusieurs identifiants et peut-être signer par plusieurs certificats "openPGP", ce qui permet de former une toile de confiance. Les navigateurs modernes intègrent une liste de certificats provenant de différentes autorités de certification choisie par les développeurs du navigateur.

La mise en place d'un serveur web basé sur le protocole sécurisé HTTPS nécessite la génération d'une paire de clés publique & privée, puis une demande de signature est envoyée au "CA" sous forme de "CSR" Certificate Signing Request, La "CSR" contient la clé publique ainsi que l'identité du propriétaire. La "CA" procède à la vérification de l'identité du demandeur par l'autorité d'enregistrement "RA". L'autorité de certification signe le "CSR" et envoie le certificat à l'entité qu'il a demandée. Le certificat envoyé par la "CA" sera placé dans le serveur web du propriétaire. Ainsi, lorsqu'une personne veut se connecter au serveur web en utilisant le protocole HTTPS, le serveur web lui transmettra le certificat précédemment installé. Une fois l'utilisateur connecté, le navigateur procédera à l'authentification du serveur auprès de l'autorité de certification intégrée dans le navigateur, ainsi, le "CA" authentifié l'identité du serveur à l'utilisateur. Le navigateur de l'utilisateur envoie ensuite une demande "OCSP" "Online Certificate Status Protocol " [31] pour vérifier si le certificat du serveur n'a pas été révoqué.

2.3.4 Le certificat électronique

Le certificat électronique est un ensemble de données utilisé pour garantir la sécurité des systèmes d'informations à savoir : l'authentification, la confidentialité et l'intégrité des données ainsi que la non-répudiation. Le certificat électronique ou numérique est composé de deux parties à savoir :

1. L'information d'identification du certificat :
   — Le nom du propriétaire.
   — L'adresse du propriétaire.
   — La date de validité du certificat.
2. La clé publique du propriétaire et la signature de la "CA" pour prouver l'exactitude des informations du certificat.

Les certificats électroniques peuvent être utilisés dans différents domaines à savoir : les serveurs web, la messagerie électronique [32], dans les VPNs "Réseau virtuel privé" avec "IPSEC" [33].

2.3.5 La structure d'un certificat

Le certificat X.509 définit par RFC 5280 [29] peut contenir les champs qui sont illustrés dans la Figure 2.6.

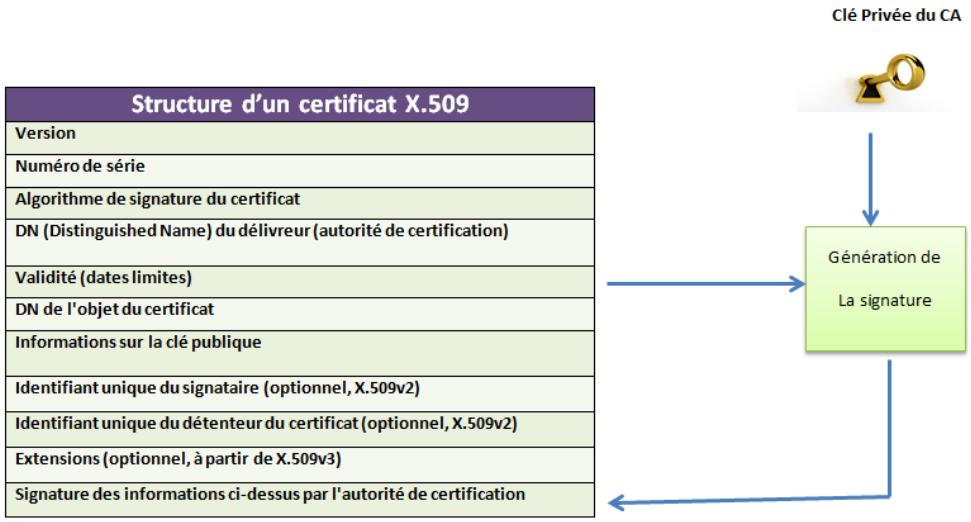

FIGURE 2.6 – La structure d'un certificat X.509

Parmi les champs :

1. La version : indiquant la version du certificat.
2. Le numéro de série.
3. Le nom de l'émetteur du certificat.
4. Les dates de validations.

5. Les informations concernant la clé publique.
6. Des champs optionnels à savoir : identifiant du signataire, etc.
7. La signature de la "CA".

Le certificat électronique sera signé avec la clé privée de l'autorité de certification afin de prouver l'authenticité du certificat.

2.4 Le chiffrement à base d'attributs "ABE"

Le chiffrement par attributs "Attribute-Based Encryption ABE" est une technique de cryptographie de la famille de chiffrement asymétrique dans laquelle la clé de chiffrement d'un utilisateur dépend des attributs qui lui sont assignés.
Ce type de chiffrement permet d'instaurer un contrôle d'accès basé sur le rôle. Le concept de chiffrement par attributs a été proposé la première fois par Adi Shamir [34] dans "Identity-Based cryptosystems and schemes".

Le système proposé par "Shamir" repose sur un schéma de cryptographie basé sur l'identité de l'utilisateur. La clé de chiffrement est dérivée de l'identité de l'utilisateur $Ke = I$ et la clé de déchiffrement est dérivée de l'identité de l'utilisateur et une clé aléatoire K, $Kd = f(I, K)$.
Ce système repose sur une entité de génération de clés fiables, son unique rôle consiste a délivré à chaque utilisateur une "Smart Carte SC" dès qu'il rejoint le réseau de communication. Les informations stockées dans la "SC" permettent à l'utilisateur de chiffrer et de signer les messages envoyés, déchiffrer et vérifier les messages reçus grâce à la signature intégrée dans le message.

La clé publique de l'utilisateur Ke est une combinaison de son nom et son numéro de sécurité sociale, ou son adresse ,ou son numéro de téléphone, etc. Dans ce cas-là, l'utilisateur ne pourra pas nier une action entreprise avec sa clé publique. "Sahai" et "Waters" ont proposé un nouveau type de "Identity-Based Encryption IBE" en 2005 appelé "Fuzzy Identity-Based Encryption FIBE" [35]. Dans "FIBE" l'identité de l'utilisateur est vue comme un ensemble d'attributs descriptifs permettant une certaine flexibilité aux erreurs concernant l'identité choisie.

Le schéma proposé par "Sahai" et "Waters" permet à un utilisateur en possession de la clé privée avec une identité I de déchiffrer une donnée chiffrée avec une identité I', seulement si les deux identités I et I' sont proches avec une certaine tolérance mesurée. Le schéma "FIBE" peut être utilisé dans le chiffrement basé sur la biométrie. Un exemple de l'utilisation de "FIBE" est dans le scanner d'iris, en se basant sur l'aspect de "la fuzzy", les données peuvent être déchiffrées avec une tolérance légère aux erreurs. Le "FIBE" schéma est basé sur une stratégie de seuil, dans laquelle un utilisateur peut crypter une donnée en précisant un ensemble d'attributs et un nombre k, de sorte que seul un destinataire avec au moins k des attributs donnés peut décrypter l'information. Cependant, l'architecture de "FIBE" proposée est basée sur l'existence d'une seule autorité de confiance qui surveille tous les attributs et émet toutes les clés de déchiffrement.

D'autres travaux ont été publiés dans la même philosophie à savoir le travail de Bethencourt et al [14], Zhou et al [36] et Shao et al [37]. Ces auteurs ont proposé une solution d'ABE plus pratique et flexible.
Dans le chiffrement par attributs, il existe deux types de politique d'accès à savoir : la politique d'accès autour du message chiffré et la politique d'accès basé sur la clé de chiffrement. Les deux approches sont connues comme CP-ABE et KP-ABE respectivement.

2.5 La classification des solutions ABE

Le chiffrement par attribut est une nouvelle technique qui a prouvé son efficacité dans un environnement de **cloud computing**. C'est une solution prometteuse en matière de cryptographie par rapport aux solutions de chiffrements traditionnelles. Le chiffrement par attribut permet d'avoir des applications plus sécurisées et plus performantes en comparaison à d'autres solutions. Le chiffrement par attribut peut être classifié selon la Figure 2.7 en six catégories à savoir :

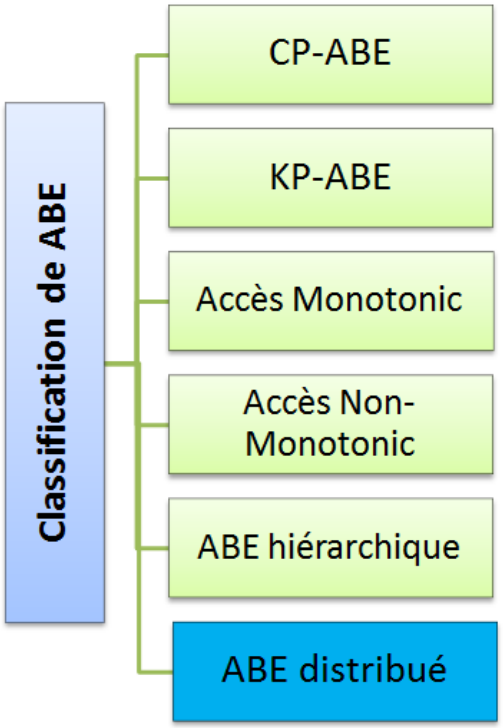

FIGURE 2.7 – La classification de ABE

1. CP-ABE.

2. KP-ABE.
3. Solutions ABE avec une formule d'accès monotonic.
4. Solutions ABE avec une formule d'accès non-monotonic.
5. Solution ABE hiérarchique.
6. Solution ABE distribuée

2.5.1 Le schéma CP-ABE Ciphertext Policy Attribut Based Encryption

Le premier schéma de "CP-ABE Ciphertext Policy Attribut Based Encryption" a été proposé par Bethencourt et al [14]. Le "CP-ABE" est basé sur la politique d'accès sur le message crypté. Ce schéma consiste à définir une politique d'accès associé au message chiffré. De ce fait, un utilisateur est en mesure de décrypter une donnée chiffrée si et seulement si les attributs associés à son identité correspondent à la politique d'accès définie pour la donnée. La politique d'accès est définie par des opérations de conjonctions et disjonctions et de plus associe un seuil au nombre d'attributs pour déchiffrer une donnée.

Exemple :

Un ensemble d'attributs $A = (I, J, K, L)$. Un utilisateur pourra envoyer un message avec une politique $(I et K)$ ou L, un utilisateur est en possession de l'attribut L pourra déchiffrer le message, un autre utilisateur est en possession des attributs $(I et L)$ ne pourra pas le décrypter. Le chiffrement CP-ABE est basé sur quatre algorithmes comme illustré dans la Figure 2.8.

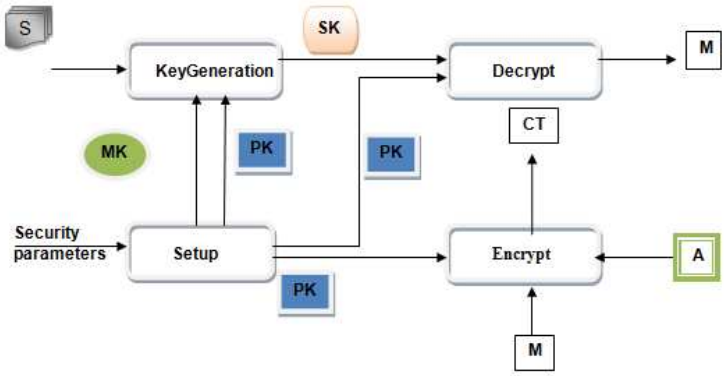

FIGURE 2.8 – Le schéma de CP-ABE "Ciphertext Policy Attribut Based Encryption"

1. Algorithme d'initialisation.
2. Algorithme de génération de clés
3. Algorithme de chiffrement.
4. Algorithme de déchiffrement.

Algorithme d'initialisation : l'algorithme d'initialisation ou de "setup" est utilisé pour générer la clé maîtresse "Master Key" MK et la clé Publique PK. Elles sont générées par l'autorité d'attributs, qui seront utilisées par la suite dans l'algorithme de génération de clés.
Algorithme de génération de clés : l'objectif principal de cet algorithme est la génération de clés, il prend comme paramètres la clé maîtresse MK et la clé publique PK et un ensemble d'attributs S, $KeyGeneration(S, PK, MK) = SK_u$. La clé SK_u décrit l'utilisateur et possède l'ensemble des attributs qui permet à l'utilisateur de déchiffrer le texte chiffré CT.
Algorithme de chiffrement : Cet algorithme permet de générer un texte chiffré "CipherText CT" du message "M" pris comme paramètres avec une politique d'accès sous forme de conjonction et disjonction.
Algorithme de déchiffrement : Cet algorithme utilise un certain nombre de paramètres à savoir : SK_u représentant la clé secrète de l'utilisateur avec l'ensemble d'attributs S, la clé publique PK et le texte chiffré avec la politique d'accès. Le résultat de cet algorithme est le message "M" en clair si l'utilisateur avec son ensemble d'attribut satisfait la politique d'accès, sinon un message d'erreur sera affiché à l'utilisateur.
Algorithme de délégation : Cet algorithme prend comme paramètre la clé secrète SK générée par l'algorithme de génération de clés et un ensemble d'attributs $S' \subseteq S$. Le résultat est une clé secrète SK' pour un ensemble d'attributs S'. Si l'utilisateur est en possession de l'ensemble d'attributs qui satisfait la politique d'accès A, le message d'origine M sera déchiffré par l'algorithme de déchiffrement.

2.5.2 Le schéma KP-ABE Key-Policy Attribut Based Encryption

Le schéma "KP-ABE Key-Policy Attribut Based Encryption" a été proposé par Goyal et al [38]. Le "KP-ABE" est basé sur la politique d'accès sur la clé secrète. La clé de l'utilisateur est associée à la politique d'accès et le texte est chiffré avec un ensemble d'attributs. L'utilisateur est en mesure de décrypter le texte chiffré si les attributs associés à sa clé correspondent aux attributs liés au message chiffré.

Exemple :

Un ensemble d'attributs $A = (I, J, K, L)$. Un utilisateur est en possession d'une clé avec une politique d'accès $(IetK)$ ou L. Il est en mesure de décrypter le message avec les attributs L, mais il ne pourra pas sur un message associé avec les attributs $(IetJ)$ Le chiffrement KP-ABE est basé sur 4 algorithmes comme illustré dans la Figure 2.9 :

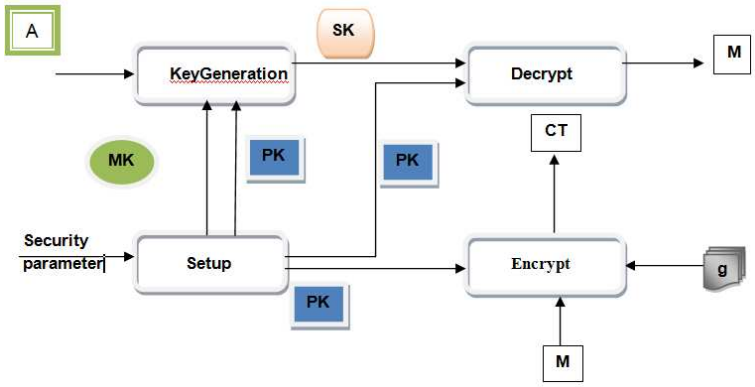

FIGURE 2.9 – Le schéma de KP-ABE "Key Policy Attribut Based Encryption"

1. Algorithme d'initialisation.
2. Algorithme de génération de clés
3. Algorithme de chiffrement.
4. Algorithme de déchiffrement.

Algorithme d'initialisation : l'algorithme d'initialisation ou de "setup" est utilisé pour générer la clé maîtresse "Master Key" MK et la clé Publique PK, qui seront utilisées par la suite dans l'algorithme de génération de clés.
Algorithme de génération de clés : l'objectif principal de cet algorithme est la génération des clés des utilisateurs, il prend comme paramètres la Master key MK et la clé publique PK et la politique d'accès d'attributs A, $KeyGeneration(A, PK, MK) = SK_u$. La clé SK_u contenant la politique d'accès permet à l'utilisateur de déchiffrer le message crypté.
Algorithme de chiffrement : Cet algorithme permet de générer un texte chiffré "CipherText CT" du message "M", il prend comme paramètre la PK,la MK et un ensemble d'attributs g.
Algorithme de déchiffrement : Cet algorithme utilise un certain nombre de paramètres à savoir : SK_u représentant la clé secrète de l'utilisateur avec la politique d'accès

A, la clé publique PK et le texte chiffré avec l'ensemble d'attributs. Le résultat de l'algorithme est le message M en clair si l'utilisateur satisfait les attributs associe au message crypté.

La politique d'accès est un ensemble d'attributs représente par :

— Une structure d'accès monotone.

— Des portes AND, OR et nous pouvons trouver un seuil K de n attributs. Exemple (2 of 3) des attributs comme illustré dans la Figure 2.10.

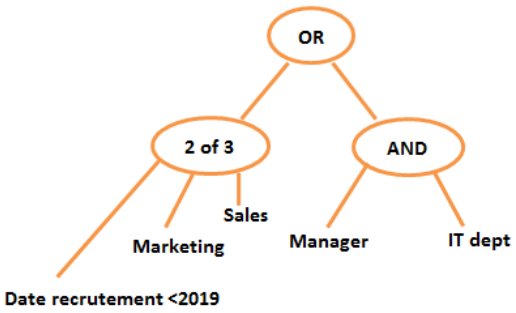

FIGURE 2.10 – La politique d'accès sous forme d'arbre "Tree"

2.5.3 Les solutions ABE avec une formule d'accès monotonic

Une formule d'accès monotonic consiste en la génération d'une structure d'accès en utilisant les portes AND, OR et elle peut être exprimée sous forme de seuil $n - de - m$ attributs. Dans CP-ABE [14] et KP-ABE [38] la structure d'accès est exprimée sous forme de formule monotone avec des contraintes positives. Exemple : l'utilisateur en possession de la politique d'accès suivante pourra décrypter la donnée (départ-info AND chef-départ) OR doyen-Faculté. La limitation de cette formule et qu'elle ne peut pas être exprimée sous forme de contraintes négatives (not départ-info AND chef-départ) OR doyen-Faculté.

2.5.4 Les solutions ABE avec une formule d'accès non-monotonic

Pour résoudre le problème des contraintes négatives, plusieurs travaux ont été proposés, Ostrovsky et al [39] ont proposé un schéma de KP-ABE supportant n'importe quelle formule d'accès en incluant les formules non-monotonics. Le premier schéma de CP-ABE supportant les contraintes négatives a été proposé par Cheung et al [40], la

solution proposée est basée seulement sur les portes AND et NOT. Les auteurs dans [41]ont proposé un schéma de CP-ABE incluant les portes AND, OR et la négation des contraintes.

2.5.5 Les solutions ABE Hiérarchique

Le modèle ABE hiérarchique "HABE" est structuré sous forme d'une arborescence, plusieurs travaux ont été réalisés dans ce modèle, Gentry et Silverberg[42] ont proposé "Hierarchical Identity-Based Encryption HIBE", leur schéma est basé sur CP-ABE et l'hypothèse de Bilinear Diffie-Hellman "BDH" [43], cette dernière consiste en une hypothèse calculatoire dans le problème du calcul du logarithme discret.

Un autre travail a été proposé par Boneh et Boyen [44] basé sur la sécurité sélective des ID "IDentifier" et l'hypothèse de "BDH". Les deux schémas proposés souffrent de temps de chiffrement et de déchiffrement qui augmentent avec la profondeur d'un destinataire dans la hiérarchie.

Dans le travail publié par Waters et Brent [45], ils ont proposé un système appelé "fully secure IBE and HABE" en utilisant "dual system encryption", qui consiste en une simple hypothèse de "BDH" et une hypothèse linéaire décisionnelle. D'autres travaux récents ont été proposés, Li et al[46] ont présenté "Hierarchical attribute based encryption with continuous leakage-resilience", Wei et al[47] ont proposé un schéma d'accès basé sur des attributs hiérarchiques pour un partage sécurisé des dossiers de santé électronique dans le cloud public, ALi et al[48] ont proposé un système de HABE pour l'internet des objets.

2.5.6 Le schéma ABE distribué

Les variantes de "ABE" présentées ci-dessus sont basées en général sur une seule autorité d'attributs. Avec cette configuration la solution souffre de problèmes de flexibilité et d'évolutivité, cela permet de créer une vulnérabilité appelée "single point of failure" point de défaillance unique. Les chercheurs se sont focalisés sur ce problème afin de proposer des solutions qui seront basées sur une architecture d'ABE distribuées.

Plusieurs travaux ont été développés permettant un contrôle d'accès flexible dans les systèmes de stockage du "cloud computing", cela permettra d'avoir un stockage de données sécurisées. Parmi ces travaux nous citons : Wang et al.[49] qui ont proposé un système de contrôle d'accès pour le "cloud storage". Les auteurs Muller et al[50], Liu et al[51] ont proposé une architecture basée sur une autorité centrale qui manage les

différentes autorités, les solutions proposées soufrent de problèmes de performance dans une architecture distribuée à grande échelle et l'autorité centrale représente un maillant faible et une source de vulnérabilité.

Une solution proposée par les auteurs Lewko et Waters[52] basée sur une architecture "CP-ABE" décentralisée avec multi-autorités dans laquelle l'autorité centrale est éliminée, cette solution ne prend pas en compte le système de révocation de clés des utilisateurs. Une autre architecture avec multi-autorités en prenant en considération la révocation des clés des utilisateurs a été proposée par Yang et al [53] par contre l'architecture comprenait une autorité centrale. Ruj et al dans[54] ont proposé une solution de multi-autorités décentralisées permettant d'avoir un contrôle d'accès avec une authentification anonyme sur les données stockées sur le cloud.

2.6 Le cloud computing

Le cloud computing est un nouveau concept permettant aux utilisateurs d'accéder à la demande à une panoplie de ressources informatiques configurables, exemple : réseaux, serveurs, stockage, applications et services et qui peuvent être libérés rapidement, avec une gestion minimale.

2.6.1 Les caractéristiques du cloud computing

Le modèle du cloud computing est caractérisé par différentes caractéristiques à savoir :

- **Un service libre et à la demande :** L'utilisateur a la capacité de s'approvisionner des ressources informatiques à la demande et d'une manière libre à savoir : la capacité de stockage, réseaux, mémoire, etc. Cela sans avoir besoin de contacter le fournisseur de services.
- **Un large accès au réseau :** L'ensemble des ressources sont disponibles avec un accès réseau permettant aux utilisateurs une exploitation des services avec un ensemble d'outils à savoir : les smartphones, les tablettes, les ordinateurs portables, etc.
- **La mise en commun des ressources :** Le fournisseur de services utilise les ressources selon un modèle multi-tenant. Ce modèle est déployé pour servir plusieurs consommateurs. Les ressources sont disponibles sous forme physique et virtuelle, elles sont allouées dynamiquement en fonction de la demande. Avec la virtualisation et l'allocation dynamique des ressources. Les utilisateurs n'ont aucun contrôle sur les données externalisées et leur emplacement physique et cela pose un problème de confiance envers le fournisseur du cloud.
- **Une élasticité rapide :** Les consommateurs sont en possession d'un système d'approvisionnement dynamique, il répond à leurs besoins instantanément en fonction de la demande. Le besoin des utilisateurs peut être satisfait en quantité et à tout moment et la capacité des fournisseurs cloud est illimitée.
- **Un service mesuré :** Les services du cloud sont basés sur le paiement à l'utilisation ou la facturation à l'utilisation. Le fournisseur de services optimise les ressources d'une manière automatique à savoir : le stockage, le traitement à grande masse, la bande passante, etc. Les services proposés par le fournisseur du cloud surveillent, contrôlent et rapportent tout ce qui se passe sur la plateforme et informent les consommateurs afin d'assurer une transparence sur leur utilisation.

2.6.2 Les modèles de déploiement du cloud

Le cloud computing peut être déployé sous différents modèles [55] :

2.6.2.1 Le cloud privé

L'infrastructure du cloud est destinée à une utilisation unique et exclusive par une seule entreprise. Ce cloud peut être administré et géré par l'entreprise elle même ou bien délégué à un tiers. L'infrastructure physique dans un cloud privé est à la charge de l'entreprise. Les entreprises font recours à un cloud privé parce qu'elles ne font pas confiance aux fournisseurs du cloud sur leurs données.

2.6.2.2 Le cloud publique

Dans ce modèle du cloud, l'infrastructure est destinée aux grands publics, ce type de cloud peut être managé par une entreprise tierce. Le cloud public est proposé sous forme de service à savoir IaaS "infrastructure as a Service", Paas "Plateform as a Service" ou bien Saas "Software as a Service". Ces services sont gérés et managés par des tiers comme Google, Amazon et Microsoft, etc. Avec ce type du cloud, n'importe quel utilisateur ou entreprise peut y héberger ses applications et données. Dans ce cas-là, aucun investissement n'est demandé aux clients. Le provider du cloud facture l'utilisation de ses services selon la consommation et garantit une disponibilité avec un contrat de garantie "SLA Service Level Agreement" [56]

2.6.2.3 Le cloud hybride

Le cloud hybride est une composition de cloud public et privé. Les entreprises peuvent utiliser les deux technologies d'une manière distincte. Elles sont en mesure de déployer des applications à caractère privé dans un cloud privé géré par leurs propres équipes et faire recours à un service de cloud public pour des données moins critiques en termes de confidentialité.

2.6.3 Les différents services du cloud

Les services proposés par le cloud computing les plus connus sont IaaS, PaaS et SaaS comme illustré dans le Figure 2.11, ils fournissent un service complet aux consommateurs.

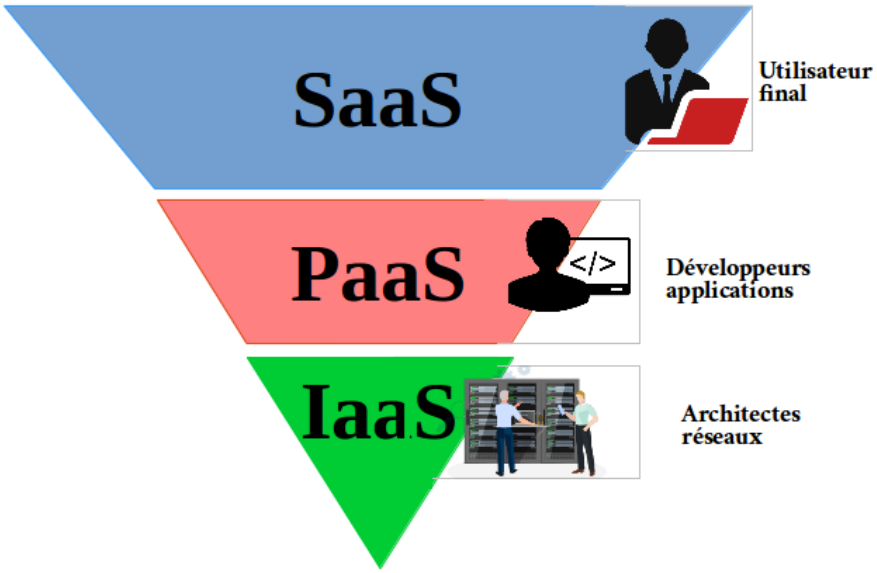

FIGURE 2.11 – Les différents services proposés par le cloud

2.6.3.1 L'infrastructure comme un service "IaaS"

Le service "IaaS" fournit aux consommateurs une capacité de traitement, de stockage du réseau et d'autres ressources informatiques telles que les routeurs et les switchs. Ce service permet aux consommateurs d'héberger et d'exécuter leurs applications, ou encore stocker des données. Les fournisseurs du cloud disposent d'une infrastructure physique sur laquelle nous trouvons une solution de virtualisation permettant la création de machines virtuelles et des datacenters.

2.6.3.2 La plateforme comme un service "PaaS"

La plateforme comme service est destinée à développer, exécuter et déployer des applications. Le fournisseur de cloud prépare une infrastructure dotée des services et des outils tels que les langages de programmation, les bibliothèques permettant aux consommateurs de déployer leurs propres applications. L'infrastructure sous-jacente à savoir le réseau, les serveurs, les systèmes et le stockage ne sont pas gérés ni contrôlés par le consommateur. Une fois les applications sont déployées, le propriétaire n'a le contrôle que sur ce qui a été déployé.

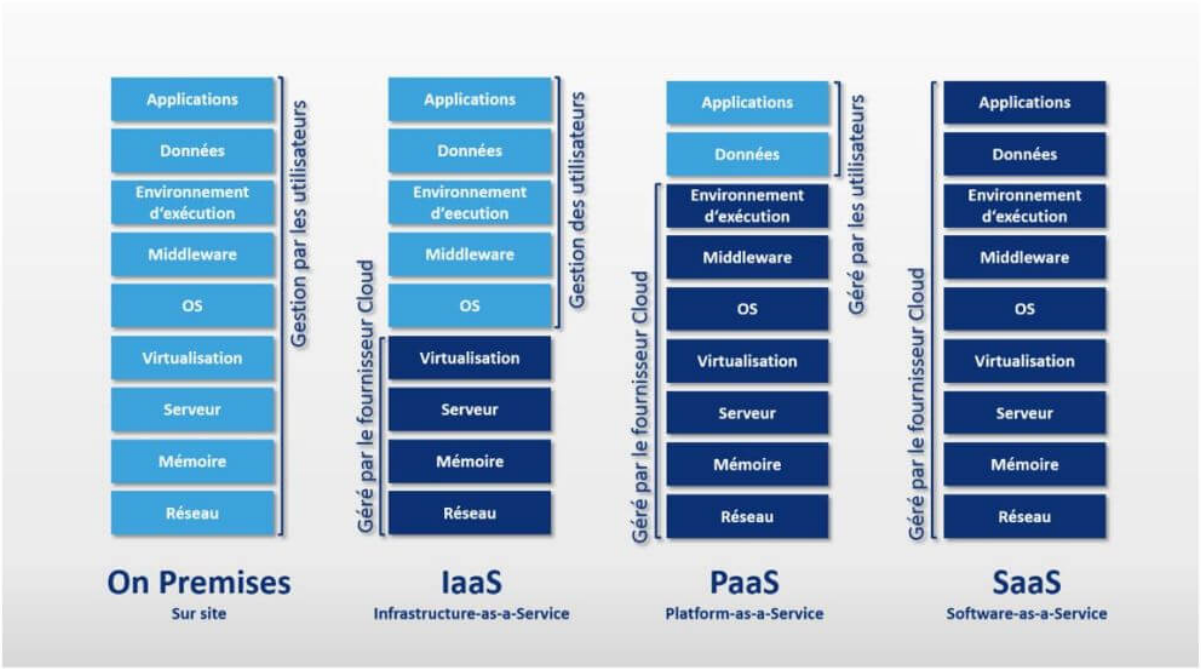

FIGURE 2.12 – La gestion des service Iaas, Paas et Saas par le fournisseur du cloud [1]

2.6.3.3 Le logiciel comme un service "SaaS"

Dans ce type de service, le fournisseur du cloud offre aux consommateurs des applications fonctionnelles clés en main, elles sont accessibles à partir de différents dispositifs comme les clients légers. L'infrastructure sous-jacente à savoir le réseau, les serveurs, les systèmes et le stockage ne sont pas gérés ni contrôlés par le consommateur à l'exception de quelques paramètres de configuration. Le déploiement, la veille sur le bon fonctionnement, la maintenance des applications, la gestion des données(la sauvegarde, la restauration) sont de la responsabilité du fournisseur. Plusieurs types d'application pouvant être fournis aux consommateurs à savoir CRM, outils de travail collaboratif, la messagerie, etc.

D'autres services en général existent à savoir :

2.6.3.4 Le stockage comme un service "STaaS"

Le stockage comme un service est une plateforme dédiée au stockage de données des entreprises. Le fournisseur de services fournit une infrastructure de stockage dans laquelle les entreprises où les particuliers peuvent externaliser leurs données. Ce service de cloud

représente une méthode pratique aux entreprises afin de sauvegarder des données sans avoir besoin d'investissement en matière de matériels et humaines.

Les différents services proposés par le cloud permettent aux utilisateurs finaux de concentrer sur leur travail et laisser la partie gestion des différentes couches du service à la charge du fournisseur cloud. Comme illustré dans la Figure 2.12. Lorsque une solution est dite "on premises" c'est-à-dire installée dans les serveurs de l'entreprise, la gestion de toute la pile du service est à la charge de l'entreprise. Elle est en mesure d'avoir le contrôle sur leurs données.

Concernant les autres services, le degré de la gestion entre le fournisseur et les utilisateurs change selon la solution. Dans le cas d'un service SaaS, les utilisateurs vont se focaliser sur leur travail et laisser la partie déploiement, maintenance et la mise à jour à la charge du fournisseur. Donc, toutes les briques du service sont sous le contrôle du fournisseur en commençant du réseau jusqu'aux applications.

2.6.3.5 Les avantages d'utilisation d'une solution cloud

L'utilisation des services cloud permettent aux entreprises d'avoir [57] :

1. Aucun investissement en matière de matériels et de ressources humaines.
2. Un déploiement et une gestion de services simplifiés.
3. Un paiement à la consommation.
4. Des services à grande disponibilité.
5. Une puissance de calcul, stockage et mémoire assurées par le fournisseur du cloud.
6. Une sauvegarde et restauration des données simplifiées, elles seront assurées par le fournisseur.
7. Une évolutivité "scalibility" s'adaptant aux besoins des clients.

Malgré les différents avantages qu'offre le cloud mentionnés ci-dessus, ce dernier à des inconvénients, les principaux risques liés au cloud sont :

— Le problème majeur est la sécurité des données, en adoptant cette technologie, les entreprises acceptent de confier leurs données privées à des tiers et cela pourrait potentiellement imposer un grand risque de confidentialité de données à l'entreprise.

— Une fois les données externalisées vers le cloud, l'entreprise perdra le contrôle sur ses données. Nous citons le cas du service SaaS Figure 2.12, le client n'a pas de gestion sur les différentes couches du serveur, il peut avoir quelques configurations à faire pour adapter certaines fonctionnalités à ses besoins spécifiques.

2.7 Conclusion

Dans ce chapitre, nous avons abordé les différents types de chiffrement à savoir le chiffrement symétrique et asymétrique et nous avons illustré le fonctionnement de chaque type de cryptographie. Par la suite, nous avons présenté l'infrastructure à clés publiques et ses différents composants ainsi que le cycle de génération d'un certificat.
La deuxième partie du chapitre a été dédiée au chiffrement par attributs "ABE" dans laquelle nous avons présenté une classification des solutions à base d'attributs. La solution qui nous a intéressé le plus est le schéma d'attributs "ABE" distribué permettant d'éviter le problème du "point de défaillance unique". La dernière partie du chapitre a été dédiée au cloud computing, dans laquelle les différents modèles ainsi que les services du cloud ont été présentés.
Le chapitre suivant sera dédie à notre nouvelle approche basée sur "ABE" distribuée dans le but d'améliorer la protection de la vie privée dans les réseaux sociaux en ligne.

Chapitre 3

VERS UNE APPROCHE ABE DISTRIBUÉE POUR LA PROTECTION DE LA VIE PRIVÉE DANS LES RÉSEAUX SOCIAUX EN LIGNE

Sommaire

3.1 Introduction 39
3.2 Les menaces liées aux réseaux sociaux en ligne 40
3.2.1 Les menaces liées aux fournisseurs de services 40
3.2.2 Les menaces liées aux applications tierces 41
3.2.3 Les menaces liées aux utilisateurs 42
3.3 Le CloudSN framework 49
3.3.1 La gestion de la sécurité dans CloudSN 50
3.3.2 Une vue globale de CloudSN 51
3.4 Évaluation des performances 56
3.4.1 Setup 56
3.4.2 L'analyse des performances 57
3.5 L'analyse de la sécurité 59
3.5.1 l'analyse de la robustesse 59
3.5.2 Résistance aux attaques 60
3.6 Conclusion 65

3.1 Introduction

De nos jours, les réseaux sociaux en ligne "Online Social Networks OSNs" jouent un rôle clé dans la vie quotidienne des utilisateurs. Ils partagent leurs données personnelles en ligne. Cela peut entraîner de graves problèmes de confidentialité, en raison du risque de fuite de données privées vers des tiers non-autorisés.
Une grande quantité d'information est partagée sur le Web : publications, actualités, commentaires, vidéos, etc. Les OSNs collectent toutes les activités et informations sur les utilisateurs, y compris leurs contacts, leurs relations et opinions [8]. Ces données peuvent être utilisées dans un but purement commercial, de la publicité ou dans un objectif politique [9]. Les réseaux sociaux permettent aux utilisateurs de présenter leurs profils d'une manière très détaillée [10]. Même avec les paramètres de confidentialité, les utilisateurs ne connaissent pas toujours leurs configurations, ils ont tendance à utiliser les paramètres par défaut, ce qui peut nuire à leur vie privée.

Une fois que les données sont partagées par les utilisateurs sur les OSNs, elles sont accessibles à tout moment et n'importe où, les utilisateurs n'auront aucun contrôle dessus et la confidentialité des données est menacée. Pour assurer une meilleure accessibilité, les OSNs répliquent les données sur leurs data-centers, en conséquence, l'utilisateur ne peut pas localiser ses données.

Un autre problème rencontré dans les OSNs est l'utilisation des APIs "Application programming interfaces", qui consistent en un ensemble de règles, d'instructions et de fonctions, permettant l'accès aux services d'une application. Les APIs permettent à des parties-tierces d'accéder aux données personnelles de l'utilisateur, ce qui met en péril la vie privée de l'utilisateur [58].

Pour apporter des solutions à certains de ces problèmes, nous proposons un nouveau framework appelé "CloudSN", basé sur un schéma d'ABE distribué "distributed multi-authority Attribute-Based Encryption ABE scheme" pour protéger la confidentialité des données de l'utilisateur. Notre framework est appliqué sur "Facebook" puisqu'il s'agit du réseau social en ligne le plus utilisé. Les principales contributions sont décrites comme suit :

— Un modèle de chiffrement "multi-authority attribute-based encryption" est proposé. Les utilisateurs peuvent concevoir leur propre politique d'accès permettant uniquement aux amis autorisés d'avoir accès aux données. Ce schéma réduit le risque de point de défaillance unique "single point of faillure" [59].

— L'évaluation des performances par simulation en utilisant différents scénarios avec plusieurs paramètres, notamment le nombre d'attributs, le temps de chiffrement et le temps de déchiffrement.
— Une analyse de la sécurité est présentée, elle montre que notre solution est robuste et résistante à plusieurs attaques et vulnérabilités telles que les attaques de coalition, les vulnérabilités causées par le provider, les utilisateurs et les applications tierces.

3.2 Les menaces liées aux réseaux sociaux en ligne

Dans cette section, nous présentons et classons les vulnérabilités liées aux réseaux sociaux en ligne. Dans les OSNs, les parties prenantes qui interagissent entre elles sont le fournisseur de services, les utilisateurs et les applications tierces [60]. Il existe des menaces qui sont liées aux fournisseurs de services, les menaces causées par les utilisateurs, ainsi que des menaces qui sont liées aux applications tierces. Les menaces sur les utilisateurs peuvent être classées en deux catégories : attaques classiques et attaques modernes comme illustré dans la Figure 3.1.

3.2.1 Les menaces liées aux fournisseurs de services

L'utilisateur partage sur les OSNs une quantité étonnante d'informations personnelles. Il fait confiance à un fournisseur de services pour protéger ses informations. Ainsi, les données de l'utilisateur sont disponibles pour le fournisseur, qui peut les partager et les vendre à des fins commerciales, publicitaires et politiques [9]. Le fournisseur a le pouvoir d'accéder aux données de l'utilisateur à tout moment. Une fois que les données de ce dernier sont sur les serveurs du fournisseur, l'utilisateur en perd le contrôle. Ainsi, le fournisseur peut se conformer aux demandes légales sur les données des utilisateurs émanant du gouvernement [61].

Yabing et al.[62] mesurent le problème de l'ampleur de la gestion de la confidentialité en interrogeant 200 utilisateurs de Facebook. Il en résulte que 36% du contenu reste partagé avec les paramètres de confidentialité par défaut. Seuls 37% des paramètres de confidentialité correspondent aux attentes des utilisateurs, le contenu est exposé à plus d'utilisateurs que souhaité. Les paramètres par défaut ont tendance à être plus ouverts. Même si les utilisateurs sont plus sensibles à la confidentialité, ils ont du mal à gérer leurs paramètres[62].
(Ces paramètres de confidentialité ou recommandé pour le contenu partagé sont tout

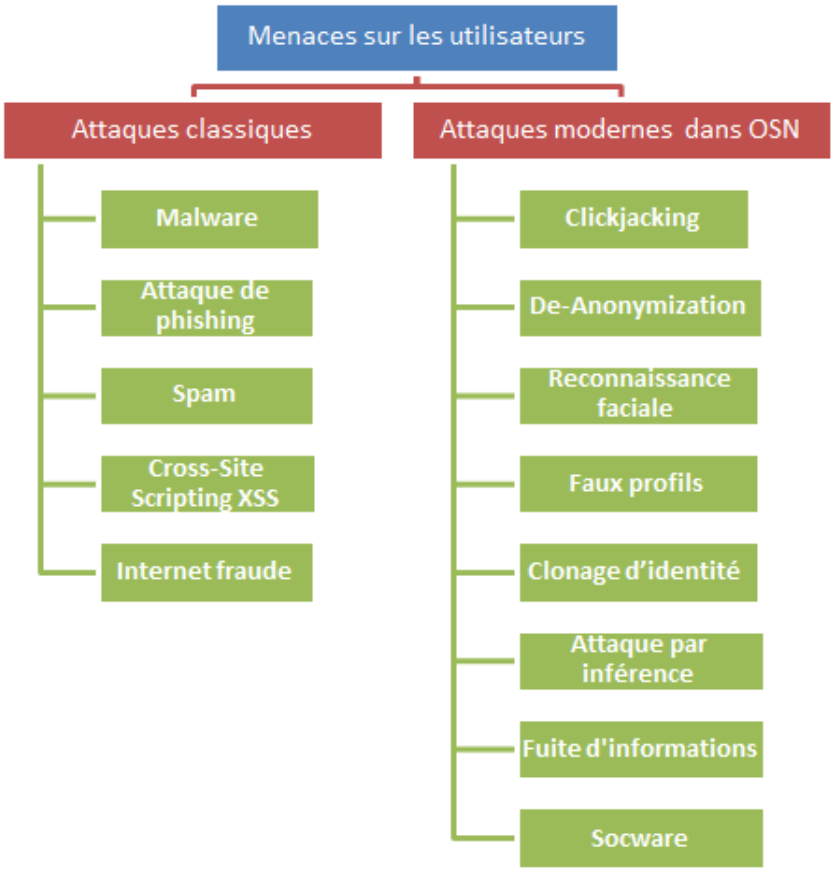

FIGURE 3.1 – Les Menaces des utilisateurs dans OSN

le monde). Ainsi, tous les utilisateurs de Facebook peuvent le voir. Seule une minorité d'utilisateurs modifient leurs paramètres. Les problèmes avec les paramètres par défaut sont l'exposition du contenu à tous, ce qui peut porter une atteinte à la confidentialité des données [63].

3.2.2 Les menaces liées aux applications tierces

Les OSNs fournissent de nouvelles fonctionnalités pour offrir de nouveaux services aux utilisateurs. Ils proposent le développement d'applications tierces. Ces dernières peuvent avoir un accès aux données de l'utilisateur après qu'il les ait installées. Les fournisseurs et les utilisateurs ne savent pas exactement quelles sont les informations accessibles par ces applications.

Le mécanisme pour surveiller comment ces applications manipulent les données de l'utilisateur est manquant. Un exemple des applications qui manipulent les données des

utilisateurs permettant de comparer un groupe d'amis et demande aux utilisateurs d'exprimer leur opinions sur leurs amis. Une fois les données sont collectées, le propriétaire de l'application a proposé de vendre ces données [64].

3.2.3 Les menaces liées aux utilisateurs

Les utilisateurs malveillants combinent différents types d'attaques afin de créer d'autres attaques plus sophistiquées et plus nuisibles aux données privées des utilisateurs des OSNs. Les attaques les plus dangereuses sont celles qui visent les enfants mineurs. Comme cité précédemment, les menaces contre les utilisateurs de réseaux sociaux en ligne peuvent être classées sous différentes catégories :

3.2.3.1 Les attaques classiques

Les attaques classiques sont une catégorie d'attaque qui touchent les utilisateurs d'internet en général, parmi ces attaques nous trouvons les malwares, le phishing, spam, cross-site scripting et internet fraude. Malgré que ce type d'attaque a été traité par le passé, ils sont devenus de plus en plus viraux en raison de la structure et de la nature des OSNs.

Le malware

Le malware est un logiciel développé par un utilisateur malveillant dans le but de nuire au bon fonctionnement de la machine d'une victime, en collectant les identifiants de cette dernière afin d'avoir accès à ses données personnelles. Dans les OSNs, le malware se propage parmi les utilisateurs et leurs amis. Koobface [65] est le premier malware à avoir affecté les plateformes des réseaux sociaux telles que Facebook, Twitter, etc. Son but était de collecter les identifiants des utilisateurs, contrôler leurs machines et les faire de leurs machines des "botnets".

Les attaques de phishing

Le "phishing" est une forme d'attaque permettant de dérober les données sensibles et privées des utilisateurs en se faisant passer par un tiers de confiance. Les auteurs dans [66] montrent que les utilisateurs interagissant avec les plateformes des réseaux sociaux ont un risque plus élevé d'un phishing. Dans un rapport publié par Microsoft Security Intelligence [67], 84,5% de toutes les attaques de phishing ciblent les utilisateurs de sites de réseaux sociaux. L'attaque consiste à attirer l'utilisateur vers une fausse page

qui ressemble au site d'origine dans le but de lui voler ses identifiants afin d'effectuer d'autres types d'attaques comme illustré dans le Figure 3.2.

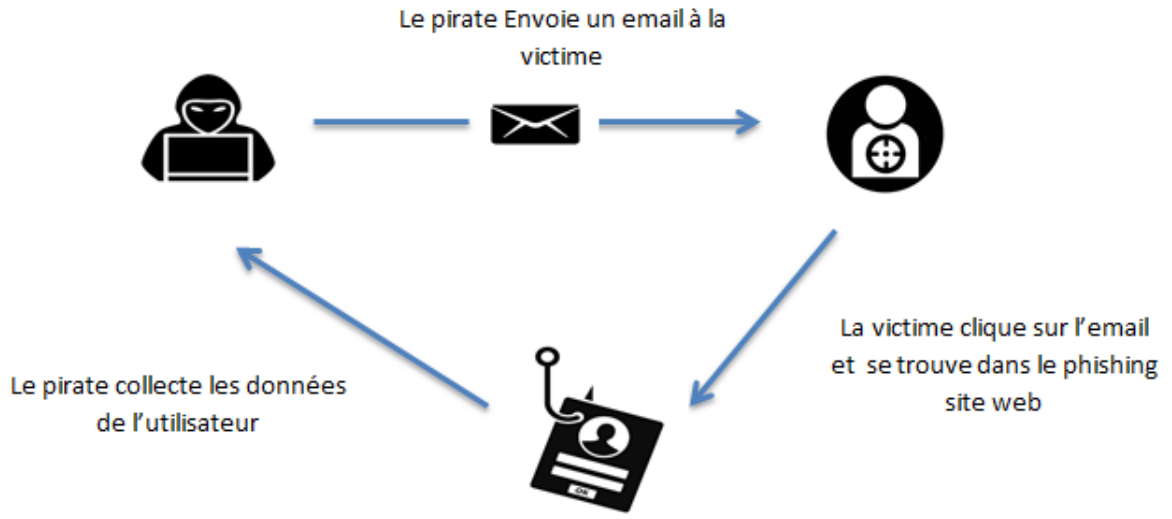

FIGURE 3.2 – L'attaque de phishing

Les spams

Une attaque de type spam consiste à envoyer une masse de messages électroniques indésirables aux utilisateurs à savoir les annonces publicitaires, etc. Les utilisateurs peuvent créer de faux profils sur les plateformes des réseaux sociaux dans le but d'envoyer des messages aux utilisateurs. Les mêmes profils peuvent servir pour ajouter des messages et des commentaires aux pages consultées par le grand public.

Le Cross-Site Scripting (XSS)

Dans ce type d'attaque, un attaquant profite de la confiance de l'utilisateur dans les applications web afin de lui faire exécuter un code malveillant capable de collecter des données privées. Comme illustré dans le Figure 3.3, un pirate injecte du script malveillant dans un site et pratique de l'ingénierie sociale afin de mettre les victimes en confiance. Une fois les personnes visitent le site et clique sur des liens, leurs données comme les session et les cookies sont envoyés aux pirates.

Les réseaux sociaux en ligne sont les plateformes les plus exposées aux attaques du type XSS. Un attaquant peut exploiter une faille XSS dans les plateformes OSNs

en créant un worm (ver) XSS pouvant se propager dans ces plateformes. Dans l'année 2009, un XSS worm appelé "Mikeyy" a touché le réseau social Twitter, ce dernier s'est propagé d'une manière automatique et affecté plusieurs utilisateurs [68].

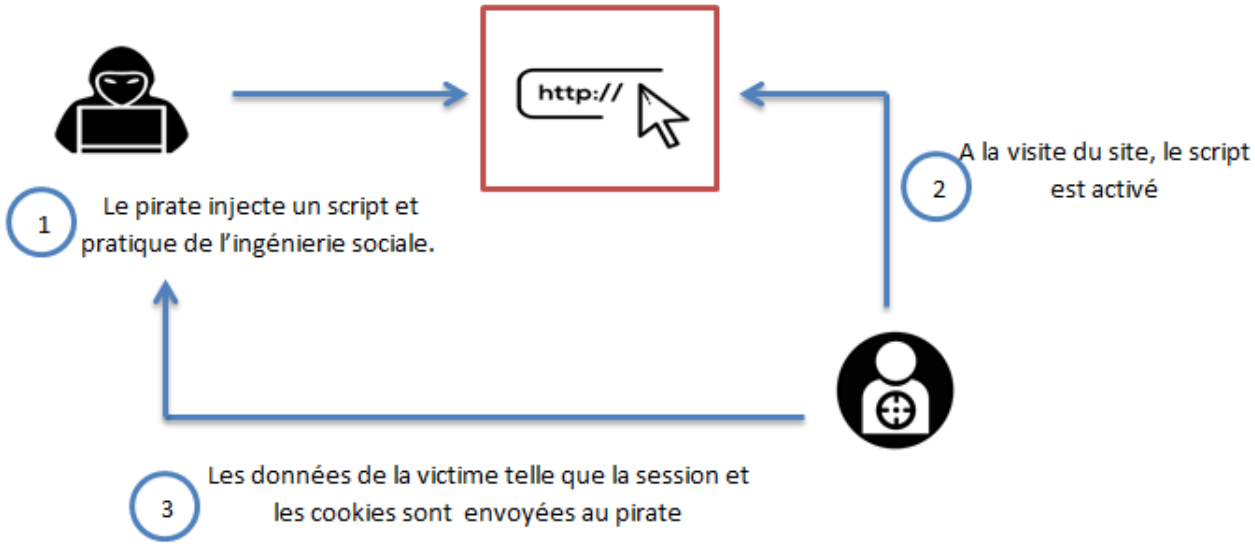

FIGURE 3.3 – L'attaque de cross-site scripting "XSS"

La fraude sur internet

La fraude sur internet est une attaque connue aussi comme cyber-fraude, elle consiste à utiliser l'accès à internet pour arnaquer les internautes. Alors que les réseaux sociaux permettent de connecter des personnes partageant les mêmes intérêts. Les escrocs infiltrent ces plateformes à la recherche de victimes. Selon "North American Securities Administrators Association" [69], les escrocs en s'activant sur les réseaux sociaux et en participant dans la communauté, ils gagnent la confiance des utilisateurs afin d'exploiter les données personnelles publiées dans les profils en ligne des victimes et de tirer profit aussi des données de leurs amis. Un exemple cité par "Theguardian" [70], "Abigail Pickett" une étudiante britannique voyageant en Colombie, a découvert que son compte avait été piraté et qu'il était utilisé pour envoyer des demandes d'argent à des amis sous prétexte qu'elle était "bloquée" dans la Colombie.

3.2.3.2 Les attaques modernes

Les menaces modernes sont généralement propres aux environnements OSN. Habituellement, ces menaces visent spécifiquement les informations personnelles des utilisateurs, ainsi que celles de leurs amis.

L'attaque de clickjacking

L'attaque par clickjacking est une technique malicieuse utilisée pour détourner l'intention des utilisateurs et de cliquer sur une cible comme illustré dans la Figure 3.4. Le but principal est de manipuler l'utilisateur afin de poster des messages spams sur son timeline, ou de faire des j'aime sur des liens sans le savoir "likeJacking". Une attaque de type clickjacking a été enregistrée sur Twitter en 2009. L'attaquant a tweeté un lien indiquant sur ce dernier ne pas cliquer, lorsque les utilisateurs de Twitter ont cliqué sur le lien, le message a été automatiquement diffusé d'une manière virale [71].

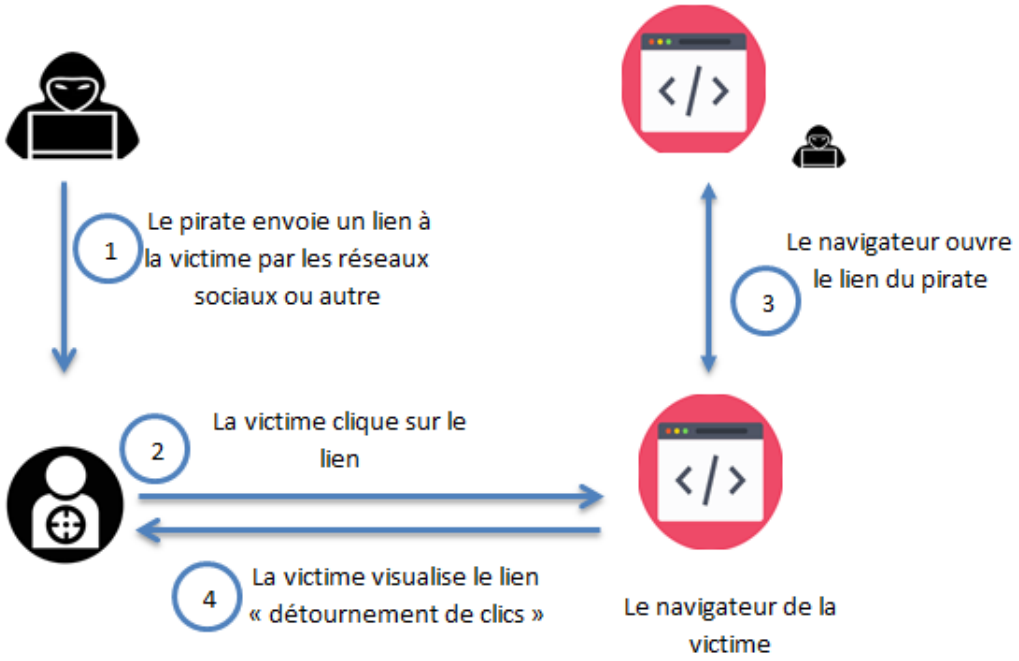

FIGURE 3.4 – L'attaque de clickjacking

L'attaque par re-identification "de-Anonymization"

Dans les réseaux sociaux afin qu'un utilisateur protège sa vie privée et son anonymat il utilise des pseudonymes. L'attaque par de-anonymization consiste à utiliser des

techniques telles que le "tracking cookies", la topologie du réseau et les appartenances à des groupes d'utilisateurs pour découvrir l'identité réelle de l'utilisateur.
Dans [67], les auteurs ont démontré qu'il était possible pour des tierces applications de découvrir l'identité des utilisateurs sur les OSNs en reliant des informations partagées via les plateformes des réseaux sociaux. Les auteurs ont démontré que les utilisateurs des réseaux sociaux peuvent voir leurs identités divulguées via des mécanismes de suivi, tels que le tracking cookies.

La reconnaissance faciale

Les utilisateurs utilisent les OSNs pour télécharger des photos d'eux-mêmes et de leurs amis. Des millions des photos sont téléchargées sur Facebook chaque jour. De plus, de nombreuses photos de profil d'utilisateur Facebook sont accessibles au public pour les visualiser et les télécharger.
Dans un site accessible en ligne appelé "The face of Facebook"[72], ce dernier permet aux internautes de visualiser les images de profil de plus de 1,2 milliard d'utilisateurs de Facebook. Ces photos peuvent être utilisées à des fins malveillantes comme la création d'une base de données biométrique, qui peut ensuite être utilisée pour identifier des utilisateurs OSN sans leur consentement.
Les auteurs dans [73] ont démontré avec des expériences sur les menaces de la reconnaissance faciale sur la vie privée. Ils ont montré qu'il est possible de faire une correspondance entre les images de profil d'un utilisateur de Facebook accessible au public pour ré-identifier les profils sur l'un des sites de rencontres les plus populaires aux États-Unis.
Une autre expérience conduite par les auteurs Acquisti et al [73] montrent qu'il est possible de prédire des informations personnelles et sensibles à partir d'une image de profil, les intérêts et les activités de la personne.

Les faux profils

Les faux profils (également appelés "sybils attack" ou "socialbots"), ce sont des profils automatiques ou semi-automatiques qui imitent les comportements humains dans les OSNs. Les faux profils peuvent être utilisés pour collecter les données personnelles des utilisateurs sur les réseaux sociaux. En envoyant des demandes d'amitié aux utilisateurs des OSNs, ces derniers finissent souvent par les acceptées.
Les "socialbots" peuvent collecter les données personnelles d'un utilisateur qui ne devraient être exposées qu'à ses amis. Les faux profils peuvent être utilisés pour lancer

des attaques telles que "Sybil attaque" [74], envoyer les messages spams [75], voir même manipuler les statistiques des OSNs [76],[77].

Dans un article publié par "The New YorkTimes" [78], il affirme que le marché de l'achat de faux followers et de faux tweets est une affaire de plusieurs millions de dollars. Une expérience a été menée par deux chercheurs Robin et Thomas entre le 26 décembre 2009 et 23 janvier 2010 pour mesurer la propagation d'un faux profil dans les réseaux sociaux tels que Facebook, LinkedIn, Twitter, Google et Blogger [79]. Avec cette expérience le profil fictif de "Robin Sage" s'est connecté à des centaines d'utilisateurs, en utilisant leurs contacts, Thomas a pu accéder à des informations privées des utilisateurs.

L'attaque par clonage d'identité

Dans cette attaque, l'attaquant clone le profil de la victime dans le même réseau ou bien à travers plusieurs plateformes sociales, dans le but de créer une relation de confiance avec les amis de la victime. L'attaquant peut utiliser cette confiance pour collecter des informations personnelles sur les amis de la victime ou pour effectuer divers types de fraude en ligne.
Un exemple d'attaque par clonage dont le commandant en chef de L'OTAN a été victime l'amiral James Stavridis [80], son profil a été cloné puis utilisé pour collecter des données sur les responsables du ministère de la défense et d'autres représentants du gouvernement.

L'attaque par inférence

Ce type d'attaque est utilisé pour prédire les informations personnelles et sensibles de l'utilisateur que ce dernier n'a pas choisi de divulguer, telles que l'appartenance religieuse, civilité, emploi ...
Ces types d'attaques peuvent être implémentés en utilisant des techniques de data mining combinée avec les données accessibles au public sur les réseaux sociaux, telles que la topologie du réseau et des données d'amis des utilisateurs. Un exemple d'attaque par inférence a été démontré par Mislove et al. [81], dans lequel ils ont présenté une technique permettant de prédire les attributs de l'utilisateur en se basant sur les attributs de ses amis.

La technique a permis de déduire différents attributs des utilisateurs de Facebook à savoir : des informations pédagogiques, leurs préférences personnelles et des informations géographiques. Un autre exemple d'attaque par inférence lancé par Fire et al. sur des organisations [82]. Les auteurs ont proposé un algorithme permettant de déduire les

attributs OSN pour ses organisations. Ils ont utilisé les données disponibles dans les profils des employés des organisations, ce qui a permis de déduire certaines données à caractère confidentielles.

La fuite d'informations

Les réseaux sociaux permettent aux utilisateurs de partager et échanger leurs informations avec leurs amis. Dans certaines situations, les utilisateurs partagent volontairement leurs données sensibles et les données de leurs amis, telles que les informations relatives à la santé [83].
Dans l'étude présentée par les auteurs, elle démontre que la fuite des informations sensibles peut engendrer un impact négatif sur les utilisateurs. Par exemple les compagnies d'assurance peuvent utiliser les données des OSN pour les clients potentiellement à risque [84].

De plus, les employeurs utilisent les OSNs pour sélectionner et enquêter sur les candidats à l'emploi [85]. Avec la croissance de l'utilisation des smartphones, les utilisateurs utilisent les OSNs pour partager leur localisation ou bien celle de leurs amis. Cette attitude peut engendrer de grave conséquence. Ce type d'information peut être utilisé par les criminels dans le but de nuire la victime. Par exemple, "Israel Hyman" de "l'Arizona" a posté sur Twitter qu'il était impatient de passer les vacances de sa famille à "Saint-Louis". Il a également posté une fois arrivé au "Missouri". Quand Hyman est rentré chez lui, il a découvert que sa maison avait été cambriolée [86].

les socwares

Le socware est une nouvelle technique utilisée par les utilisateurs malveillants pour propager les spams et les malwares. Le socware peut attirer les cibles en offrant de fausses récompenses "rewards" pour les utilisateurs qui installent l'application. Après l'installation de l'application, cette dernière envoie des messages au nom de l'utilisateur aux amis de l'utilisateur, en aidant essentiellement la propagation virale du logiciel [87]. Dans une étude lancée par Rahman et al.[88], ils ont trouvé que 13% des 111 000 applications étudiées étaient des applications malveillantes susceptibles de contribuer à la diffusion de logiciels malveillants.

3.3 Le CloudSN framework

Le framework que nous proposons à pour objectif d'atténuer les menaces qui pèsent sur la vie privée des utilisateurs dans les réseaux sociaux en ligne. Nous prenons l'exemple de Facebook, puisqu'il s'agit de la plateforme la plus utilisée. Afin de protéger les données de l'utilisateur, nous avons divisé son profil en deux parties :

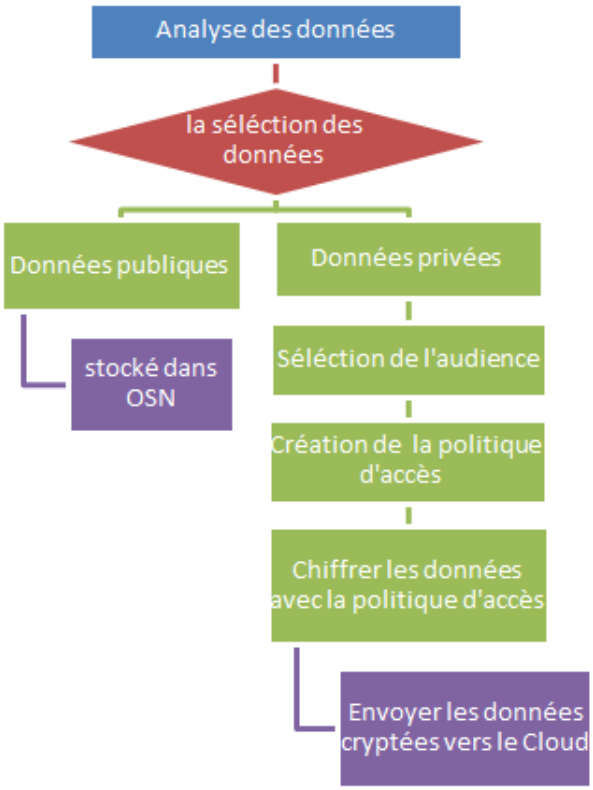

FIGURE 3.5 – Le processus de classification des données de l'utilisateur

1. les données publiques.
2. les données privées.

Les données publiques restent hébergées sur OSN et seront accessibles à tous les amis de l'utilisateur. En ce qui concerne les données privées, l'utilisateur sélectionne un public et crée une politique d'accès. Ensuite, les données seront cryptées sous un contrôle d'accès et elles seront externalisées vers le cloud computing.
Dans la figure 3.5, nous présentons le processus de classification des données d'un utilisateur sous forme d'un organigramme.

3.3.1 La gestion de la sécurité dans CloudSN

Dans cette section, nous présentons la gestion de la sécurité dans "CloudSN" Figure 3.6 et les différents mécanismes utilisés afin de garantir la confidentialité et l'intégrité des données.
Les utilisateurs utilisent les réseaux sociaux pour communiquer et partager leurs données personnelles. La sécurité de ces informations critiques est nécessaire pour les partager sur les plateformes des réseaux sociaux.

3.3.1.1 Les mécanismes cryptographiques

Les techniques cryptographiques sont utilisées afin de garantir un accès sécurisé aux données partagées. Le système de chiffrement basé sur les attributs convient le plus pour les groupes et la communauté composant les réseaux sociaux. Les problèmes de l'intégrité et la confidentialité dans les réseaux sociaux peuvent être atténués par des techniques cryptographiques telles que le chiffrement basé sur les autorisations d'accès.

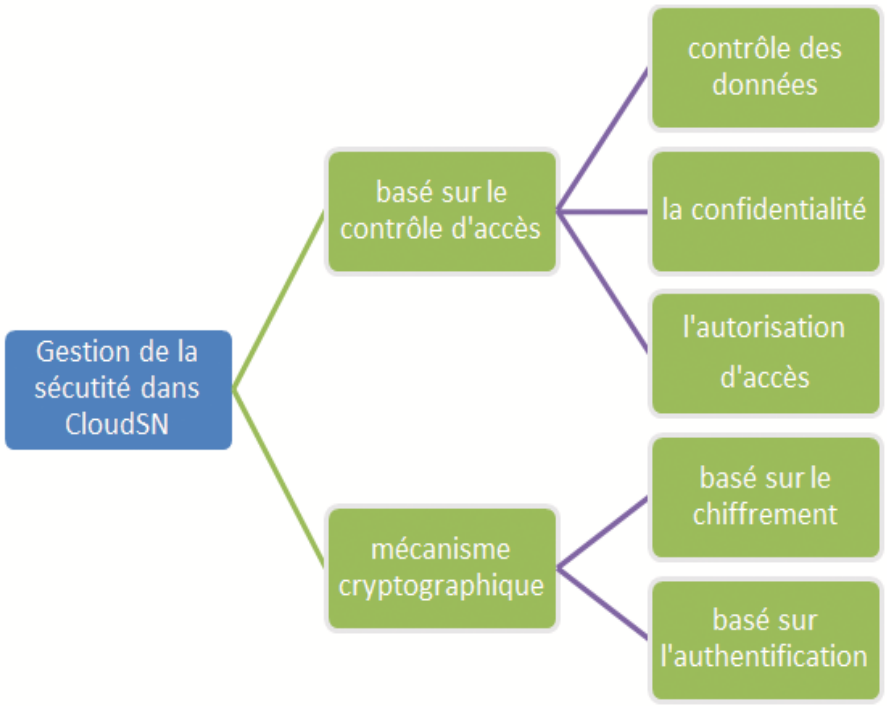

FIGURE 3.6 – Gestion de la sécurité dans CloudSN.

A)Le chiffrement

Le chiffrement est une technique permettant de crypter les données de l'utilisateur en se basant sur différentes méthodes existantes telle que le cryptage basé sur les attributs " Attribute Based Encryption ABE".

B)L'authentification

La sécurité basée sur l'authentification est un mécanisme basé sur un protocole qui sera utilisé afin de garantir un partage de données sécurisées entre les utilisateurs.

3.3.1.2 La sécurité basée sur le contrôle d'accès

Le contrôle d'accès comme son nom l'indique servi à contrôler les accès aux données partagées entre les utilisateurs. Le contrôle d'accès permet de restreindre le partage d'informations non souhaitées sur l'espace public des OSNs.

A)Le contrôle des données

Le contrôle de données permet de faire un verrou sur l'information partagée toute en préservant l'anonymat. La fuite de données représente un vrai problème de violation de la vie privée et de leur l'intégrité. Appliqué un contrôle d'accès permet de maintenir l'anonymat des données en fournissant un accès seulement aux utilisateurs autorisés.

B)La confidentialité

Les données partagées sur les réseaux sociaux soulèvent des problèmes de confidentialité et nécessitent une application des techniques de chiffrement afin de garantir la confidentialité des données.

C)L'autorisation d'accès

L'autorisation d'accès permet à l'utilisateur de partager ses données sur les plateformes des réseaux sociaux et de créer un contrôle d'accès permettant aux utilisateurs autorisés de déchiffrer les données partagées.

3.3.2 Une vue globale de CloudSN

Dans cette sous-section, nous présentons le framework CloudSN qui repose sur trois modules :

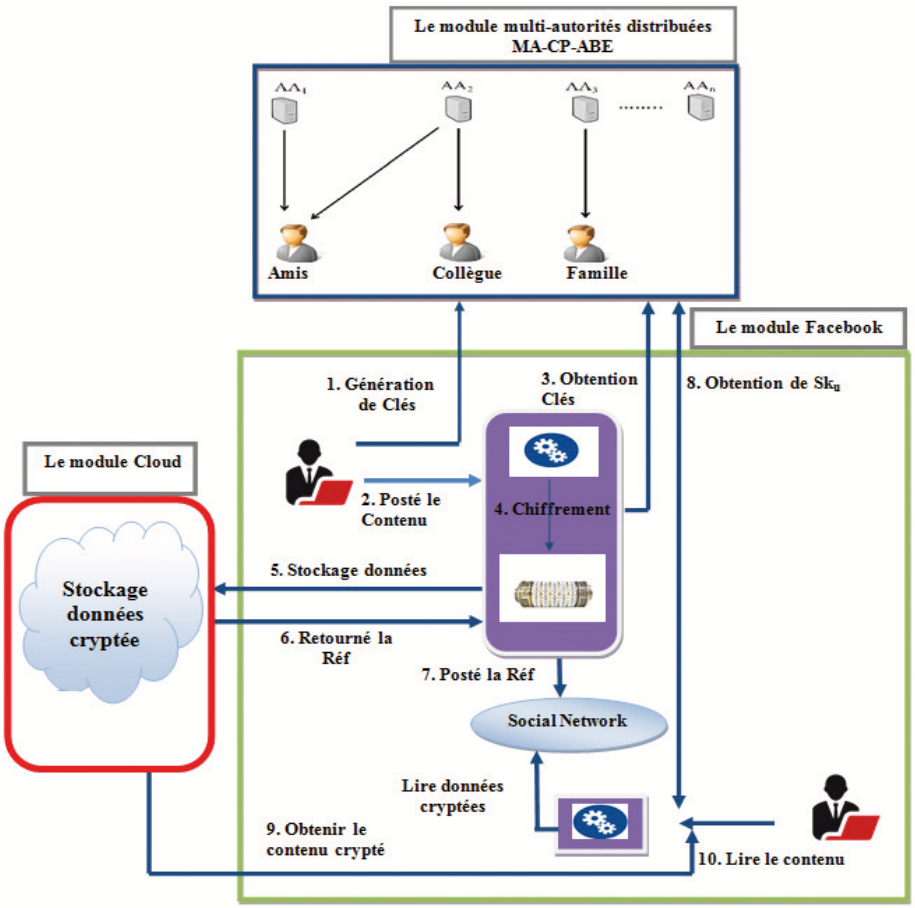

FIGURE 3.7 – Une vue globale sur l'architecture.

1. le module de Facebook.
2. le module du cloud computing.
3. Le module multi-autorités distribuées "ABE", comme illustré dans la figure 3.7.

Le module Facebook : Le module Facebook dans notre framework est représenté par la partie côté client, dans laquelle un utilisateur publie et partage du contenu avec ses amis et d'autres utilisateurs. L'utilisateur peut utiliser son compte pour chiffrer le contenu sous des clés générées par ABE (Distributed Multi-Authority). Le contenu crypté sera externalisé vers le module cloud.

Le module cloud computing : Le module cloud permet de stocker des données cryptées sous le contrôle de l'utilisateur. Les données de l'utilisateur seront externalisées et stockées dans ce module. L'externalisation des données privées et les confier à des tiers peut poser d'importants problèmes de confidentialité, car le risque de fuite de

données privées vers des tiers non autorisés est plus élevé. Pour assurer le contrôle de l'utilisateur sur ses données externalisées, nous proposons d'utiliser un système ABE (Distributed Multi-Authority), qui peut fournir un accès évolutif et flexible aux données de l'utilisateur.

Le module multi-autorités distribuées (MA-CP-ABE) : Nous présentons les détails de la conception et les fonctionnalités de notre solution proposée. Nous utilisons des mécanismes de cryptographie pour protéger les données via le chiffrement basé sur les attributs "ABE" [14],[89]. La technique d'ABE est utilisée pour contrôler l'accès aux données partagées entre les utilisateurs. Seuls les utilisateurs autorisés peuvent les récupérer.

Dans les OSNs, un utilisateur peut avoir plusieurs groupes avec des attributs. L'utilisateur définit les accès de contrôle en fonction des attributs associés à ses groupes. Seuls les utilisateurs avec bon contrôle d'accès peuvent récupérer Les données.

La phase d'initialisation du système :

L'utilisateur commence la phase d'initialisation comme le montre la figure 3.7, étape (1). Nous avons un ensemble de paramètres globaux générés et partagés entre tous les "AA" les Authorités d'Attributs "Attributes Authorities"

1. deux groupes cycliques multiplicatifs G_0 et G_1 d'ordre premier p.
2. g est un générateur de G_0, avec une application bilinéaire $e : G_0 * G_0 \rightarrow G_1$. Nous utilisons une fonction de hachage $H : \{0,1\} \rightarrow Z_p^*$

Nous avons le k^th AA noté AA_k tandis que l'ensemble d'attributs administré par AA_k est noté AT^k.

AA_k choisit deux exposants aléatoires α_k , $\beta_k \in Z_p^*$ et calcule : $X_k = g_k^{\beta}, Y_k = e(g,g)^{\alpha_k}$.

Un identifiant aléatoire $t_{k,i} \in Z_p^*$, pour chaque élément i dans AT_k est sélectionné, chaque attribut administré par AA_k est associé à un attribut public $T_{k,i}$ où $T_{k,i} = g^{t_{k,i}}$. AA_k aura respectivement une Master Key "clé maîtresse MK_k" (3.1) et une Public Key "clé publique PK_k" (3.2) :

$$MK_k = \{\alpha_k, \beta_k, t_{k,i}\}_{i=1.2...|AT^k|} \tag{3.1}$$

$$PK_k = \{X_k, Y_k, T_{k,i}\}_{i=1.2...|AT^k|} \tag{3.2}$$

La phase de distribution des clés d'attributs :

Supposons que l'utilisateur U_m souhaite acquérir des clés d'attributs pour l'ensemble

d'attributs AT_m représenté dans la Figure 3.7 module Facebook.
Soit AT_m^k le sous-ensemble d'attributs dans AT_m qui devrait être obtenu à partir de AA_k.
Le processus de distribution de la clé d'attribut, comme illustré à la figure 3.7 étape (3), est le suivant :

1. AA_k lié l'identité de U_m à un identificateur unique noté $r_m \in Z*_p$
2. La clé secrète de chaque attribut demandée est générée comme suit :

$$SK_m^k = \{SK_0^k, SK_i^k\}_{i=1,2...|AT_m|} \tag{3.3}$$

et

$$SK_0^k = g^{\frac{\alpha_k - r_m}{\beta_k}}, SK_i^k = g^{\frac{r_m}{t_{k,i}}} \tag{3.4}$$

Où $t_{k,i}$ est le composant MK de l'attribut i^{th} dans AT_m^K défini par AA_k.
Nous notons que la clé secrète SK_0^k associé l'identité de l'utilisateur à l'identité de l'autorité émettrice AA_k et que la clé secrète SK_i^k associé l'identité de l'utilisateur à l'attribut lui-même.

La phase de chiffrement :
Si l'utilisateur veut chiffrer les données $M \in G_1$, il génère d'abord la structure d'accès (τ) et en déduit un ensemble de sous-structures d'accès $\{\tau_k\}_{k=1,2,,,,,,q}$. Le texte chiffré de M est donné par $E(M)$ comme illustré dans la figure 3.7 étape (4) :

$$E(M) = (\tau, \{E_k\}_{k=1,2...q}). \tag{3.5}$$

E_k est le texte chiffré de M codé avec la sous-structure d'accès τ_k.
La k^th sous-structure τ_k contient m attributs qui sont gérés par l AAs avec $l \leq n$, où n est le nombre total d'AA. Nous supposons que n'importe quelle AA peut administrer plus d'un attribut des m attributs considérés.
E_k peut être représenté C_0, $\{C_i^{'}\}_{i=1,2...l}$ et $\{C_i^{''}\}_{i=1,2...m}$
Pour calculer E_k, l'utilisateur génère un exposant aléatoire $s \in Z_p^*$ et utilise les clés publiques de l'AA pour calculer :

$$C_0 = M \prod_{i=1}^{l} Y_i^s = Me(g,g)^{s \sum_{i=1}^{l} \alpha_i} \tag{3.6}$$

$$C_i^{'} = X_i^s = g^{\beta_i} s \tag{3.7}$$

Pour calculer $\{C^{''}\}$, la clé secrète de s est affectée à chaque attribut dans τ_k :

1. Pour chaque attribut dans τ_k sauf le dernier, une valeur aléatoire l'exposant $s_i \in Z_p^*$ est attribué et le dernier élément est affecté avec la valeur $ls - \sum_{i=1}^{m-1} s_i$.
2. Puis nous calculons $C_i^{''} = T_i^{s_i}$

Tel que T_i correspond à l'exposant de l'attribut publique de i^{th} attribut dans τ_k.
Le propriétaire des données génère des textes chiffrés pour toutes les sous-structures de τ, puis il envoie les données chiffrées au cloud computing, comme illustré dans la figure 3.7, étape (5) et (6), une référence est publiée sur le réseau social étape (7).

La phase de déchiffrement :
Lorsque un utilisateur U_m veut avoir accès aux données stockées dans le cloud, il doit d'abord envoyer une demande d'accès aux données correspondantes, comme illustré dans la figure 3.7 étape (8), puis le cloud computing récupère la structure correspondante τ associée aux données et la renvoie à l'utilisateur U_m comme indiqué dans la figure 3.7 étape (9). L'attribut appartenant à U_m est noté AT_m.

U_m détermine le plus petit sous-ensemble d'attributs $AT_m^{'}$ qu'il possède et qui satisfait le τ reçu, il génère la sous-structure $\tau^{'}$ et l'envoie au cloud, conformément à $\tau^{'}$, le cloud renvoie le texte chiffré E' à l'utilisateur U_m, ce qui lui permet de le déchiffrer à l'aide des clés secrètes d'attribut appropriées, comme illustré dans la figure 3.7 étape (10).

$$E^{'} = (\tau^{'}, C_0, \{C_i^{'}\}_{i=1,2...l}, \{C_i^{''}\}_{i=1,2...m}) \tag{3.8}$$

Soit $\{SK_i\}_{i=1,2...m}$ la clé secrète d'attribut appartenant à U_m pour le sous-ensemble d'attributs $AT_m^{'}$ et $\{SK_0^i\}_{i=1,2...l}$ l'ensemble de clés secrètes qui relie l'identité de U_m aux $lAAs$.
Nous avons $SK_0^i = g^{\frac{\alpha_i - r_m}{\beta_i}}$ et $SK_i = g^{\frac{r_m}{t_i}}$ tel que t_i est le MK défini par AA qui gère l'attribut correspondant, pour déchiffrer $E^{'}$. L'utilisateur U_m évalue :

$$\prod_{i=1}^{m} e(C_i^{''}, sk_i) = \prod_{i=1}^{m} e(T_i^{s_i}, g^{\frac{r_m}{t_i}}) = e(g,g)^{ls(r_m)} \tag{3.9}$$

puis :

$$\prod_{i=1}^{l} e(C_i^{''}, sk_0^i) = \prod_{i=1}^{l} e(g^{s\beta_i}, g^{\frac{\alpha_i - r_m}{\beta_i}}) = e(g,g)^{s\sum_{i=1}^{l}\alpha_i - l - s(r_m)} \tag{3.10}$$

L'utilisateur U_m pourra calculer M

$$\frac{C_0}{e(g,g)^{s\sum_{i=1}^{l}\alpha_i}} = \frac{Me(g,g)^{s\sum_{i=1}^{l}\alpha_i}}{e(g,g)^{s\sum_{i=1}^{l}\alpha_i}} = M \tag{3.11}$$

Révocation des clés

Lorsqu'un attribut appartenant à un utilisateur est révoqué, l'utilisateur ne doit pas en mesure d'utiliser les clés secrètes liées à cet attribut dans toute transaction ultérieure. Dans notre système, le processus de révocation est géré par l'AA qui est responsable de l'attribut à révoquer, comme indiqué dans la figure 3.7 (module MA-CP-ABE). Nous supposons que AA_k veut révoquer l'attribut a de l'utilisateur U_m, l'exposant secret associé à a est donné par t_a. Le processus fonctionnera comme suit :

1. Un nouvel exposant secret aléatoire $t_a^{'}$ est généré et l'exposant d'attribut public associé $g^{t_a^{'}}$ est généré et publié.
2. une modification dans l'exposant de l'attribut secret affectera la clé secrète associée à l'attribut considéré. La nouvelle clé secrète sera donc générée à l'aide de $t_a^{'}$.
3. le message M crypté avec l'attribut a sera affecté, ainsi le cryptage du message M sera recalculé à l'aide de la phase de cryptage, l'attribut AA_k génère la clé de révocation notée $RE\_key = \frac{t_a^{'}}{t_a}$. Ensuite, le message sera chiffré encore $C_{new}^{''} = C^{''RE\_key} = g^{t_a^{'}s}$
4. Le nouveau texte chiffré recevra $E_{new}(M) = (\tau_1, C_0, C^{'}, C_{new}^{''})$

Après le processus de révocation, un utilisateur révoqué U_m ne pourra plus utiliser ses anciennes clés secrètes correspondantes à l'attribut a pour déchiffrer des messages. Les autres utilisateurs pourront utiliser les nouvelles clés secrètes pour leurs transactions futures.

3.4 Évaluation des performances

Dans cette section, nous présentons notre implémentation en décrivant les differents modules de l'application :

3.4.1 Setup

Nous implémentons un plugin appelé **CloudSN**. C'est une extension de "Firefox" basée sur HTML, CSS et JavaScript. Différentes interfaces sont considérées pour notre plugin, telles que :

1. Un gestionnaire d'utilisateurs, dans lequel un utilisateur administre sa liste d'amis et ajoute différents groupes.

2. Le partage de texte, dans cette partie, un utilisateur crée un contenu à partager avec ses amis. Il spécifie les groupes et crée la sous-structure d'accès. Par exemple $\tau' = friends \vee coworkers$. Ainsi, les utilisateurs ayant les clés secrètes correspondantes à ces attributs peuvent décrypter le message.
3. Le texte partagé, l'utilisateur ne pourra pas trouver les messages partagés par ses amis seulement s'il est en possession des clés secrètes qui peuvent déchiffrer les messages.

Avant d'utiliser toutes fonctionnalités de notre plugin, l'utilisateur doit être connecté à son compte Facebook. Nous mettons en oeuvre le protocole "Oauth" [90] pour utiliser les fonctionnalités de connexion de Facebook, ensuite l'utilisateur pourra gérer sa liste de ses amis et de ses groupes.

3.4.2 L'analyse des performances

Nous avons évalué notre implémentation de "CloudSN" sur un ordinateur de bureau utilisant un processeur de "core i5" de "2,00 GHz" et "8 Go" de RAM. Pour le module cloud, nous avons utilisé Juju cloud [91], un outil de modélisation d'application open source. Nous pouvons déployer, configurer, mettre à l'échelle et opérer sur un cloud public ou privé. LXD [92] est déployé en tant que cloud local, il est utilisé pour le cloud computing hors ligne. Il offre une expérience utilisateur similaire à celle des machines virtuelles en utilisant des conteneurs Linux. Il fonctionne comme un hyperviseur d'une machine virtuelle. Juju charms pourraient également être déployé sur de nombreux clouds en ligne tels que Amazon AWS, Google GCP, Microsoft Azure et ainsi de suite. Nous générons un test de 0 à 200 utilisateurs de Facebook [93].
Nous simulons la multi-autorité distribuée avec 6 autorités "AA", chaque autorité gère 10 attributs. Nous générons 6 cas pour déterminer l'évolution du temps de chiffrement et le temps de déchiffrement en fonction du nombre des attributs gérés par les autorités. Les différents cas sont présentés ci-dessous :

1. Tous les attributs sont gérés par le même AA
2. Tous les attributs sont gérés par 2 AA.
3. Tous les attributs sont gérés par 3 AA
4. Tous les attributs sont gérés par 4 AA.
5. Tous les attributs sont gérés par 5 AA.
6. Tous les attributs sont gérés par 6 AA.

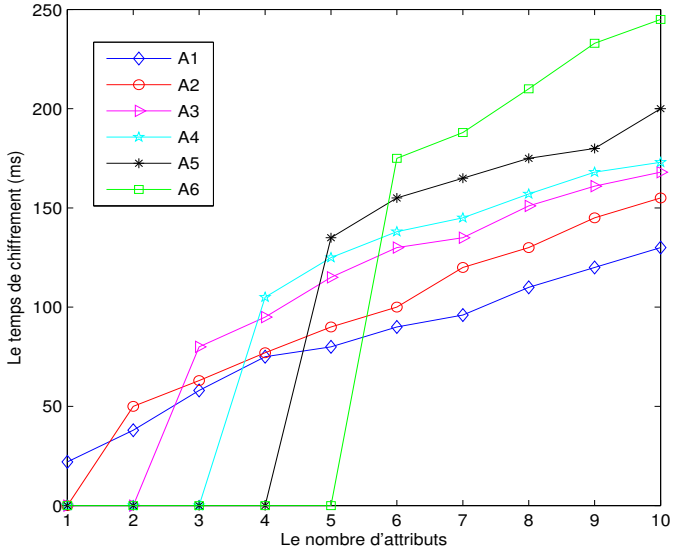

FIGURE 3.8 – Temps de chiffrement en fonction du nombre d'attributs

Les résultats de notre simulation sont illustrés dans la figure 3.8 qui représente la variation du temps du chiffrement en fonction des attributs, la figure 3.9représente la variation du temps du déchiffrement en fonction des attributs.

Les résultats montrent que le temps de chiffrement et le temps de déchiffrement augmentent avec le nombre d'attributs. Nous pouvons aussi observer que le temps du déchiffrement est légèrement inférieur au temps de chiffrement, car le processus de chiffrement prend en compte plus de paramètres par rapport au processus de déchiffrement.

Nous observons que lorsque tous les attributs sont gérés par la même autorité d'attribut, le temps de chiffrement est faible, comme illustré à la figure 3.8 (A1). Dans cette situation, notre framework est basé sur une autorité d'attribut unique qui représente le point de défaillance unique "single point of failure".
Lorsque les attributs sont gérés par plusieurs autorités, la durée de chiffrement augmente légèrement et la structure devient plus résistante contre le point de défaillance unique.
Le même processus sera observé en temps du déchiffrement, comme illustré dans la figure 3.9, où le temps augmente avec le nombre d'autorités d'attributs. Notez que nous avons considéré un maximum de sept attributs dans la sous-structure d'accès τ, nous rencontrons rarement une sous-structure ayant plus de cinq attributs dans la pratique [89]. Dans un tel contexte, il est important de prendre en compte la taille d'un message crypté. Ainsi, nous utilisons des messages variant entre 512 et 1024 bits.

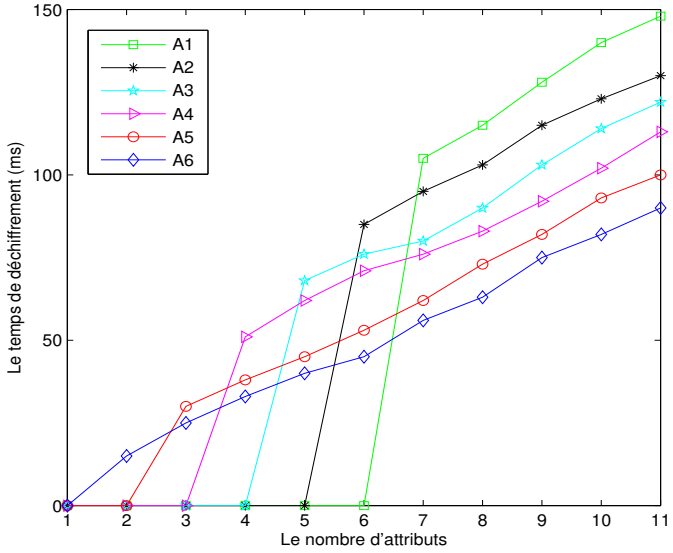

FIGURE 3.9 – Temps de déchiffrement en fonction du nombre d'attributs

3.5 L'analyse de la sécurité

Dans cette section, nous mettons en œuvre une analyse de la sécurité de notre solution proposée et nous discutons de certaines propriétés importantes de la sécurité :

3.5.1 l'analyse de la robustesse

Dans cette sous-section, nous présentons l'analyse de la robustesse de notre solution :

1. Les autorités d'attributs distribuées remplacent toutes les clés des utilisateurs et se combinent avec le cloud computing pour accéder aux données cryptées. Cette brèche est difficile voir impossible à exploiter, dans ce cas, tout le système (le cloud et les autorités d'attributs) sont malveillants.
2. Un utilisateur malveillant prétend être un ami, il peut avoir accès aux données partagées d'un utilisateur. Ensuite, l'utilisateur malveillant peut accéder et divulguer des données privées sur OSN. Cette violation est commune à tous les systèmes sécurisés et pour y faire face, il est important d'informer les utilisateurs de ce risque.
3. L'application tierce combine avec les autorités d'attributs distribuées et le cloud computing pour déchiffrer les données accessibles, cette violation ne peut pas être

exploitable. (Cela veut dire que même le cloud et les autorités d'attributs sont des complices avec les applications pour fournir des données des utilisateurs.)

3.5.2 Résistance aux attaques

Dans cette sous-section, nous présentons la résistance aux attaques de notre solution telles que :

A)Les menaces liés aux fournisseurs, aux utilisateurs et aux applications tierces

Lorsqu'un utilisateur partage des données à l'aide de notre solution "CloudSN", les données cryptées ne seront pas accessibles via "OSN", elles seront externalisées vers le cloud computing. Par conséquent, les données ne seront pas exploitables même si le fournisseur y a accès. Les données sont cryptées et seules les personnes autorisées peuvent les décryptées. Ainsi, ses données ne seront pas utilisées à des fins commerciales, publicitaires ou dans un objectif politique [9].

Les utilisateurs qui ne font pas partie du réseau partagé ne pourront pas accéder aux données. Seuls les amis possédant les clés de déchiffrement pourront les déchiffrées. En ce qui concerne l'application tierce, lorsqu'un utilisateur installe une application sur un OSN, elle ne pourra pas accéder aux données cryptées, car elle ne dispose pas des clés de déchiffrement.

B)La résistance aux attaques classiques

Comme nous l'avons vu dans la section 3.2.3, plusieurs attaques peuvent surgir sur les plateformes des réseaux sociaux en ligne. Ces attaques peuvent être classées en deux grandes catégories à savoir : les attaques classiques et les attaques modernes. Ces dernières sont spécifiques aux réseaux sociaux. Dans cette section, nous allons voir comment notre solution "CloudSN" fait face aux différentes attaques.

Les malwares : Le but de cette attaque est de voler les identifiants des utilisateurs, afin de prendre le contrôle sur leurs comptes. Face à cette attaque, notre solution ne peut rien faire si l'utilisateur perd le contrôle de son compte. Il doit être vigilant et attentif s'il reçoit un courrier avec un nom de domaine qui se termine par un ensemble de lettres bizarres, il faut être vigilant et ne pas cliquer sur un lien quelconque.

Le phishing : Le risque de cette attaque consiste à voler des données sensibles des

utilisateurs. Si l'utilisateur répond à des fausses pages en envoyant ses identifiants et les données personnelles, aucune solution ne peut les récupérer. Donc, l'utilisateur doit être sensible à ce genre d'attaques et de ne pas exposer ses données avant de vérifier le lien ou le nom du domaine du site.

Les spams : Ce type d'attaque se base essentiellement sur l'envoi des courriers indésirables aux utilisateurs, afin d'inciter ces derniers à cliquer sur des liens frauduleux. Dans ce cas, les utilisateurs doivent être conscient de ces pratiques et de ne pas faire confiance aux courriers malveillants.

Le Cross-Site Scripting (XSS) : Dans cette attaque, l'utilisateur malveillant exploite les applications web afin de collecter les données privées des utilisateurs en injectant un code malicieux. Avec notre solution "CloudSN", même si l'utilisateur perd ses données, elles ne seront pas exploitables, parce qu'elles sont chiffrées avec "ABE" et l'utilisateur malveillant n'est pas en possession des clés du déchiffrement qui sont gérées par MA-CP-ABE.

La fraude sur internet : La fraude sur internet est une attaque très répandue dans les plateformes des réseaux sociaux. Les escrocs activent dans la communauté dans le but de gagner la confiance des victimes et afin de tirer profit de ces dernières. En utilisant la solution "CloudSN", l'utilisateur chiffre via notre solution les données qui juge privée et ne donne accès à ses données qu'à ses amis. Donc même si l'utilisateur est victime d'une fraude, ses données reste protégées et ne seront accessibles que par les personnes autorisées.

B)La résistance aux attaques modernes

L'attaque de clickjacking : Le but principal de cette attaque est de manipuler les utilisateurs afin de partager des messages spams sur leurs profils. L'utilisateur doit être informé sur les risques de cliquer sur des liens et des messages de sources inconnues. Même si par malchance l'utilisateur clique sur des liens frauduleux, s'il utilise la solution "CloudSN", ses données privées resteront protéger et seulement les utilisateurs en possession des clés du déchiffrement peuvent récupérer le contenu crypté.

L'attaque par de-Anonymization Cette attaque consiste à traquer les utilisateurs en se basant sur l'appartenance à des groupes d'utilisateurs dans le but de divulguer leurs

identités. En utilisant la solution "CloudSN", les données cryptées resteront inaccessibles pour les personnes non autorisées. Même si l'identité de l'utilisateur est divulguée.

La reconnaissance faciale : Les utilisateurs doivent être informés et éduqués sur le risque de partager leurs intimités dans les plateformes des réseaux sociaux. Une fois les photos sont envoyées sur les OSNs, les utilisateurs en perdent le contrôle sur elles. Les utilisateurs doivent être conscients des actions et les conséquences qui peuvent être engendrées en partageant leurs photos sur les OSNs.

Les faux profils : Les attaques dans cette catégorie sont connues aussi comme "Sybil attaque". Les faux profils sont utilisés pour collecter des données personnelles des utilisateurs sur les plateformes des réseaux sociaux. Avec "CloudSN", si un utilisateur rentre en contact avec un faux profil, ce dernier ne pourra pas accéder aux données chiffrées s'il ne fait pas partie du groupe du partage.

L'attaque par clonage d'identité : Ce type d'attaque est un peu compliqué, l'utilisateur doit faire attention à ne pas partager ses données avec des amis sans être sûr de l'identité réelle de ces derniers. Même avec notre solution "CloudSN", si l'utilisateur partage des données privées avec un profil cloné, ses données risquent d'être partagées avec des personnes malveillantes.

L'attaque par inférence : Cette attaque consiste à employer des techniques de data mining avec la combinaison des données partagées en grand public dans le but de déduire des données privées. En utilisant "CloudSN", même si les utilisateurs malveillants exploitent une attaque par inférence, les données cryptées ne seront pas accessibles, vu qu'ils ne possèdent pas le droit d'accès. Dans cette attaque seule les données publiques qui seront exploitées.

La fuite d'informations : Vu la nature des réseaux sociaux en ligne, les utilisateurs ont tendance à partager leur données privées ainsi que les données de leurs amis, ce qui engendre la fuite de leurs données à des tiers qui peuvent être malveillants. En utilisant "CloudSN", l'utilisateur a le choix de partager ses données privées tout en gardant leur accès sous son contrôle. Les données seront cryptées avec une politique et un droit d'accès, le risque de fuite de données ne se présente pas dans ce cas.

Le socware : Avec cette technique d'attaque, un utilisateur malveillant attire l'attention de l'utilisateur en l'incitant à installer des applications malveillantes afin de participer à la propagation virale des logiciels. Dans ce cas-là, il faut informer les utilisateurs de ne pas installer des applications de source inconnues et cela dans son intérêt personnel. Avec "CloudSN", si l'utilisateur installe par erreur une application malveillante, cette dernière n'aura pas accès aux données cryptées, car elle ne possède pas les autorisations nécessaires.

3.5.2.1 La résistance à la coalition d'attributs :

Il est très important d'éviter la coalition d'attributs, qui peut potentiellement conduire à un accès illégitime aux données, comme illustré à la Figure 3.10. Supposons que deux utilisateurs S_b et S_t souhaitent combiner les clés secrètes de deux attributs PHD et PHY, qui appartiennent à S_b et S_t respectivement. Nous avons : PHD géré par AA_1 et PHY géré par AA_2 avec t_1 et t_2 qui sont les exposants secrets de l'attribut correspondant définis par AA. Le texte chiffré encodé avec la sous-structure d'accès $\tau' = PHD \wedge PHY$ est :

$$E^{'} = (\tau^{'}, C_0, \{C_i^{'}\}_{i=1,2...l}, \{C_i^{''}\}_{i=1,2...m}) \tag{3.12}$$

Nous avons : $C_0 = Me(g,g)^{\alpha_1+\alpha_2}s$, $C_i^{'} = g^{\beta_i s}$,$C_i^{'} = g^{t_i s_i}$. Les clés secrètes de S_b et S_t correspondant aux attributs Phd et Phy sont données comme suit : $(g^{\frac{r_1}{t_1}}, g^{\frac{\alpha_1 - r_1}{\beta_1}})$ et $(g^{\frac{r_2}{t_2}}, g^{\frac{\alpha_2 - r_2}{\beta_2}})$. Pour déchiffrer E, S_b et S_t peuvent calculer :

$$tmp_1 = e(g^{t_1 s1}, g^{\frac{r_1}{t_1}})e(g^{t_2(2s-s_1)}, g^{\frac{r_2}{t_2}}) \tag{3.13}$$

$$tmp_2 = e(g^{\frac{\alpha_1 - r_1}{\beta_1}}, g^{\beta_1 s})e(g^{\frac{\alpha_2 - r_2}{\beta_2}}, g^{\beta_2 s}). \tag{3.14}$$

L'utilisateur peut calculer $tmp_1.tmp_2$ pour déterminer M :

$$K = tmp_1.tmp_2 \tag{3.15}$$

$$K = e(g,g)^{(\alpha_1+\alpha_1)s}e(g,g)^{r_1 s_1}e(g,g)^{r_2(2s-s_1)}e(g,g)^{-(r_1+r_2)s} \tag{3.16}$$

Pour déchiffrer M à partir de C_0, le résultat de K doit être équivalent à $e(g,g)^{(\alpha_1+\alpha_2)s}$ et cela n'est possible que si la condition suivante est vérifiée :

$$e(g,g)^{r_1 s_1}e(g,g)^{r_2(2s-s_1)}e(g,g)^{-(r_1+r_2)s} = 1 \tag{3.17}$$

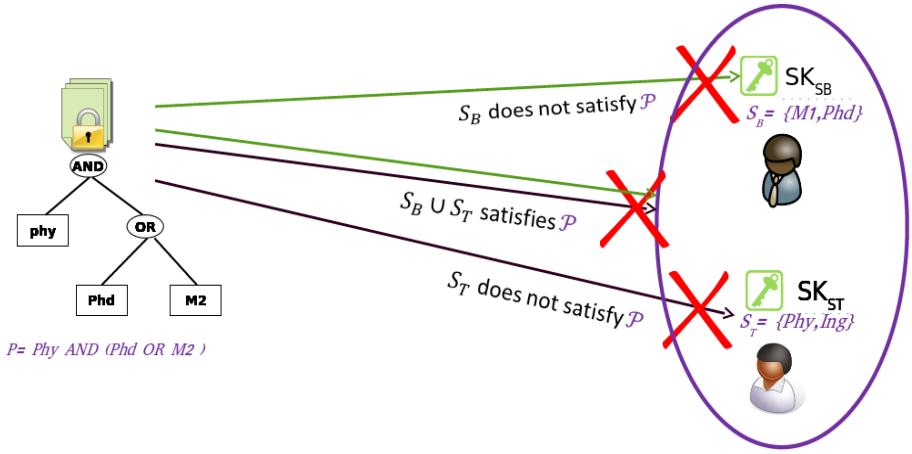

FIGURE 3.10 – MA-CP-ABE résistance aux coalitions

La condition ci-dessus est vérifiée uniquement si $r_1 = r_2$. Par conséquent, le déchiffrement de E via les clés secrètes de l'attribut en coalition n'est pas possible.

Dans la sous-section suivante, nous comparons notre solution proposée "CloudSN" à des solutions similaires trouvées dans la littérature.

TABLE 3.1 – Comparaison de CloudSN avec des solutions existantes

Solution proposée	Management des attributs	Contrôle d'accès	Plateforme basée sur	Stockage des données sensibles
Personna	Centralisée	ABE	OSN	Application doc wall
Scramble	centralisée	Clés publique	Pas sur OSN	Machine de l'utilisateur
CloudSN	Décentralisée	MA-CP-ABE	Pas sur OSN	Cloud computing

Nous comparons notre solution proposée "CloudSN" aux solutions similaires trouvées dans la littérature. Nous comparons notre solution à "Scramble vos données" proposées dans [11] et "Persona" proposée dans [12]. La comparaison est illustrée dans le tableau 3.1, dans laquelle nous prenons plusieurs paramètres tels que : la gestion des attributs, le contrôle d'accès, la plateforme utilisée et le stockage des données sensibles.

Pour la gestion des attributs et le contrôle d'accès, les auteurs dans "Personna" ont utilisé la gestion des attributs centralisés et un contrôle d'accès basé sur ABE. Avec cette configuration la solution souffre de problèmes de flexibilité et d'évolutivité et cela permet de créer une vulnérabilité appelée le point de défaillance unique. Dans la solution "Scramble", les auteurs ont utilisé une solution centralisée basée sur un mécanisme de clés publiques pour protéger les données contre les intrusions. Cependant avec "CloudSN",

ces problèmes sont évités en utilisant une gestion distribuée des attributs et un contrôle d'accès basé sur MA-CP-ABE.

Concernant la plateforme utilisée et le stockage des données sensibles, dans la solution "Persona", les auteurs ont proposé une application appelée "doc wall", qui est basée sur la plateforme OSN. Malgré l'utilisation du mécanisme "ABE" pour contrôler l'accès aux données, cette solution dépend de la plateforme de Facebook. Cependant avec la solution "Scramble", Beato et al [12] ont utilisé les clés publiques de tous les utilisateurs d'un groupe pour chiffrer les messages. Toutes ces clés sont ensuite stockées sur la machine locale de l'utilisateur. Notre solution ne repose pas sur la plateforme d'OSN. Les données cryptées sont externalisées vers le cloud computing, ce qui permet aux utilisateurs d'avoir accès à leurs données partout et à tout moment.
Dans notre solution proposée, nous utilisons une multi-autorité d'attributs distribuée. Contrairement à l'autorité d'attribut centralisée, lorsqu'une autorité est hors-service, le système continuera à fonctionner, et seules les données gérées par cette autorité ne seront pas accessibles. Cependant, dans un système centralisé, quand ce dernier est compromis, tout sera hors-service.

3.6 Conclusion

Dans ce chapitre, nous avons présenté un nouveau framework appelé "CloudSN" basé sur un schéma d'ABE distribué. Ce dernier permet de protéger la confidentialité des données des utilisateurs. Ces derniers peuvent concevoir leur propre politique d'accès permettant uniquement aux amis autorisés d'avoir accès à leurs données. Notre schéma proposé réduit le risque de "point de défaillance unique".
Une analyse de sécurité a été présentée montrant que notre solution est robuste et résistante à plusieurs attaques et vulnérabilités telles que les attaques de coalition, les vulnérabilités causées par le provider, les utilisateurs et les applications tierces.

La partie suivante sera dédié à notre nouvelle approche qui est basée sur la blockchain et le "Software-Defined Vehicular Networks" pour sécuriser les réseaux sociaux véhiculaires. À cette fin, nous allons introduire les réseaux sociaux véhiculaire dans le chapitre suivant.

Chapitre 4

LES RÉSEAUX SOCIAUX VÉHICULAIRES

Sommaire

4.1 Introduction 67
4.2 Définition des réseaux sociaux véhiculaires 69
4.3 Architecture des réseaux sociaux véhiculaires 69
4.3.1 Architecture centralisée 69
4.3.2 Architecture distribuée ou décentralisée 70
4.3.3 Architecture hybride 70
4.4 Applications des réseaux sociaux véhiculaires 70
4.4.1 Les applications de sécurité 71
4.4.2 Les applications basées sur la commodité 71
4.4.3 Les applications basées sur le confort 71
4.4.4 Les applications basées sur le divertissement 71
4.5 Conclusion 72

4.1 Introduction

Avec la croissance rapide de la technologie et l'utilisation des smart-phones, des smart-watches et les voitures connectées, les utilisateurs à savoir les conducteurs et les passagers ont la possibilité de communiquer entre eux ainsi qu'avec l'infrastructure située au bord de la route.
Le réseau ad-hoc sans fil "a wireless ad-hoc netowrk" est constitué d'un ensemble d'unité mobile qui sont capables de communiquer sans passer par une entité centrale pour gérer les données. La particularité des réseaux ad-hoc sans fil est que chaque entité faisant partie du réseau contribue dans le routage des données. Les réseaux mobiles ad-hoc "MANET" ainsi que les réseaux véhiculaires ad-hoc "VANET" font partie de la famille des réseaux ad-hoc sans fil. Le MANET est un ensemble de noeuds mobiles auto-formés présentant un nombre de caractéristiques à savoir : une topologie dynamique, sécurité physique limitée, une autonomie et une bande passante limitée ainsi qu'une variation des capacités de liaison des nœuds [94]. Le VANET est un ensemble de véhicules connectés où chaque entité est équipée avec un "On-board Unit OBU", c'est un dispositif de communication assurant une liaison "V-2-V" véhicules avec véhicules et "V-2-I" véhicules avec l'infrastructure et "V-2-X" véhicule avec n'importe quels supports.

Avec l'arrivée des réseaux sociaux Facebook, Twitter, Linkedin, Google+, YouTube et ResearchGate, un nouveau type d'application est apparue à savoir les réseaux sociaux véhiculaires "VSN". Un "VSN" est un ensemble de véhicules connectés avec un aspect social permettant aux différentes entités de communiquer et d'échanger des données telles que : des images, des vidéos, des audios et des informations sur le trafic routier. Dans le tableau 4.1, nous présentons une comparaison entre VANET, MANET et VSN, la comparaison est faite sur l'architecture de déploiement, le coût, la sécurité physique, l'autonomie, les ressources et les applications.

TABLE 4.1 – La comparaison entre les réseaux MANET, VANET et VSN

Les MANETs	Les VANETs	Les VSNs
Une auto-configuration. Sans infrastructure. Les mobiles se connectent en réseau sans fil. Architecture basé sur connexion nœud à nœud	Une sous-classe des MANETs **«Roadside Unit»** une infrastructure permettant aux véhicules de coopérer. Connexion V-2-V et V-2-I , V-2-X	Une sous-classe des MANETs **«Roadside Unit»** une infrastructure permettant aux véhicules de coopérer. Connexion V-2-V et V-2-I , V-2-X utilisant l'aspect social
Liberté de mouvement dans n'importe quelle direction . Changement fréquent de liens de connexion. Variation des capacités de liaison et de nœud.	Liberté de mouvement dans n'importe quelle direction bien encadré . Changement fréquent de liens de connexion.	Liberté de mouvement dans n'importe quelle direction bien encadré et dans le même intérêt social.
Le déploiement est facile pour mettre en œuvre il n'est pas coûteux,	Le déploiement n'est pas facile pour le mettre en place et il est relativement coûteux.	Le déploiement n'est pas facile pour le mettre en place et il est relativement coûteux.
Application dans le domaine Militaire, catastrophe (spécifique)	Applications sécurité, circulation, paiement	Applications sociales véhiculaires, applications géolocalisées
Sécurité physique limité, Une autonomie et une bande passante limitée,	Sécurité physique dépend des dispositifs impliquée. Véhicule non limité par énergie et espace de stockage,	Sécurité physique dépend des dispositifs impliquée. Véhicule non limité par énergie et espace de stockage.

4.2 Définition des réseaux sociaux véhiculaires

Les réseaux sociaux véhiculaires sont composés d'un certain nombre de véhicules $V = \{v_1, v_2.....v_n\}$. Ils sont équipés d'unité embarquée "on-board unit" et ils sont connectés aux unités routières "RoadSide Units". Les véhicules peuvent communiquer entre eux (communication "véhicule à véhicule V-2-V"), ainsi qu'avec RSU, communication "véhicule à infrastructure V-2-I" comme ils peuvent communiquer avec n'importe quels supports "V-2-X". Ces types de communications peuvent se faire en utilisant "3G/4G", "WLAN/WIFI", "WIMAX et "DSRC/WAVE" [95]. Les réseaux sociaux permettent aux utilisateurs de communiquer et de partager des données sans aucune limite. L'intégration du réseau social dans le réseau véhiculaire offre de nouvelles applications principalement liées à la sécurité et aux divertissements.

La gestion intelligente du trafic aide les utilisateurs à ajuster leurs comportements et cela grâce aux données collectées en temps réel à partir de différents capteurs intégrés. Il est possible de générer une carte du trafic routier en temps réel qui indique les niveaux de trafic à différents endroits afin d'éviter la congestion du trafic.

Les principaux composants de VSN sont les participants et l'infrastructure réseau. Nous pouvons trouver des conducteurs, des passagers, des piétons, OBU et des RSUs. Tous ces participants peuvent faire partie de la communication. Des dispositifs intelligents intégrés dans les véhicules, les conducteurs et les piétons peuvent détecter le voisinage et partager du contenu comme des fichiers audios, des vidéos, etc.

4.3 Architecture des réseaux sociaux véhiculaires

Les utilisateurs le long des routes rencontrent d'autres utilisateurs qui partagent les mêmes intérêts sociaux. Les utilisateurs ont tendance à utiliser les mêmes itinéraires pour aller travailler ou voyager et partager un ensemble de données à savoir vidéos, audios, photos de trafic routier et d'autres informations provenant de différents capteurs intégrés. L'architecture de communication physique de VSN dépend de l'infrastructure réseau qui peut être centralisée, distribuée ou hybride.

4.3.1 Architecture centralisée

Dans l'architecture centralisée, les appareils communiquent avec le serveur qui surveille et gère leurs échanges. Dans une telle architecture, les appareils ne peuvent pas communiquer directement. Toutes les données sont stockées sur un serveur distant. Le

serveur agit comme un intermédiaire entre les entités VSN pour communiquer. Cette architecture peut permettre aux utilisateurs de mettre à jour leurs profils et leurs intérêts.

Un système centralisé est moins sensible à la densité du trafic sur les routes et peut-être déployer sur une zone géographique plus large permettant aux utilisateurs des VSN de communiquer même s'ils ne sont pas proches les uns des autres. Cependant, le coût de la communication dans une telle architecture est supérieur à celui d'une architecture distribuée. En outre, l'architecture centralisée peut entraîner une communication inefficace entre les utilisateurs finaux, une capacité de stockage faible et une charge de trafic dans les zones urbaines très dense.

4.3.2 Architecture distribuée ou décentralisée

Dans l'architecture VSN distribuée, les entités VSN communiquent entre elles et collaborent d'une manière ad-hoc. Les véhicules et les voyageurs communiquent sans aucune infrastructure centralisée. Les nœuds intermédiaires stockent les paquets de données sociaux jusqu'à ce que la destination soit trouvée. La diffusion des données sur l'architecture distribuée nécessite la coopération des entités VSN. De plus, la transmission et la diffusion de données dans l'architecture distribuée sont sensibles au comportement malveillant des entités intermédiaires. La communication dans cette architecture est plus efficace que l'architecture centralisée pour assurer une communication directe entre entités VSN et réduire la charge de trafic sur les RSUs.

4.3.3 Architecture hybride

Dans l'architecture hybride, les véhicules communiquent en utilisant "V-2-V" ou "V-2-I" communications. Les utilisateurs peuvent communiquer en utilisant une connexion de données cellulaires si l'infrastructure "RSU" n'est pas disponible. Les véhicules connectés via internet peuvent partager des informations susceptibles d'améliorer la qualité du trafic sur les routes.

4.4 Applications des réseaux sociaux véhiculaires

Dans cette partie nous allons aborder les différents types d'applications de VSN. Le VSN est une combinaison de réseau social et réseau véhiculaire. Par conséquent, le concept de VSN peut être largement utilisé pour améliorer la communication entre les utilisateurs tout le long des routes avec une multitude d'applications. Les applications peuvent être classées en quatre catégories à savoir :

1. Les applications de sécurité.
2. Les applications basées sur la commodité.
3. Les applications basées sur le confort.
4. Les applications basées sur le divertissement.

4.4.1 Les applications de sécurité

Ce type d'application est utilisé pour améliorer la sécurité routière en partageant des informations utiles aux utilisateurs pour diminuer la probabilité d'accidents de la circulation. Les informations partagées peuvent être la position du véhicule, la vitesse, la direction, la distance parcourue et la position de collision calculée pour éviter de tels accidents. Ces informations peuvent être partagées entre les véhicules ou les RSUs.
Les applications peuvent être de type avertissement "warning" de type accidents ou collision, condition de circulation, etc. Les véhicules et les "RSUs" sont utilisés pour envoyer périodiquement des informations afin d'améliorer les conditions routières.

4.4.2 Les applications basées sur la commodité

Les applications basées sur la commodité sont utilisées pour améliorer les conditions de voyage et à éviter les encombrements et à réduire le temps de voyage. Les voyageurs sur la route peuvent créer une sorte de réseau virtuel pour partager des informations de trafic en temps réel avec des utilisateurs d'intérêts communs. Ces informations peuvent être exploitées pour choisir ou modifier un itinéraire afin d'éviter les embouteillages.

4.4.3 Les applications basées sur le confort

Ce type d'application permet aux utilisateurs d'accéder à des services tout le long du trajet, ils peuvent payer des parkings, stations de péage, recherche d'espace de stationnement, stations de services, etc. Toutes ces applications permettent d'améliorer le confort des usages.

4.4.4 Les applications basées sur le divertissement

Ces applications permettent aux usages d'avoir accès aux contenus multimédias et de partager/télécharger des fichiers audios, des vidéos, des photos ou jouer à des jeux. Durant les heures de pointe, les utilisateurs peuvent profiter des applications de divertissement afin d'oublier les moments de la congestion routière.

4.5 Conclusion

Cette partie a été dédiée aux réseaux sociaux véhiculaires "VSN", qui est un nouveau domaine de communication où le concept a été inspiré de deux disciplines à savoir le réseau ad-hoc "VANET" et le réseau social mobile "MSN". Ce paradigme émergeant présente de nouveaux domaines de recherche pour le partage de contenu. Les utilisateurs le long des routes rencontrent d'autres utilisateurs qui partagent les mêmes intérêts sociaux. L'architecture de communication physique de VSN dépend de l'infrastructure réseau qui peut être centralisée, distribuée ou hybride. Le concept de VSN peut être largement utilisé pour améliorer la communication entre les utilisateurs tout le long des routes avec une multitude d'applications.
Le chapitre suivant sera dédié aux applications de la Blockchain dans l'Internet des Objets "IoT", qui représente un outil très pertinent qui nous a beaucoup servi dans nos contributions.

Chapitre 5

APPLICATIONS DE LA BLOCKCHAIN POUR L'IOT "INTERNET OF THINGS"

Sommaire

5.1 Une vue globale sur la Blockchain 74
5.2 Applications de la Blockchain dans l'IoT 75
5.2.1 Internet des objets dans la santé "Internet of healthcare things" 75
5.2.2 Fog computing 76
5.2.3 IoT pour devices 77
5.2.4 Software-defined networking 77
5.2.5 Internet des véhicules IoV 78
5.3 Conclusion 81

5.1 Une vue globale sur la Blockchain

La "Blockchain" est un nouveau concept basé sur la "crypto-coins", introduit pour la première fois dans l'œuvre de Nakamoto [96]. Le concept de la Blockchain est de conserver les transactions d'une manière distribuées et authentiques. Les transactions regroupées dans un bloc sont validées à l'aide de la puissance de traitement des appareils. Les blocs validés seront ajoutés à la chaîne.

Les caractéristiques de la Blockchain tels que la transparence, la confidentialité et la facilité de traitement assurent un champ d'application beaucoup plus vaste [97, 98]. Nous pouvons trouver des applications de la Blockchain comme "Registre", il garantit une meilleure traçabilité des produits et des actifs, des "contrats intelligents" [99] et un système de vote basé sur la Blockchain [100] etc.

Comme définition de la Blockchain, elle est organisée sous la forme d'enregistrements. Un groupe de nœuds du réseau appelé "mineurs" prouve une liste de transactions et les ajoutes à la Blockchain. Les transactions regroupées dans un bloc sont validées en résolvant un problème mathématique à l'aide d'un algorithme de hachage. Ces opérations sont appelées "Proof of work", ce qui indique que les nœuds de mineurs ont bien pris le temps pour résoudre le problème.

La particularité de la Blockchain est qu'il n'y a pas de point central pour gérer ou valider les transactions. Chaque nœud peut agir comme un point central. Comme on peut le voir dans la Figure5.1. Un bloc peut contenir une liste de champs tels qu'un numéro de bloc unique, un nonce qui est un nombre entier, des données et le précèdent et l'actuel hachage du bloc.

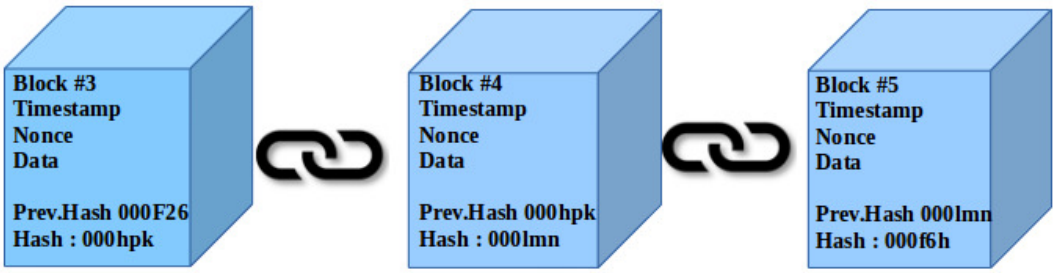

FIGURE 5.1 – Architecture de la Blockchain.

Les algorithmes de hachage ont de nombreuses propriétés intéressantes. Les blocs sont liés par le hachage, chaque bloc fait référence au précédent bloc basé sur l'algorithme de hachage. Par conséquent, si un attaquant tente de modifier un bloc déterminé, cette activité rendra les hachages de tous les blocs invalides.

La connexion entre des blocs utilisant un hachage rend la Blockchain inviolable par rapport aux structures de base de données standard. Le rôle des mineurs consiste à fournir la dernière valeur de hachage du bloc ajouté à la Blockchain.

Nous considérons la fonction de hachage "SHA256", elle génère un nombre hexadécimal à 64 chiffres. La Blockchain comporte d'autres champs tel que le "timestamp" représentant l'heure Unix actuelle. Ils servent d'entrées pour la fonction de hachage pour calculer le hachage du bloc actuel.

$$SHA256(Blocknumber, timestamp, nonce, data, previousblock'shash) -> hash$$

La "proof of work" est réalisé en incrémentant le "nonce" dans le bloc, jusqu'à ce que le bloc soit exploité avec succès. Quand de nouvelles transactions sont diffusées aux mineurs, ils les rassemblent dans un bloc et travaillent à trouver une "proof of work". Quand le mineur réalise une "proof of work", il diffuse le bloc à tous les nœuds et sera ajouté à la Blockchain. Un exemple de proof of woork consiste à coder une variation d'une chaîne de caractère en utilisant la fonction de hachage SHA-256 et cela jusqu'à ce que une empreinte qui débute par sept zéros sera trouvée. Cette "proof of work" est simple a réalisé avec les systèmes moderne, mais dans la crypto-monaie [96] la "proof of woork" sont beaucoup plus complexes à faire.

5.2 Applications de la Blockchain dans l'IoT

La technologie de la Blockchain peut en effet être appliquée dans presque tous les domaines de l'IoT [101], comme le montre la Figure 5.2

5.2.1 Internet des objets dans la santé "Internet of healthcare things"

L'utilisation de l'IoT dans la santé nous permet de fournir aux systèmes de santé des données relatives aux patients. Ces données sont appelées dossiers médicaux électroniques "EMRs". L'utilisation des dossiers de santé électroniques "EHRs" facilite la portabilité des données des utilisateurs. Liang et al.[102] ont présenté un modèle permettant de partager les données dans des applications de santé basées sur la Blockchain. Esposito et al.[103] ont proposé une solution basée sur la Blockchain pour conserver les informations de santé stockées dans le cloud computing. Dans le modèle proposé, les modifications appliquées aux données du patient sont perceptibles par tous les membres du réseau. Tout changement illégal peut être découvert. De plus, Guo et al.[104] ont

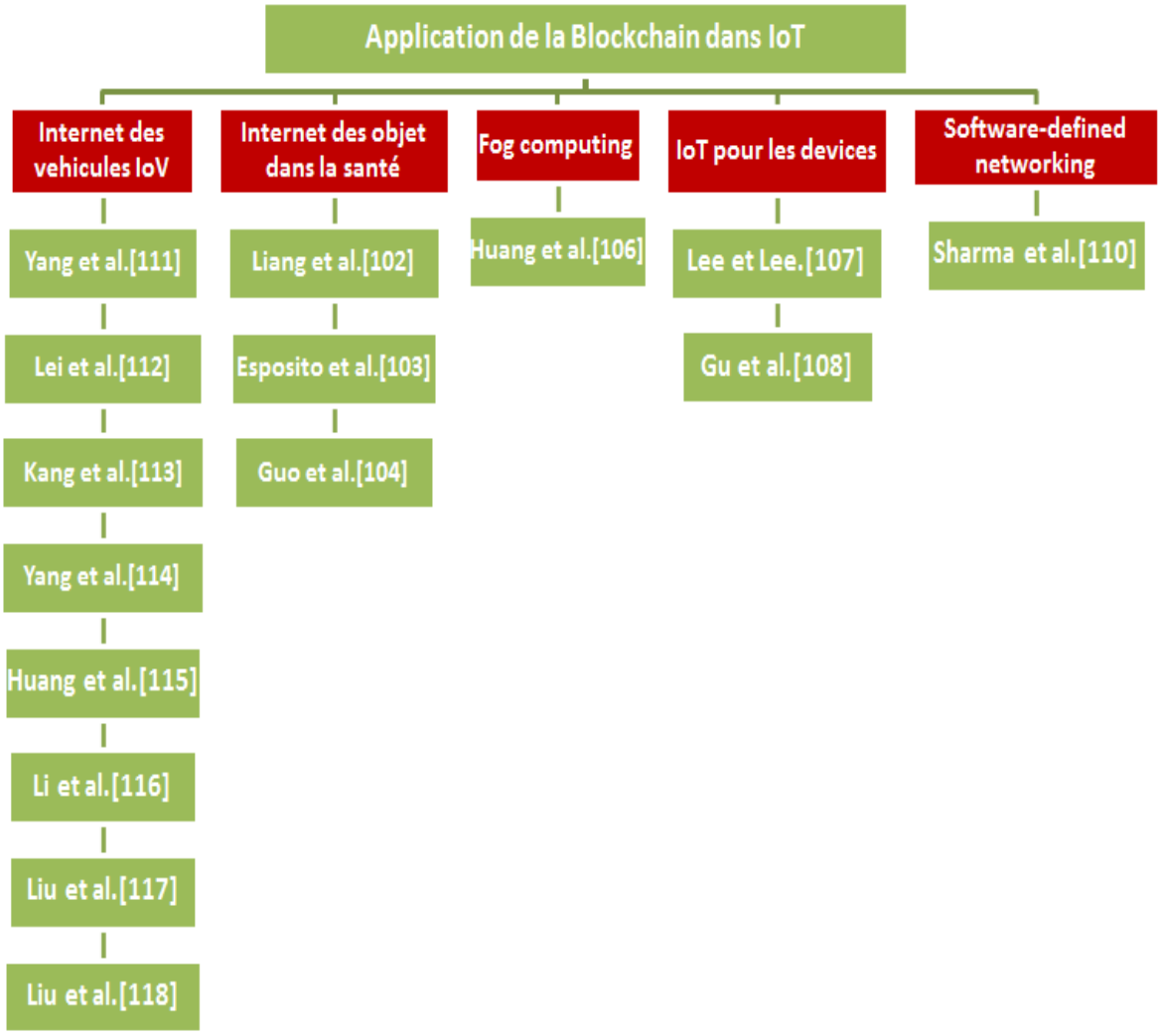

FIGURE 5.2 – Applications de la Blockchain dans IoT.

proposé un système fondé sur plusieurs autorités "MA-ABS". Le système "MA-ABS" peut être résistant aux attaques de collusion qui peuvent être lancées par les autorités corrompues à "N-1".

5.2.2 Fog computing

Le Fog computing, également appelé "edge computing" est un système dans lequel divers dispositifs coopèrent et communiquent entre eux et avec le réseau, dans le but de réaliser des actions telles que le stockage et le traitement de données sans tiers [105]. Huang et al [106] ont mis en place un système de paiement basé sur le "bitcoin". Ils

ont proposé un protocole de paiement utilisant des propriétés de sécurité telles que l'exhaustivité, l'équité et la responsabilité.

5.2.3 IoT pour devices

Un attaquant tente d'obtenir les données de IoT device en utilisant des scripts malveillants. Lee et al.[107] ont introduit un microcode basé sur la Blockchain pour vérifier en toute sécurité la version du microcode. Pour obtenir les mises à jour du microcode, un device envoie sa demande en utilisant une blockchain peer-to-peer d'une manière décentralisée. Gu et al.[108] ont proposé "CB-MDEE", qui est un framework basé sur la Blockchain, il est utilisé pour détecter les logiciels malveillants sur les appareils mobiles. Le framework est basé sur la logique floue dans le but d'atténuer le ratio de faux positif et améliorer la détection des logiciels malveillants.

5.2.4 Software-defined networking

Les scientifiques ont proposé un logiciel pour gérer le réseau appelé "software-defined networking SDN". L'utilisation du contrôleur SDN fournit un routage intelligent et simplifie la prise de décision[109]. Les réseaux traditionnels utilisent du matériels et des logiciels pour manager le réseau. Le "SDN" permet d'administrer un réseau tout en virtualisant les différents matériels tels que le firewall, la répartition de charge "load-balancer" etc. Le "SDN" sépare la gestion du réseau en :

- Le plan de contrôle "control plane" : il permet une gestion centralisée du réseau en déterminant les chemins à emprunter en utilisant des protocoles de routages.
- Le plan de données "data plane" : c'est la partie responsable de la gestion du flux de trafic en se basant sur des fonctionnalités et des process afin de gérer les données transitant d'une interface à une autre.

Sharma et al.[110]ont proposé "Distblocknet", qui est un contrôleur sur un réseau basé sur la Blockchain. L'architecture proposée est sans un point central, elle assurera l'évolutivité et la flexibilité de la solution. Le "Distblocknet" est basé sur le contrôleur/vérification et demande/réponse des nœuds. En ce qui concerne le nœud de vérification, il conserve les informations de règles de flux mises à jour. Le deuxième noeud qui est le device de transfert IoT, il met à jour la table des règles dans la Blockchain.

5.2.5 Internet des véhicules IoV

Dans cette sous-section, nous présentons les travaux liés à l'internet des véhicules "Iov". Comme nous pouvons le voir dans la Table5.1, tous les travaux traitant "IoV" prennent la sélection des mineurs différemment. Ils sont basés sur les "RSUs" la plupart du temps. Ainsi, ils délèguent le traitement des mineurs aux stations de base "RSUs". Cependant, la sélection des mineurs dans notre approche est différente de ces propositions.

TABLE 5.1 – Comparaison des travaux existants liés à la sélection des mineurs

Année	Contribution	Proposition	Défis de la recherche	La sélection des Mineurs
2017	Yang et al. [111]	A blockchain-based reputation system for data credibility assessment in vehicular networks	La validité des messages reçus en utilisant la réputation de l'expéditeur.	Basé sur des véhicules dotés de capacités de détection plus importantes. Le processus de sélection n'a pas été mentionné.
2017	Lei et al. [112]	Blockchain-based dynamic key management for heterogeneous intelligent transportation systems	Aucune autorité externe, la gestion des clés la vérification et l'authentification sont basées sur SM	Base sur un le Manager de Sécurité (SM). Les SM sont des stations de base qui jouent le rôle de mineurs.
2017	Kang et al.[113]	Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains	PETCON est proposé en utilisant un système de commerce peer-to peer. Un agrégateur local est proposé pour examiner et contrôler les transactions	Un agrégateur local (LAG) est utilisé pour contrôler les transactions. Les GAL sont utilisés en tant que courtiers en énergie « energy broker » pour donner accès à divers services.
2018	Yang et al.[114]	Blockchain-based decentralized trust management in vehicular networks.	Mesurer la crédibilité des informations reçues.	Basé sur des « roadside units » Les RSUs sont le point central de toutes les actions.
2018	Huang et l.[115]	LNSC: a security model for electric vehicle and charging pilemanagement based on blockchain ecosystem.	Sur la base d'outils cryptographiques, un modèle appelé «LNSC» est proposé pour assurer l'alimentation électrique.	Les stations de charge fixes servent à valider la blockchain.
2018	Li et al.[116]	CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles	Le schéma proposé appelé "CreditCoin" basé sur la blockchain. Un protocole est construit pour assurer une communication sécurisée.	Les RSUs sont utilisées dans le système de vote pour inciter l'utilisateur à transmettre des données
2018	Liu et al. [117]	Blockchain-enabled security in electric vehicles cloud and edge computing.	Les véhicules électriques (EV) fournissent des informations de flux qui changent.	Les RSUs vérifient les enregistrements de véhicules avant de les ajouter à la blockchain.
2018	Liu et al.[118]	Evolutionary game for mining pool selection in blockchain networks	Modèle basé sur le jeu évolutif pour décrire mathématiquement le processus dynamique de sélection de « mining-pool ».	La sélection minière est basée sur deux aspects, le taux de hachage et le délai de propagation.

Nous introduisons un nouveau framework basé sur le "Software-Defined Vehicular Networks" (SDVN). Nous utilisons le paradigme de la Blockchain, à cette fin, un nouvel algorithme a été proposé à savoir "Distributed Miners Connected Dominating Set algorithm DM-CDS", ce dernier est utilisé pour sélectionner les nœuds "mineurs". En effet, dans les travaux liés aux IoV utilisant la Blockchain, la sélection des mineurs est basée sur une architecture centralisée, et l'architecture que nous proposons est basé sur une architecture semi-distribuée, Yang et al.[111] ont proposé un système de réputation basé sur la Blockchain pour mesurer la fiabilité des informations. Les véhicules évaluent les messages reçus et les encapsulent dans un bloc. Un véhicule sélectionné est chargé de diffuser l'information aux autres. En utilisant les informations stockées sur la Blockchain, les véhicules évaluent la réputation de l'émetteur, ainsi, une décision sur la crédibilité des messages est prise.

Lei et al.[112]ont proposé un système de gestion de clés basé sur la Blockchain pour un système de transport intelligent hétérogène. Dans lequel les autorités externes sont supprimées et la vérification de la gestion de la clé et l'authentification sont basées sur le gestionnaire de sécurité.
Kang et al.[113]ont proposé un framework appelé "PETCON" basé sur un système de commerce peer-to-peer. Il est basé sur des agrégateurs locaux "LAGS" utilisés pour contrôler les transactions et donner accès à divers services. Yang et al.[114] ont proposé un modèle de confiance basé sur la Blockchain décentralisée pour mesurer la crédibilité des informations reçues. Sur la base des résultats d'évaluations, les véhicules attribuent des notations et les envoient aux RSUs, qui calculent la valeur de confiance des véhicules concernés et les ajoutent à un bloc. La Blockchain est maintenue par tous les RSUs, qui collaborent pour maintenir une Blockchain de confiance fiable et cohérente.

Huang et al.[115] ont proposé un modèle basé sur la Blockchain pour un véhicule électrique permettant de charger des piles. Basé sur des outils cryptographiques, un modèle appelé "LNSC" est proposé pour assurer l'alimentation électrique. Li et al.[116] ont proposé un modèle de confidentialité basé sur une annonce de récompense pour un système de transport intelligent "ITS". Le schéma proposé est appelé "CreditCoin" basé sur la Blockchain, dans lequel un protocole est construit pour assurer une communication sécurisée.

Liu et al.[117] ont proposé un véhicule électrique basé sur le cloud computing et l'edge computing utilisant la Blockchain. Les véhicules électriques "VE" fournissent des informations de flux qui changent. Un utilisateur malveillant peut capturer des informations via le réseau. Pour résoudre ce problème, la Blockchain est introduite avec deux

fonctionnalités. Décentralisé signifie que toutes les opérations de données telles que la comptabilité, le stockage et la transmission sont basés sur une approche distribuée. La deuxième caractéristique est la co-participation, signifie que tous les véhicules électriques "EVs" participeront à la formation des transactions. Les auteurs se sont concentrés sur des questions liées aux échanges de données et de l'énergie. L'utilisation du paradigme de la Blockchain dans le but de renforcer la sécurité et la protection des données. Les données du véhicule seront cryptées et organisées en blocs. Les RSUs vérifient les enregistrements des véhicules avant de les ajouter à la Blockchain.

Liu et al.[118] ont proposé une sélection dynamique des ressources des mineurs basées sur la Blockchain et la théorie des jeux évolutionnaires utilisant le protocole de consensus de Nakamoto[96].
Les auteurs prennent deux facteurs tels que la puissance de calcul et le délai de propagation qui définissent le résultat de la sélection. Ils proposent un modèle basé sur le jeu évolutif pour décrire mathématiquement le processus dynamique de sélection. Les auteurs se sont concentrés sur la mise en commun des ressources par les mineurs. En tout état de cause, ils n'ont pas discuté du processus de sélection des mineurs.

Tous ces travaux ont pris la Blockchain différemment. Dans les travaux de Yang et al.[114], les auteurs parlent de la crédibilité des données, à cette fin, ils ont proposé un framework décentralisé pour la gestion de la confiance. Les RSUs jouent un rôle important dans la mise à jour des valeurs de confiance. Les auteurs de ces articles n'ont pas expliqué comment sélectionner des nœuds du réseau pour agir en tant que mineurs. Dans les travaux de Liu et al.[117], les auteurs ont utilisé la Blockchain sans se focaliser sur la sélection des mineurs.

5.3 Conclusion

Dans ce chapitre nous avons abordé le concept de la Blockchain dont le rôle consiste à certifier les transactions échangées dans un réseau. Nous avons présenté les différents champs d'applications de la Blockchain comme le système de vote, les registres et les contrats intelligents, etc. La dernière partie du chapitre a été dédiée aux différents domaines d'application de la Blockchain à savoir : la santé, le fog computing et l'IoT pour les devices, etc. Une comparaison des différents travaux liés à la sélection des mineurs a été réalisée dans le domaine véhiculaire.
Le chapitre suivant sera dédié à notre nouvelle approche qui est basée sur la Blockchain et le "Software-Defined Vehicular Networks" pour sécuriser les réseaux sociaux véhiculaires

Chapitre 6

VERS UNE APPROCHE BASÉE SUR LA BLOCKCHAIN ET "SOFTWARE-DEFINED VEHICULAR NETWORKS" POUR SÉCURISER LES RÉSEAUX SOCIAUX VÉHICULAIRES

Sommaire

6.1 Introduction 83
6.2 Un framework basé sur l'architecture de la Blockchain . . . 84
6.2.1 Présentation de l'architecture 85
6.2.2 Module de la sécurité et de la confidentialité 88
6.2.3 Modèle de confiance 89
6.3 La sélection des mineurs basée sur l'algorithme CDS 95
6.4 Analyse des performances 99
6.4.1 La configuration de la simulation 99
6.4.2 Analyse des résultats de la simulation 101
6.5 Analyse de sécurité 105
6.5.1 Résistance aux attaques 105
6.6 Conclusion 110

6.1 Introduction

Le réseau social véhiculaire "VSN" est un nouveau concept prometteur combinant deux types de réseaux, à savoir les réseaux de véhicules et les réseaux sociaux[119, 120]. Dans le VSN, un véhicule est équipé de plusieurs capteurs capables de collecter de multiples données spatio-temporelles. La dimension sociale est principalement considérée comme la capacité du conducteur à analyser, utiliser et partager ses données avec d'autres navetteurs partageant les mêmes intérêts ou confronter à des conditions de trafic similaires. Le VSN intègre des fonctionnalités pertinentes du réseau véhiculaire et du réseau social. Le réseau véhiculaire assure l'infrastructure de communication réseau qui peut être déployée en mode centralisé, distribué ou hybride.

Le VSN est un système de communication hétérogène, dans lequel plusieurs périphériques peuvent échanger des informations tout le long de la route, tels que des unités embarquées "On-Board Unit" (OBU), des unités routières " Road Side Unit" (RSU) et des périphériques intelligents exploitant le comportement social pour communiquer [121]. Le VSN prend en charge un large éventail d'application, il ne se limite pas à la gestion du trafic et à la sécurité routière, il permet également aux voyageurs de partager des données telles que des vidéos, des audios, des photos de route et d'autres informations provenant de différents capteurs intégrés.

Les principales solutions existantes reposent principalement sur une architecture entièrement centralisée. La mobilité des véhicules rend l'accès à l'infrastructure non garanti. L'architecture entièrement décentralisée souffre de différents inconvénients, tels que les responsables de niveau supérieur disposent de moins d'informations sur les opérations locales dans les entités VSN, tout est à la charge des ces dernières, ce qui conduit à un manque de contrôle. La qualité du service devient plus difficile à assurer.

Dans cette partie, nous proposons d'introduire le paradigme de la Blockchain. Il a été introduit la première fois par Satoshi dans "Système de paiement électronique peer-to-peer"[96]. Les données sont envoyées d'une manière transparente, en toute sécurité et sans un point de contrôle central. De plus, le système basé sur la Blockchain est une solution prometteuse en matière de protection de la vie privée qui sera basée sur l'anonymat et la sécurité des informations échangées sur le réseau. La Blockchain est composée de blocs, ça consiste en plusieurs transactions qui sont liées à un bloc dans une chaîne. Pour assurer la fiabilité des blocs ajoutés, un processus spécial de résolution d'un problème du calcul appelé preuve de travail "proof of work" est utilisé.
La génération de blocs est assurée par des noeuds dans des réseaux appelés "Mineurs".

La transaction consiste en un contenu partagé entre les entités VSN, telles que les embouteillages, les conditions météorologiques, l'info-divertissement, les places de stationnement vacantes, des itinéraires de remplacement, etc. De plus, afin d'introduire la Blockchain dans le réseau social véhiculaire, nous introduisons trois niveaux de contrôleurs :

— Contrôleur principal (PC).
— Roadside unit (RSU).
— Un contrôleur local "Mineurs".

Le PC a une vue globale de la topologie de VSN. Le RSU est un dispositif intermédiaire entre le PC et les mineurs. Les contrôleurs locaux agissent non seulement comme des mineurs en termes de sécurité, mais aussi en tant que relayeurs. Afin de sélectionner les mineurs, nous avons proposé l'algorithme "Distributed Miners Connected Dominating Set" (DM-CDS). La sélection des mineurs dépend d'un paramètre de confiance basé sur un modèle et des paramètres de réseau tels que le degré de connectivité "Deg", l'indicateur de qualité de liaison moyenne "LQI" et le rang "distance en termes de sauts à partir du RSU". Les principales contributions de ce chapitre sont décrites comme suit :

— Un framework en vue de software-defined vehicular network "SDVN" est proposé. Cela dépend de différents contrôleurs tels que le PC, le RSU et les mineurs.
— Le système de Blockchain est appliqué pour assurer la protection et la vérification des informations. Nous proposons un algorithme appelé DM-CDS utilisant plusieurs paramètres tels que : la métrique de confiance et des paramètres de réseau tels que le degré de connectivité, l'indicateur de qualité de liaison et le rang.
— L'analyse des performances est réalisée à l'aide de simulations avec des situations complètement différentes et plusieurs d'autres paramètres tels que la densité des noeuds, la portée radio et la métrique de confiance.

6.2 Un framework basé sur l'architecture de la Blockchain

Cette section décrit en détail l'architecture proposée. Il s'agit d'une approche hybride capable de prendre en charge un contrôle centralisé et semi-distribué. Le concept de base est de sélectionner des noeuds particuliers pour jouer un rôle de contrôleurs locaux [122, 123]. Dans cet objectif, nous avons différents types de contrôleurs, tels que le contrôleur principal, le roadside unit et les mineurs, présentés dans la Figure 6.1. Dans la Figure 6.2, nous avons illustré l'interaction entre les différents modules qui composent notre architecture. Ils sont divisés en modules principaux tels que le module de contrôle,

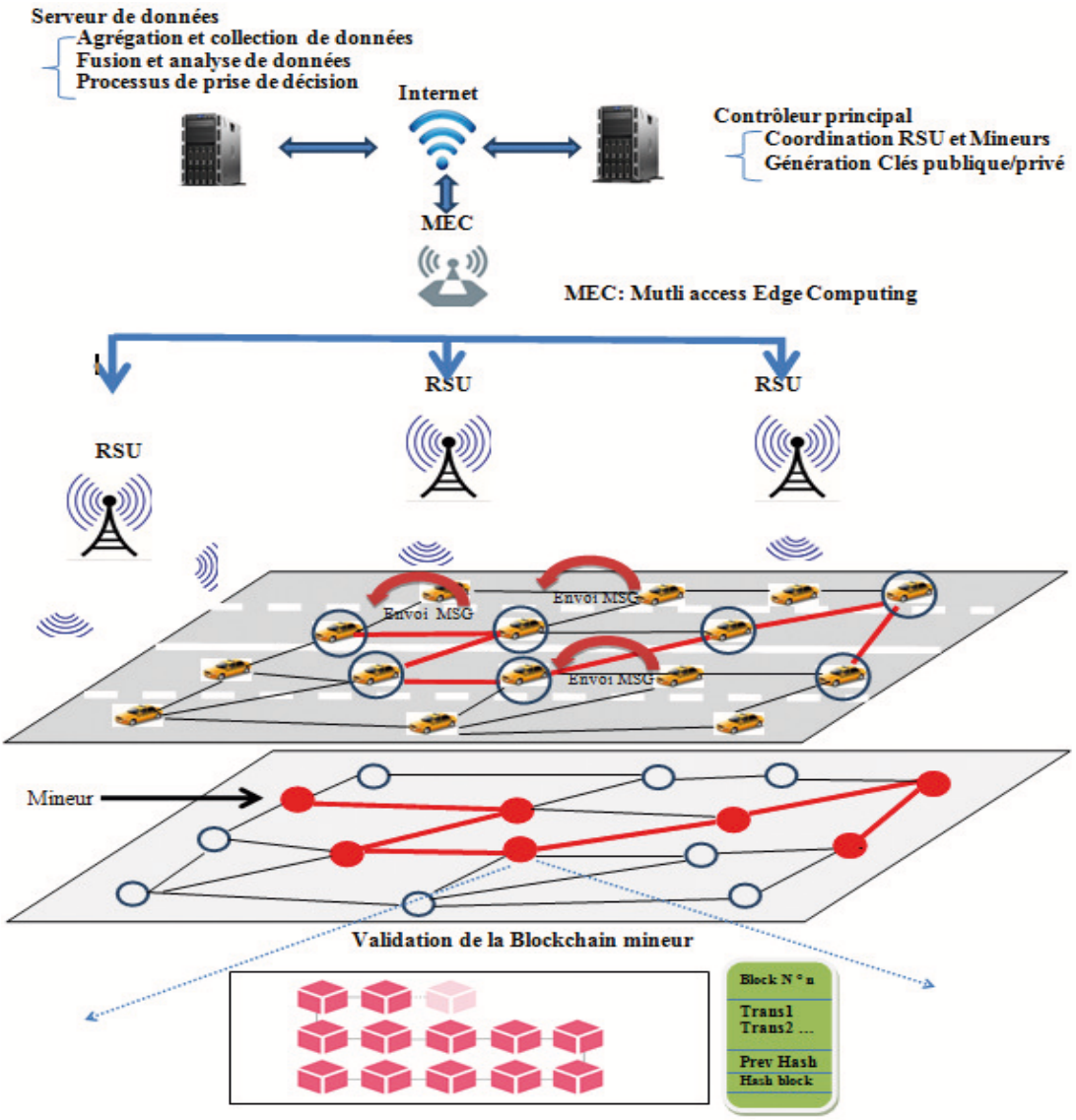

FIGURE 6.1 – Présentation de l'architecture

le module de données, le module de cloud computing, le module de confidentialité et le module d'utilisateur final.

6.2.1 Présentation de l'architecture

Dans cette sous-section, nous nous concentrons sur les différents contrôleurs et modules de l'architecture proposée.

6.2.1.1 Le module de contrôle

Nous classons le module de contrôle en trois types à savoir :

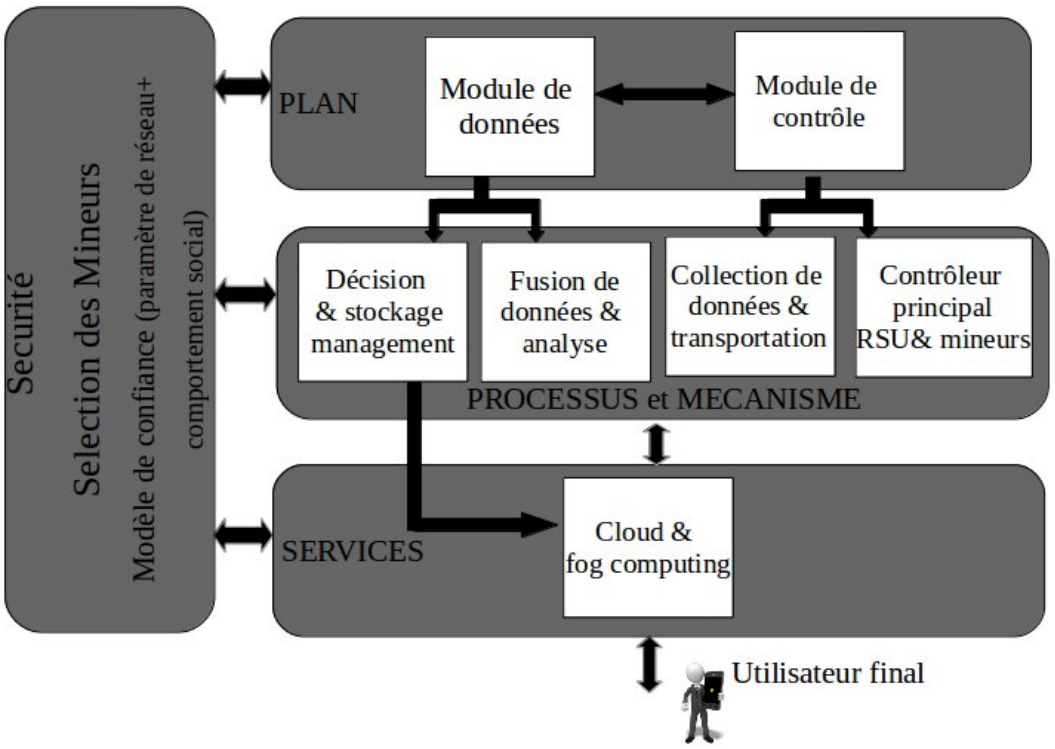

FIGURE 6.2 – Interaction entre différents modules de l'architecture

— Le contrôleur principal "PC".
— Le roadside unit "RSU".
— Les mineurs.

Le Contrôleur Principal : Le PC est un contrôleur centralisé situé au premier niveau de l'architecture (comme illustré dans la Figure 6.1). Le PC a une vue globale du réseau en matière de topologie. Les principaux rôles du PC sont illustrés comme suit : coordonne les RSUs et les mineurs, configuration du réseau, gestion des différentes ressources du réseau. Nous considérons que la distribution de clés est un problème important dans VSN, nous supposons donc que la distribution de clés se fait via le PC, comme illustré dans la Figure 6.1.

Le contrôleur RSU : Le RSU est un équipement situé sur la route qui est connecté à l'infrastructure et à internet. Les RSUs agissent en tant que noeud intermédiaire entre le PC et l'unité embarquée (OBU). Ils sont conçus pour gérer un groupe de véhicules au sein de leur plage de communication. Le RSU participe à la sélection des OBUs pertinents pour agir en tant que mineurs. Le processus de sélection est basé sur l'approche des ensembles dominés connectés (CDS) et en particulier sur un "Distributed Miner Connected Dominating set algorithm" (DM-CDS).

Le contrôleur mineur : Les mineurs sont des noeuds spécifiques du réseau d'accès, leurs rôles consistent à valider et à certifier les transactions en utilisant la Blockchain. La sélection des mineurs est basée sur plusieurs paramètres tels que : le degré de connectivité, l'indicateur de qualité du lien avec leur noeuds voisins, leur position dans la topologie du réseau et la métrique de confiance.

6.2.1.2 Le module de données

Le module de données est représenté par un serveur de données chargé de la gestion des données échangées entre les entités VSN. Le rôle principal du module de données est : la collection, l'analyse et la gestion des données.

La collection et l'analyse des données : La collection et l'analyse de données représentent les techniques d'une collection intelligente. Elles sont utilisées pour extraire des informations pertinentes de différentes entités VSN avec des contraintes de réseau qui doivent être prises en compte à savoir la bande passante, la latence et la tolérance aux pannes. e.

Le processus de décision : Le processus de décision est fondé sur différents aspects tels que la collection de données, l'analyse de données et l'utilisation d'outils intelligents pour prendre des décisions pertinentes. Parmi les divers outils et techniques pouvant être utilisés le R-learning et Q-learning [124]. Dans notre architecture présentée, le PC interagit avec les différents contrôleurs tels que les RSUs et les mineurs pour prendre des décisions et adapte la sélection des mineurs aux contraintes du réseau.

6.2.1.3 Le module Cloud et le Fog computing

Le cloud et le Fog computing peuvent fournir divers services aux noeuds de notre architecture proposée. Parmi ces services, nous citons software as a service “Saas” qui peut être utilisé par les navetteurs. Les entités VSN qui partagent la même route et ayant des intérêts similaires peuvent partager de la voix, données de trafic et les vidéos. Le multi access edge computing (MEC) désigne l'informatique au niveau du "edge computing". L'utilisation de la "MEC" est dans le but de réduire la congestion du réseau et d'améliorer les performances des applications, ainsi que la diffusion du contenu sur mesure à l'utilisateur final.

Le serveur MEC peut être installé à différents endroits à la périphérie du réseau : au niveau de la station de base macro (4G/LTE), à la technologie (3G/LTE) et au site du contrôleur de réseau radio " Radio Network Controller" RNC [125]. Le fog computing étend la périphérie du réseau, il couvre plus de surface que le edge computing. Il est utilisé

pour pré-traiter les données collectées au niveau de la couche "edge" et les envoyées au cloud computing. Le "fog" computing fonctionne avec l'edge computing pour exécuter une application tout en offrant des services de transmission intelligents avec des capacités informatiques de stockage et de communication.
Notre architecture proposée prend en compte divers aspects tels que l'évolutivité, la flexibilité, l'interopérabilité et la nature semi-distribuée de l'architecture, d'où le "MEC" où le fog computing est le choix le mieux adapté pour rendre les services plus sûrs et efficaces. Le "MEC" est considéré comme une technologie efficace pour le support VANET/Internet des véhicules [126, 127].

6.2.2 Module de la sécurité et de la confidentialité

Ce module est une partie importante de l'architecture qui est utilisée pour garantir la confidentialité des données échangées. L'architecture proposée prend en compte divers aspects de la sécurité tels que la traçabilité, l'intégrité, la confidentialité et l'accessibilité. Nous introduisons le paradigme de la Blockchain dans le cas de la gestion distribuée de la confiance[112]. Il peut suivre de manière dynamique le comportement des entités VSN (entités égoïstes et malveillantes).

Nous introduisons la mesure de confiance dans le but de suivre le comportement malveillant des entités VSN [128, 129]. Nous notons que les noeuds avec une métrique de confiance inférieure ($Tm \leq$ seuil)seront éliminés de la sélection des mineurs. La Figure 6.3 illustre la sélection des mineurs qui est basée sur les paramètres de comportement social et du réseau. Le comportement social est positivement corrélé avec la confiance. Il est basé sur la connectivité, la fitness et la satisfaction. Plus de détails seront donnés dans la section suivante. Les paramètres de réseau incluent l'indicateur de qualité de la liaison, le degré de connectivité et le rang. La Blockchain est une base de données contenant l'historique de tous les échanges effectués entre les entités VSN depuis sa création.

Avec la Blockchain, nous pouvons suivre le comportement des entités VSN. Si l'une d'entre elles se comporte mal (égoïste, fausses nouvelles, etc.), elle sera placée sur une liste noire et sa métrique de confiance sera égale à zéro (Tm = 0).

Nous avons deux types de Blockchains :
La Blockchain publique, elle est partagé avec toutes les entités VSN.
La Blockchain privée, dont l'accès et l'utilisation sont limités aux entités VSN qui sont en relations. Pour commencer le processus, une transaction est demandée, cette dernière est diffusée via peer-to-peer à l'autre VSN qui constitue le réseau de la Blockchain. Les

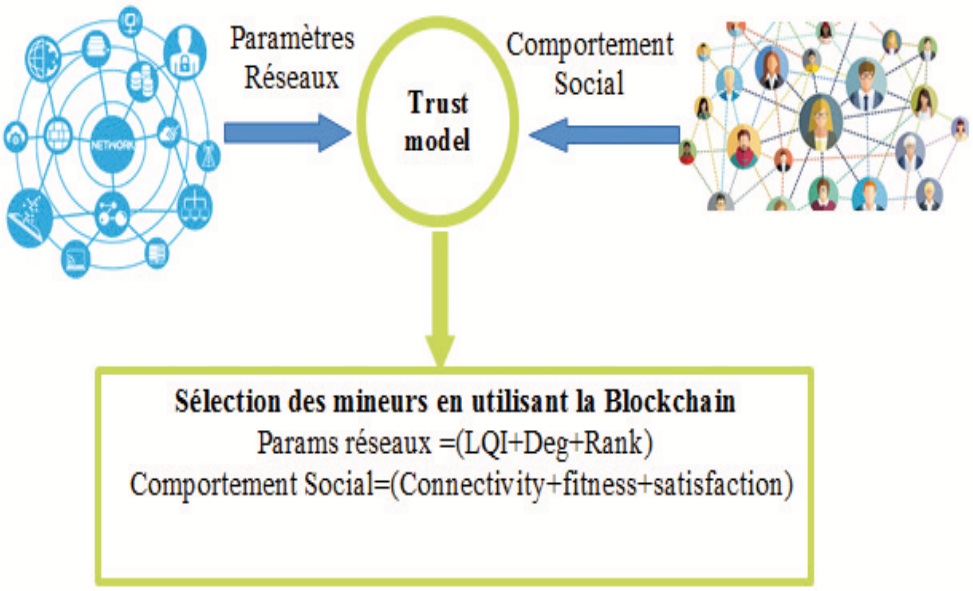

FIGURE 6.3 – Processus de selection des mineurs

transactions sont regroupées dans un bloc validé par les mineurs. Le bloc est attaché à la Blockchain.
La Blockchain privée est réservée aux entités VSN connectées comme les amis. Ils partagent des contenus sociaux tels que les vidéos, les audios, les photos, etc. La Blockchain publique est partagée par toutes les autres entités VSN, elle est utilisée dans les applications de divertissement et de sécurité.

6.2.3 Modèle de confiance

Dans cette sous-section, nous proposons un modèle de confiance dynamique pour les noeuds dans le réseau social [130]. Cette approche permet de détecter les noeuds qui se conduisent mal, y compris les noeuds malicieux, égoïstes et lançant des attaques par conspiration. Le framework de confiance est basé sur quatre parties :

1. La détection du comportement.
2. La délivrance de la confiance.
3. Le traitement de la confiance.
4. La décision de confiance.

La détection de comportement est utilisée pour détecter les problèmes de comportement d'entités VSN en matière de transmission de messages, la non-coopération et la remise de messages. Le modèle de confiance proposé par Wang et al [130] repose sur trois

paramètres tels que la connectivité, la fitness et la satisfaction. Pour calculer le degré de confiance, nous utilisons des entités VSN intermédiaires à "deux sauts" pour générer des messages d'accusés de réception pour les entités émettrices.

6.2.3.1 Valeur de la confiance directe

La plus mauvaise conduite qui peut se produire fréquemment dans le réseau des VSNs est l'égoïsme (selfishness), le complot (conspiracy) et le flooding. Le modèle de confiance classique se basant sur un modèle probabilistique ne permet pas de révéler efficacement le comportement erroné susmentionné. Nous utilisons un vecteur basé sur trois paramètres : **connectivité, fitness et satisfaction**.

La connectivité : c'est la puissance d'un noeud à être attaché à un autre noeud du réseau. La connectivité est aléatoire, la fréquence de connexion peut être comptée. La connectivité est décrite comme suit (6.1) :

$$C_{i,j}^{d,c} = \frac{2 * n_{fwd} + n_{meet}}{2 * n_{fwd} + n_{meet} + N} \tag{6.1}$$

$C_{i,j}^{d,c}$: décrit la connectivité entre le noeud i et le noeud j.

n_{fwd} : représente le nombre de fois que le noeud j est un noeud intermédiaire associé dans un chemin de transmission.

n_{meet} : représente la quantité de connexion entre le noeud i et le noeud j.

N : représente tous les noeuds qui composent le réseau.

La fitness : Ce paramètre est utilisé pour évaluer le comportement d'un noeud. Il détecte le "flooding" et le trou noir"blackhole" attaques. Chaque message à son itinéraire approprié, qui inclut les noeuds entre la source et la destination. La valeur de la fitness est fondée sur plusieurs valeurs de messages, telles que le nombre de messages envoyés par les noeuds sources, les messages reçus et les messages de refus et de transfert. La fitness est calculée comme suit (6.2) :

$$T_{i,j}^{d,h} = \frac{n_{fwd} + n_{rec} + 1}{n_{src} + n_{fwd} + n_{rec} + n_{deny} + 2} \tag{6.2}$$

$T_{i,j}^{d,h}$: représente la valeur de la fitness entre les noeuds i et j.

n_{fwd} : représente la quantité de messages transmis par le noeud j.

n_{rec} : représente la quantité de noeud j recevant des messages du noeud i.

n_{src} : représente la quantité de messages envoyés par le noeud j.

n_{deny} : représente la quantité de refus de messages.

La satisfaction : elle représente la manière dont un noeud est satisfait de la distribution effectuée par les noeuds intermédiaires. La satisfaction est calculée à l'aide de deux types de messages : les messages d'accusés de réception et les messages de transfert. Lorsque les entités VSN reçoivent les messages ACK, elles enregistrent le nombre de noeuds intermédiaires qui transmettent les messages. Sinon, si après un certain temps, le message ACK n'est pas reçu, le transfert est considéré comme un échec et le compte ne sera pas incrémenté.

Nous prenons un exemple entre deux entités A et B pour calculer la satisfaction. L'entité A envoie un message à B, B envoie un message à C, ce dernier envoie un message ACK à A lors de l'obtention d'un message. Ensuite, A approuve le bon comportement du noeud B. Lorsque le message sera transmis à la destination D. Le noeud D envoie le message ACK final à l'entité A. À cette fin, le noeud A approuve le bon comportement de tous les noeuds de la voie de transmission.

$$T_{i,j}^{d,s} = \begin{cases} \frac{n_{ack}}{n_{rec}+1} & if path(j) = 0 \\ \frac{n_{Fackj}+n_{ack}}{n_{Fackj}+n_{rec}+1} & if path(j) > 0 \end{cases} \tag{6.3}$$

$T_{i,j}^{d,s}$: représente la satisfaction directe entre les noeuds i et j.
n_{ack} : représente le nombre de messages d'accusés de réception recueillis.
n_{rec} : représente le nombre de fois où le noeud j reçoit des messages.
n_{Fackj} : représente la quantité d'apparence du noeud j dans les messages d'accusés de réception final.
$path(j)$: représente l'apparence du noeud j dans la voie d'acheminement des messages. Lorsque l'entité source reçoit les messages d'accusés de réception du noeud cible, ceci confirme le bon comportement des noeuds dans le chemin de transfert.

6.2.3.2 La livraison du modèle de confiance

La livraison de la métrique de confiance permet aux noeuds de connaître le comportement des autres. Le noeud recueille les recommandations d'autres noeuds qui sont utilisés pour calculer un vecteur de confiance, dans le but d'avoir plus précisément sur la valeur de la confiance. Nous avons deux catégories de recommandations :

1. Les noeuds avec un degré de confiance supérieur à un seuil particulier.

2. Les autres noeuds ont une similitude de confiance avec le noeud actuel.

Le choix de la plus grande valeur de confiance est plus approprié. La seconde catégorie, si les noeuds ont une similarité dans leur liste noire sur les noeuds d'une mauvaise réputation, leurs recommandations de confiance peut être acceptée. Exemple : si un noeud A veut prendre une décision concernant la recommandation, deux conditions doivent être vérifiées.

1. Le degré de confiance doit être supérieur ou égal à un certain seuil.
2. La similarité sur leurs listes noires.

Pour évaluer la ressemblance entre la liste noire du noeud i et j, nous avoir la formule (6.4) :

$$Sim(i,j) = \frac{|B_i \cap B_j|}{|B_i \cup B_j|} \tag{6.4}$$

B_i and B_j : représente le groupe de la liste noire des noeuds i et j.
$|B_i \cap B_j|$: représente la jonction du groupe de listes noires des noeuds i et j.
$|B_i \cup B_j|$: représente l'union du groupe de la liste noire des noeuds i et j.

la valeur de la confiance indirecte est donnée par :

$$T_{i,m}^{ind,X}(t) = \begin{cases} \frac{\sum_{k \in R_i}(T_{i,j}^{d} x T_{j,m}^{d,X})}{\sum_{j \in R_i} T_{i,j}^{X}(t)} & if T_{i,j}^{X}(t) > \tau \\ \frac{\sum_{j \in R_i}(Sim(i,j) x T_{j,m}^{d,X}(t))}{\sum_{j \in R_i} Sim(i,j)} & if T_{i,j}^{X}(t) <= \tau, Sim(i,j) > \nu \end{cases} \tag{6.5}$$

X : décrit les attributs de la confiance correspondante.
$T_{i,j}^{d}(t)$: représente le degré de confiance entre le noeud i et j au moment t.
$Sim(i,j)$: représente la similitude de listes noires du noeud i et j.
τ et ν représentent respectivement le seuil de confiance et le seuil de similarité.

6.2.3.3 Mise à jour de la confiance

Nous avons deux situations de mises à jour de confiance. La confiance directe et indirecte. Dans le cas de la confiance directe, lorsque le noeud i a une interaction avec le noeud j pendant la période $|t, t + \Delta t|$. Le second cas est présenté lorsque le noeud i

n'a pas d'interaction avec le noeud j dans $|t, t + \Delta t|$. La mise à jour de la connectivité, de la fitness et de la satisfaction sont données par (6.6) :

$$T_{i,j}^{d,X}(t + \Delta t) = \begin{cases} \exp^{-\lambda \delta t} * T_{i,j}^{d,X}(t). \\ \alpha * \exp^{-\lambda \delta t} * T_{i,j}^{d,X}(t) + (1 - \alpha) * T_{i,j}^{d,X}(t + \delta t). \end{cases} \tag{6.6}$$

En ce qui concerne la confiance indirecte, il existe deux situations. Le cas où la recommandation n'est pas envoyée par le noeud j pendant la période $|t, t + \Delta t|$. Le second cas, il n'y a aucune recommandation indirecte à recevoir. Le calcul est donné par (6.7) :

$$T_{i,j}^{ind,X}(t + \Delta t) = \begin{cases} \exp^{-\lambda \delta t} * T_{i,j}^{ind,X}(t). \\ \beta * \exp^{-\lambda \delta t} * T_{i,j}^{ind,X}(t) + (1 - \beta) * T_{i,j}^{ind,X}(t + \delta t). \end{cases} \tag{6.7}$$

La confiance globale est obtenue avec la confiance directe et indirecte. Pour chaque attribut X, la confiance du noeud i au noeud j est donnée par (6.8) :

$$T_{i,j}^{d,X}(t + \Delta t) = \gamma T_{i,j}^{d,X}(t + \Delta t) + (1 - \gamma) T_{i,j}^{ind,X}(t + \Delta t) \tag{6.8}$$

γ peut prendre plusieurs valeurs en fonction de l'état du réseau. Lorsque le réseau fonctionne, il aura tendance à être en confiance indirecte. Pour que le noeud i fait confiance au noeud j, la capacité de transmission est donnée sous la forme (6.9) :

$$T_{i,j}(t + \Delta t) = \sum_{X}^{all} \omega^X T_{i,j}^X(t + \Delta t) \tag{6.9}$$

ω^X représente le ratio de l'attribut X dans tous les attributs. X est associé à la fitness, la connectivité et à la satisfaction.

6.2.3.4 La décision de confiance

La décision de confiance est divisée en quatre catégories :

La décision de recevoir des messages : La décision est basée sur la valeur de la fitness. Si le taux de la fitness est inférieur à un certain seuil pour la demande d'un noeud, le noeud qui reçoit la demande refusera le transfert du message, comme illustré dans la Figure 6.4. Les noeuds ayant moins de valeur de fitness peuvent avoir un mauvais comportement comme les spams, flooding, un déni de service ou de refuser la transmission des messages. Refuser la demande de transfert de message pour un noeud peut motiver ce dernier à bien se comporter

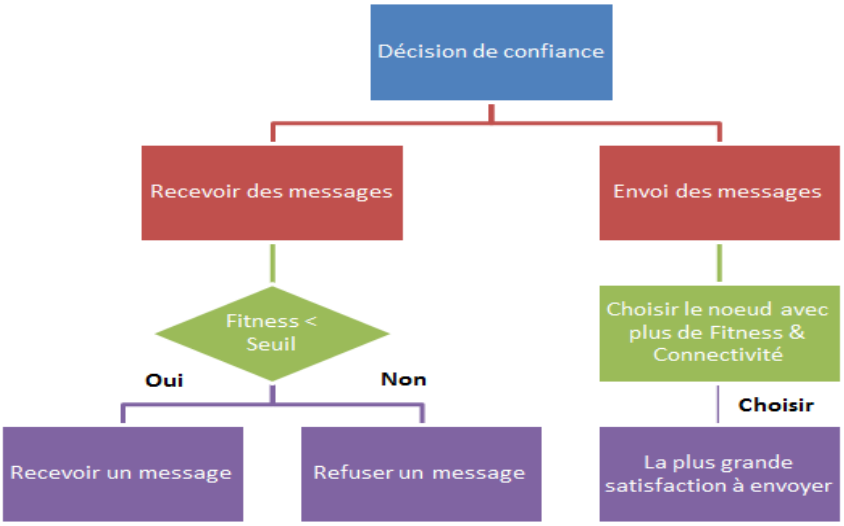

FIGURE 6.4 – L'organigramme de la décision de confiance

La décision d'envoi du message : Pour envoyer des messages, les entités choisissent des entités avec une connectivité et une fitness optimales. La satisfaction est utilisée pour décider le degré du service. Le taux de transmission réussie est en corrélation positive avec la satisfaction. Les noeuds pour transférer les messages, ils choisissent ces entités avec une plus grande satisfaction et prennent en compte leurs connectivités.

La décision d'acceptation de la recommandation de confiance : La recommandation basée sur la confiance dépend du seuil de confiance et de la similarité de la liste noire. Avec ces deux paramètres pertinents, nous pouvons assurer la fiabilité et l'efficacité des recommandations.

La décision de la liste noire : Pour prendre la décision de mettre un noeud en liste noire, la fitness ou la satisfaction doit être inférieure à un certain seuil. Ainsi, ces noeuds seraient placés sur une liste noire et leurs informations seront diffusées aux voisins.

6.3 La sélection des mineurs basée sur l'algorithme CDS

Cette section décrit le processus de sélection des noeuds mineurs "Miners", ces derniers ont une fonction importante dans le réseau en matière de validation des transactions échangées entre les entités VSN. Basé sur l'approche DSP "Distributed Single Phase", qui produit de meilleures performances en matière de nombre de mineurs connectés. Dans les travaux qui existent, nous distinguons deux principales approches de CDS à savoir : l'approche centralisée et distribuée qui se base sur des algorithmes de plusieurs ou une seule phases.
Dans l'approche centralisée, la topologie du réseau doit être connue au départ ce qui n'est pas le cas dans certains types de réseaux ad hoc. Cependant, dans le cas d'une approche décentralisée, les informations du réseau local sont essentielles, la décision pour devenir un noeud dominant est prise d'une manière distribuée [131]. Pour plus de détails sur la classification et la performance des algorithmes CDS, une comparaison des travaux sur la construction des CDS est fournie par Yin et al .[132].

À cette fin, nous présentons notre algorithme CDS qui est utilisé pour sélectionner un sous-ensemble de noeuds agissant en tant que noeuds mineurs.
L'algorithme commence par attribuer un drapeau blanc à chaque noeud. Après avoir exécuté les phases distinctes de "Distributed Single Phase Connecting Dominating Set algorithm" (DSP-CDS), certaines entités VSN changent leur drapeaux en noir. Seules les entités avec un drapeau noir seront sélectionnées comme des mineurs.

Nous présentons une solution appelée "Distributed Miners Connected Dominating set algorithm" DM-CDS. Elle repose sur divers paramètres, notamment le degré de connectivité, l'indicateur de qualité de lien, la métrique de confiance et le rang. Dans l'algorithme proposé, chaque entité VSN possède des propriétés telles que : ID unique (**NodID**), sous-ensemble des entités VSN connectées, lors de la première exécution, VSN possède un ID distinct (**SetID**). Il existe trois **flags** (drapeau) utilisés pour spécifier le statut des entités VSN :

- **white** noeud non dominant.
- **grey** phase intermédiaire.
- **noir** noeud prédominant.

Nous discernons deux phases principales :
(1)**la phase de démarrage :** cette phase est impliquée dans l'identification et l'initialisation du statut de chaque noeud. Elle lance la fonction "miner_score", dans le but de

donner une importance distincte à chaque VSN selon des critères différents.
(2)**La phase de traitement :** cette phase est impliquée dans la prise de décision pour les entités VSN de changer leurs drapeaux en blanc ou en noir. Comme nous le voyons dans l'organigramme présenté dans la Figure 6.5. Nous présentons le processus de notre algorithme DM-CDS, ce processus représente une approche de sélection des mineurs basé sur le module de contrôle.

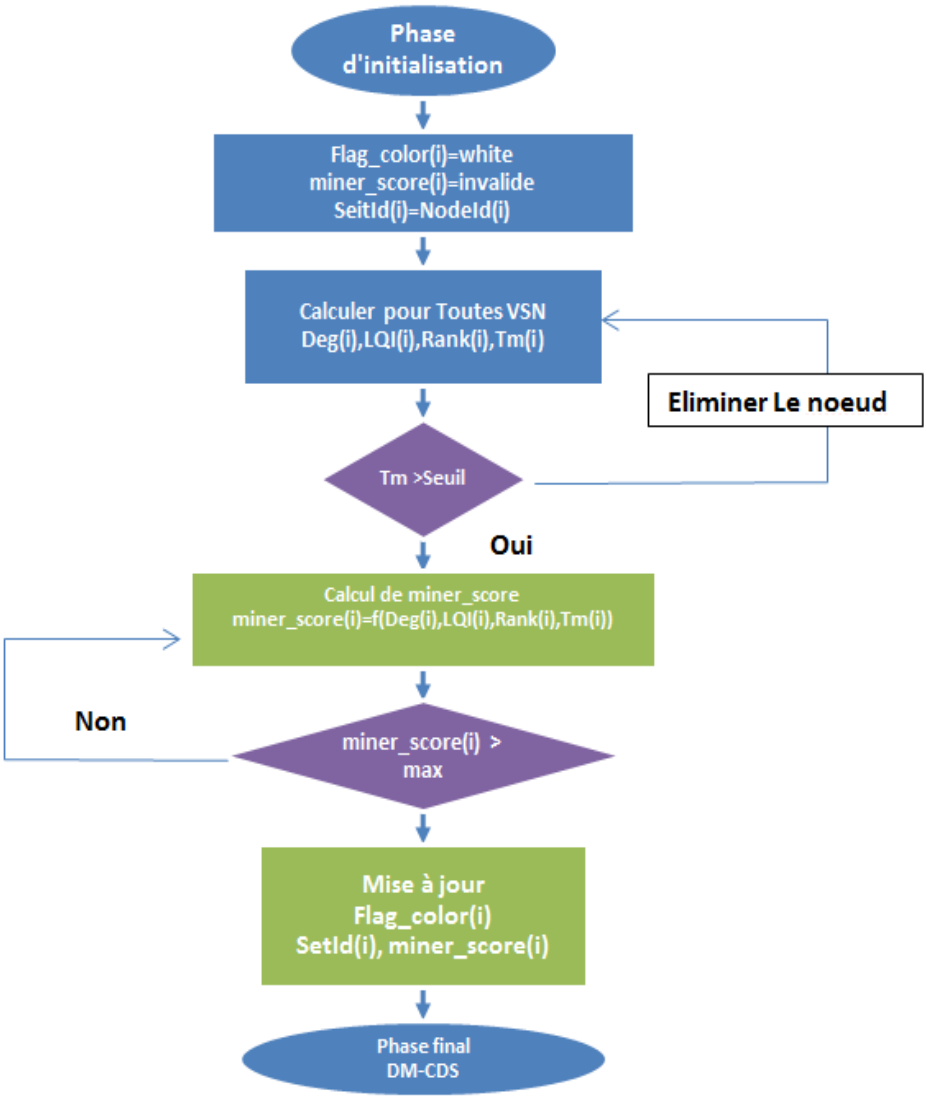

FIGURE 6.5 – L'organigramme du processus de sélection des mineurs

Phase de démarrage : Dans cette phase appelée processus de démarrage, toutes les entités VSN ont la même couleur d'indicateur comme blanc et leur "mineur_score" n'est pas disponible (invalide) pour la première fois. De plus, la valeur du numéro de

sous-ensemble est identique à celle du numéro d'entité du VSN, l'identité de SetId est la même que NodID. Toutes les entités VSN ont un score initial pour la métrique de confiance "Tm"[133]. Chaque noeud VSN a le statut suivant :

- **NodId**.
- flag_color=white.
- SetId=**NodId**.
- miner_score est invalide.

La phase d'évaluation des paramètres réseau : A cette étape, chaque entité VSN calcule les paramètres regroupés par :

Paramètres de réseau :

- **Le degré de connectivité** : décrit le nombre de voisins directement connectés.
- **L'indicateur de qualité de lien** : décrit le lien moyen avec les entités.
- **Le rang** : indique le nombre de sauts à partir de RSU roadside units.

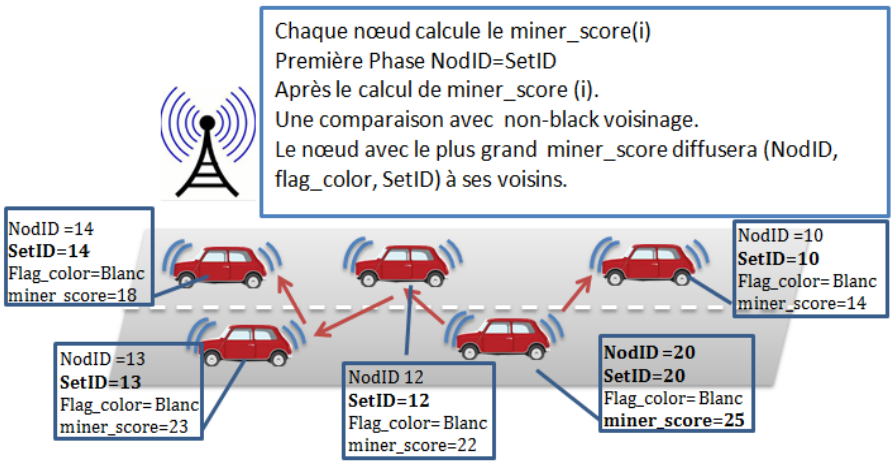

FIGURE 6.6 – Processus de sélection des mineurs la phase de compétition

Paramètre de confiance :

- **La métrique de confiance** : décrit le degré de confiance et l'intégrité des entités VSN.

En utilisant ces paramètres, le "mineur_ score" est calculé.

Compétition et phase de décision : Chaque entité VSN calcule son propre "mineur_score" par rapport aux paramètres vus dans la phase précédente. Afin de sélectionner les mineurs et de tirer des conclusions. Nous avons deux algorithmes : "Algorithm_sender", qui est exécuté au niveau de l'entité VSN de l'expéditeur. "Algorithm_receiver" qui exécuté au niveau de l'entité VSN du destinataire.

Algorithm 1 Phase de compétition au niveau de VSN émetteur

Input NodID, Score, SetID, list_voisins(i),i.
Output Décision pour changer "flag_color".
N représente toutes les entités VSN.
for $(VSN\_node(i) \in N)$ **do**
    miner_score(i)=compute_score()
    if $((miner\_score(i) \neq 0)$ and $(i.flag\_color \neq Noir))$ **then**
        for $(K \in Non\_noir\_voisin)$ **do**
            S=grand_score(K)
            if (miner_score(i) > S) **then**
                i.flag_color=Noir
                i.SetID=i.NodID
                diffusé (i.NodID, flag_color, i.SetID, miner_score(i))
            end if
        end for
    end if
end for

En ce qui concerne l'entité VSN expéditrice, elle calcule son "miner_score" et fait une comparaison avec le voisinage "non_black". Après cela, une décision sera prise concernant son "flag_color". Lorsque la couleur des drapeaux devient noir, les paramètres suivants seront diffusés :"NodID", "flag_color", "SetID" et "miner_score" pour tous les voisins du VSN, comme illustrés dans la Figure 6.6 et la Figure 6.7.
En ce qui concerne le récepteur VSN noir ou gris, s'il reçoit un paquet de l'entité VSN noir avec une grande valeur de SetID, le noeud récepteur modifie alors son SetID pour

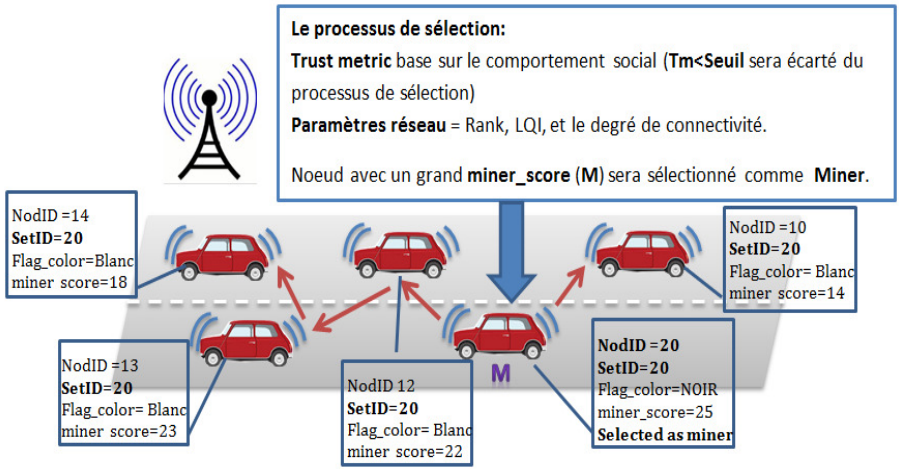

FIGURE 6.7 – Processus de sélection des mineurs la phase de décision

devenir également dans le même sous-ensemble. Néanmoins, dans le cas du récepteur VSN avec un drapeau blanc, il mettra à jour son SetID, comme on peut le voir dans "Algorithm_receiver" et changera son "flag_color" en gris.

6.4 Analyse des performances

Cette section est consacrée à l'évaluation et à la communication des performances de notre algorithme "DM-CDS". Nous considérons différentes mesures de performance avec différents scénarios. Nous implémentons l'algorithme "DM-CDS" et nous débattons les résultats obtenus. La simulation est nécessaire pour fournir une méthode d'analyse importante et une solution valable. Cela permet l'expérimentation sur une représentation valide de nos algorithmes proposés. C'est une simulation avec un aspect réseau, qui permet de contrôler la sélection des mineurs, en tenant compte des contraintes temporelles telles que la distance par rapport à la RSU, l'indicateur de qualité des liens et le modèle de confiance. Chaque noeud exécute la phase d'évaluation des paramètres de réseau, après cela, il exécute la phase de compétition et de décision dans le but de prendre la décision de devenir un noeud mineur ou non.

6.4.1 La configuration de la simulation

Au cours de la simulation, tous les noeuds sont déployés d'une manière aléatoire dans une longueur carrée L variée de 40 km à 120 km. La plage est variée entre 10 et 20. Le nombre de noeuds (N) est donné par $N = L * L * \rho$, tel que ρ représente la densité de noeuds. Par exemple, si nous prenons un réseau $40 * 100$ avec une densité $\rho = 0.01$,

Algorithm 2 Phase de compétition au niveau de VSN récepteur

Input NodID, SetID, flag_color,miner_score.
Output Un ensemble de noeuds Mineurs.
for (entité VSN k reçoit un packet de l'entité Noir i) **do**
  if $((k.flag\_color = Noir) OR (k.flag\_color = Gris))$ AND $(i.miner\_score > k.miner\_score)$ **then**
    k.SetID=i.SetID
    if (k.flag_color=Blanc) **then**
      k.SetID=i.SetID
      k.flag_color=Gris
    end if
  end if
end for

$N = 40 * 100 * 0.01 = 40$ noeuds. Les détails des scénarios et les paramètres de simulation sont présentés dans le tableau 6.1, qui utilisent la configuration réseau de "DSP-CDS" [132]. Nous nous concentrons sur quatre scénarios, comme le montre le tableau 6.1. La métrique d'évaluation est le nombre de mineurs. Nous avons utilisé différents paramètres pour évaluer le nombre de mineurs, tels que le nombre de noeuds, la longueur du réseau et les paramètres les plus importants sont la densité des noeuds ρ, la portée radio, la mobilité des noeuds et la métrique de confiance.

La densité des noeuds : La densité des noeuds est le paramètre le plus important influant sur la connectivité du réseau, qui définit le nombre de voisins qu'un noeud peut il avoir . La densité des noeuds et la taille du réseau jouent un rôle important dans la détermination du nombre de noeuds mineurs. Chaque noeud du réseau peut devenir un mineur. Le noeud avec le plus grand "miner_ score" a une chance de devenir un noeud mineur. Il couvre plus de voisins et partage le même $SetId$.

La mobilité des noeuds : il s'agit d'un paramètre important basé sur la stabilité de la liaison qui influence la connectivité du réseau. Un petit groupe de noeuds se retirent et rejoignent le réseau de manière arbitraire lors de la sélection des mineurs en se basant sur l'algorithme DM-CDS.

la portée radio "Radio range" : La portée radio est le troisième paramètre majeur. Le nombre de noeuds voisins augmente relativement avec la portée radio. Cela peut augmenter leur degré de connectivité. Dans la simulation, nous faisons varier la plage radio entre 10 et 20 pour évaluer l'exécution de notre algorithme "DM-CDS".
La densité relative des noeuds est donnée par "$\pi * R^2 * \rho$". Par exemple, lorsque la portée radio est donnée à $R = 20$, la densité de noeud $\rho = 0.02$. la densité relative est égale à 25.12. Les deux paramètres tels que la densité de noeud et la portée radio ont un impact significatif sur le nombre de noeuds mineurs.

La métrique de confiance : La métrique de confiance est le paramètre le plus important, qui influence le nombre de noeuds mineurs. Il mesure la confiance des entités VSN. Dans le cas ou $Tm \leq$ seuil, le noeud est exclu du processus de sélection des noeud mineurs. Les simulations effectuées montrent l'effet des divers paramètres sur la sélection des mineurs, tels que la densité des noeuds ρ, la métrique de confiance, la mobilité des noeuds et la portée radio R.

Les scénarios de simulation décrits ci-dessus se déroulent en plusieurs itérations. Ainsi, à chaque tour, le noeud prend la décision de changer son "$flag\_color$" pour qu'il corresponde au "mineur_score" de ses voisins.

TABLE 6.1 – Paramètres de simulation de l'algorithme DM-CDS.

Scénario de réseau	Nombre de nœuds (N)	Densité du nœud	Longueur réseau	Portée radio	mobilité
S1	64 à 567	0.03	40 à 120	10	N.A
S2	64 à 567	0.04	40 à 120	10 à 20	Retrait
S3	64 à 567	0.05	40 à 120	10 à 20	Joindre
S4	64 à 567	0.06	40 à 120	10 à 20	Mouvement

6.4.2 Analyse des résultats de la simulation

Dans cette section, à l'aide de diverses simulations, nous mesurons les performances du framework proposé. La Figure 6.8 et la Figure 6.9 représentent respectivement l'impact de la densité des nœuds ρ et de la portée radio pour déterminer le nombre de mineurs. Dans la Figure 6.10 et la Figure 6.11 montrent l'impact de la mobilité basée sur la "stabilité des liens" sur le nombre des mineurs. Enfin, la Figure 6.12 décrit l'impact de la métrique de confiance pour déterminer le nombre de mineurs.

L'impact de la densité de nœuds : La Figure 6.8 montre l'impact de la densité des nœuds et la longueur du réseau sur le processus de sélection des nœuds mineurs. Comme indiqué ci-dessus, la stratégie de sélection est basée sur le rang, l'indice de qualité du lien (LQI) et le degré de connectivité (deg). Les nœuds dont LQI est faible ne sont pas pris en compte dans le processus de sélection.

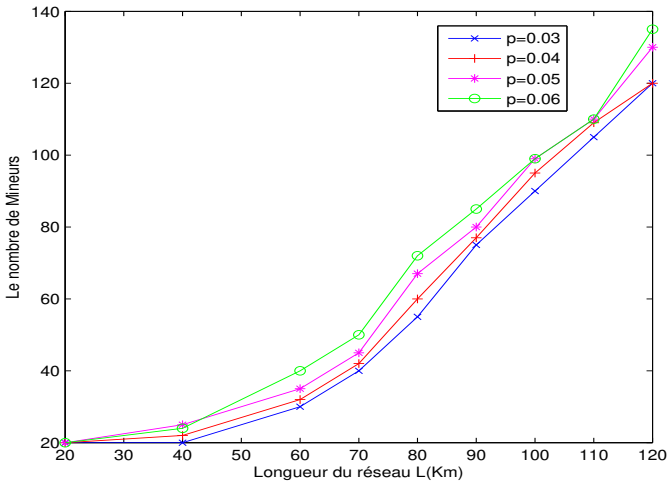

FIGURE 6.8 – Le nombre de nœuds mineurs en fonction de la densité de nœuds.

Dans la Figure 6.8, nous remarquons que la densité des nœuds et la longueur du réseau ont un impact sur le nombre de mineurs sélectionnés. Lorsque la densité des nœuds augmente, cela signifie que le nombre de nœuds voisins augmente et le nombre de mineurs sélectionnés augmente également. Nous remarquons le même impact lorsque la longueur du réseau augmente. Le nombre des nœuds mineurs augmente est principalement dû au nombre important de nœuds qui participent dans la phase de sélection.

L'impact de la portée radio "radio rang" :

La Figure 6.9 illustre le nombre de mineurs sélectionnés en fonction de la portée radio avec plusieurs densités de nœuds. Nous remarquons que la portée radio a un impact important sur le processus de sélection des nœuds mineurs. Lorsque la portée radio augmente, le paramètre de degré de connectivité (Deg) sera plus élevé, en raison de la densité des nœuds voisins, ainsi le nombre de mineurs sélectionnés augmentera également. En outre, lorsque la densité de nœuds augmente le nombre de nœuds mineurs augmente également jusqu'à une certaine limite en raison du paramètre LQI. Dans l'algorithme "DM-CDS", lorsque l'indice de qualité de liaison moyenne (LQI) du nœud candidat est faible, ce nœud sera exclu de la phase de sélection.

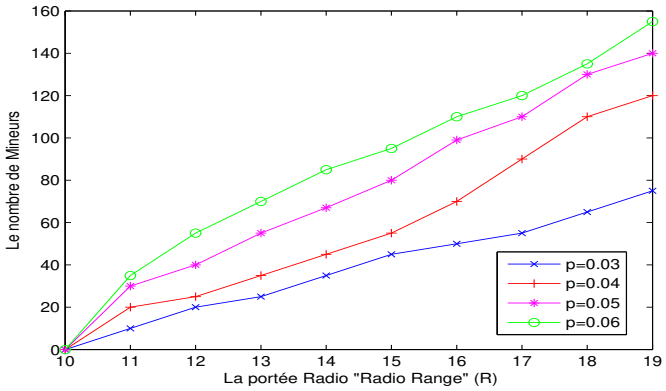

FIGURE 6.9 – Le nombre de nœuds mineurs en fonction de la portée radio.

L'impact de la mobilité des noeuds : L'impact de la mobilité est simulé en fonction de la stabilité de la liaison qui est représentée par deux paramètres principaux : le retrait et la jonction. La Figure6.10 montre le nombre de nœuds mineurs connectés en fonction de la longueur du réseau et de la stabilité de la liaison en matière de pourcentage de retrait des noeuds. Nous remarquons que lorsqu'un pourcentage de nœud se retire au hasard du réseau entre 0% à 10%. Le nombre de mineurs sélectionnés est stable "la variation est faible".

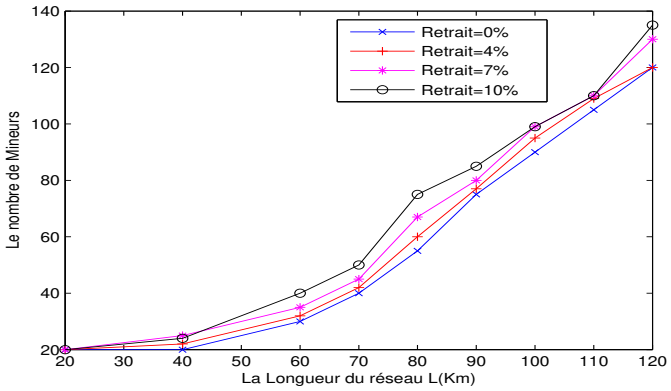

FIGURE 6.10 – Le nombre de mineurs en fonction de noeuds qui se retire du réseau.

La Figure 6.11 illustre l'impact de l'adhésion de nœuds "création de liens" sur le nombre de mineurs sélectionnés. Nous remarquons que l'impact est limité sur le nombre de mineurs sélectionnés lorsque le nombre de nœuds qui se joignent est inférieur à "10%". Depuis les figures6.10 et 6.11, nous concluons que dans le cas un mouvement des noeuds est faible, l'impact sur le nombre de mineurs connectés est limité. Cela prouve que l'algorithme "DM-CDS" soutient la faible mobilité des nœuds.

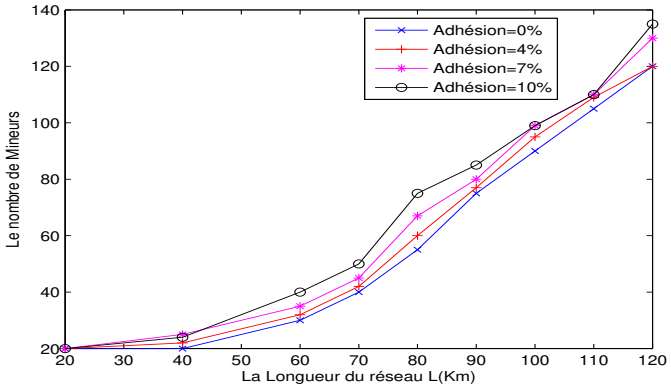

FIGURE 6.11 – Le nombre de mineurs en fonction de l'adhésion des noeuds au réseau.

L'impact de la métrique de confiance : la Figure 6.12 montre l'impact de la variation de la métrique de confiance "Tm" sur le nombre de mineurs connectés. Nous remarquons que la métrique de confiance a un impact important sur la sélection des nœuds mineurs.

Lorsque la métrique de confiance augmente, cela signifie que les nœuds ont un niveau de confiance plus élevé et plus fiables, ainsi que le nombre de mineurs augmente

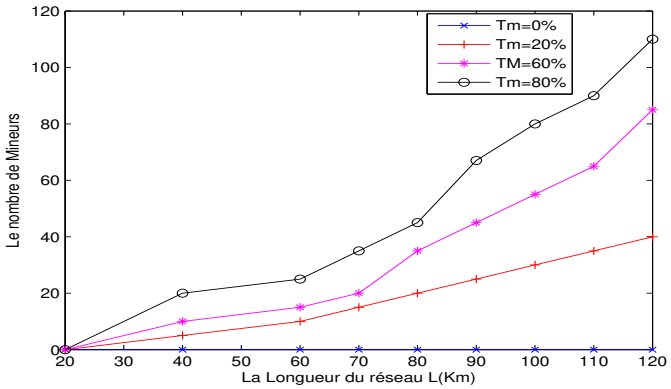

FIGURE 6.12 – Le nombre de mineurs selon la métrique de confiance.

également. Dans le cas de nœuds avec une métrique de confiance faible "Tm < seuil", le nombre de mineurs est égal à zéro.

Nous remarquons pour la performance du "DM-CDS", il y a une différence de "40%" des mineurs générés dans le réseau avec la variation de la métrique de confiance entre "20% et 60%", en raison de l'impact de la Tm sur l'algorithme "DM-CDS".

Nous avons modifié les paramètres de simulation, tels que la densité des nœuds, la métrique de confiance, comme indiqué dans le tableau 6.2.

TABLE 6.2 – La variation de la métrique de confiance

Scénario de réseau	La densité des nœuds	High TM	Faible TM	Moyenne TM
S1	0.3->0.4	20%	80%	0%
S2	0.3->0.4	80%	20%	0%
S3	0.3->0.4	30%	40%	30%

Comme nous le voyons dans la Figure 6.12, nous notons que la métrique de confiance n'a pas d'influence négative sur la construction des nœuds mineurs. Dans le cas d'un réseau de faible densité 0,3< ρ<0,4 et une longueur du réseau <80, la connectivité des nœuds peut avoir une incidence négative sur la construction des nœuds mineurs. Ceci s'explique par le fait qu'un nœud n'a pas de voisin et il a une faible chance d'être sélectionné en tant que nœud mineur. Nous allons comparer notre DM-CDS proposé à l'algorithme DSP-CDS [132], en termes de processus de sélection des nœuds mineurs.

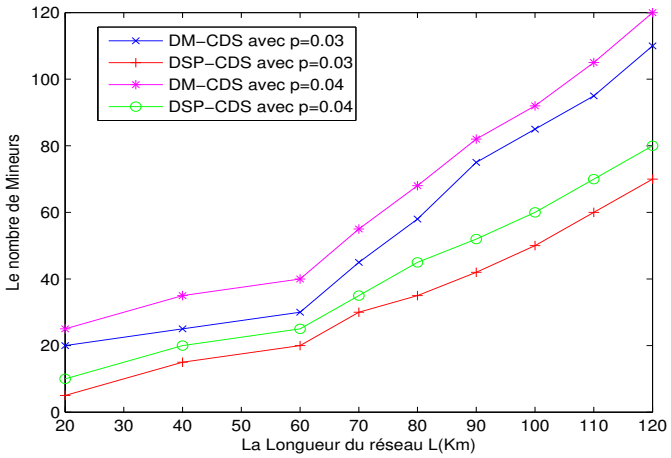

FIGURE 6.13 – Comparison entre DM-CDS et DSP-CDS algorithmes.

La stratégie de sélection de l'algorithme "DSP-CDS" est fondée sur un paramètre, à savoir le degré de connectivité. Dans ce cas, le "DSP-CDS" donne à chaque nœud la possibilité de devenir un nœud mineur. En ce qui concerne l'algorithme "DM-CDS", des contraintes supplémentaires sont ajoutées : Rank, Deg, LQI et TM. Les nœuds avec un indicateur de qualité de liaison médiocre sont ignorés. Par conséquent, le LQI a un effet sur le processus de sélection des nœuds mineurs. La Figure 6.13 illustre la comparaison entre les algorithmes "DM-CDS" et "DSP-CDS". Cela montre que notre algorithme proposé, "DM-CDS", surpasse le DSP-CDS avec une variance de "40%" en matière de nœuds mineurs. Cet écart entre les deux algorithmes est dû au processus de sélection adopté par chaque algorithme. Les résultats montrent que notre algorithme proposé DM-CDS par rapport à DSP-CDS converge rapidement avec un minimum de nœuds mineurs.

6.5 Analyse de sécurité

Cette section est dédiée à l'analyse de la sécurité de notre framework. Nous discutons et présentons une analyse de la sécurité de l'architecture proposée :

6.5.1 Résistance aux attaques

Nous présentons la résistance aux attaques basée sur deux types de problèmes de sécurité, à savoir un modèle de confiance distribuée et les attaques dans un réseau social véhiculaire. En ce qui concerne les attaques dans un réseau social véhiculaire, elles

peuvent être classées en trois classes, comme illustré dans la Figure 6.14 à savoir : attaque d'identité, attaque par espionnage et attaque par service.

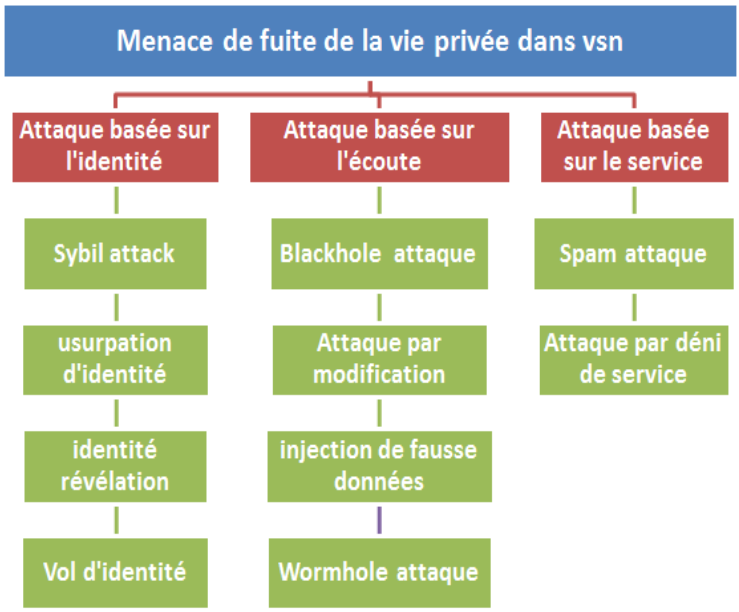

FIGURE 6.14 – Classification des attaques dans un réseau social véhiculaire.

6.5.1.1 La métrique de confiance distribuée

Le modèle de réputation est proposé pour créer un lien crédible et honnête entre les nœuds sélectionnés agissant en tant que mineurs. Nous appliquons le modèle proposé par Haddadou et al [133], dans lequel les entités VSN sont en possession d'un dispositif matériel proposé par le groupe TPM [134, 135], qui est utilisé dans les travaux de Guette et al[136, 137] et Wang et al [138].

Notre solution proposée est semi-distribuée. Les entités VSN communiquent entre elles sans passer par les RSUs. Notre architecture proposée est basée sur la Blockchain, elle est utilisée pour renforcer l'intégrité des informations échangées entre les entités VSN et nous permet de protéger les données personnelles [139] :

1. La Blockchain est utilisée pour garantir l'anonymat des informations échangées en remplaçant l'adresse de l'expéditeur et du destinataire par un hachage.
2. L'utilisation de la clé privée pour signer les données avant les échanges nous permet de garantir leurs intégrités.

3. Tous les nœuds malicieux et mal intentionnés sont recherchés et mis sur une liste noire.
4. La transparence : tous les échanges réseau effectués par les entités VSN sont enregistrés dans la Blockchain.
5. En utilisant la Blockchain, la menace de fraude est atténuée et une fois la transaction validée et ajoutée au bloc, nous ne pouvons plus l'annuler.
6. La métrique de confiance est utilisée pour filtrer les nœuds avec une Tm faible.

6.5.1.2 Les attaques dans un réseau social véhiculaire

Les attaques dans cette partie peuvent être classées en trois classes, comme illustré dans la Figure 6.14 attaque d'identité, attaque par espionnage et attaque par service.

A) Les attaques sur l'identité

Diverses attaques peuvent être trouvées dans cette catégorie, à savoir l'attaque Sybil, l'attaque d'emprunt d'identité, les attaques de divulgation d'identité et les attaques de vol d'identité.

-L'attaque par Sybil

Un utilisateur malveillant tente de perturber le réseau en créant un certain nombre de fausses identités, afin d'être la destination des données sur le réseau. Ce type d'attaque ne peut pas se produire dans notre solution proposée en raison de la signature des données avant leur envoi. Ainsi, si un utilisateur malveillant souhaite altérer ou falsifier des données sur le réseau, il sera suivi et éliminé du réseau.

-L'attaque par usurpation d'identité

Les attaques de cette catégorie sont liées à l'enregistrement de l'identité des victimes lors de la procédure de souscription. Cette attaque peut être exploitée par un utilisateur malveillant dans le but d'effectuer un autre type d'attaque à savoir : le vol d'identité [140] et attaque par révélation d'identité [141]. Ce type d'attaque ne peut pas se produire dans notre architecture proposée en raison de l'utilisation de la Blockchain et du remplacement des identités de l'expéditeur et du destinataire par un hachage, qui utilise en outre la signature des données avant de les transmettre.

B)Les attaques basées sur l'écoute

L'attaque basée sur l'espionnage est principalement basée sur le réseau d'écoute, nous trouvons l'attaque d'espionnage et l'attaque de trou noir "black hole".

-L'attaque basée sur l'écoute

L'attaque par écoute illicite peut se produire lorsqu'un attaquant tente d'atteindre une communication échangée entre des entités du réseau social véhiculaire. Par la suite, il tente de mener des attaques, à savoir une attaque par modification, une attaque par falsification et attaque par analyse de paquets. En utilisant la Blockchain, cette catégorie d'attaques ne peut pas arriver. Tous les échanges entre entités sont signés avant leur livraison. Un attaquant qui tente d'opérer par falsification peut-être filtrée à l'aide de la "Tm".

-L'attaque par "Hole"

Cette attaque comprend les éléments suivants : "wormhole attaque", "black hole attaque", et "grey hole attaque". En ce qui concerne le "wormhole attaque", une entité malveillante tente de créer de faux plans et informe qu'ils sont plus courts que les autres comme illustré dans la Figure 6.15. Ce genre d'attaque est détectable dans notre architecture proposée en utilisant les nœuds intermédiaires "à deux sauts". En ce qui concerne l'attaque par déni de service, qui est basée sur l'attaque "black hole", l'attaquant transfère les paquets à des entités inexistantes afin de supprimer le paquet entier. Certaines entités suppriment les paquets de manière sélective. Ce type d'attaque s'appelle l'attaque de "grey hole". En utilisant les messages ACK, notre approche présentée peut détecter et éviter ces attaques en calculant la satisfaction et en excluant les nœuds s'ils se comportent mal.

-Attaque par injection de fausses données

Un attaquant peut mener des attaques contre la sécurité des véhicules en se comportant mal et en diffusant des données incorrectes en attaquant les véhicules voisins comme illustré dans la Figure 6.16. Dans notre schéma proposé, l'attaque par injection des données incorrectes ne peut pas se produire en raison de l'utilisation de la Blockchain. Toutes les données livrées sont signées avant leur envoie. En utilisant la "Tm", l'entité malveillante peut être filtrée et mise sur la liste noire.

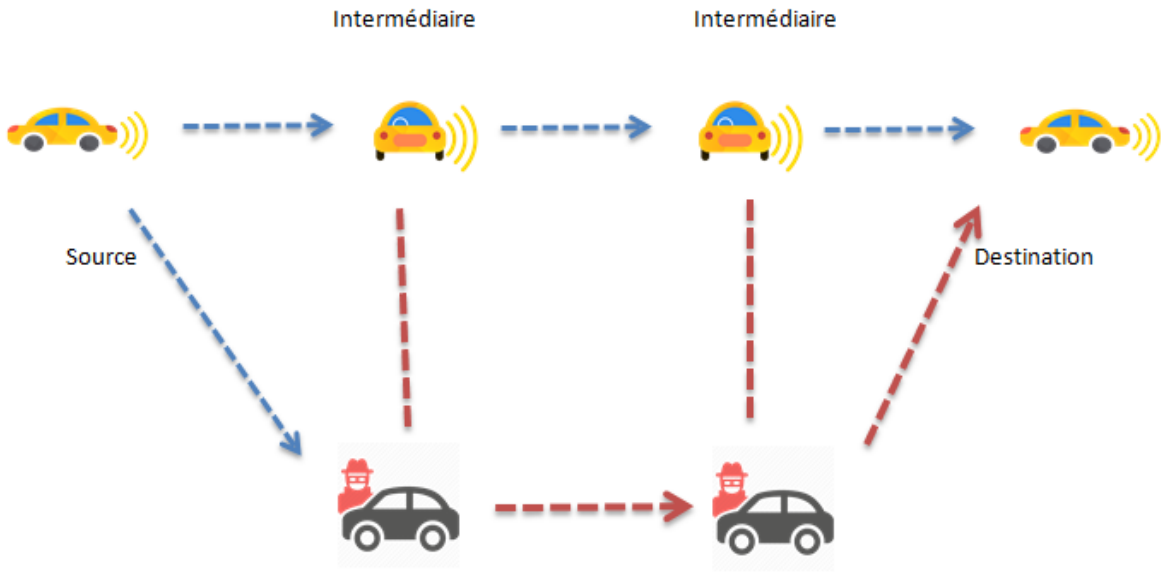

FIGURE 6.15 – L'attaque par wormhole.

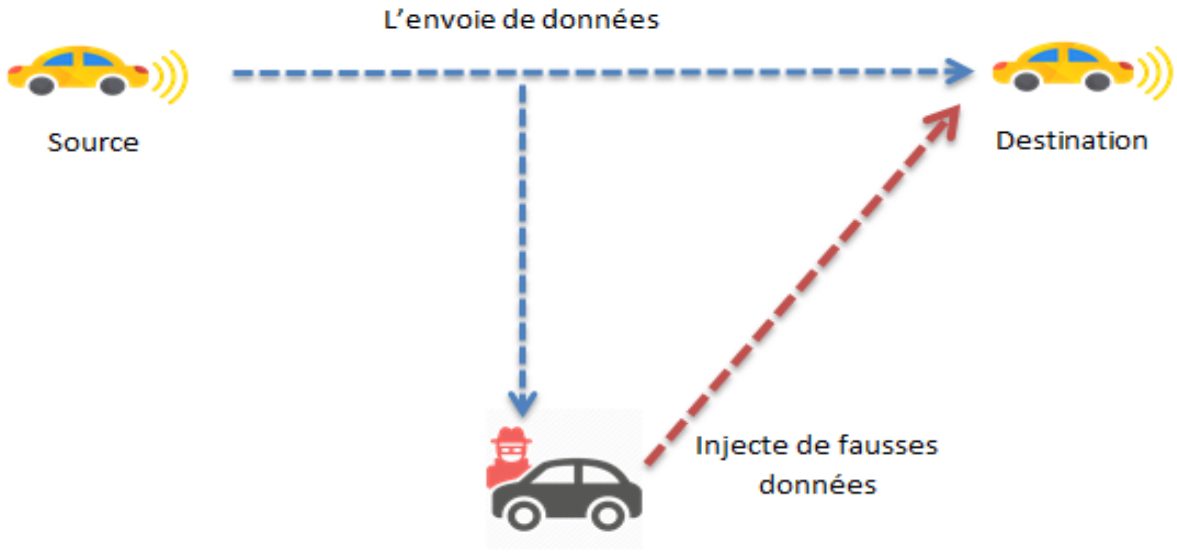

FIGURE 6.16 – L'attaque injection de fausses données.

C)Les attaques basées sur le service

Les attaques de cette catégorie reposent sur deux types d'attaques, à savoir les attaques de spam et les attaques par déni de service, dans le but de rendre les entités

hors-service.

-L'attaque par des spams

Le but de cette attaque est de mettre hors-service le stockage d'entités VSN et de perturber les données sur le réseau. Ce type d'attaque peut être évité dans notre architecture proposée en utilisant des messages ACK et en excluant les nœuds qui se comportent mal.

-L'attaque par déni de service

L'attaquant de cette catégorie tente de mettre les entités hors-service en injectant des paquets pour saturer le support de communication. En utilisant la métrique de confiance vue ci-dessus, nous pouvons détecter les nœuds qui se conduisent mal et les mettre en liste noire.

Comme toute autre solution proposée, notre architecture souffre de certaines faiblesses :

1. Dans le cas d'un nombre d'entités VSN limité, l'application de l'architecture proposée n'est pas évidente.
2. La sélection des mineurs est basée sur le PC et le RSU. Par conséquent, lorsque l'infrastructure n'est pas présente, la sélection n'est pas possible.
3. Dans le cas ou toutes les entités VSN ayant un $TM \leq seuil$, cela signifie qu'elles se comportent mal, ainsi, la sélection des mineurs n'est pas possible.

6.6 Conclusion

Dans cette partie, nous avons proposé une nouvelle architecture basée sur deux approches : "Software-Defined Vehicular Networks "SDVN" et la "Blockchain" pour le réseau social véhiculaire "VSN". En outre, l'algorithme de sélection des nœuds mineurs basé sur l'approche "Connected Dominating Set CDS" est proposé. En matière d'approche SDVN, nous avons introduit trois niveaux de contrôleurs : principal, "RoadSide Unite RSU" et mineurs comme "contrôleur local". L'idée est de distribuer certaines fonctions du contrôleur et rendre les services plus proches des véhicules. À cette fin, nous avons proposé un nouveau algorithme appelé "DM-CDS".
Afin d'évaluer notre architecture proposée et l'algorithme "DM-CDS", nous avons effectué des simulations intensives avec divers scénarios. Les résultats obtenus montrent

l'importance du modèle proposé, sa sensibilité et sa réactivité aux différents paramètres de réseau et la métrique de confiance "TM".

Le dernière partie de cette thèse sera dédié à la conclusion générale et nos orientations et travaux de recherches futurs.

Chapitre 7

CONCLUSION GÉNÉRALE & PERSPECTIVES

Sommaire

7.1 Conclusion générale & perspectives 113
7.2 Conclusions 113
7.3 Orientations de nos travaux futurs 115

7.1 Conclusion générale & perspectives

Dans cette partie nous allons résumer les différentes thématiques traitées dans cette thèse. Nous avons étudié le problème lié à la protection de la vie privée dans les réseaux sociaux en ligne OSN, de plus, nous avons traité un nouveau paradigme à savoir l'intégration des réseaux sociaux dans les "VANETs" vehicular Ad-hoc network. Cette intégration donne un nouveau concept les réseaux sociaux véhiculaires "Vehicular Social Network VSN". Les aspects de la sécurité et de la confidentialité restent encore les préoccupations les plus importantes dans les réseaux sociaux véhiculaires.

En se basant sur l'analyse et la discussion mentionnées, nous soulignons les principales contributions de cette thèse et nous allons discuter les perspectives et les orientations de recherche et les travaux futurs.

7.2 Conclusions

Dans cette thèse, nous avons proposé deux schémas pour la sécurité et de protection de la vie privée pour les OSNs et les VSNs.

— Pour atténuer le problème concernant la protection de la vie privée dans les réseaux sociaux en ligne, nous avons proposé un schéma de filtrage permettant un meilleur contrôle sur les données partagées sur les plateformes des réseaux sociaux. Nous avons proposé un framework appelé **CloudSN**, Ce dernier est composé de deux concepts à savoir : le chiffrement a base d'ABE et le cloud computing. Le modèle de chiffrement est basé sur des attributs multi-autorités, les utilisateurs peuvent concevoir leur propre politique d'accès et permettre uniquement aux amis autorisés d'avoir accès aux données. L'utilisation d'un schéma distribué réduit considérablement le problème du "point de défaillance unique".
Afin de valider notre solution proposée, nous avons procédé à une évaluation des performances par simulation, nous avons réalisé différents scénarios avec plusieurs paramètres, notamment le nombre d'attributs, le temps de chiffrement et le temps de déchiffrement.
La simulation est suivie d'une analyse de la sécurité, dans laquelle nous avons montré la robustesse et la résistance de notre framework proposé à plusieurs attaques et vulnérabilités telles que les attaques de coalition, les vulnérabilités causées par le provider, les utilisateurs et les applications tierces.

— Le réseau social véhiculaire "VSN" est un nouveau concept prometteur, combinant les deux types de réseaux à savoir les réseaux véhiculaires et les réseaux sociaux. Dans ce type de réseau, les véhicules sont équipés par des capteurs permettant de collecter les données spatio-temporelle qui seront analysées et utilisées pour améliorer le quotidien des usages. Le VSN est basé sur un système de communication hétérogène permettant aux conducteurs et aux voyageurs de partager des données telles que les vidéos, les audio et les photos de route. Afin de gérer d'une manière efficace la sécurité et le contrôle du réseau, nous avons proposé un framework basé sur deux concepts émergents à savoir le SDN "Software-Defined Network et la Blockchain. L'utilisation du SDN rend le réseau programmable, virtualisé et partitionnable. Cependant, se basé sur le SDN crée une vulnérabilité bien connue "le point de défaillance unique". Par conséquent, nous proposons d'introduire le paradigme de la Blockchain qui permettra la certification des transactions et assurera l'anonymat des données et des communications de manière entièrement distribuée. Dans notre architecture, nous avons utilisé trois niveaux de contrôleurs à savoir : un contrôleur principal "PC" dont son rôle consiste dans la coordination des RSUs et les mineurs, la configuration du réseau et la gestion des différentes ressources du réseau.
Le contrôleur "RSU", c'est un noeud intermédiaire entre le PC et l'unité embarquée "OBU". Le RSU participe à la sélection des mineurs dont le processus de sélection est basé sur l'approche des ensembles dominés connectés (CDS) et en particulier sur "Distributed Miner Connected Dominating set algorithm" (DM-CDS).
Le contrôleur mineur est un noeud spécifique du réseau d'accès, son rôle consiste à valider et à certifier les transactions en utilisant la Blockchain. Leur sélection est basée sur plusieurs paramètres à savoir : le degré de connectivité, l'indicateur de qualité des liens avec leur noeuds voisins, leur position dans la topologie du réseau et la métrique de confiance.
La performance de l'algorithme "DM-CDS" proposé est évaluée à travers plusieurs scénarios à l'aide de différents paramètres, tels que la métrique de confiance, la densité des nœuds, la mobilité des nœuds et la portée radio. Les résultats obtenus soulignent l'importance d'une telle architecture, notamment en termes de nombre des mineurs sélectionnés.

7.3 Orientations de nos travaux futurs

Dans cette thèse, nous avons introduit le problème de la sécurité et la protection de la vie privée dans les réseaux sociaux en ligne, ainsi que la protection des données et l'anonymat des échanges dans les réseaux sociaux véhiculaires. Bien que certains résultats préliminaires sur la sécurité et la confidentialité des données dans les OSN et le SVN soient fournis, il existe encore plusieurs directions de recherche ouvertes :

— **Le calcul du trafic et la mobilité des véhicules :** Le calcul du trafic et la mobilité des véhicules permet aux conducteurs et aux voyageurs de connaître les conditions routières et les événements actuels et puis choisir les routes alternatives afin d'éviter la congestion et les problèmes rencontrés dans les routes tels que les accidents. Le calcul de nouvelles routes peut être obtenu en se basant sur la collaboration de tous les véhicules.

Les véhicules se trouvant ensemble dans des zones géographiques peuvent coopérer. Ils collectent les données spatio-temporelle grâce aux capteurs dont ils disposent, ils traitent et partagent les informations afin que les conducteurs peuvent prendre des décisions selon la pertinence des données.

— **Internet des Véhicules IoV :** L'internet des véhicules "IoV" est une convergence des réseaux mobiles et de l'internet des objets "IoT". L'IoV est un concept émergeant incluant différents composants à savoir : les capteurs embarqués dans le véhicule, le MEC "Multi-acces Edge", le fog computing et le cloud véhiculaire avec ces différentes utilisation (la virtualisation, l'authentification etc). L'IoV s'ouvre sur de nombreuses possibilités de recherche notamment sur les services, ainsi le fog computing, la confidentialité, la sécurité et la confiance, la qualité de service, la machine learning, etc.

BIBLIOGRAPHIE

[1] ionos 1and1, "Container-as-a-service : comparaison des offres caas." https ://www.ionos.fr/digitalguide/serveur/know-how/caas-comparaison-des-offres-de-container-as-a-service/. Online, accessed 25 April 2020.

[2] J.Clement, "Number of monthly active facebook users worldwide as of 4th quarter 2019." https ://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. Online, accessed 2 april 2020.

[3] K. Smith, "53 incredible facebook statistics and facts." https ://www.brandwatch.com/blog/facebook-statistics/. Online, accessed 7 april 2020.

[4] Facebook, "Data centers year in review." https ://engineering.fb.com/data-center-engineering/data-centers-2018/. Online, accessed 7 april 2020.

[5] Y. Yahiatene, D. E. Menacer, M. A. Riahla, A. Rachedi, and T. B. Tebibel, "Towards a distributed abe based approach to protect privacy on online social networks," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, IEEE, 2019.

[6] Y. Yahiatene and A. Rachedi, "Towards a blockchain and software-defined vehicular networks approaches to secure vehicular social network," in *2018 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 1–7, IEEE, 2018.

[7] Y. Yahiatene, A. Rachedi, M. A. Riahla, D. E. Menacer, and F. Nait-Abdesselam, "A blockchain-based framework to secure vehicular social networks," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 8, p. e3650, 2019.

[8] Facebook, "Graph API facebook, Permissions Reference - Facebook Login." `https://developers.facebook.com/docs/facebook-login/permissions/v2.5`, 2016. Online ; accessed 01 November 2016.

[9] The guardian, "Cambridge analytica facebook." `https://goo.gl/adXNjv`. Online ; accessed 22 May 2018.

[10] K. S. Raynes-Goldie, *Privacy in the age of Facebook : Discourse, architecture, consequences*. PhD thesis, Curtin University, 2012.

[11] F. Beato, M. Kohlweiss, and K. Wouters, "Scramble ! your social network data," in *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 211–225, Springer, 2011.

[12] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona : an online social network with user-defined privacy," in *ACM SIGCOMM Computer Communication Review*, vol. 39, pp. 135–146, ACM, 2009.

[13] M. M. Lucas and N. Borisov, "Flybynight : mitigating the privacy risks of social networking," in *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, pp. 1–8, 2008.

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*, pp. 321–334, IEEE, 2007.

[15] M. Conti, A. Hasani, and B. Crispo, "Virtual private social networks," in *Proceedings of the first ACM conference on Data and application security and privacy*, pp. 39–50, 2011.

[16] W. Luo, Q. Xie, and U. Hengartner, "Facecloak : An architecture for user privacy on social networking sites," in *2009 international conference on computational science and engineering*, vol. 3, pp. 26–33, IEEE, 2009.

[17] Gnupg, "Openpgp." https ://www.gnupg.org/. Online ; accessed 15 November 2016.

[18] G. S. A. Tootoonchian and A. Z. Hatahet, "Fine grained access control in online social networks," tech. rep., Citeseer, 2007.

[19] S. Guha, K. Tang, and P. Francis, "Noyb : Privacy in online social networks," in *Proceedings of the first workshop on Online social networks*, pp. 49–54, 2008.

[20] P. Patil, P. Narayankar, D. Narayan, and S. M. Meena, "A comprehensive evaluation of cryptographic algorithms : Des, 3des, aes, rsa and blowfish," *Procedia Computer Science*, vol. 78, pp. 617–624, 2016.

[21] J. Daemen and V. Rijmen, "Aes proposal : Rijndael," 1999.

[22] W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques," in *Proceedings of the June 7-10, 1976, national computer conference and exposition*, pp. 109–112, ACM, 1976.

[23] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[24] B. Kaliski, "The mathematics of the rsa public-key cryptosystem," *RSA Laboratories*, 2006.

[25] D. Eastlake and P. Jones, "Us secure hash algorithm 1 (sha1)," 2001.

[26] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X. 509 internet public key infrastructure online certificate status protocol-ocsp," tech. rep., RFC 2560, 1999.

[27] P. R. Zimmermann and P. R. Zimmermann, *The official PGP user's guide*, vol. 5. MIT press Cambridge, 1995.

[28] GlobalSign, "les hiérarchies d'ac et pourquoi en avons-nous besoin." `https://www.globalsign.fr`. Accessed : 2020-01-15.

[29] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Rfc 5280 : Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile," *IETF, May*, 2008.

[30] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "Rfc 4880-openpgp message format," *Informe técnico, Internet Engineering Task Force (IETF)*, 2007.

[31] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X. 509 internet public key infrastructure online certificate status protocol-ocsp.," *RFC*, vol. 6960, pp. 1–41, 2013.

[32] P. Hoffman, "Rfc 2634 : Enhanced security services for s/mime," *Request For Comment, Network Working Group*, 1999.

[33] S. Frankel and S. Krishnan, "Ip security (ipsec) and internet key exchange (ike) document roadmap. rfc 6071 (informational)," 2011.

[34] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*, pp. 47–53, Springer, 1984.

[35] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, Springer, 2005.

[36] J. Zhou, Z. Cao, X. Dong, and X. Lin, "Tr-mabe : White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems," in *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2398–2406, IEEE, 2015.

[37] J. Shao, R. Lu, and X. Lin, "Fine-grained data sharing in cloud computing for mobile devices," in *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2677–2685, IEEE, 2015.

[38] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98, 2006.

[39] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 195–203, 2007.

[40] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 456–465, 2007.

[41] Y. Cheng, H. Zhou, J. Ma, and Z. Wang, "Efficient cp-abe with non-monotonic access structures," in *International Conference on Cloud Computing and Security*, pp. 315–325, Springer, 2017.

[42] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in *International conference on the theory and application of cryptology and information security*, pp. 548–566, Springer, 2002.

[43] G. Hanaoka and K. Kurosawa, "Efficient chosen ciphertext secure public key encryption under the computational diffie-hellman assumption," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 308–325, Springer, 2008.

[44] D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in *International conference on the theory and applications of cryptographic techniques*, pp. 223–238, Springer, 2004.

[45] B. Waters, "Dual system encryption : Realizing fully secure ibe and hibe under simple assumptions," in *Annual International Cryptology Conference*, pp. 619–636, Springer, 2009.

[46] J. Li, Q. Yu, and Y. Zhang, "Hierarchical attribute based encryption with continuous leakage-resilience," *Information Sciences*, vol. 484, pp. 113–134, 2019.

[47] J. Wei, X. Chen, X. Huang, X. Hu, and W. Susilo, "Rs-habe : Revocable-storage and hierarchical attribute-based access scheme for secure sharing of e-health records in public cloud," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[48] M. Ali, M.-R. Sadeghi, and X. Liu, "Lightweight revocable hierarchical attribute-based encryption for internet of things," *IEEE Access*, vol. 8, pp. 23951–23964, 2020.

[49] H. Wang, Z. Zheng, L. Wu, and D. He, "New large-universe multi-authority ciphertext-policy abe scheme and its application in cloud storage systems," *Journal of High Speed Networks*, vol. 22, no. 2, pp. 153–167, 2016.

[50] S. Müller, S. Katzenbeisser, and C. Eckert, "Distributed attribute-based encryption," in *International Conference on Information Security and Cryptology*, pp. 20–36, Springer, 2008.

[51] Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in *European Symposium on Research in Computer Security*, pp. 278–297, Springer, 2011.

[52] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Annual international conference on the theory and applications of cryptographic techniques*, pp. 568–588, Springer, 2011.

[53] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dac-macs : Effective data access control for multiauthority cloud storage systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1790–1801, 2013.

[54] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE transactions on parallel and distributed systems*, vol. 25, no. 2, pp. 384–394, 2013.

[55] P. Mell, T. Grance, *et al.*, "The nist definition of cloud computing," 2011.

[56] P. Patel, A. H. Ranabahu, and A. P. Sheth, "Service level agreement in cloud computing," 2009.

[57] A. Apostu, F. Puican, G. Ularu, G. Suciu, G. Todoran, *et al.*, "Study on advantages and disadvantages of cloud computing–the advantages of telemetry applications in

the cloud," *Recent Advances in Applied Computer Science and Digital Services*, vol. 2103, 2013.

[58] A. Felt and D. Evans, "Privacy protection for social networking platforms," Citeseer, 2008.

[59] G. S. Lynch, *Single point of failure*. Wiley Online Library, 2009.

[60] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," *IEEE Internet Computing*, vol. 15, no. 4, pp. 56–63, 2011.

[61] Facebook, "Government requests for user data." https ://transparency.facebook.com/government-data-requests, 2017. Online ; accessed 01 december 2017.

[62] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings : user expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pp. 61–70, ACM, 2011.

[63] N. B. Ellison, C. Steinfield, and C. Lampe, "The benefits of facebook "friends :" social capital and college students' use of online social network sites," *Journal of computer-mediated communication*, vol. 12, no. 4, pp. 1143–1168, 2007.

[64] K. Singh, S. Bhola, and W. Lee, "xbook : Redesigning privacy control in social networking platforms.," in *USENIX Security Symposium*, pp. 249–266, 2009.

[65] J. Baltazar, J. Costoya, and R. Flores, "The real face of koobface : The largest web 2.0 botnet explained," *Trend Micro Research*, vol. 5, no. 9, p. 10, 2009.

[66] R. Lundeen, J. Ou, and T. Rhodes, "New ways im going to hack your web app," *Blackhat AD*, pp. 1–11, 2011.

[67] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," in *Proceedings of the 2nd ACM workshop on Online social networks*, pp. 7–12, ACM, 2009.

[68] I. Paul, "Twitter worm : A closer look at what happened." http ://bit.ly/2VAzv6H. Online ; accessed 23 September 2019.

[69] NASAA, "Informed investor advisory : Social networking." http ://bit.ly/314SsPW. Online ; accessed 23 Sptember 2019.

[70] Theguardian, "Facebook fraud a major issue." http ://bit.ly/2IC2f9Q. Online ; accessed 24 Sptember 2019.

[71] R. McMillan, "Researchers make wormy twitter attack,pcworld, san francisco, ca, usa." http ://bit.ly/2voV3dO. Online ; accessed 24 Sptember 2019.

[72] N. Rojas, "The faces of facebook." http ://app.thefacesoffacebook.com/. Online ; accessed 28 Sptember 2019.

[73] A. Acquisti, R. Gross, and F. Stutzman, "Faces of facebook : Privacy in the age of augmented reality," *BlackHat USA*, no. 2, pp. 1–20, 2011.

[74] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*, pp. 251–260, Springer, 2002.

[75] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, pp. 35–47, ACM, 2010.

[76] C. Taylor, "Startup claims 80% of its facebook ad clicks are coming from bots." https ://tcrn.ch/3a0BdVe. Online ; accessed 28 Sptember 2019.

[77] G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Y. Zhao, "Follow the green : growth and dynamics in twitter follower markets," in *Proceedings of the 2013 conference on Internet measurement conference*, pp. 163–176, ACM, 2013.

[78] N. Perlroth, "Fake twitter followers become multimillion-dollar business." shorturl.at/grsyO. Online ; accessed 28 Sptember 2019.

[79] T. Ryan and G. Mauch, "Getting in bed with robin sage," in *Black Hat Conference*, 2010.

[80] J. Lewis, "How spies used facebook to steal nato chiefs' details." shorturl.at/crM79. Online ; accessed 30 Sptember 2019.

[81] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel, "You are who you know : inferring user profiles in online social networks," in *Proceedings of the third ACM international conference on Web search and data mining*, pp. 251–260, ACM, 2010.

[82] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks : threats and solutions," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2019–2036, 2014.

[83] S. Torabi and K. Beznosov, "Privacy aspects of health related information sharing in online social networks," in *Presented as part of the 2013 {USENIX} Workshop on Health Information Technologies*, 2013.

[84] L. Scism and M. Maremont, "Insurers test data profiles to identify risky clients," *The Wall Street Journal*, vol. 19, p. 2010, 2010.

[85] J. Vicknair, D. Elkersh, K. Yancey, and M. C. Budden, "The use of social networking websites as a recruiting tool for employers.," *American Journal of Business Education*, vol. 3, no. 11, pp. 7–12, 2010.

[86] L. Humphreys, P. Gill, and B. Krishnamurthy, "How much is too much ? privacy issues on twitter," in *Conference of International Communication Association, Singapore*, Citeseer, 2010.

[87] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, "Efficient and scalable socware detection in online social networks," in *Presented as part of the 21st {USENIX} Security Symposium ({USENIX} Security 12)*, pp. 663–678, 2012.

[88] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, "Frappe : detecting malicious facebook applications," in *Proceedings of the 8th international conference on Emerging networking experiments and technologies*, pp. 313–324, ACM, 2012.

[89] H. S. Gardiyawasam Pussewalage and V. A. Oleshchuk, "A distributed multi-authority attribute based encryption scheme for secure sharing of personal health records," in *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, pp. 255–262, ACM, 2017.

[90] D. H. M. Jones, "The oauth 2.0 authorization framework." https ://oauth.net/2/. Online ; accessed 31 March 2017.

[91] Ubuntu, "juju cloud." https ://jujucharms.com/. Online ; accessed 08 January 2018.

[92] Linux, "Lxd containers." https ://linuxcontainers.org/lxd/. Online ; accessed 10 January 2018.

[93] Facebook, "Test users for applications." `https://developers.facebook.com/docs/apps/test-users?locale=en_US`. Online ; accessed 09 September 2017.

[94] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking : imperatives and challenges," *Ad hoc networks*, vol. 1, no. 1, pp. 13–64, 2003.

[95] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of network and computer applications*, vol. 37, pp. 380–392, 2014.

[96] S. Nakamoto *et al.*, "Bitcoin : A peer-to-peer electronic cash system," 2008.

[97] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts : Architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics : Systems*, 2019.

[98] H. Orman, "Blockchain : The emperors new pki ?," *IEEE Internet Computing*, vol. 22, no. 2, pp. 23–28, 2018.

[99] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract : Securing a blockchain applied to smart contracts," in *2016 IEEE international conference on consumer electronics (ICCE)*, pp. 467–468, IEEE, 2016.

[100] M. Pilkington, "11 blockchain technology : principles and applications," *Research handbook on digital transformations*, vol. 225, 2016.

[101] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things : Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[102] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5, IEEE, 2017.

[103] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain : A panacea for healthcare cloud-based data security and privacy ?," *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

[104] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[105] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog : Towards a comprehensive definition of fog computing," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 27–32, 2014.

[106] H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, "Bitcoin-based fair payments for outsourcing computations of fog devices," *Future Generation Computer Systems*, vol. 78, pp. 850–858, 2018.

[107] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017.

[108] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12118–12128, 2018.

[109] K. Kalkan and S. Zeadally, "Securing internet of things with software defined networking," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 186–192, 2017.

[110] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "Distblocknet : A distributed blockchains-based secure sdn architecture for iot networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017.

[111] Z. Yang, K. Zheng, K. Yang, and V. C. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*, pp. 1–5, IEEE, 2017.

[112] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

[113] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[114] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

[115] X. Huang, C. Xu, P. Wang, and H. Liu, "Lnsc : A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[116] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin : A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, 2018.

[117] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, 2018.

[118] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 760–763, 2018.

[119] F. Xia, L. Liu, J. Li, J. Ma, and A. V. Vasilakos, "Socially aware networking : A survey," *IEEE Systems Journal*, vol. 9, no. 3, pp. 904–921, 2013.

[120] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, "Vehicular social networks : Enabling smart mobility," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 16–55, 2017.

[121] A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, and S. K. Das, "Vehicular social networks : A survey," *Pervasive and Mobile Computing*, vol. 43, pp. 96–113, 2018.

[122] D. Bendouda, A. Rachedi, and H. Haffaf, "An hybrid and proactive architecture based on sdn for internet of things," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 951–956, IEEE, 2017.

[123] D. Bendouda, A. Rachedi, and H. Haffaf, "Programmable architecture based on software defined network for internet of things : Connected dominated sets approach," *Future Generation Computer Systems*, vol. 80, pp. 188–197, 2018.

[124] A. Schwartz, "A reinforcement learning method for maximizing undiscounted rewards," in *Proceedings of the tenth international conference on machine learning*, vol. 298, pp. 298–305, 1993.

[125] E. Borcoci, M. Vochin, and S. Obreja, "Mobile edge computing versus fog computing in internet of vehicles," in *The Tenth International Conference on Advances in Future Internet AFIN 2018 At : Venice, Italy*, p. 15, 2018.

[126] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles : Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[127] F. Yang, J. Li, T. Lei, and S. Wang, "Architecture and key technologies for internet of vehicles : a survey," *Journal of Communications and Information Networks*, vol. 2, no. 2, pp. 1–17, 2017.

[128] T. Gazdar, A. Benslimane, A. Rachedi, and A. Belghith, "A trust-based architecture for managing certificates in vehicular ad hoc networks," in *2012 International Conference on Communications and Information Technology (ICCIT)*, pp. 180–185, IEEE, 2012.

[129] A. Rachedi and A. Benslimane, "A secure and resistant architecture against attacks for mobile ad hoc networks," *Security and communication networks*, vol. 3, no. 2-3, pp. 150–166, 2010.

[130] E. K. Wang, Y. Li, Y. Ye, S.-M. Yiu, and L. C. Hui, "A dynamic trust framework for opportunistic mobile social networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 1, pp. 319–329, 2017.

[131] M. T. Thai, F. Wang, D. Liu, S. Zhu, and D.-Z. Du, "Connected dominating sets in wireless networks with different transmission ranges," *IEEE transactions on mobile computing*, vol. 6, no. 7, pp. 721–730, 2007.

[132] B. Yin, H. Shi, and Y. Shang, "An efficient algorithm for constructing a connected dominating set in mobile ad hoc networks," *Journal of Parallel and Distributed Computing*, vol. 71, no. 1, pp. 27–39, 2011.

[133] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE transactions on vehicular technology*, vol. 64, no. 8, pp. 3657–3674, 2014.

[134] T. P. M. (TPM), "Trusted platform module (tpm)," 2018.

[135] T. Main, "Part 2 tpm structures," *Specification version*, vol. 1, 2007.

[136] G. Guette and O. Heen, "A tpm-based architecture for improved security and anonymity in vehicular ad hoc networks," in *2009 IEEE Vehicular Networking Conference (VNC)*, pp. 1–7, IEEE, 2009.

[137] G. Guette and C. Bryce, "Using tpms to secure vehicular ad-hoc networks (vanets)," in *IFIP International Workshop on Information Security Theory and Practices*, pp. 106–116, Springer, 2008.

[138] J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1138–1149, 2011.

[139] M. Swan, *Blockchain : Blueprint for a new economy.* " O'Reilly Media, Inc.", 2015.

[140] B.-Z. He, C.-M. Chen, Y.-P. Su, and H.-M. Sun, "A defence scheme against identity theft attack based on multiple social networks," *Expert Systems with Applications*, vol. 41, no. 5, pp. 2345–2352, 2014.

[141] H. Lu, J. Li, and M. Guizani, "A novel id-based authentication framework with adaptive privacy preservation for vanets," in *2012 Computing, Communications and Applications Conference*, pp. 345–350, IEEE, 2012.