Stratégie de sécurité Zero Trust dans un environnement de cloud communautaire

Kouadio Rodrigue N'Goran

THESE DE DOCTORAT DE

L'ÉCOLE NATIONALE SUPERIEURE
MINES-TELECOM ATLANTIQUE BRETAGNE PAYS DE LA LOIRE-
IMT ATLANTIQUE (FRANCE) ET DE L'INSTITUT NATIONAL
POLYTECHNIQUE FELIX HOUPHOUET BOIGNY DE
YAMOUSSOUKRO (COTE D'IVOIRE)

ÉCOLE DOCTORALE N° 648
Sciences pour l'Ingénieur et le Numérique
Spécialité : Informatique

Par

Kouadio Rodrigue N'GORAN

Stratégie de sécurité Zero Trust dans un environnement de cloud communautaire

Thèse présentée et soutenue à IMT Atlantique, Brest, le 15/12/2023
Unité de recherche : Lab-STICC (IMT Atlantique) et UMRI 78 (INP-HB Yamoussoukro)
Thèse N° : 2023IMTA0381

Rapporteurs avant soutenance :

Frédéric CUPPENS	Professeur, Polytechnique Montréal
Jérémy BUISSON	Maître de conférences, École de l'Air et de l'Espace

Composition du Jury :

Président :	Christophe CLARAMUNT	Professeur, École navale
Rapporteurs :	Frédéric CUPPENS	Professeur, Polytechnique Montréal
	Jérémy BUISSON	Maître de conférences, École de l'Air et de l'Espace
Examinateurs :	Jamal EL HACHEM	Maître de conférences, Université de Bretagne Sud
	Jean-Louis TETCHUENG	Chargé d'enseignement, Orange Labs Rennes
	Hyacinthe KONAN	Maître de conférences, ESATIC Côte d'Ivoire
Dir. de thèse :	Yvon KERMARREC	Professeur, IMT Atlantique
Co-dir. de thèse :	Olivier ASSEU	Professeur, INP-HB Yamoussoukro

Table des matières

Table des figures

Liste des tableaux

Liste des acronymes

3C Community Cloud Computing. 16, 29, 30, 126, 128
5G Cinquième génération. 28

ABAC Attribute-based access control. 38
ABC Artificial Bee Colony. 67
ACA-Py Aries Cloud Agent-Python. 122, 123, 125
ACL Access Control List. 70
AES Advanced Encryption Standard. 53
ANSI American National Standards Institute. 56
ANSSI Agence nationale de la sécurité des systèmes d'information française. 43
API Application Programming Interface. 26, 36, 38, 123, 125
APT Menaces persistantes avancées. 39
AWS Amazon Web Services. 25

BLS Boneh, Lynn and Shacham. 20, 54, 57, 58, 83, 84, 122, 139

CDM Système de diagnostic et d'atténuation continus. 41, 43
CIA Contrat intelligent d'authentification. 81, 82
CIE Contrat intelligent d'enregistrement. 81, 82
CISA Cybersecurity and Infrastructure Security Agency. 42
COT Cercle of Trust. 49
CSA Cloud Security Alliance. 26, 58
CSC consommateur de service cloud . 35
CSMIC Cloud Services Measurement Initiatives Consortium. 86, 104
CTSS Commpatible Time Sharing System. 39
CVSS Common Vulnerability Scoring System. 91, 96, 106

DAC Discretionary Access Control. 70, 75
DEP Défense en Profondeur . 32
DES Data Encryption Standard. 53

DiD Identifiants décentralisés . 48, 51, 79–82, 84, 85, 123, 124
DRT Confiance directe ou recommandée. 127

ECC Elliptic Curve Cryptography. 55, 56
ECDSA Elliptic curve digital signature algorithm. 54–57

FeeM Feedback Manager. 95
FoF Friend of Friend. 90, 100
FoM Friend of multiple friends. 90, 100
FS Fournisseur de service. 48
FSC fournisseur de service cloud . 35

GCP Google Cloud Platform. 25
GSA General Services Administration. 42, 43

HACS Highly Adaptive Cybersecurity Services. 43
HTTP Hypertext Transfer Protocol. 50
HTTPS Hypertext Transfer Protocol Secure. 50

IA Intelligence Artificielle. 16, 28, 139
IaaS Infrastructure as a service. 25, 37, 134
IBM International Business Machines Corporation. 39
ID-FF Identity Federation Framework. 50
ID-SIS Identity Service Interface Specifications. 50
ID-WSF Identity Web Services Framework. 50
IDE Environnement de développement . 126
IdP Fournisseur d'identité. 48–50
IDS Système de détection d'intrusion. 32
IoT Internet des Objets. 16, 28, 59, 139
IPS Système de prévention d'intrusions. 32
ISO Organisation Internationale de Standardisation. 63, 103

LDAP Lightweight Directory Access Protocol. 38, 49

MAC Mandatory Access Control. 70, 75
MAS Systèmes Multi-Agents. 74
MFA Authentification multifacteur. 38, 40
MIT Massachusetts Institute of Technology. 39, 43, 47, 55

NIST National Institute of Standards and Technologies. 16, 23–25, 39, 40, 42, 48, 56, 63

OASIS Organization for the Advancement of Structured Information Standards. 49

OMB Office of Management and Budget. 43
OrBAC Organization Based Access Control. 20, 71–74, 113, 140

PA Administrateur de politique. 40
PaaS Platform as a service. 25, 37, 134
PDP Point de décision de politique. 40, 41
PE Moteur de politique. 40
PEP Point d'application de la politique. 41
PKI Infrastructure à clé publique. 41, 54, 104
PME Petite ou moyenne entreprise. 141

QoRM Gestionnaire de paramètres de qualité de ressources. 95
QoS Qualité de service. 67, 68

RBAC Role-Based Access Control. 38, 70–75
RepM Manager des valeurs de réputation. 91, 95
ResM Gestionnaire de Ressources . 91
REST Representational state transfer. 125
RPOT taux de participations des organisations fiables aux transactions. 127
RSA Rivest-Shamir-Adleman . 54–56
RSSI Responsable de la sécurité des systèmes d'information. 47

SaaS Software as a service. 25, 37, 134
SAML Security Assertion Markup Language. 49, 50
SIEM Système de gestion des informations et des événements de sécurité. 42
SL Logique subjective. 93
SLA Accord de niveau de service. 37, 67, 68, 113, 126
SMI Service Measurement Index. 19, 68, 86, 103, 104, 129
SRTG Taux de succès de transactions d'organisations fiables. 127, 129, 133
SSH Secure Socket Shell. 55
SSL Secure Sockets Layer. 55
SSO Sigle Sign On. 38, 49, 50

TLS Transport Layer Security. 55
TNA-SL Trust Network Analysis with Subjective Logic. 67, 68, 127–129, 133, 136
TON Trust overlay Network. 86
TraM Manager de transaction. 91, 92, 95
TruC Calculateur de valeurs de confiance. 91, 94

UpdM Gestionnaire de mise à jour de valeur de confiance et de réputation. 91
URL Uniform Resource Locator. 50

VC Informations d'identifications vérifiables. 48, 52, 79–81, 85

VON-Network Verifiable Organizations Network. 122, 123

VPN Réseau privé virtuel. 32

W3C World Wide Web Consortium. 51, 59

XML Extensible Markup Language. 49, 50, 113

Remerciements

Outre les exigences et la rigueur scientifique renforcées durant cette thèse, ces trois dernières années m'ont permis de vivre une aventure humaine et professionnelle enrichissante. Cette thèse est le fruit d'une collaboration impliquant plusieurs acteurs (personnes et institutions) dans le cadre d'une cotutelle internationale entre l'IMT Atlantique (France) et l'INP-HB Yamoussoukro (Côte d'Ivoire).

Mes premiers mots de remerciements vont à l'endroit de Messieurs Yvon KERMARREC, Olivier ASSEU et Jean-Louis TETCHUENG, respectivement, Directeur, Co-Directeur de thèse et encadrant, pour leur encadrement de qualité durant ces trois ans. Je me suis senti chanceux de pouvoir bénéficier de leurs expériences, directives et connaissances, ainsi que de leur disponibilité et soutien sans faille tout au long de ce parcours.

Je tiens à exprimer ma gratitude envers M. Philippe LENCA et Thierry DUVAL, respectivement directeurs des départements LUSSI et INFO, qui nous ont accueillis pendant nos séjours de recherche en France. En outre, je tiens à remercier l'ambassade de France en Côte d'Ivoire à travers son Service de Coopération et d'Action Culturelle (SCAC) pour le financement et l'accompagnement de qualité Mme N'TAKPE Juliette lors de nos séjours de recherche. Je voudrais, par ailleurs, adresser ma profonde reconnaissance à M. KONATE Adama, directeur général de l'ESATIC et à tout le comité de direction, pour leur indéfectible soutien en autorisant ces séjours malgré nos charges administratives au sein de cette institution. Je tiens également à remercier Monsieur Benjamin YAO, Directeur de l'École Doctorale Polytechnique de l'INP-HB et Monsieur HABA Cissé, Directeur de l'UMRI 78, pour leurs efforts en vue de promouvoir la recherche en Côte d'Ivoire.

Je voudrais exprimer mes sincères remerciements aux membres du jury qui ont accepté d'évaluer nos travaux :

- M. Christophe CLARAMUNT, Professeur à l'École navale, Président du jury
- M. Frédéric CUPPENS, Professeur à Polytechnique Montréal
- M. Jérémy BUISSON, Maître de conférences à l'École de l'Air et de l'Espace
- Mme Jamal EL HACHEM, Maître de conférences à Université de Bretagne Sud
- M. Hyacinthe KONAN, Maître de conférences à l'ESATIC (Côte d'Ivoire)
- M. Jean-Louis TETCHUENG, Chargé d'enseignement à Orange Labs Rennes
- M. Yvon KERMARREC, Professeur à l'IMT Atlantique
- M. Olivier Pascal ASSEU, Professeur à l'INP-HB Yamoussoukro (Côte d'Ivoire)

Je tiens particulièrement à exprimer ma reconnaissance envers M. Frédéric CUPPENS, ainsi qu'à M. Jérémy BUISSON pour m'avoir fait l'honneur d'évaluer ma thèse en tant que rapporteurs.

J'exprime ma profonde gratitude à M. Philippe TANGUY pour avoir été l'une des premières personnes (avec Yvon) à faciliter et à me donner l'opportunité d'effectuer un stage au sein l'IMT Atlantique. Ce stage fut le début de cette belle aventure. Par ailleurs, je remercie M. Emmanuel Braux pour sa disponibilité et toutes les nouvelles compétences acquises auprès de lui lors de ce stage.

Je remercie également le personnel administratif, technique, enseignant de l'ESATIC et les membres du laboratoire LASTIC particulièrement Messieurs Pandry KOFFI, Aliou BAMBA, Aladji KAMAGATE, Pacôme BROU, Désiré KONE et tous ceux qui ont été une oreille attentive soit pour m'écouter, soit pour me donner des conseils.

À toutes ces personnes que cette aventure m'a fait rencontrer et qui sont devenues comme une seconde famille, KAMAGATE Zakarya, KAMAGATE Nouho, CHERIF Karim, SALIF Sidibé, OUATTARA Aladji, YOHOU Anderson, ADOU Emmanuel, à tous mes amis et ainés (ADOU Michel, TANOH Jean-Yves, KOUAME Emile, KONAN Hyacinthe, etc.). Encore merci d'avoir été là quand j'en avais besoin.

Mes remerciements vont également à l'endroit du personnel administratif de l'IMT Atlantique, particulièrement à Ghislaine, Armelle et Delphine qui ont été d'un soutien inestimable dans la compréhension et la gestion des démarches administratives parfois complexes de la cotutelle.

Je veux remercier mes amis doctorants du SCAC (Marc, Christelle et Stéphanie) ainsi que tous les doctorants (SILUE KoLo, COULIBALY Mamadou, etc.) qui ont participé à cette aventure.

J'ai une pensée particulière pour ma famille. Je tiens à remercier mes frères et sœurs (Emma, Romaric, Nina), mon oncle M. SARAKA Kouassi, ma fille et toute la famille, pour leur soutien indéfectible, leurs prières et leurs conseils dans les moments les plus difficiles et de doutes. Je ne pense pas que j'y serais arrivé sans vous.

Enfin, je dédie ce mémoire à mon père, à ma mère et à mon oncle Feu N'GORAN Boniface.

Résumé

De nos jours, la société est caractérisée par une mobilité importante des populations et des besoins croissants en termes de partage de gros volumes de données sensibles au sein des entreprises et de collaboration avec des organisations partenaires ou concurrentes. Ces collaborations procurent de nombreux avantages aux entreprises en termes d'évolutivité et de croissance économique. Cependant, les systèmes informatiques de ces organisations sont exposés à divers types de menaces et cyberattaques de plus en plus sophistiquées. Les stratégies traditionnelles de sécurisation des infrastructures fondées sur le périmètre ne sont plus suffisantes. Le modèle de sécurité Zero Trust est une approche de cybersécurité qui considère toutes les entités d'une infrastructure comme potentiellement vulnérables en tout temps et en tout lieu. Cette stratégie se positionne comme une réponse à la problématique de sécurisation de ces systèmes hétérogènes, complexes, dynamiques et distribués. Cependant, sa mise en œuvre varie en fonction du contexte du système, et exige des changements organisationnels et culturels. En effet, les systèmes de collaboration sont caractérisés par la nécessité de garantir l'autonomie des entités engagées, la confiance entre elles et le besoin de protection des informations sensibles de diverses natures échangées.

Dans cette thèse, nous proposons, une stratégie de sécurité Zero Trust dans un contexte de collaboration entre des organisations au sein d'un cloud communautaire. Le modèle présente une architecture hiérarchique pour sécuriser les échanges au sein et entre des organisations. Il fournit un système de gestion décentralisée des identités des utilisateurs et des organisations grâce aux identifiants décentralisés et aux informations d'identifications vérifiables. Cette méthode expose un moyen d'authentification continue des entités et de stockage des données dans un registre distribué de type blockchain. Par ailleurs, la démarche propose une technique d'évaluation de la confiance entre les organisations. En outre, la stratégie inclut un mécanisme de spécification de règles de politique d'accès et de suivi de contrat de collaboration. Des expérimentations ont été menées afin de prouver l'efficacité et la fiabilité des mécanismes proposés, fournissant ainsi une architecture et des mesures de sécurité associées pour le déploiement d'une stratégie Zero Trust dans un environnement de collaboration.

Mots clés : Zero Trust, Confiance, Identités décentralisées, Blockchain, Contrôle d'accès, Cloud communautaire

Abstract

Today's society is characterized by a highly mobile population and growing needs in terms of sharing large volumes of sensitive data within companies and collaborating with partner or competitor organizations. These collaborations bring many benefits to companies in terms of scalability and economic growth. However, the IT systems of these organizations are exposed to various types of increasingly sophisticated threats and cyberattacks. Traditional perimeter-based infrastructure security strategies are no longer sufficient. The Zero Trust security model is a cybersecurity approach that considers all entities in an infrastructure as potentially vulnerable at all times and everywhere. This strategy is positioned as a response to the problem of securing these heterogeneous, complex, dynamic and distributed systems. However, its implementation varies according to the system context, and requires organizational and cultural changes. Indeed, collaborative systems are characterized by the need to guarantee the autonomy of the entities involved, the trust between them and the need to protect sensitive information of various kinds exchanged.

In this thesis, we propose a Zero Trust security strategy in the context of collaboration between organizations within a community cloud. The model presents a hierarchical architecture for securing exchanges within and between organizations. It provides a decentralized management system for user and organizational identities using decentralized identifiers and verifiable credentials. This method exposes a means of continuous authentication of entities and storage of data in a blockchain-type distributed ledger. Furthermore, the approach offers a technique for assessing trust between organizations. The strategy also includes a mechanism for specifying access policy rules and monitoring collaboration contracts. Experiments have been carried out to prove the effectiveness and reliability of the proposed mechanisms, providing an architecture and associated security measures for deploying a Zero Trust strategy in a collaborative environment.

Keywords : Zero Trust, Trust, Decentralized identities, Blockchain, Access control, Community cloud

Introduction Générale

« Renforcer le climat de confiance par des mesures garantissant notamment la sécurité de l'information et la sécurité des réseaux, l'authentification ainsi que la protection de la vie privée et du consommateur est un préalable au développement de la société de l'information et à l'établissement de la confiance parmi les utilisateurs des TIC. Une culture globale de la cybersécurité doit être encouragée, développée et mise en œuvre en coopération avec tous les partenaires et tous les organismes internationaux compétents.»

Déclaration de principes - Sommet Mondial sur la Société de l'Information (SMSI) - Genève Décembre 2003

La démocratisation du télétravail ces dernières années, principalement due à la pandémie de la Covid-19, a entraîné un changement sans précédent dans le mode de vie des populations et des entreprises. Favorisant la collaboration et le partage d'informations au sein des entreprises ou entre organisations tout en accélérant la migration de leurs systèmes d'information vers l'informatique dématérialisée. De ce fait, le paradigme de cloud computing, qui consiste à fournir des ressources informatiques (matérielles et logicielles) sur demande par le biais du réseau Internet, se présente comme un levier pour ce nouveau monde « tout en ligne ». Il est ainsi qualifié de cinquièmes services d'utilité publics après l'eau, l'électricité, le gaz et le téléphone, et propose divers outils de collaboration et des services variés permettant de réduire ou d'éliminer la notion de distance entre les individus [40]. Selon les estimations de Gartner [90], les revenus mondiaux issus du cloud computing passeront de 655 milliards de dollars en 2023 à 917 milliards en 2025. Le cloud computing garantit ainsi aux entreprises l'agilité et la résilience nécessaire pour rester compétitives et pérennes. C'est aussi un levier indispensable pour les technologies émergentes telles que l'Intelligence Artificielle (IA), l'Internet des Objets (IoT) et la blockchain. Ces avantages sont l'une des raisons pour lesquelles le gouvernement américain a émis, en 2021, une circulaire [101] recommandant aux organisations fédérales de migrer leurs systèmes d'information traditionnels vers des environnements cloud sécurisés.

Cependant, malgré les atouts et l'engouement pour les technologies cloud, une enquête de NetAPP [156] réalisée en 2023, révèle les difficultés rencontrées dans la mise en place d'infrastructures cloud et les réticences de certaines organisations à l'utilisation de services cloud et à la migration de leurs infrastructures sur site (On Premise) vers le cloud. Ce scepticisme à l'égard des services cloud se justifie notamment par des problèmes de dépendances à l'égard des fournisseurs de services cloud, de transparence sur la localisation des infrastructures d'hébergement, l'utilisation et le stockage des données [167]. Par ailleurs, les coûts de déploiements élevés en ressources humaines et financières constituent un frein à l'adoption de cette technologie par de nombreuses organisations telles que les PME et les Startups. Le modèle de déploiement de cloud communautaire ou community cloud computing (3C) permettrait de surmonter ces différents obstacles.

Le National Institute of Standards and Technologies (NIST) définit le cloud communautaire comme une infrastructure regroupant plusieurs organisations et soutenue par une communauté spécifique dans le but de partager des ressources [72]. Chaque organisme met à la disposition de la communauté ses ressources excédentaires ou inutilisées sous forme de services. Ces ressources peuvent être matérielles ou logicielles. Il s'agit principalement d'infrastructures physiques virtualisées (stockage, réseaux, serveurs, postes de travail, etc.), d'applications et des données. Les organisations membres de la communauté sont alors des fournisseurs et/ou des demandeurs de ressources informatiques. Ces coopérations entre organisations et ces échanges de ressources dans la communauté permettent de répartir les coûts de déploiement et de gestion de l'infrastructure, et ainsi réduire les frais supportés par chaque entité. En outre, cela permet de générer plus de revenus ainsi qu'une gouvernance commune et transparente des données.

Contexte de la thèse et problématique

Le succès d'une communauté d'entités autonomes, hétérogènes, réunies dans le but de collaborer par le partage de ressources variées, implique de relever différents défis. En effet, l'établissement de relations durables et l'incitation à la collaboration nécessitent de la confiance entre les acteurs engagés ainsi qu'un suivi permanent de la qualité des ressources partagées. La confiance est un élément déclencheur qui favorise des interactions sociales et productives au sein d'une communauté. Les problèmes de confiance rencontrés sont alors dus à l'incertitude sur la qualité des ressources et des entités engagées. La qualité d'une ressource quant à elle peut être examinée sous un angle sécuritaire ou fonctionnel. Par conséquent, assurer la sécurité et un suivi qualitatif de l'infrastructure (organisations et ressources), est un moyen de garantir un niveau de confiance optimal. Dans un environnement tel que le cloud communautaire, la capacité des organisations à fournir des ressources de qualité de façon durable permet de disposer d'une plateforme prospère et pérenne. Il est donc important de mettre en place des mécanismes permettant de sécuriser les ressources et de suivre les engagements de collaboration de chaque organisation. Ces dernières années, les technologies émergentes [88] et les cyberattaques de plus en plus massives [186] ont conduit à repenser les stratégies de sécurité des systèmes informatiques devenus très complexes et ouverts. Les approches traditionnelles de cybersécurité fondées sur la défense périmétrique et en profondeur [68] ne sont plus suffisantes face à l'augmentation des attaques aussi diverses que sophistiquées.

Le modèle Zero Trust « Never Trust, Always Verify » propose de répondre à ces problèmes. Cette stratégie étend la sécurité du système au-delà du concept de périmètre, suggère de ne faire confiance à aucune entité (utilisateurs, périphériques, ressources, etc.) et de toujours vérifier leur fiabilité, en tout lieu, en tout temps et en toute situation. Adopter la philosophie Zero Trust, c'est appliquer de la défense en profondeur, dynamique et automatisée [14]. C'est un ensemble de principes de sécurité qui considère chaque composant, service et utilisateur d'un système comme continuellement exposé et potentiellement compromis par un adversaire malveillant [166]. Pour reprendre l'analogie du château-fort qui considère toute personne à l'intérieur de la muraille digne de confiance et toute entité extérieure suspecte, avec le Zero Trust, tout le monde (du serviteur au souverain) doit prouver son identité à chaque entrée dans une pièce et la légitimité de chaque action à tous les niveaux. Même si ces fondements datent de quelques années, cette démarche connait un bond significatif dans son adoption par les entreprises ces dernières années. Le décret du gouvernement américain de 2021 recommandant son adoption dans le but de faciliter les échanges entre les agences fédérales et garantir un niveau de sécurité élevé est une illustration de ce regain d'intérêt [101].

La sécurité des utilisateurs et des ressources dans un contexte de collaboration a toujours été une question cruciale pour les spécialistes de la sécurité des systèmes d'informations. La stratégie de sécurité Zero Trust vise à fournir un cadre sécurisé, propice au partage et à la collaboration. Cependant, elle ne propose pas d'exemples standards d'architectures avec un large champ d'application et son implémentation varie en fonction de l'organisation. De plus, la philosophie du Zero Trust est une culture qui se fonde sur un ensemble de principes de conception, même si certaines compagnies la présentent comme un produit commercial à des fins de marketing. En dépit des divergences autour de sa définition et du manque d'architecture standardisée, la stratégie Zero Trust se présente comme un atout majeur dans l'adoption des technologies cloud et la sécurisation des données et ressources des entreprises [89]. Cette stratégie permettrait ainsi de répondre aux différents défis de sécurité, d'autonomie et de confiance

rencontrées par les systèmes collaboratifs tels que le cloud communautaire. Toutefois, la mise en place de cette stratégie dans un cloud communautaire nécessite de se poser les questions suivantes :

QR1 Comment identifier et authentifier les acteurs de manière continue pour assurer la traçabilité des actions et des échanges ?

QR2 Comment évaluer la confiance entre les organisations et leur capacité à fournir des ressources de qualité (disponibilité, niveau de vulnérabilité mesurée et réduite, délai de livraison, etc.) ?

QR3 Comment favoriser l'intégration équitable, consensuelle et sécurisée des nouveaux membres dans la communauté ?

QR4 Comment garantir et maintenir l'autonomie des organisations et des utilisateurs tout en favorisant la collaboration grâce à un contrôle fiable et transparent des accès aux ressources ?

QR5 Quelles approches faut-il adopter pour établir et suivre des contrats de collaboration en fonction des spécificités de la communauté et des engagements de chaque partie ?

Ces interrogations justifient notre proposition d'architecture de collaboration sécurisée fondée sur les principes du Zero Trust pour des infrastructures de cloud communautaire.

Objectifs de la thèse

L'objectif principal de ces travaux de thèse est de proposer un cadre (*framework)* de gestion de la confiance et de la sécurité des ressources partagées entre des organisations dans un cloud communautaire. Il s'agit pour nous, sur la base du triptyque « confiance, sécurité, collaboration » d'apporter une réponse à la question de l'influence des systèmes informatiques fiables et sûres dans le développement d'entreprises prospères à fort impact social. Afin de mener à terme notre projet, des objectifs spécifiques ont été établis.

Tout d'abord, nous présentons le cloud computing, les besoins et enjeux en termes de collaboration, de sécurité ainsi que les mécanismes déployés pour répondre à ces problématiques.

L'étape suivante consiste à proposer des méthodes d'identification et d'authentification continue des organisations dans un cloud communautaire. Le but est d'assurer de manière transparente et consensuelle l'intégration et le départ des organisations, et ainsi disposer d'un registre distribué et sécurisé des membres de la communauté. Après avoir identifié les organisations grâce à un mécanisme de gestion décentralisé des identités, il sera question d'évaluer la confiance et la qualité des ressources au travers d'un système de gestion de la confiance. Ensuite, on examinera la collaboration grâce à un mécanisme de négociation et de création de contrat associé à un modèle de définition de politique et de contrôle d'accès aux ressources. Ce qui permettra de suivre le respect des accords de collaboration, et ainsi de garantir le caractère dynamique des opinions de confiance entre les organisations.

Enfin, le dernier objectif consistera à fournir une implémentation des différentes techniques proposées et une évaluation de notre solution.

Structure du manuscrit et contributions

Contributions

En réponse aux questions énumérées et aux objectifs présentés dans les sections précédentes, des contributions ont été réalisées lors de ce travail de thèse. Ces contributions sont décrites ci-dessous :

- la première contribution (C_1) examine la gestion des identités et l'authentification des organisations et des utilisateurs. Elle propose un système de gestion des identités fondé sur les identifiants décentralisés et la technologie blockchain. Cette contribution a fait l'objet d'une publication.

R. N'goran, J.-L. Tetchueng, Y. Kermarrec, P. Brou, and O. Asseu. "Blockchain-based Identity and Access Management in a Community" *2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, IEEE,2023, DOI :10.23919/SoftCOM58365.2023.10271602

- la deuxième contribution (C_2) est consacrée à la gestion de la confiance entre les organisations et à la sécurité des ressources de la communauté. Elle présente un modèle d'évaluation de la confiance (SeComTrust) fondé sur une architecture de cloud communautaire subdivisée en différents domaines de sécurité. Par ailleurs, une amélioration (C_3) de ce modèle propose une évaluation de la qualité des ressources sur la base des attributs de mesure de qualité de service SMI (Service Measurement Index) [202]. Ces deux contributions ont fait l'objet des publications suivantes :

* R. N'goran, J.-L. Tetchueng, G. Pandry, Y. Kermarrec, and O. Asseu. "Trust Assessment Model Based on a Zero Trust Strategy in a Community Cloud Environment"*Engineering*, 14(11) :479–496, 2022. DOI : 10.4236/eng.2022.1411036

* R. N'goran, L. Vallee, G. Johnson, J.-L. Tetchueng, Y. Kermarrec and O. Asseu. "Shared Resource Quality Monitoring and Dynamic Trust Management in a Community Cloud"*Open Journal of Applied Sciences* , 12, 1898-1914, 2022. DOI : 10.4236/ojapps.2022.1211131

- la quatrième contribution (C_4) traite de la spécification des règles de politique d'accès aux ressources. Elle présente un modèle de contrôle d'accès établi à partir des systèmes multi-agents. Cette contribution a fait l'objet d'une publication.

R. N'goran, Y. Kermarrec, J.-L. Tetchueng, and O. Asseu. "Community-OrBAC : un modèle de contrôle d'accès établi à partir des agents pour les systèmes de collaboration centrés sur la communauté " *Journées Francophones sur les Systèmes Multi-Agents*, Cepadues Éditions,2023,ISBN : 9782383950349

- la dernière contribution (C_5) présente une implémentation et une évaluation d'une stratégie de cybersécurité Zero Trust dans un système de collaboration. Cette stratégie s'appuie sur les différents mécanismes de sécurité présentés dans les sections précédentes, notamment : une gestion décentralisée des identités grâce à la blockchain, un algorithme d'évaluation et de sélection d'une organisation de

confiance et enfin un modèle de contrôle d'accès et d'établissement de contrat de collaboration. Cette contribution a fait l'objet d'une publication.

K. R. N'goran, A. P. B. Brou, K. G. Pandry, J. -L. Tetchueng, Y. Kermarrec and O. Asseu, "Zero Trust Security Strategy for Collaboration Systems," *2023 International Symposium on Networks, Computers and Communications (ISNCC), Doha, Qatar*, IEEE, 2023, pp. 1-6, doi : 10.1109/ISNCC58260.2023.10323911.

Plan

Ce document est organisé en quatre chapitres, comme il est décrit ci-dessous.

Le premier chapitre présente le contexte de nos travaux, notamment le cloud computing, ainsi que les concepts de collaboration et de partage de ressources dans ce type d'environnement. Nous évoquons de manière détaillée les définitions, les caractéristiques, les modèles de services, de déploiements et les défis de sécurité auxquels sont confrontés les acteurs du cloud. Par ailleurs, nous abordons la question du besoin croissant de collaboration et des moyens de partage offerts par le cloud, notamment par le cloud communautaire. Enfin, les stratégies de sécurité des infrastructures informatiques, y compris celles utilisées dans les environnements de cloud computing, sont présentées.

Le deuxième chapitre présente un état de l'art sur la gestion des identités et du contrôle d'accès dans le cloud ainsi que des techniques d'évaluation de la confiance. Une analyse des avantages et des limites de chaque approche est effectuée en fonction des exigences d'un environnement de collaboration centré sur la communauté, ce qui nous permet d'affiner notre solution proposée dans la section suivante.

Le troisième chapitre a pour objet d'exposer notre stratégie de sécurité Zero Trust. Dans un premier temps, nous présentons notre proposition de gestion des identités des acteurs de la communauté. En nous basant sur la signature numérique BLS (Boneh, Lynn and Shacham) [38], la technologie blockchain et ses technologies connexes (contrats intelligents, identifiants décentralisés et les oracles), nous proposons un système de gestion décentralisée des identités et d'authentification des organisations et des utilisateurs.

Ensuite, nous proposons un système d'évaluation de la confiance entre les membres de la communauté. Cette évaluation est faite grâce à la logique subjective [110] et un algorithme de sélection de fournisseurs de confiance. De plus, un suivi de la qualité des ressources et des services est effectué en utilisant des attributs de mesure de qualité des services. Enfin, la dernière partie de ce chapitre met en évidence les spécificités de la collaboration entre des organisations autonomes et les propriétés nécessaires à la mise en place d'un modèle de définition de politique de sécurité et de contrôle d'accès. Nous proposons ainsi le *Community-OrBAC*, un cadre fondé sur le modèle de contrôle d'accès OrBAC [120], qui permet d'élaborer des règles de sécurité en tenant compte du contexte de sécurité et du contexte social.

Le quatrième et dernier chapitre décrit la manière dont tous les mécanismes présentés peuvent être déployés dans une stratégie de cybersécurité Zero Trust au sein d'un cloud communautaire. Par ailleurs, une mise en œuvre suivie de l'évaluation de la stratégie est présentée.

Notre travail s'achève par une conclusion qui met en relief les propositions et leur mise en œuvre, et suggère des perspectives de recherche et de travaux futurs autour

des contributions présentées dans ce manuscrit. Le diagramme de Venn de la figure 0.1 ci-dessous présente les relations entre les différents chapitres de notre travail, nos contributions et le triptyque « Sécurité, Collaboration, Confiance ».

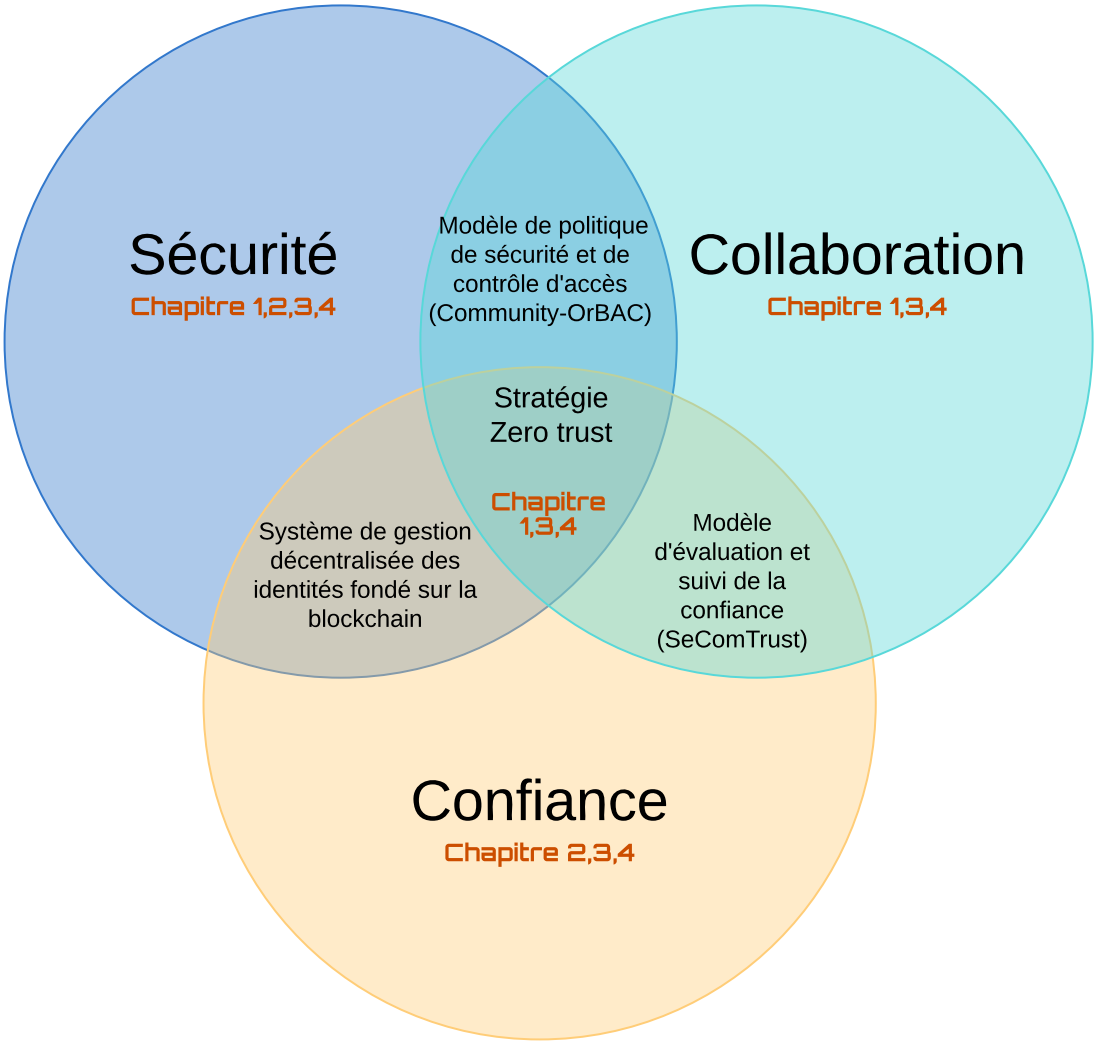


FIGURE 0.1 : Diagramme de Venn de la Thèse

Chapitre 1

Collaboration et stratégie de sécurité dans le cloud computing

« Sortir des politiques de sécurité "alibi", que l'on rédige pour se donner bonne conscience, pour aller vers des pratiques concrètes, réellement ancrées dans les processus de gestion de l'information, voilà donc l'enjeu pour les années à venir… »

Laurent BELLEFIN - Pour le Groupe de Travail « Enquête sur les menaces informatiques et les pratiques de sécurité », 2008

Sommaire

1.1 Introduction

L'usage de services cloud est en pleine croissance ces dernières années et constitue un atout majeur dans l'atteinte des objectifs de développement durables [83]. Un intérêt croissant des entreprises pour le cloud computing justifié par la réduction des coûts opérationnels, une offre de services innovants et diversifiés, mais surtout des gains importants, en termes de revenus financiers [90]. Par ailleurs, la digitalisation accélérée des entreprises et la mobilité accrue de leurs utilisateurs ont renforcé les exigences de performances (stockage, puissance de calcul, etc.) des systèmes d'informations et les besoins de collaboration et de partage de ressources. Toutes ces exigences ne pouvant être satisfaites par les systèmes informatiques traditionnels, le cloud computing se présente alors comme la solution adéquate pour fournir des produits innovants et avec des délais de mise en service relativement court.

Cependant, certaines organisations exerçant dans des domaines très réglementés (banques, santé, militaire, etc) avec des considérations juridiques et des exigences de sécurité élevées, demeurent réservées quant à l'utilisation des offres des fournisseurs de cloud public [152][154][55]. Ainsi, elles restent fidèles à leurs infrastructures sur site ou contraints de s'orienter vers des solutions de cloud privé très onéreuses en ressources financières et humaines.

Dans ce chapitre, nous présentons dans un premier temps une vue d'ensemble du cloud computing à travers sa définition, ses caractéristiques, ses modèles de services et de déploiements. Ensuite, nous analysons le modèle de déploiement de cloud communautaire, ses spécificités, ses avantages et les défis sécuritaires auxquels il est confronté. Dans la seconde partie du chapitre, nous abordons les différentes stratégies et les mécanismes utilisés pour assurer la sécurité des infrastructures informatiques en général et en particulier de cloud computing.

1.2 Le cloud computing

1.2.1 Définition et caractéristiques

Plusieurs propositions ont été faites dans la littérature afin de donner une définition claire et précise au cloud computing. La plus largement acceptée est celle du National Institute of Standards and Technology (NIST) qui définit le cloud comme « *un modèle qui permet un accès réseau omniprésent, facile et à la demande à un ensemble partagé de ressources informatiques (réseaux, serveurs, stockage, applications et services) configurables, qui peuvent rapidement être provisionnées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur du service* » [150]. Ainsi, le cloud computing met en relation des fournisseurs de services de cloud et des clients (particuliers, entreprises, organisations) qui sollicitent des ressources hébergées dans des centres de données géographiquement localisés dans les quatre coins du monde.

Au regard de son fonctionnement et de sa définition, cinq caractéristiques majeures du cloud ont été identifiées par le NIST [150] :

- **Libre-service à la demande** : selon leurs besoins, les utilisateurs de service cloud sollicitent des ressources (espace de stockage, puissance de calcul, etc.) auprès des fournisseurs de service cloud. Les ressources sont fournies de manière automatisée, sans interaction humaine avec le prestataire de service et grâce à un mode de facturation défini par celui-ci.
- **Large accès réseau** : les ressources cloud sont accessibles via les réseaux de communication standard, en l'occurrence, Internet et disponibles sur différents types

de terminaux légers ou lourds (poste de travail, ordinateur portable, téléphone mobile, tablette).

- **Mise en commun des ressources** : sur la base d'un modèle multi-locataire, les ressources informatiques du fournisseur de service cloud sont regroupées afin de satisfaire les besoins de plusieurs clients. Ces services sont alloués de façon dynamique et consommés en fonction des demandes.
- **Élasticité rapide** : les besoins des clients étant dynamique, par conséquent l'approvisionnement en ressources des consommateurs se fait de manière flexible, automatique, conformément aux besoins exprimés et en fonction des capacités du fournisseur de service. Les ressources du fournisseur paraissent illimitées du point de vue du client et permettent généralement de satisfaire les besoins exprimés.
- **Service mesuré et facturation à l'usage** : les systèmes cloud disposent de mécanismes de supervision, de contrôle et de mesure de l'utilisation des ressources. Cette approche apporte de la transparence, un usage optimisé des ressources en temps réel et un mode de facturation à l'usage.

Outre ces caractéristiques, le NIST a défini trois principaux modèles de service et quatre modèles de déploiement de cloud computing.

1.2.2 Les modèles de services

Une infrastructure cloud repose sur un principe architectural en couche : une couche physique et une couche d'abstraction. La couche d'abstraction, composée de ressources logicielles déployées sur les ressources physiques (couche physique), permet de fournir différents types de services. En fonction des services proposés, les infrastructures cloud sont classées en trois principaux modèles de services illustrés sur la figure 1.1 et décrits ci-dessous :

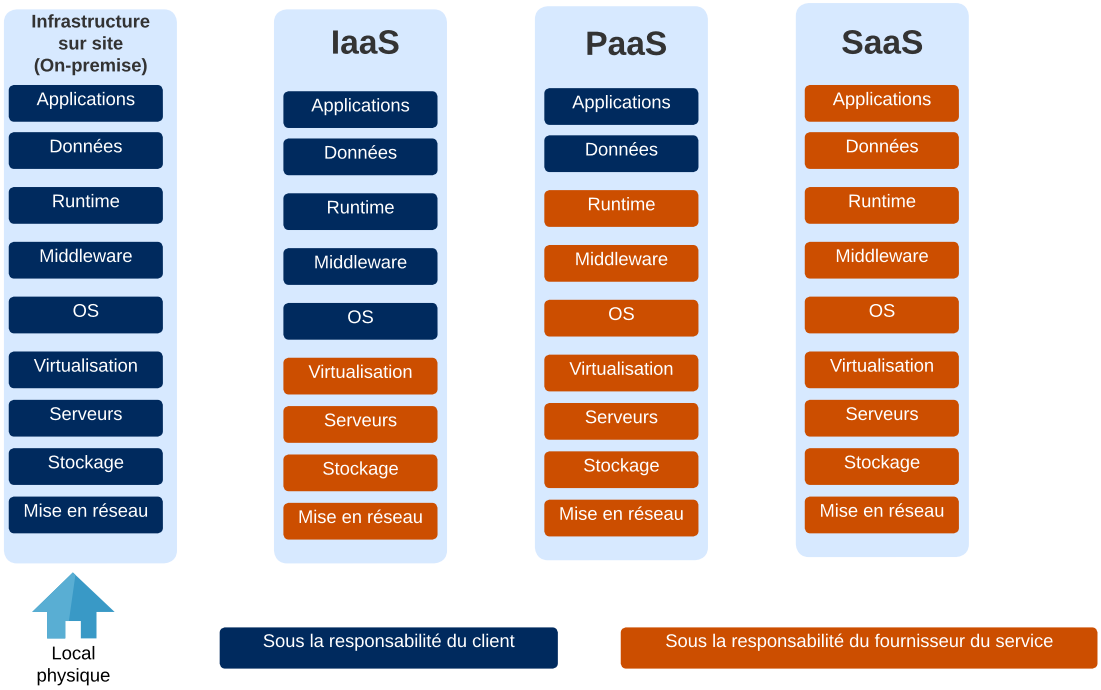


FIGURE 1.1 : Les modèles de services cloud

- **L'Infrastructure en tant que Service (IaaS)** : les ressources fournies aux clients dans ce modèle sont des serveurs (machines virtuelles), de la puissance de calcul, des espaces de stockage, des services réseaux et bien d'autres. Toute l'infrastructure physique sous-jacente est à la charge du fournisseur de service et le client est chargé de l'installation, de la configuration, de la gestion des systèmes d'exploitation et de la location du service (voir figure 1.1). Plusieurs fournisseurs de service IaaS existent dont les acteurs majeurs sont *Amazon Web Services (Amazon EC2)*, *Microsoft Azure (Azure IaaS)* et *Google Cloud Platform (Google Compute Engine - GCE)*. Les usages courants de ce type de service concernent l'hébergement des sites Internet, le stockage, la sauvegarde de données et la migration d'une infrastructure sur site vers le cloud.
- **Plateforme en tant que Service (PaaS)** : ce modèle permet de mettre à la disposition des utilisateurs de service cloud des environnements complets de développement de logiciels (versionnage de code source, outils de test, procédure de déploiement en production, etc.). Dans ce modèle, la gestion de l'infrastructure, les middlewares et bases de données relèvent du fournisseur de service, contrairement à la conception et à la maintenance des applications qui sont à la charge du client (voir figure 1.1). les plateformes *Heroku* et *Amazon RDS* sont des exemples de service PaaS.
- **Logiciel en tant que Service (SaaS)** : des applications « prêtes à l'emploi » et hébergées sur le cloud sont fournies aux clients à travers ce modèle. Le client souscrit à un abonnement généralement mensuel pour utiliser le service plutôt qu'une licence comme auparavant. Il n'a aucun contrôle sur l'infrastructure et la plateforme de développement du logiciel qui sont gérées par le fournisseur de service cloud (voir figure 1.1). Les produits comme *Office 365*, *Salesforce* sont des exemples de services SaaS.

1.2.3 Les modèles de déploiements

Selon le mode de gestion et de configuration de l'infrastructure cloud, quatre modèles de déploiement de cloud sont définis par le NIST [150] :

- **Cloud public** : il représente le modèle de déploiement le plus utilisé. Toute l'infrastructure informatique est la propriété d'un fournisseur de service cloud tel que *Microsoft Azure*, *Google Cloud Platform (GCP)*, *Amazon Web Services (AWS)*, etc. Le cloud public permet ainsi de mettre à la disposition du grand public des ressources dans un format de paiement à l'usage. Toutefois, l'infrastructure est sous le contrôle total du fournisseur, d'où la dépendance des utilisateurs vis-à-vis de celui-ci.
- **Cloud privé** : destiné à un usage exclusif d'une entreprise ou organisation, la gestion de cette infrastructure peut être assurée par l'organisation ou confiée à un fournisseur de service cloud. Ce modèle permet à l'organisation et à ses utilisateurs d'avoir un contrôle total sur leurs données. Cependant, l'adoption de ce modèle est relativement coûteuse pour les entreprises.
- **Cloud communautaire** : ce modèle permet à un ensemble d'organisations ayant des intérêts communs et des exigences élevées en termes de sécurité et de réglementations d'accéder aux différents services clouds. Il est soit fondé sur une gouvernance commune des organisations de la communauté, ou est géré par un prestataire tiers choisi par ceux-ci. Ainsi, les coûts de déploiement sont réduits, car partagés entre les organisations membres.

- **Cloud hybride** : ce type d'infrastructure est composé d'une partie privée établie à partir d'un cloud privé ou communautaire et d'une partie publique fondé sur un cloud public. Cette combinaison permet une migration progressive d'une infrastructure sur site (on-Premise) vers le cloud et de la flexibilité dans la gestion des ressources en fonction des législations et des réglementations. Cependant, l'administration de toutes ces différentes infrastructures est complexes.

  La figure ci-dessous 1.2 présente le cloud computing, ses modèles de services et de déploiements, ainsi que les principaux acteurs.

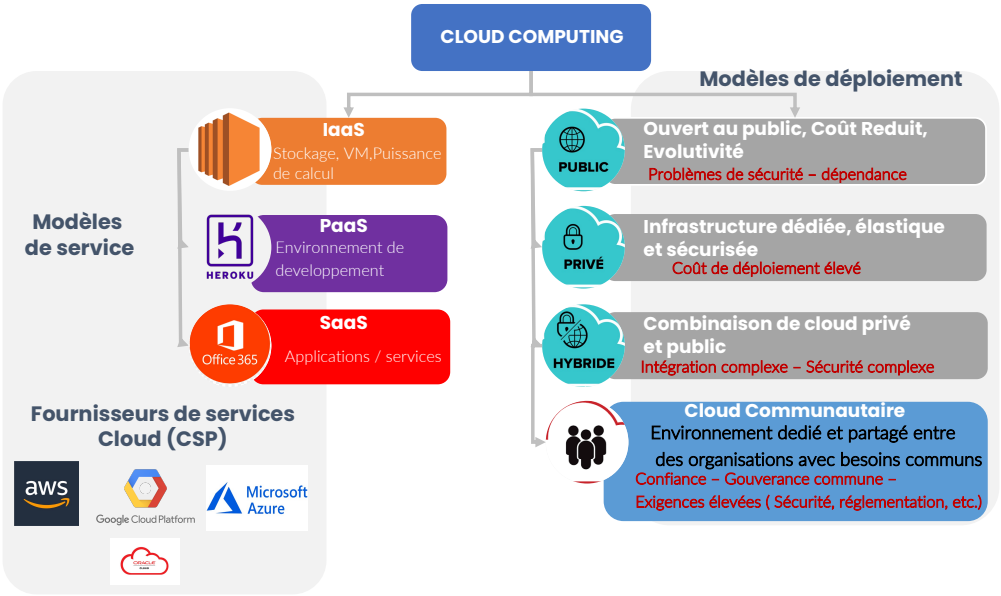


FIGURE 1.2 : Vue d'ensemble des modèles de services, de déploiements et des principaux fournisseurs de services cloud

1.2.4 Problèmes de sécurité dans le Cloud

Le cloud computing offre de nombreux avantages aux utilisateurs (entreprises, particuliers) et fournisseurs de service cloud : réduction des coûts, robustesse, élasticité, accessibilité, travail collaboratif, revenus financiers importants, etc [50]. Cependant, plusieurs facteurs freinent son adoption [16]. Parmi ceux-ci, la sécurité dans le cloud demeure l'une des préoccupations majeures selon Cloud Security Alliance (CSA) [53][52]. Ces défis sécuritaires concernent aussi bien les données, les applications et les infrastructures physiques sous-jacentes [10]. Un rapport sur les menaces de sécurité dans le cloud, réalisé auprès de 700 experts par le CSA et paru en 2022, met en exergue divers risques de sécurité. Les travaux de ce groupe de travail ont révélé que les menaces sont liées au modèle de services, à l'architecture, à la responsabilité de l'utilisateur, du fournisseur ou d'une responsabilité partagée. Les onze principales menaces identifiées sont [54] :

- Gestion insuffisante des identités, des références, des accès et des clés.
- Interfaces ou API (Application Programming Interface) non sécurisées.
- Mauvaise configuration et contrôle inadéquat des changements.
- Absence d'architecture et de stratégie de sécurité cloud.
- Développement de logiciels non sécurisés.

- Ressources tierces non sécurisées.
- Vulnérabilités du système.
- Divulgation accidentelle de données dans le cloud.
- Mauvaise configuration et exploitation des charges de travail sans serveur et des conteneurs.
- Criminalité organisée/ Hackers
- Exfiltration de données stockées dans le cloud.

Par ailleurs, les problèmes de dépendances vis-à-vis des fournisseurs, de transparence dans la localisation et l'utilisation des données des utilisateurs, de conformité à la réglementation et la confiance entre utilisateurs et fournisseurs constituent d'importantes sources de risques de sécurité.

1.3 Collaboration et partage de données dans les environnements cloud

1.3.1 Utilisation croissante des systèmes de collaboration

Un système de collaboration met en relation deux ou plusieurs parties autour d'une activité et propose une réponse commune de ces entités à une problématique, sur la base de leurs compréhensions respectives du problème et de leurs capacités [140]. Les interactions peuvent avoir lieu entre des entités situées sur le même site ou dans des environnements différents. Ils consistent à rassembler et à associer des données provenant de diverses sources pour obtenir des informations utiles pour la réalisation de projets ou la proposition de nouveaux services.

Plusieurs formes de collaboration sont proposées, allant du travail en équipe dans les entreprises à l'établissement d'alliances stratégiques (consortium industriel, coentreprises, fusion, etc) afin d'accroître la compétitivité de ces organisations [57]. Différents facteurs sont à l'origine de cette diversité des pratiques de collaboration. En effet, l'évolution vers l'agilité dans les collaborations nécessite le fractionnement des projets et des équipes engagées en de micro projets composés de membres en permanente liaison. Cette approche fournit un cadre qui a une influence sur la capacité des entreprises à créer, à proposer de nouvelles offres, faisant de la collaboration une composante essentielle à toute innovation et un pilier à la réussite d'une entreprise. Par ailleurs, l'épidémie récente de COVID-19 causée par le coronavirus a eu un impact significatif sur la société en général et sur le mode de fonctionnement des entreprises. Les employés de ces organisations sont de plus en plus mobiles et enclins à travailler hors des locaux de leur structure. Cette croissance de l'adoption du télétravail et de l'utilisation d'Internet a pour conséquence d'accroitre les besoins en termes de partage de données, ainsi que le volume de données généré par diverses sources et les technologies associées [9]. Le cloud computing grâce à sa flexibilité et sa capacité à fournir des services à la demande via Internet, a été un des acteurs majeurs ayant contribué à la résilience des entreprises face au confinement et difficultés économiques causées par la COVID-19.

Un environnement collaboratif est principalement un contexte multi-acteurs dans lequel diverses entités collaborent pour la réalisation d'objectifs communs et convergents. L'idée principale d'une collaboration se fonde sur le partage de tâches et l'échange d'informations et de ressources entre différents acteurs. Ces acteurs peuvent être issus de multiples domaines de compétences, ce qui nous permet de le qualifier d'environnement hétérogène. L'évolution des systèmes informatiques a permis de faciliter la colla-

boration, en banalisant les contraintes de mobilité et de communication. Cela a permis d'élargir le périmètre de collaboration afin de maximiser le rendement et l'efficacité du travail collaboratif. Cependant, la réussite de la collaboration exige une bonne gestion et une synchronisation des activités au sein du système. L'un des piliers de cette bonne gestion réside dans la capacité des entités collaboratives à s'adapter aux changements permanents. Une entité collaborative peut être active (un acteur humain ou un logiciel) ou bien passive (une ressource). Les réseaux sociaux sont l'une des évolutions les plus récentes et les plus riches des environnements collaboratifs. Toutefois, le challenge d'une bonne gestion au sein d'un environnement collaboratif est accentué quand on rajoute à ce dernier le caractère social.

1.3.2 Collaboration et partage de ressources dans le cloud computing

L'émergence du cloud a favorisé le développement de divers outils de travail collaboratif et des moyens de partage de données, services et applications. La collaboration dans le cloud permet aux employés d'une organisation, ainsi qu'à des entreprises autonomes, de travailler simultanément sur des projets, des applications et de se partager des données hébergées dans le cloud [58]. Plusieurs outils permettent ainsi aux utilisateurs d'interagir en temps réel, de communiquer, créer, modifier, consulter des ressources et d'en donner l'accès à d'autres utilisateurs internes ou externes à l'entreprise. La collaboration dans le cloud contribue à une augmentation significative de la productivité de l'entreprise. De plus, elle permet d'augmenter l'efficacité des employés, d'améliorer le suivi, la coordination des projets et la communication entre les entités. Les outils de collaboration proposés présentent diverses fonctionnalités, notamment :

- **le partage, la modification et le stockage de document** : Microsoft Office 365, WeTransfer, Dropbox, Google Docs, etc. ;
- **la visioconférence, Web conférence, communication d'équipe** : Microsoft Teams, Zoom, Skype, Cisco Webex, etc. ;
- **la gestion de projet (suivi, planification, etc.)** : Trello, Kanban, etc.
- **les environnements de développement d'applications et de versionning de code source)** : GitHub, GitLab, Bitbucket, etc.

Outre les avantages (efficacité, communication temps réel, etc.), la collaboration dans le cloud doit faire face à plusieurs défis de sécurité. En effet, un cadre de collaboration virtuel doit fournir les mêmes garanties de confidentialité, de disponibilité des ressources et moyens de partage que les environnements physiques de collaboration existants auparavant dans les entreprises. La possibilité offerte aux employés de travailler à distance hors des locaux de l'entreprise sur des dispositifs personnels (téléphone, ordinateurs, etc.) exposent ces utilisateurs et les ressources de l'organisation à divers types d'attaques informatiques. De plus, la pluralité des outils de collaboration augmente le risque d'utiliser des applications avec des failles de sécurité ou n'ayant pas appliqué les dernières recommandations en matière de politique de sécurité. Par ailleurs, en raison des règles de protection des données et de la vie privée, le caractère opaque et non transparent de la prestation des fournisseurs de cloud public demeure un sujet d'inquiétude et d'interrogation pour les organisations concernant la localisation, l'intégrité et la confidentialité de leurs données. Face à cette situation, les organisations vont se tourner vers des modèles de cloud souverain et de confiance qui fournissent des garanties en termes de conformité, de sécurité de leurs données et un meilleur un cadre de collaboration, de partage de ressources et de propositions de nouveaux services (Téléphonie 5G, IA, IoT, etc.) [129].

Toutefois, il est important de se questionner sur le choix du modèle de déploiement de cloud souverain pour les organisations qui exercent dans des domaines hautement réglementés (banques, finances, gouvernements, armées, industriels, etc.) et qui ont des exigences élevées en termes de sécurité. En effet, les avantages offerts par le cloud public (flexibilité, évolutivité, coûts relativement bas) sont rétrogradés au second plan par le manque de confiance accordée aux fournisseurs et de transparence de l'infrastructure. Par ailleurs, le déploiement d'un cloud privé, bien qu'il permette le plus grand contrôle sur les données et la gestion du système, exige un temps significatif, des coûts élevés et des compétences en ressources humaines. L'autre option à envisager est le cloud hybride, constitué d'une partie des ressources hébergées sur le cloud public et l'autre segment représenté par un cloud privé propre à l'organisation ou l'infrastructure sur site de cette dernière. Mais, pour les organisations fortement réglementées et strictes en matière de sécurité, recourir à un cloud privé demeure coûteux et peut ne pas être financièrement bénéfique d'une part et d'autre part, trop risqué d'utiliser les services de cloud public [144]. Le choix parfait serait d'opter pour une solution qui intègre les avantages d'un cloud public et les exigences de sécurité d'un cloud privé. Le cloud communautaire se présente alors comme l'allié idéal pour collaborer avec confiance et partager des ressources de façon sécurisée dans le cloud.

1.3.3 Collaboration et partage de ressources dans le cloud communautaire

1.3.3.1 Définition et avantages

Le cloud communautaire (3C) permet de regrouper au sein d'une communauté un ensemble d'organisation ayant des exigences (sécuritaire, juridique, etc.) et des besoins communs [144]. Le 3C vise à favoriser le partage, la mutualisation des ressources, améliorer la sécurité de l'infrastructure et de réduire les coûts d'investissement [72]. Les organisations échangent leurs ressources supplémentaires, inutilisées ou en proposent en fonction des besoins exprimés par les membres de la communauté. Chaque organisation peut fournir ou solliciter différents types de ressources matérielles ou logicielles : des machines virtuelles, des espaces de stockages, de la puissance de calcul, des applications, des données, etc. Plusieurs organisations de différents domaines (banques, institutions gouvernementales, etc.) ont déjà misé sur des infrastructures de cloud communautaire. À titre d'exemple, on peut citer : « Amadeus » pour les compagnies aériennes, « Cmed » destiné à l'industrie pharmaceutique [155], « Le projet Bleu » proposé par le gouvernement français [46]. Un cloud communautaire peut ainsi être créé pour tous les secteurs ou domaines spécialisés partagés par plusieurs entreprises. Du point de vue architectural, on distingue deux types de cloud communautaire : le modèle fédéré et le modèle basé sur un tiers de confiance. Dans le modèle fédéré, les acteurs partagent leurs ressources avec leurs pairs à la demande. Dans le tiers de confiance, « le brocker» sert d'intermédiaire entre les membres afin de garantir le bon fonctionnement de la communauté. Comme illustré à la figure 1.3 ci-dessous, un 3C pour le secteur agricole pourrait fournir des services pertinents avec des exigences spécifiques (commandes de semences, rotation des cultures, investissements des acteurs, techniques de gestion des sols, exposition de produits, etc.) et un niveau de sécurité requis (authentification, confidentialité, sécurité des communications, protection des données, protection contre le déni de service, traçabilité de la chaîne de production, etc.) pour les agriculteurs et les coopératives. Par ailleurs, d'autres acteurs, comme les chambres d'agriculture, les investisseurs et agents de l'État, pourraient avoir un accès complet ou limité à cette plateforme et ses ressources. Ces collaborations entre organisations permettent de répartir les coûts de déploiement et de gestion de l'infrastructure, et ainsi réduire les frais supportés par chaque entité. De plus, cela permet de générer plus de revenus et d'as-

surer une gouvernance commune, auditable et transparente. Par ailleurs, le 3C permet de répondre aux préoccupations des organisations membres en termes de localisation et de politique de sécurité commune de l'infrastructure. Le principe du cloud communautaire permet de préserver et de défendre les intérêts en adoptant une approche qui s'adapte aux spécificités et aux besoins du domaine d'activité [144].

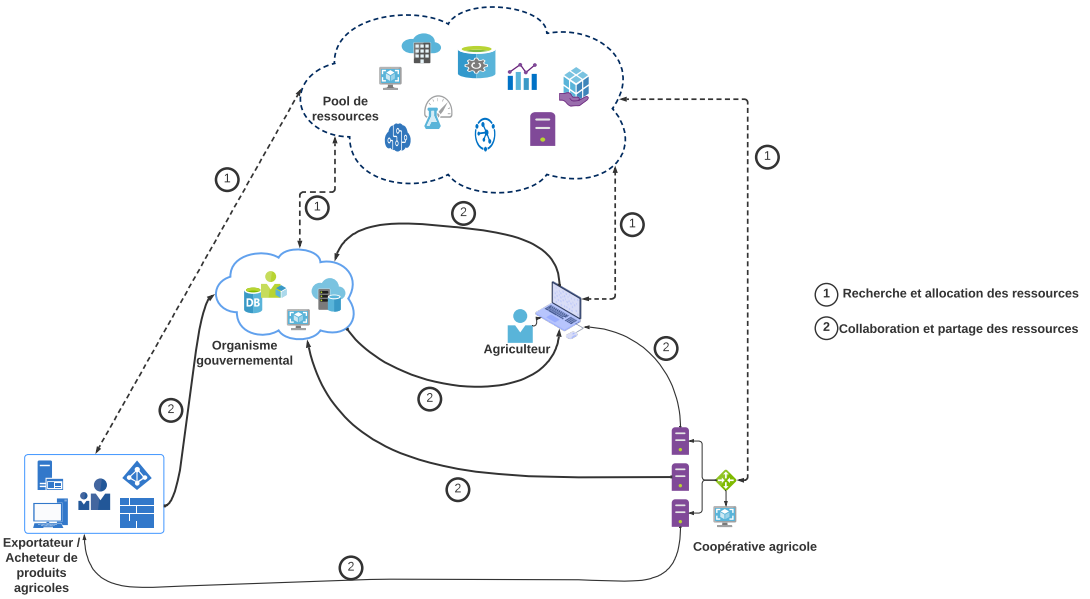


FIGURE 1.3 : un cloud communautaire pour le secteur agricole

1.3.3.2 Modèle d'engagement et de gouvernance

Le choix du modèle de gouvernance est déterminant pour la réussite d'une infrastructure de cloud communautaire. Plusieurs possibilités s'offrent aux organisations. Ainsi, la gestion de l'infrastructure peut être déléguée à une organisation tierce faisant office de fournisseur de service cloud, en qui les membres de l'organisation accordent une entière confiance. Dans ce cas, les ressources de la communauté sont hébergées sur l'infrastructure de cette organisation. Une autre option de gouvernance consiste en une gestion commune assurée par toutes les entités membres de la communauté par le biais d'un consortium. Le succès de l'infrastructure dépend du respect des engagements pris et de la responsabilité de chaque partie, peu importe le modèle choisi [144]. Le cloud communautaire peut être utilisé dans divers contextes, tels que les projets d'innovation, d'expérimentations, de développement et tests d'applications. En outre, il peut être un cadre de réflexion, de développement de compétences et de création de nouveaux services pour les entreprises engagées. Des domaines en pleine expansions telles que l'Internet des objets, l'analyse de gros volumes de données peuvent être associés au cloud communautaire afin d'élaborer des solutions pour des secteurs à haut risques tels que la cybersécurité, le nucléaire, etc.

1.3.3.3 Exigences des systèmes collaboratifs centrés sur la communauté

Les exigences ci-dessous constituent des éléments de base essentiels dans la conception d'un système de collaboration entre des organisations centré sur la communauté. La prise en compte de ces exigences permet de fournir une infrastructure prospère, durable et avec un niveau d'adoption élevé.

- **Exigences spécifiques au secteur** : la prise en compte des exigences spécifiques des membres de la communauté est un gage d'acceptabilité, de pérennité et de croissance économique.
- **Évolutivité, autonomie des organisations et flexibilité** : la communauté doit garantir l'indépendance et l'autonomie de ses membres tout en préservant leurs intérêts. La flexibilité dans l'intégration de nouveaux membres et de départ est d'une importance capitale. L'un de ces évènements ne doit pas influer sur le fonctionnement normal de la plateforme.
- **Ouverture, hétérogénéité, interopérabilité** : la communauté doit être ouverte sans autorité centrale, hétérogène et interopérable.
- **Sécurité, confidentialité et confiance** : l'infrastructure doit intégrer ou présenter des outils/ mécanismes garantissant la protection et la confidentialité des ressources partagées, la confiance entre les organisations et envers l'organisation.
- **Transparence, surveillance et auditabilité** : il est très important d'avoir des règles claires et transparentes sur le fonctionnement de la communauté, de la localisation précises des données et des outils de surveillance et d'audit de l'infrastructure. Les organisations doivent être associées à la définition des règles de sécurité, de surveillance, d'audit et de transparence de la communauté.
- **Caractère social, multipartite et multi-tenant de la communauté** : l'infrastructure est constituée de diverses organisations fournissant des ressources variées. Elle est fondée sur une structure sociale avec en ligne de mire les intérêts des membres. Elle doit être évolutive et rentable économiquement pour ses membres.
- **Disponibilité et résilience aux pannes** : l'infrastructure doit être robuste, résilientes aux pannes et disponibles afin de répondre aux besoins des différents acteurs. La défaillance d'un nœud ne doit pas avoir d'incidence sur toute l'infrastructure.
- **Rentabilité, productivité** : le système doit être bénéfique, productif et doit favoriser la rentabilité économique de ses membres à travers des mécanismes équitable. Il peut s'appuyer sur des échanges prenants en compte le caractère social de la communauté (systèmes de troc, monnaie communautaire, etc.).
- **Durabilité environnementale** : l'utilisation et le partage de ressources sous-utilisées ou inutilisées entre organisations favorisent une réduction et des économies en termes de consommations énergétiques.
- **Identification et qualité des ressources** : l'identification des ressources est un moyen de garantir une gestion optimale et une classification qualitative de ces dernières. La surveillance de la qualité des ressources est un gage de pérennité et permet de garantir la confiance entre les acteurs, la disponibilité et la diversité des ressources proposées et le respect des accords de niveau de service.
- **Mécanismes d'incitation** : la durabilité de l'infrastructure dépend de la participation active des acteurs. Des mécanismes d'incitation doivent être mis en place dans le but d'encourager les membres à échanger des ressources.

1.3.3.4 Spécificités et exigences sécuritaires d'un cloud communautaire

Le cloud communautaire procure les avantages du cloud public (coûts réduits, flexibilité, etc.) et apporte les réponses aux exigences de sécurité offertes par un cloud privé (propriété exclusive, contrôle de l'infrastructure et confidentialité des données, etc.) [144]. Ce modèle est principalement axé sur le partage et la réutilisation des res-

sources, une gouvernance commune des organisations, et la proposition de fonctionnalités adaptées aux exigences d'offres de service et de performances. Néanmoins, dans un contexte très compétitif, certaines organisations sont réticentes à partager ou à établir des partenariats en raison de l'absence de garanties nécessaires. En outre, le cloud communautaire hérite des problèmes de sécurité du cloud en général (protection des données, confidentialité, intégrité) [198] et fais face à des défis propres à ses caractéristiques, en occurrence : l'identification et l'authentification des organisations, la confiance entre elles, le maintien de leur autonomie, la transparence dans la gouvernance (souplesse dans l'intégration et le départ de membres), l'incitation à la collaboration et le suivi des accords de niveau de service [144]. Des politiques et des stratégies de sécurité répondraient à ces questions, et ainsi proposer des communautés d'organisation bâties autour de cloud communautaire de confiance, sécurisé et transparent.

1.4 Mécanismes et stratégies de sécurité dans le cloud

La sécurité des systèmes d'information en général et en particulier des infrastructures cloud est un enjeu capital pour le monde informatique. Un fait justifié par la croissance des menaces de sécurité, la récurrence et la diversité des cyberattaques. Ainsi, différentes solutions et mécanismes de sécurité sont proposés par les acteurs du secteur. Les mesures proposées reposent principalement sur des techniques de virtualisation, des pare-feu physiques et logiques, des réseaux privés virtuels (VPN), des systèmes de détections (IDS) et de prévention d'intrusions(IPS) [28]. Toutefois, le véritable défi pour les responsables de sécurité informatique, demeure la mise en place de stratégies fiables établies à partir de ces techniques et en conformité avec les objectifs de l'organisation. Ces stratégies doivent être fondées sur des politiques de sécurité qui traduisent la vision globale des instances dirigeantes en termes de règles de sécurité et de plan d'action pour garantir un niveau élevé de sécurité [196]. Les politiques de sécurité sont la matérialisation de l'importance accordée par la direction générale à la protection des données et à la sécurité du système d'information de l'entreprise. Face à cette problématique, les experts de la cybersécurité ont proposé une démarche intégrant l'incertitude et la vigilance en superposant les différentes mesures de sécurité citées ci-dessus dans des systèmes de défenses proactives et réactives contre les cyberattaques [124]. Cette approche appelée défense en profondeur (Defense in Depth) s'appuie sur des pratiques de défense militaire contre les cybermenaces [109][68].

1.4.1 La défense en profondeur dans le cloud computing

1.4.1.1 Définition

Selon les historiens, la première référence à la notion de « défense en profondeur » remonte à l'an 2900 avant Jésus-Christ à Hierakonpolis en Égypte. Ce terme est originaire du domaine militaire et consiste à mettre en place un système de défense de territoires composé de barrières indépendantes et de troupes [86]. L'objectif de cette stratégie est de se protéger de l'ennemi grâce à plusieurs obstacles et points de défense successifs pour l'affaiblir et freiner son avancement. Cette technique a été reprise et a ensuite été appliquée dans les domaines du nucléaire et de la sécurité des systèmes d'information. Dans le monde de la cybersécurité, la défense en profondeur (DEP) est une démarche qui consiste à superposer plusieurs mécanismes de sécurité informatique offrant une protection redondante, globale, dynamique et de qualité du système d'information [68]. Avec cette approche composée de plusieurs couches de sécurité, l'échec d'une mesure sécurité fait place à une autre, renforçant la capacité à résister et à neutraliser différents types d'attaques. D'où son appellation « approche forteresse » en comparaison

des systèmes de défense déployés dans les châteaux à l'époque médiévale [124]. À titre d'exemple, la défense en profondeur de Vauban dans la baie de Saint-Malo illustrée à la figure 1.4 et celle du château de Fougères représentée à la 1.5 [73].

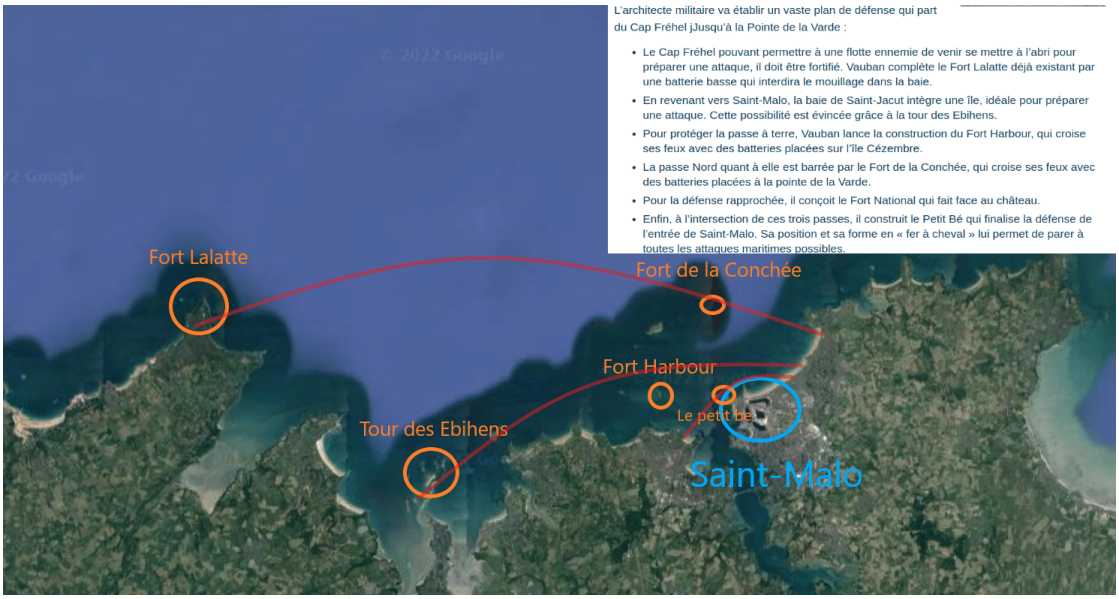


FIGURE 1.4 : La défense en profondeur de Vauban dans la baie de Saint-Malo[73]

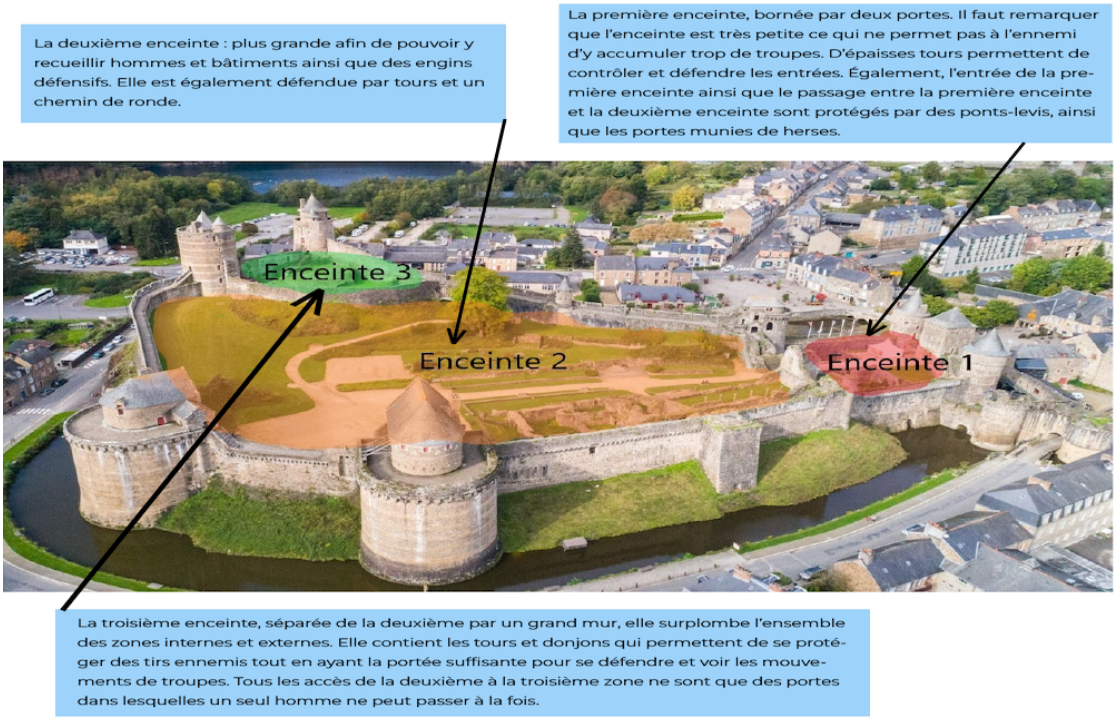


FIGURE 1.5 : Les différentes enceintes défensives du château de Fougères[73]

1.4.1.2 La défense en profondeur dans les systèmes informatique

Le concept de défense en profondeur dans les systèmes informatique est fondé sur des principes spécifiques [68]. En effet, la défense déployée dans cette démarche doit être :

- **Globale** : elle doit considérer autant les aspects organisationnels, techniques que la mise en œuvre.
- **Cordonnée** : les outils utilisés sont capables d'alerter et de diffuser en réponse à plusieurs incidents liés entre eux.
- **Dynamique et suffisante** : elle doit être proactive, avec un plan d'action précis, bien planifié, avec une classification des niveaux de gravité.
- **Complète** : elle doit intégrer au moins trois lignes de défense, proposer une protection des ressources en fonction de leur criticité et une traçabilité des évènements survenus.
- **Démontrée** : elle doit être homologuée et validée en conformité avec les objectifs du système d'information. Par ailleurs, elle dispose d'un niveau de qualification.

L'application d'une démarche de défense en profondeur établie sur la base des principes énumérés ci-dessus se déroule en cinq étapes principales [68] présentées dans la figure 1.6 ci-dessous.

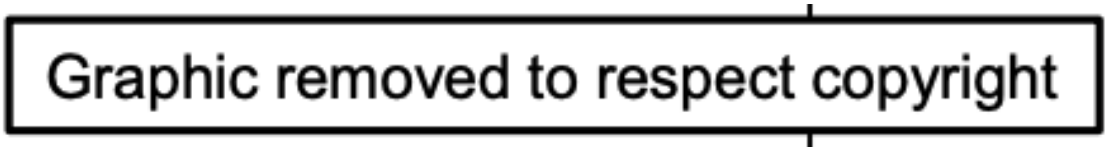


FIGURE 1.6 : Les étapes de la défense en profondeur[68]

La première étape concerne l'identification des ressources et des objectifs de sécurité. Elle permet, à travers une analyse des ressources et des risques de sécurité, de classifier les ressources en fonction de leurs niveaux de criticité. En définitive, cette étape propose une échelle de gravité pour classer les incidents de sécurité selon leur impact sur chaque ressource et sur le système d'information. La deuxième étape consiste à identifier les nœuds les plus vulnérables du système ainsi que les mesures de sécurité à appliquer aux différentes lignes de défense entre la ressource protégée et la source de menace. Cette opération permet de déterminer la profondeur du dispositif, d'établir un répertoire des mesures prises, de modéliser les systèmes critiques afin de les évaluer et de fixer les incidents sur l'échelle de gravité proposée à la première étape. La troisième étape décrit l'élaboration de la politique de défense. Elle est subdivisée en deux phases : une consacrée à la détermination de défense globale (identification des points de contrôle, détection des attaques, alerte, remontée des incidents, etc.) et une autre axée sur la planification (plans de réactions, reconfiguration, etc). La quatrième étape permet de valider l'organisation et l'architecture à travers la qualification de la défense en profondeur. Il s'agit, d'abord, de vérifier le respect des principes généraux

de la défense en profondeur et de sa formalisation en conformité avec les objectifs de l'organisation. Ensuite, évaluer la cohérence du système dans une approche démonstrative à travers des études de cas. La cinquième étape a pour objet l'évaluation à la fois permanente et périodique du système de défense. C'est la phase d'audit et de contrôle. Elle permet de présenter à l'instance dirigeante, l'approche utilisée pour satisfaire les besoins de sécurité du système énumérés à la première étape. Et, d'en déduire une décision d'homologation et de reconnaissance de la capacité du système à gérer des données d'un niveau de sensibilité donné. Cependant, l'homologation du système est dynamique et demeure en accord avec les objectifs et l'évolution du système [68].

1.4.1.3 La défense en profondeur pour le cloud computing

Le recours aux services cloud computing a pour effet de bouleverser les habitudes de gestion des systèmes d'information en général, et en particulier les politiques de modèles de sécurité traditionnels des entreprises. Les organisations doivent ainsi adapter leurs stratégies de défense en profondeur pour assurer la protection des données et services dans le cloud. Par ailleurs, elles doivent se défendre contre les nouvelles attaques et les utilisateurs malveillants découlant des nombreux projets de digitalisation. En conséquence, l'application des principes de la défense en profondeur nécessite une identification claire et précise des vulnérabilités et menaces auxquelles sont exposés les ressources cloud et les différentes mesures de sécurité à appliquer. En outre, une maitrise du lien entre ces risques, les actions à mener, la capacité des infrastructures cloud et la responsabilité de chaque acteur (utilisateurs et fournisseurs de service cloud) est primordiale pour disposer d'un système de défense optimal [109]. La figure 1.7 montre les concepts clés et les relations entre les composants de la défense en profondeur dans le cloud computing.

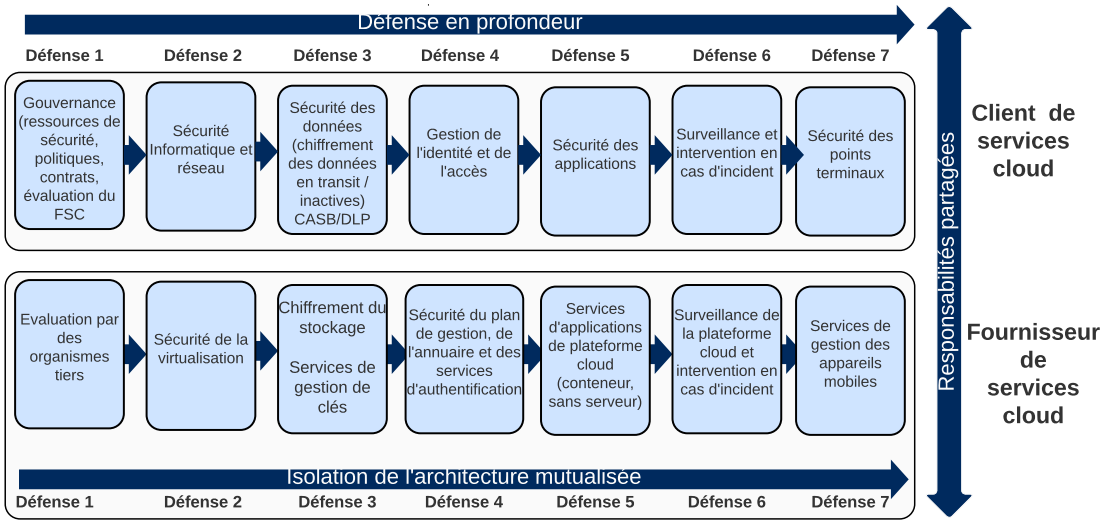


FIGURE 1.7 : Les composants de la défense en profondeur dans le cloud[109]

Trois composants essentiels se dégagent de cette architecture modulaire de la défense en profondeur dans le cloud : la responsabilité partagée, l'isolation des infrastructures mutualisées et les points de défense.

- **La responsabilité partagée** : une infrastructure cloud fait intervenir deux types d'acteurs principaux : un utilisateur ou consommateur de service cloud(CSC) et un fournisseur de service cloud (FSC). En fonction du modèle de déploiement, une entreprise peut-être soit utilisatrice de service cloud (cloud public), soit four-

nisseur de service cloud (cloud privé). La responsabilité partagée fixe les responsabilités des utilisateurs et des fournisseurs de services cloud en matière de sécurité et de conformité des infrastructures cloud [172]. Les tâches de sécurité de chaque entité varient en fonction du modèle de service. La figure 1.8 résume les responsabilités respectives du fournisseur et des utilisateurs en fonction du modèle de service.

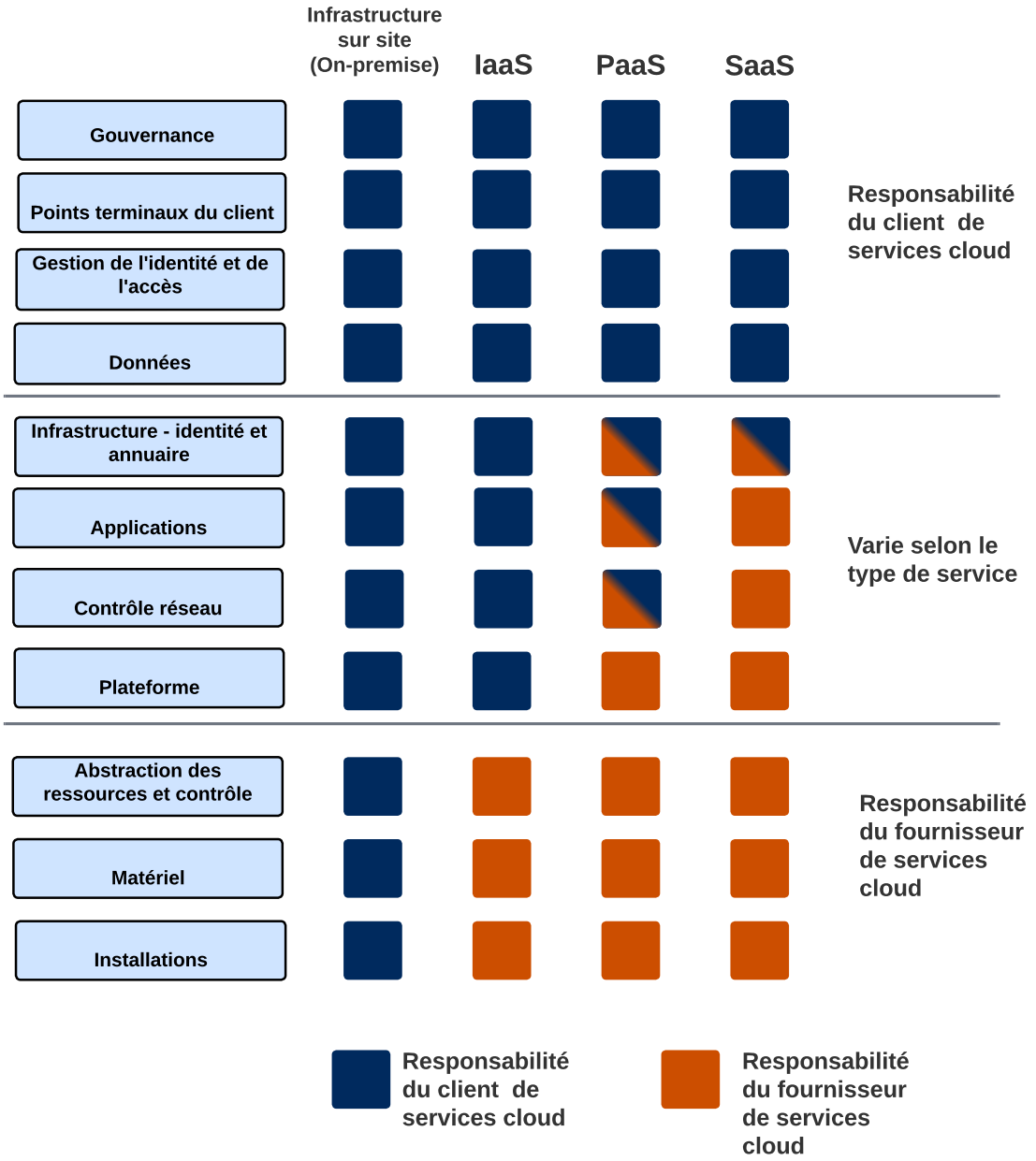


FIGURE 1.8 : Responsabilités partagées et défense en profondeur[109]

Ainsi, le fournisseur de service cloud est généralement responsable de :

- la sécurité de l'infrastructure physique et réseau ;
- la sécurisation des API et des applications ;
- la virtualisation des ressources physiques ;
- la gestion des identités, des authentifications et du contrôle d'accès aux données ;

- la sécurisation des données stockées (chiffrement, gestion des clés, etc.).

Concernant les utilisateurs (particuliers, organisations), ils ont la responsabilité de mettre en place des mesures et des contrôles de sécurité des ressources à leur charge dans le modèle choisi. Ainsi, pour un service de type IaaS, l'utilisateur est chargé des configurations de sécurité des systèmes d'exploitation et utilitaires installés sur les instances, ainsi que de l'administration des groupes de sécurités sur les pare-feux. Pour les services de types PaaS et SaaS, les consommateurs ont la responsabilité entre autres de la gestion des identités, du contrôle d'accès aux données et aux applications. Afin d'appliquer efficacement et d'auditer les responsabilités communes, des accords de niveau de service (SLA) sont établis entre les clients et les fournisseurs de service de cloud [109]. Ce contrat est un moyen d'arbitrage en cas de désaccord ou de conflits sur la qualité et la sécurité des services fournis par l'infrastructure cloud.

- **L'isolation des ressources mutualisées** : l'une des caractéristiques principales du cloud est la mise en commun des ressources afin d'offrir la possibilité à plusieurs entités (locataires) de partager les coûts d'exploitation et réaliser des économies [150]. Cette architecture mutualisée ainsi offerte par le cloud doit être considérée dans l'établissement de défense de sécurité afin d'éviter qu'un nœud compromis n'affecte toute l'infrastructure et ne la rende indisponible [109]. D'où le principe d'isolation des ressources mutualisées. Cette tâche d'isolation des ressources est du ressort du fournisseur de service cloud et est un indicateur important pour qualifier le niveau de la défense de l'environnement cloud.
- **Les points de défense** :
  - *Point de défense gouvernance et gestion des risques* : ces deux concepts permettent de définir les lignes directrices (rôles, responsabilité, réglementaires, conformité) et d'attribuer des ressources de sécurité (humaines et moyens techniques) de la défense en profondeur d'une organisation. De plus, ils constituent un cadre pour la spécification de contrats de niveau service et la proposition de systèmes d'évaluation de la sécurité de l'organisation par des organismes tiers [109].
  - *Point de défense réseau* : ce point permet de déployer la politique de défense du système sur les ressources réseaux physiques et virtuels. Ainsi, des techniques de segmentation réseau sont utilisées et des règles de sécurité et de routage sont appliquées sur des pare-feu, des systèmes de détection et de prévention d'intrusion afin de se protéger contre divers types d'attaques [109].
  - *Point de défense informatique* : il concerne la configuration de la sécurité des hôtes physiques, des machines virtuelles (création d'images, mise à jour, reconfiguration, suppression, etc.), ainsi que l'automatisation et le provisionnement d'instances et de conteneurs [109].
  - *Point de défense des données* : il représente l'un des points principaux de défense dans la mesure où il vise à proposer une réponse au défi crucial de la protection des données des utilisateurs de service cloud. La démarche consiste à élaborer une stratégie de sécurisation pour des données en transit, en traitement et inactives. Ainsi, des techniques de chiffrement doivent être appliquées aux données en transit et stockées. En outre, la transparence sur la localisation des données (emplacement, réglementation), le contrôle d'accès aux données et les systèmes de réplication de données sont des moyens pour assurer la confidentialité, l'intégrité et la haute disponibilité des don-

nées [109].

- *Point de gestion de l'identité et de l'accès* : ce point permet de déterminer, pour une ressource donnée, les utilisateurs autorisés à exécuter une action donnée à une période précise et dans des conditions spécifiques. Permettant ainsi de réguler l'accès aux données, services et applications et de se prémunir contre les accès non autorisés, les violations de confidentialité et les compromissions de l'intégrité des données. La gestion de l'identité et d'accès est un processus qui consiste à proposer, au travers de fournisseurs d'identité, des services d'annuaire et d'authentification unique (SSO) ou multifacteur (MFA) permettant la création, la propagation et la suppression d'identité. Par ailleurs, l'autorisation d'accès aux ressources est réalisée grâce à des protocoles d'accès annuaire (LDAP, Active Directory) et des modèles de contrôle d'accès (RBAC, ABAC, etc.) [109].
- *Point de défense des applications* : il est relatif aux différentes mesures de sécurité du développement des applications, telles que les bonnes pratiques de codage et d'analyse des algorithmes, les tests de sécurité unitaires et fonctionnels. Par conséquent, les stratégies de développement des applications doivent être orientées sur des architectures de micro-services, intégrer des processus d'automatisation et de déploiement continu (API et pipeline sécurisé), et appliquer des droits d'accès de moindre privilège [109].
- *Point de surveillances et reprise après incident* : la stratégie de défense en profondeur doit être dynamique et proactive afin de répondre aux éventuelles menaces quotidiennes. Il convient donc de disposer d'outils de surveillance et d'actualisation de la politique de sécurité de l'organisme. Ainsi, la stratégie globale de sécurité doit inclure des ressources humaines et moyens technologiques permettant d'anticiper, réduire et éliminer les menaces et proposer des plans de reprise après sinistre sans préjudices graves pour l'organisation [109].
- *Point de défenses des points terminaux* : les dispositifs qui permettent aux utilisateurs d'accéder aux services cloud (poste de travail, appareils mobiles, etc.) doivent être considéré lors la définition des exigences et règles de sécurité. L'approche consiste à installer des patchs correctifs, des antivirus, à automatiser le déploiement des logiciels, etc.

Les stratégies de défense en profondeur permettent d'améliorer la sécurité des infrastructures informatiques. Toutefois, face à des architectures cloud de plus en plus complexes, décentralisées, dynamiques et exposées en permanence à différents types d'attaques, la défense en profondeur présente ses limites. En effet, les ressources cloud (dispositifs, applications, données) sont de diverses natures, proviennent de différentes sources et se retrouvent aussi bien sur les installations locales des entreprises que chez des fournisseurs de cloud tiers. Les approches de sécurité traditionnelles, qui consistent à l'établissement de zones sécurisées pour interdire l'accès à d'éventuels acteurs malveillants, ne sont plus appropriées. Face à cette situation, les experts de la sécurité des systèmes d'information préconisent l'adoption de la stratégie de sécurité Zero Trust.

1.4.2 Stratégie de sécurité Zero trust

1.4.2.1 Historique et principes

L'incident de sécurité lié au système d'exploitation, Commpatible Time Sharing System (CTSS) pour les mainframes IBM au sein du Massachusetts Institute of Technology (MIT) [207] et la cyberattaque de l'opération Aurora fondée sur les menaces persistantes avancées (APT) [147] ont montré les limites de la défense périmétrique dans les systèmes d'informations. En effet, ces deux attaques ont été causées par la compromission d'éléments internes au périmètre sécurisé, ce qui a eu un impact sur tout le reste de l'infrastructure. Cette situation a entraîné une prise de conscience des experts en cybersécurité. Ces derniers vont réadapter leurs stratégies de sécurité pour adopter un modèle qui considère toutes les parties du système comme potentiellement vulnérables et sources de menace, qu'elles soient à l'extérieur ou dans un périmètre précédemment désigné comme « sécurisé ». Les premières références à cette approche dénommée Zero Trust « Never Trust, Always Verify » datent du forum « Jericho» [81] et des travaux de John Kindervag [126]. Toutefois, le modèle d'architecture de sécurité BeyondCorp [212] de Google apportera les éléments fondamentaux à la standardisation du Zero Trust en 2020 [178]. Les travaux clés de l'évolution du Zero Trust sont illustrés par la figure 1.9 ci-dessous.

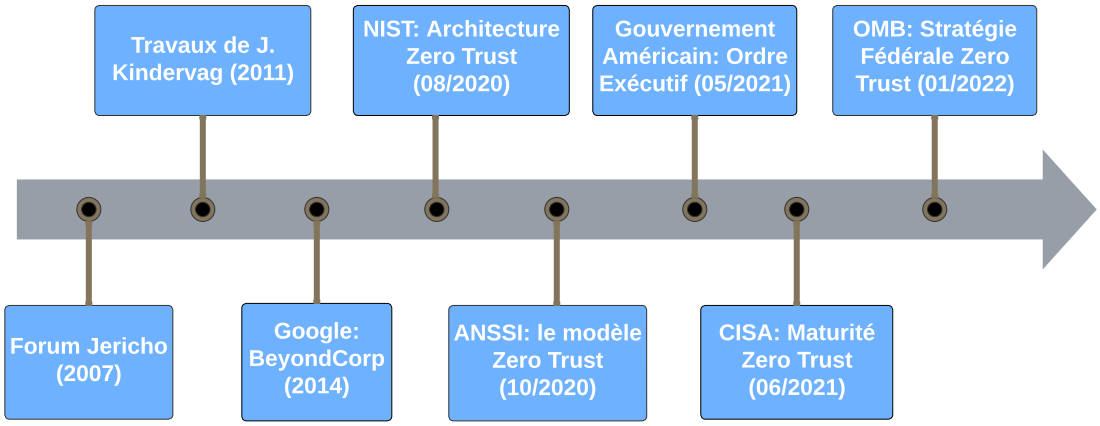


FIGURE 1.9 : Historique du Zero Trust

Le NIST défini le modèle Zero Trust ou « confiance zéro » comme une démarche fondée sur le principe que la confiance n'est accordée à aucun élément de l'infrastructure informatique et que toutes les entités doivent être soumises à un contrôle permanent, de bout en bout, grâce à divers mécanismes de sécurité (authentification, moindres privilèges d'accès, etc.). Par ailleurs, une stratégie Zero Trust repose sur sept(7) principes fondamentaux ci-dessous [178][98] :

- tous les services informatiques et les sources de données sont considérées comme des ressources ;
- toutes les communications doivent être sécurisées, quel que soit l'emplacement du réseau. Ainsi, tout le trafic réseau interne et ceux provenant de l'extérieur de l'infrastructure (Internet) doivent être soumis aux mêmes niveaux de contrôle de sécurité ;
- l'accès à chaque ressource est accordé par session. Pour une ressource donnée, le demandeur doit être authentifié et sa confiance évaluée avant autorisation d'accès sur la base de droit avec le minimum de privilèges requis pour l'action ;

- des politiques dynamiques doivent être établies sur la base de règles considérant plusieurs types d'attributs de sécurité (identification des ressources, authentification des utilisateurs, attribution de droits d'accès) et des critères contextuels précis ;
- toutes les ressources sont potentiellement considérées comme des sources de menaces. Ainsi, le niveau de sécurité de chaque ressource doit être évalué et des mécanismes de surveillance et de diagnostics doivent être déployés pour appliquer les correctifs éventuels ;
- l'authentification et l'autorisation des ressources doivent être dynamiques et systématiques avant tout accord d'accès à une ressource. Cela nécessite des systèmes de gestion d'identité et d'authentification multifactorielles (MFA) ;
- des informations sur le niveau de sécurité du système et de ses ressources doivent être collectées en temps réels afin de prévenir d'éventuelles attaques, servir de critères de déclenchement et d'amélioration de la politique globale de sécurité.

L'application de ces principes est cruciale pour la conception et le déploiement d'une stratégie Zero Trust efficace. Cependant, ils ne sont toujours pas tous mis en œuvre dans une stratégie pour une organisation donnée.

1.4.2.2 Architecture et composants logiques

L'architecture du modèle Zero Trust, proposée par le NIST [178], est constituée de plusieurs composants logiques. La figure 1.10 illustre ces composants et leurs interactions.

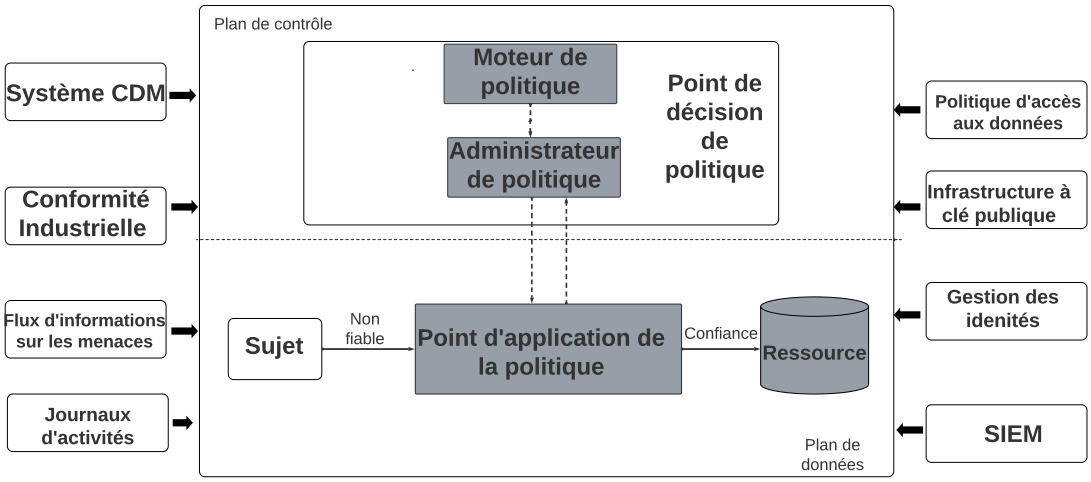


FIGURE 1.10 : Architecture Zero Trust - NIST 800-207 [178]

Les éléments de cette architecture Zero Trust sont décrits ci-dessous :

- **Moteur de politique (PE)** : il a pour rôle principal d'autoriser l'accès ou non à une ressource suite à une requête donnée. Cette décision est prise sur la base des règles et des paramètres régissant la politique de sécurité de l'organisation et des informations fournies les sources de données externes.
- **Administrateur de politique (PA)** : ce composant est chargé d'exécuter la décision d'autorisation ou de refus d'accès transmise par le moteur de politique. Il met ainsi en relation un sujet et une ressource durant une session (jeton de session, authentification, etc.). Son association avec le moteur de politique représente le point de décision de politique (PDP) de l'architecture. Toutefois, certaines im-

plémentations considèrent ces deux composants comme une seule entité.

- **Point d'application de la politique (PEP)** : il représente le nœud central et sert de passerelle de surveillance de toutes les communications (démarrage, suivi, interruption) relatives aux requêtes d'accès aux ressources. Le traitement d'une demande d'accès à une ressource débute par l'authentification du demandeur à travers un système d'authentification (authentification multifactorielle, etc.). Ensuite, le PEP communique avec le point de décision de politique (PDP) qui refuse ou valide l'accès à la ressource grâce au moteur de politique. Enfin, l'accès à la ressource est établi via l'administrateur de la politique. Les décisions prises par les composants de l'architecture et les actions qu'elles exécutent sont fondées sur les règles de politiques de sécurité, ainsi que sur des informations fournies par différentes sources de données externes et internes.

  Nous distinguons comme sources de données principales :

  - *Le système de diagnostic et d'atténuation continus (CDM)* : ce système récolte les informations de sécurité sur l'état courant des ressources sollicitées afin de les mettre à la disposition du moteur de politique pour la validation ou non de la demande d'accès. Par ailleurs, il applique les éventuelles mises à jour de configuration et des règles sur les ressources de l'organisation ;
  - *Système de conformité industrielle :* il permet de définir les règles, de surveiller et de garantir la conformité de la politique de sécurité des systèmes en fonction des normes et des exigences des systèmes d'information du domaine de l'organisation ;
  - *Flux de renseignements sur les menaces :* c'est un ensemble d'informations de sécurité (niveau de vulnérabilité, failles logicielles, utilisateurs malveillants, etc.) mis à la disposition du moteur de politique afin de faciliter la gestion des autorisations d'accès.
  - *Journaux d'activité du réseau et du système :* ces données concernent les activités telles que le trafic réseaux, l'historique des accès aux ressources, des métadonnées logicielles et bien d'autres évènements qui fournissent un diagnostic sur le niveau de sécurité courant de l'infrastructure.
  - *Politiques d'accès aux données* : il s'agit d'un ensemble de règles et de critères qui régissent les conditions d'accès aux ressources. Ces règles peuvent être définies manuellement par un administrateur ou de manière dynamique grâce au composant moteur de politique. La politique de sécurité est établie en fonction des besoins et objectifs de l'organisation et doit être en conformité avec les réglementations et lois auxquelles elle est soumise.
  - *Infrastructure à clé publique de l'entreprise (PKI) :* elle est chargée de la création, de l'attribution, du stockage des certificats et des clés d'authentification et de session émise par l'organisation à l'endroit des ressources (données, services, dispositifs, applications) et des utilisateurs. Cette gestion est assurée par une autorité de certification interne de l'organisation, qui doit être capable de communiquer avec d'autres autorités de certification extérieures si nécessaire.
  - *Système de gestion des identifiants :* c'est le fournisseur des informations d'identifications (attributs, rôles, etc.) de l'infrastructure. Il permet ainsi de créer, stocker et révoquer les comptes d'utilisateurs. Ce système peut être membre d'une fédération d'identité avec la possibilité de gérer des utilisateurs extérieurs ou diffuser les informations d'identité de ses utilisateurs à d'autres

fournisseurs d'identité.

- *Système de gestion des informations et des événements de sécurité (SIEM) :* il a pour mission de collecter les informations et les événements de sécurité de l'organisation. Par la suite, ces données sont analysées pour prévenir les éventuelles menaces et améliorer les règles de la politique de sécurité.

1.4.2.3 Stratégie Zero Trust et Cloud computing

Les principes et les composants logiques ci-dessus décrits et proposés par le NIST constituent les outils de base nécessaires à la mise en œuvre d'une architecture Zero Trust. Ils peuvent être utilisés pour la mise en place de cette stratégie de sécurité dans des infrastructures sur site (on Premise) ou de cloud computing. Plusieurs travaux ou recommandations ont été proposés pour encourager, conseiller et faciliter le déploiement de politiques de sécurité reposant sur cette démarche dans les environnements cloud. Ainsi, le 12 mai 2021, une circulaire de la présidence des États unis, visant à améliorer la cybersécurité du pays, a ordonné aux organisations fédérales de migrer leur infrastructure sur site vers le cloud et d'élaborer des plans de mise en œuvre de l'architecture Zero [101]. À la suite de ce décret, l'agence pour la cybersécurité et la sécurité des infrastructures (CISA) a publié, en juin 2021, un guide de référence pour la sécurité des environnements cloud et un modèle de maturité Zero Trust pour accompagner les agences gouvernementales dans l'adoption de cette stratégie [51]. Ce modèle présenté à la figure 1.11 repose sur cinq (5) piliers (Identité, Équipement, Réseau, Application et données) et trois niveaux de maturité. Ces niveaux de maturité sont respectivement : initial, avancé et optimal. Des mesures de protection plus strictes sont nécessaires pour passer d'un niveau à un autre [51].

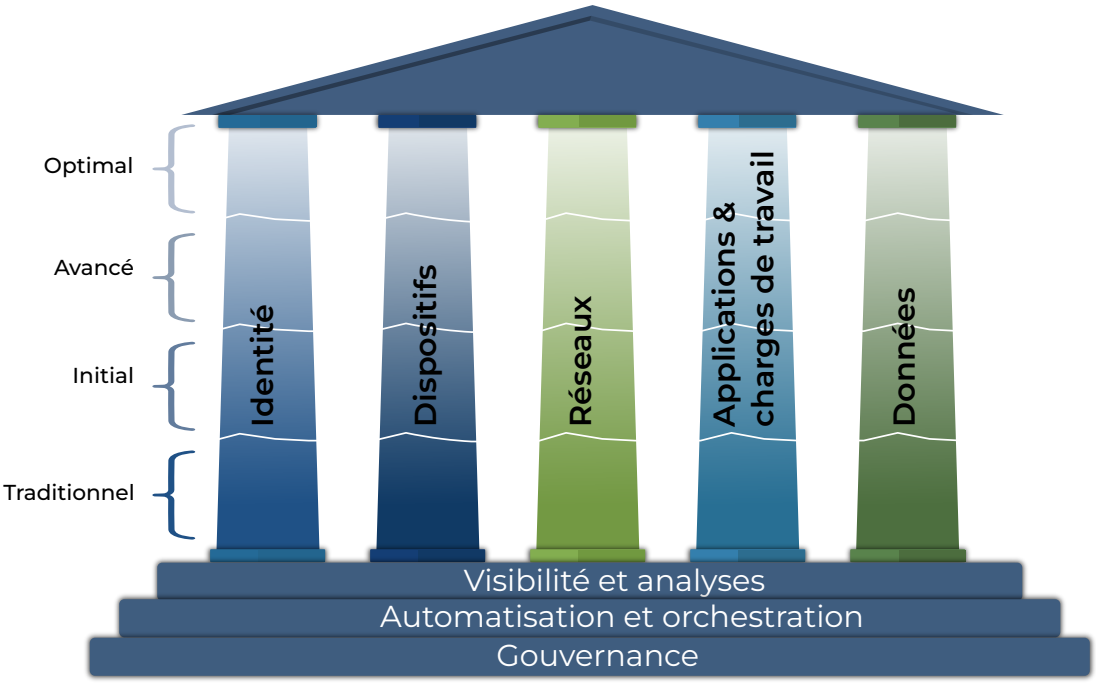


FIGURE 1.11 : Architecture modèle de maturité Zero Trust [51]

Le GSA (General Services Administration) va également proposer un guide pour aider les agences fédérales à disposer de solutions (produits et services) dans la mise en œuvre de leur stratégie Zero Trust [146]. Ce document a pour but de fournir les outils

nécessaires pour une démarche « confiance zéro » personnalisée en s'appuyant sur les capacités de l'organisation, le niveau de maturité de sa politique sécuritaire et un large choix de produits développés par le GSA (outils de diagnostic et d'atténuation continus (CDM), services de cybersécurité hautement adaptatifs (HACS), etc.). Par ailleurs, en septembre 2021, l'Office de la gestion et du budget (OMB) a publié le memorandum OMB M-22-09 [221]. Une stratégie fédérale d'architecture Zero Trust est présentée dans ce memorandum. Elle ordonne aux agences de mettre en place des politiques de sécurité conforment aux exigences en matière de cybersécurité avant la fin de l'exercice 2024. L'objet est de fournir au gouvernement américain un système de défense national de ses infrastructures informatiques, de la vie privée de ses populations contre les cyberattaques de plus en plus récurrentes et sophistiquées. Le ministère américain de la Défense a également entrepris des initiatives en finançant une étude menée par le Lincoln Laboratory du MIT. Les auteurs Chris Roeser et Jeff Gottschalk définissent le Zero Trust comme un ensemble de principes de sécurité qui juge chaque composant, service et utilisateur d'un système comme constamment exposé et potentiellement compromis par un adversaire malveillant [166]. Par conséquent, une architecture Zero Trust est donc un système informatique fondé sur le principe Zero Trust pour garantir la confidentialité, l'intégrité et la disponibilité des données et des applications. L'implémentation de cette architecture repose sur des composants pour identifier les ressources, vérifier l'identité des utilisateurs et contrôler l'accès aux ressources. Ces éléments sont coordonnés entre eux par une politique d'orchestration et sont liés à des mécanismes de surveillance et d'analyse, ainsi qu'à un ensemble d'opérations continues pour la détection et la gestion des risques. La figure 1.12 ci-dessous illustre le fonctionnement et les composants de cette architecture.

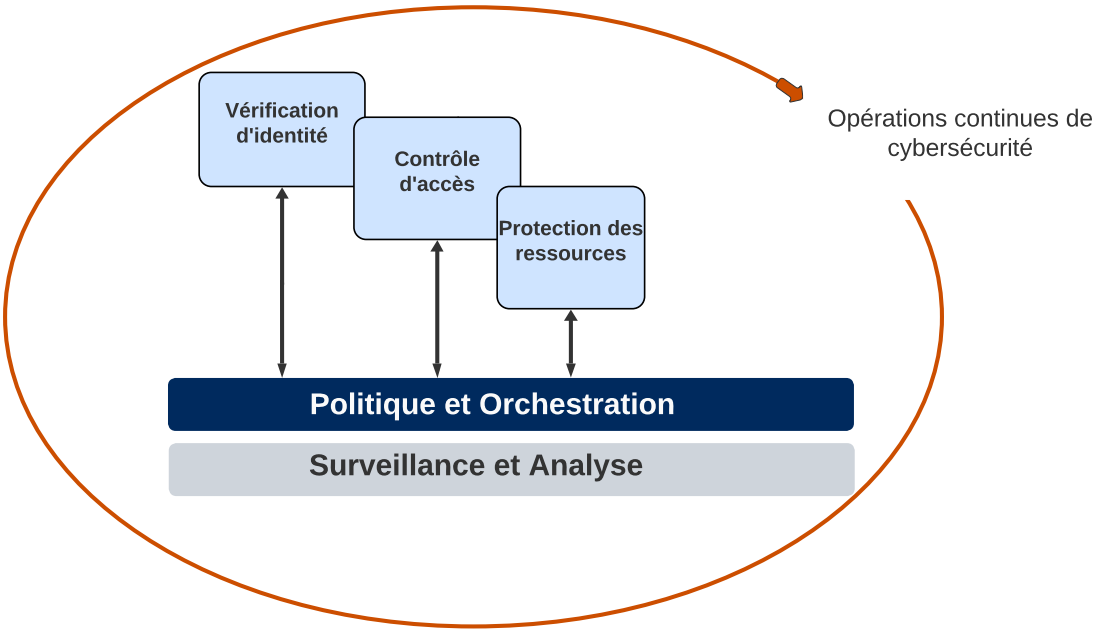


FIGURE 1.12 : Architecture Zero Trust Lincoln Laboratory [166]

Les études ci-dessus, ainsi que l'avis scientifique et technique de l'agence nationale de la sécurité des systèmes d'information française (ANSSI) [14] ont conclu que l'adoption d'une approche Zero Trust est nécessaire pour améliorer la sécurité des infrastructures informatiques de plus en plus en ouvertes, complexes et distribuées telles que le cloud computing. Cependant, cette démarche doit être effectuée de manière progressive et maitrisée. Le développement d'une architecture Zero Trust requiert d'identifier les

principes de Zero Trust applicables au contexte, ainsi que les solutions techniques (chiffrement, authentification, contrôle d'accès, etc.) existantes ou nouvelles appropriées.

1.5 Conclusion

Dans ce chapitre, nous avons d'abord présenté le cloud computing en mettant l'accent sur ses caractéristiques, ses modèles de services, de déploiements, ses avantages et les obstacles à son adoption, notamment les problèmes de sécurité. Malgré les inquiétudes et réticences à l'utilisation des services cloud, ce paradigme se présente comme un outil idéal pour apporter de la résilience, de l'évolutivité et de la flexibilité aux entreprises. La mondialisation et la transformation numérique de la société font de la collaboration, au sein et entre des organisations, un élément catalyseur de leur productivité et d'efficacité dans leurs différents projets d'innovations.

De ce fait, nous décrivons dans la deuxième partie les outils et les modèles proposés par le cloud computing pour la collaboration et le partage de ressources. Nous mettons un accent particulier sur les organisations avec des exigences strictes en termes de sécurité et de réglementation comme les institutions financières, sanitaires, les agences gouvernementales, etc. Pour cette catégorie d'organisation, le déploiement de cloud communautaire est une solution pour bénéficier des avantages de coût et de flexibilité du cloud public ainsi que des garanties de sécurité offertes par un cloud privé.

Cependant, pour un cloud communautaire où des organisations hétérogènes échangent diverses données provenant de différentes sources, les questions d'authentification, de contrôle de l'accès aux ressources et de confiance se posent. Ainsi, les différentes stratégies utilisées pour assurer la sécurité des infrastructures cloud ont été présentées dans la dernière partie de ce chapitre.

La complexité des plateformes cloud et des infrastructures distribuées a conduit les experts de la cybersécurité à adapter leurs stratégies et politiques de sécurisation de ces systèmes. La tendance actuelle est d'aller au-delà de la défense périmétrique et de considérer toutes les ressources (physiques et logicielles) de l'infrastructure comme potentiellement exposées et malveillantes. Cette stratégie de sécurité, appelée Zero Trust, consiste à proposer des mesures de sécurité sur la base d'un certain nombre de principes en tenant compte du contexte et des objectifs de l'organisation. Dans cette thèse, nous souhaitons montrer que l'adoption d'une démarche Zero Trust améliorerait la sécurité des ressources, des échanges et la confiance entre les organisations dans un cloud communautaire. Pour cela, nous proposons une démarche Zero trust fondée sur l'identification et l'authentification des organisations, l'évaluation de la confiance entre elles et le contrôle d'accès aux ressources lors des collaborations.

Une analyse bibliographique des travaux réalisés sur la gestion des identités, les systèmes d'évaluation de la confiance et les modèles de contrôle d'accès proposés pour ce type d'infrastructure sera présentée dans le chapitre suivant.

Chapitre 2

Gestion des identités, des accès et de la confiance dans le cloud

«L'identité numérique est au cœur de la confiance numérique. En effet, sans gestion fiable de l'identité numérique, il est illusoire de croire au développement des services de confiance.»

Jean-Pierre Quemard - Président de l'Alliance pour la Confiance Numérique(ACN), 2012

Sommaire

2.1 Introduction

Dans le chapitre précédent, nous avons présenté le cloud et les possibilités qu'il offre en termes de collaboration. Par ailleurs, nous avons mis en relief la question de la sécurité des interactions et des ressources partagées dans des communautés ayant des exigences élevées en matière de réglementation et de sensibilité des informations. La protection de ce type d'infrastructure complexe dépend fortement de la qualité de la gestion de l'identité numérique, particulièrement en termes d'authentification et de contrôle des accès aux ressources [136]. Et comme le dit si bien Brian Miller, responsable de la sécurité des systèmes d'information (RSSI) chez Healthfirst *« si nous pouvons contrôler l'identité, nous pouvons arrêter la plupart des attaques modernes. Si vous contrôlez l'identité, vous contrôlez chaque périmètre, chaque application, chaque conteneur, c'est-à-dire chaque partie de l'environnement »* [66]. Une assertion confirmée par les résultats des travaux du laboratoire Lincoln du MIT [166], qui recommande de consacrer les premiers efforts de déploiements d'une stratégie Zero Trust à la vérification des identités et au contrôle d'accès. Par conséquent, dans ce deuxième chapitre, nous présentons une analyse de l'état de l'art sur les systèmes de gestion d'identité et de contrôle d'accès. En outre, nous examinerons les travaux effectués sur les systèmes d'évaluation de la confiance dans le cloud. Nous discuterons des avantages et limites de ces différents mécanismes, le but étant d'identifier les éléments d'améliorations qui pourrait convenir à nos exigences de contrôle d'accès, de collaboration et de confiance tel que décrit dans le chapitre précédent.

2.2 La gestion des identités dans le cloud

2.2.1 Les identités numériques

Une identité numérique est un ensemble d'informations permettant de représenter de façon unique une entité [42]. Ces informations numériques ou attributs peuvent être de plusieurs formes en fonction du domaine et du contexte. Par exemple, une adresse électronique pour une messagerie sur Internet, un nom pour l'état civil, une empreinte digitale pour un service biométrique, etc. D'un point de vue juridique, l'identité numérique est *« ce qui fait qu'une personne est-elle même et non une autre »* [136]. Une entité est donc caractérisée par un ou plusieurs attributs et peut-être une personne physique, une personne légale ou morale (entreprise), une personne virtuelle (application), ou un ensemble d'entités [205]. En outre, une entité peut posséder plusieurs identités numériques distinctes qui peuvent être associées à des contextes et à des domaines d'applications différents (entreprise, administration, université, Internet, etc.) [43]. À titre d'illustration, une personne peut avoir une identité de chef d'entreprise d'une organisation et celle de patient dans un hôpital. Ces identités numériques qui permettent d'identifier cet individu de façon unique dans son entreprise et son hôpital sont appelées « identifiant ». Il sera alors représenté par un identifiant dans chaque domaine. Cet identifiant associé à un justificatif d'identité (mot de passe, certificat numérique, etc.) permettent d'authentifier une identité déclarée grâce un système de gestion d'identité [205].

2.2.2 Gestion des identités

Selon la norme ISO/IEC. 24760-3 [108], la gestion des identités est l'ensemble des processus, des technologies et des standards permettant de créer, d'utiliser, de mettre à jour, de suivre et de supprimer une identité numérique. Par ailleurs, elle doit permettre, à travers des identifiants distincts pour chaque entité, d'identifier, d'authentifier, de ga-

rantir l'intégrité, de contrôler et de suivre l'usage des informations d'identifications et données personnelles. C'est à juste titre que le NIST définit la gestion des identités et des accès comme une capacité fondamentale et essentielle de la cybersécurité. Elle permet de s'assurer que les bonnes entités ont le bon accès à la ressource adéquate au bon moment. Plusieurs systèmes de gestion des identités fondés sur différents types d'architectures ont ainsi été proposés [136]. Les premiers modèles reposaient sur des infrastructures centralisées. Puis, l'émergence des systèmes collaboratifs et distribués a favorisé des architectures fédérées, centrées sur l'utilisateur [136], et plus récemment les identifiants décentralisés (DiD) [69] et les informations d'identifications vérifiables (VC) [206]. La figure 2.1 représente l'évolution des systèmes de gestion d'identités dans les systèmes informatiques.

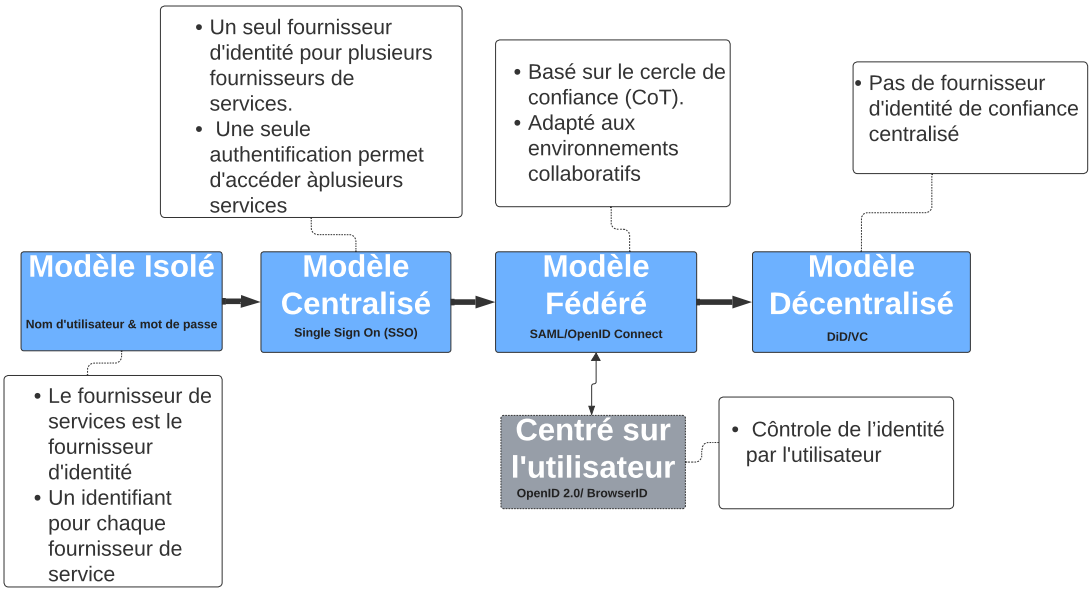


FIGURE 2.1 : Évolution des systèmes de gestion d'identité

Nous présentons ci-dessous une description de chaque système.

2.2.2.1 Le modèle de gestion isolé

Ce modèle permet à un fournisseur de service (FS) de mettre à la disposition des utilisateurs des identifiants (nom d'utilisateur et mot de passe) afin qu'ils puissent accéder aux services qu'il offre [117]. Ce fournisseur de service joue ainsi le rôle de fournisseur d'identité (IdP) dans un domaine de service donné. Pour chaque service différent auquel il souhaiterait accéder, l'utilisateur recevra des identifiants distincts de la part de chaque fournisseur de service. Cela a pour conséquence, d'obliger les utilisateurs à mémoriser et gérer plusieurs identifiants, entrainants des risques de pertes, d'oublis, d'utilisations de mots de passes identiques, et donc des problèmes de sécurité (usurpation, vol d'identité, etc.) [117][114].

2.2.2.2 Le modèle de gestion centralisé

Contrairement à la gestion isolée, la gestion centralisée fait intervenir un fournisseur d'identité unique pour plusieurs fournisseurs de service. L'IdP est chargé de créer, de tenir à jour et de gérer les informations d'identité de différentes entités (dispositifs, utilisateurs, organisations) ainsi que d'autres services liés à leurs identités [205]. Une entité peut alors accéder à plusieurs services de différents fournisseurs de services grâce

à une identité unique délivrée par le fournisseur d'identité. Cette approche peut être implémentée de plusieurs manières dont le plus couramment est le modèle d'authentification unique ou SSO [117]. Le modèle SSO permet à un utilisateur de s'authentifier qu'une seule fois auprès d'un fournisseur de service et accéder à des services d'autres fournisseurs. Ainsi, la gestion des informations d'identification auprès de tous les fournisseurs de service est déléguée au fournisseur d'identité qui a l'entière confiance de ces derniers [141]. Bien qu'elle apporte de la simplicité et de la flexibilité pour les utilisateurs, ce modèle présente une dépendance vis-à-vis du fournisseur d'identité et requiert une confiance des utilisateurs quant à la gestion et l'utilisation de leur information d'identité par l'IdP. De plus, la nature centralisée de cette architecture ne la rend pas compatible aux environnements distribués [136].

2.2.2.3 Le modèle de gestion fédérée

Le but principal de ce modèle est de proposer une solution pour la gestion des identités dans des environnements collaboratifs, permettant ainsi aux utilisateurs d'accéder à des services et ressources de différents domaines de sécurité à partir d'une même identité [168][136]. Cette architecture se fonde sur des cercles de confiance ou COT (Cercle of Trust) regroupant plusieurs fournisseurs de services et d'identités liés par des relations de confiance mutuelles grâce à des accords commerciaux et des infrastructures d'authentifications partagées telles que Shibboleth, Liberty Alliance, WS-Federation [168][136]. Ainsi, des systèmes d'authentification uniques entre plusieurs domaines peuvent être mis en place afin de permettre à un utilisateur d'accéder aux ressources des fournisseurs de services membre du cercle de confiance. Deux types de services permettent d'atteindre cet objectif, à savoir la propagation d'identité et la délégation de l'authentification [141]. La délégation de l'authentification permet aux fournisseurs de service d'authentifier un utilisateur grâce au fournisseur d'identité de son domaine d'appartenance, et ainsi lui accorder des services hors de son domaine de sécurité. La propagation d'identité consiste à diffuser les informations d'identification (nom, courrier électronique, etc.) d'un domaine de sécurité à l'autre.

La mise en œuvre de système de gestion fédéré d'identité repose sur différents types de protocoles et langages. Nous décrivons ci-dessous les principaux protocoles utilisés.

- **Le langage SAML (Security Assertion Markup Language)** : Norme proposée par l'organisation de standardisation OASIS (Organization for the Advancement of Structured Information Standards), il vise à permettre des échanges entre des fournisseurs d'identités et de services appartenant à un même cercle de confiance [103]. La version la plus récente SAML2.0, créée en 2005, permet de spécifier des assertions au format XML (Extensible Markup Language) qui décrivent les jetons d'identité sur lesquels reposent les messages échangés entre les fournisseurs d'identités et les fournisseurs de services, indépendamment des technologies utilisées (annuaire LDAP, SSO, Kerberos, etc.) [136]. Le standard SAML demeure, à ce jour, l'un des plus utilisés par les entreprises et sert de base à d'autres protocoles de sécurité tels que Liberty Alliance, Shibboleth, etc [121].
- **Shibboleth** [45] : Ce protocole, élaboré par le consortium Internet2, est fondé sur le langage SAML et fournit des fonctionnalités de fédérations d'identité qui facilitent la collaboration et l'accès à des ressources protégées dans les centres de recherche et établissements supérieurs [136][45]. Shibboleth permet à l'utilisateur de préciser son fournisseur d'identité, permettant ainsi à plusieurs systèmes d'authentification des établissements d'être fédérés indépendamment des technologies utilisées. Cependant, l'inconvénient majeur de ce protocole est son ar-

chitecture centralisée, avec une dépendance vis-à-vis d'un fournisseur d'identité centrale, ainsi qu'un manque de transparence sur l'utilisation des données personnelles et la protection de la vie privée de l'utilisateur [45].

- **Liberty Alliance** : Liberty Alliance est un consortium créé par Sun Microsystems et qui regroupe plus de deux cents organisations de différents domaines économiques et des institutions gouvernementales [11][136]. Il vise à mettre au point des standards pour la gestion d'identités fédérées et les services Web fondés sur l'identité. En outre, l'alliance propose aux entreprises qui utilisent ses normes des pratiques et des lignes directrices appropriées, ainsi qu'un programme de certification pour les produits conforme à ses spécifications [45]. Le projet Liberty Alliance repose sur une architecture de fédération d'identités distribuées et s'appuie sur d'autres standards tels que SAML, XML, etc [11]. Par ailleurs, le cadre architectural de gestion d'identité fédérée de l'alliance est composé de trois éléments principaux : ID-FF(Identity Federation Framework) [44], ID-WSF(Identity Web Services Framework) [76], et ID-SIS (Identity Service Interface Specifications) [44].
- **OpenID** : Le standard OpenID fournit les fonctionnalités requises pour une authentification décentralisée (SSO multi-domaines) [174]. Il se caractérise par sa simplicité et permet de fournir à l'utilisateur une adresse URL (Uniform Resource Locator) comme identifiant unique pour s'identifier auprès des sites web compatibles OpenID. Cette norme est également fondée sur des standards Internet, notamment HTTP (Hypertext Transfer Protocol)/HTTPS (Hypertext Transfer Protocol Secure), XML et des algorithmes de signature (SHA1, SHA256). Grâce à OpenID, l'utilisateur a le contrôle sur ses données et peut librement choisir son fournisseur d'identité parmi ceux existants tels que Google, Facebook, etc [136]. Cependant, les problèmes de sécurité constituent les principales limites de ce standard [136][168]. En effet, les utilisateurs sont exposés à des attaques de type Phishing et Spam afin de les détourner vers des sites malveillants dans le but de récupérer des informations confidentielles (mot de passe, données bancaires, etc). En outre, les problèmes de confiance entre les acteurs (IdP, fournisseur de services, utilisateurs) et la capacité de suivi des activités de l'utilisateur par l'IdP restent des défis majeurs pour la sécurité des données et la protection de la vie privée.

En raison de ses nombreux avantages, la fédération d'identité se présente comme une solution pour la gestion des identités dans les systèmes collaboratifs et distribués. Cependant, elle entraîne de nouveaux risques et menaces en termes de sécurité et de respect de la vie privée, principalement dû à la nature sensible des informations échangées, à la multiplicité et à l'hétérogénéité des standards et des protocoles d'authentification [168][121][33].

2.2.2.4 Le modèle centré sur l'utilisateur

La gestion d'identité centrée sur l'utilisateur a pour principal objectif de faciliter et de donner le contrôle à l'utilisateur sur la gestion de son identité, contrairement aux autres systèmes où les attributs d'identités étaient confiés aux fournisseurs d'identités [136]. Cette approche permet à l'utilisateur de négocier, de sélectionner les attributs d'identité qu'il souhaite transmettre à un fournisseur d'identité de son choix ou de les stocker localement sur des dispositifs inviolables (cartes à puces, poste de travail personnel, etc.) sous son contrôle [117]. Les normes OpenID, OpenAuth [161] et les projets WebID[1]

[1]https ://webid-solutions.de/ ?lang=en

du consortium World Wide Web (W3C) et U-Prove [2] de Microsoft sont des exemples de mise en œuvre de ce modèle.

Bien qu'elle vise à permettre à l'utilisateur de maîtriser la diffusion de ces identifiants, la gestion centrée sur l'utilisateur reprend sensiblement les mêmes principes des gestions fédérées et centralisées avec la présence et le rôle majeur accordé au fournisseur d'identité. Ce dernier peut être une menace pour la confidentialité et le respect de la vie privée et représenter un nœud de dépendance et de défaillance [136]. Par ailleurs, les solutions d'implémentation du modèle centré sur l'utilisateur sont difficiles à prendre en main par les utilisateurs. Il est donc nécessaire de mettre en place une nouvelle approche de gestion décentralisée des identités, qui ne repose pas sur une autorité centrale et qui permet une gestion facile et un contrôle exclusif de l'utilisateur sur son identité.

2.2.2.5 Le modèle décentralisé

L'identité décentralisée ou identité auto-souveraine (Self-Sovereign Identity) vise à répondre aux préoccupations en matière de confidentialité et de protection de données soulevées par les précédents systèmes de gestion d'identités. Le W3C, à travers deux groupes de travail, a proposé des spécifications afin de promouvoir une nouvelle identité avec des exigences jusque-là non respectées par aucun identifiant, à savoir une facilité de création, décentralisée, persistant, portable et vérifiable de manière cryptographique. il s'agit des recommandations sur les identifiants décentralisés [69] et les informations d'identifications vérifiables [206].

- **Identifiant décentralisé** : un identifiant décentralisé (DiD) [69] est un identifiant unique, vérifiable de manière cryptographique. Un DiD est associé à un document DiD qui décrit un sujet, lui donne le contrôle sur son identité et permet des interactions de confiance en mode pair à pair entre lui (détenteur) et les autres entités du réseau. La structure d'un DiD est représentée dans la figure 2.2. Elle comprend : une méthode cryptographiqueDiD et un identifiant spécifique à la méthode. Le DiD permet d'accéder au document DiD afin d'authentifier un sujet. Le document DiD est représenté par un fichier (JSON, JSON-LD, etc) généralement stocké dans des registres distribués de type blockchain et constitué d'algorithmes cryptographiques, de méthodes de vérifications et des interfaces d'accès au service.

FIGURE 2.2 : Structure d'un identifiant décentralisé (DiD) [69]

[2] https ://www.microsoft.com/en-us/research/project/u-prove/

- **Informations d'identifications vérifiables (VC)** : les informations d'identifications vérifiables (VC) [206] sont des représentations numériques de documents d'identification physiques tels que les permis de conduire, les diplômes ou les passeports. À titre d'illustration, un footballeur professionnel souhaitant participer à une compétition sportive doit prouver son appartenance à une équipe habilitée pour la compétition. Cette preuve peut être apportée au moyen d'informations d'identification vérifiables de manière cryptographique. Dans notre exemple, les informations d'identifications vérifiables du footballeur pourraient être toutes les données contenues sur une licence physique (nom, prénoms, groupe sanguin, date de naissance, adresse, date d'enregistrement, etc.). L'émetteur serait l'équipe de football. Les signatures numériques de l'émetteur et du détenteur rendent les VC dignes de confiance.

2.2.3 Les systèmes d'authentification

La gestion des identités nécessite des moyens de vérification des identités numériques des utilisateurs, des dispositifs et d'assurance de l'intégrité des données. De ce fait, l'authentification est étroitement liée à l'identité numérique. Elle permet d'apporter la preuve et l'assurance de l'identité revendiquée par une entité dans un contexte bien précis [217]. L'authentification fait intervenir deux entités. Elle peut être unilatérale en mettant en jeu un déclarant et un vérificateur ou mutuelle lorsque chaque entité est à la fois déclarante et vérificatrice. Les systèmes d'authentification reposent sur des mécanismes de sécurité qui permettent de vérifier et de valider l'identité d'une entité en fonction d'une preuve fournie par cette dernière [136]. Cette preuve de nature variable peut être :

- quelque chose que l'on possède : un support physique (une carte à puce, une clé, etc.) ;
- quelque chose que l'on sait : un mot de passe, un code, etc. ;
- ce que l'on est : une caractéristique immuable telle une empreinte digitale, une voix, l'iris, etc. ;
- quelque chose que l'on sait faire : une signature manuscrite, etc.

Ces facteurs d'authentification peuvent être combinés afin d'augmenter le niveau de robustesse du système d'authentification [136]. Les méthodes d'authentification sont généralement fondées sur des algorithmes cryptographiques. Plusieurs types d'algorithmes cryptographiques permettent ainsi de signer numériquement des messages afin d'assurer l'authentification de l'émetteur et du récepteur, leur intégrité et leur non-répudiation [136]. Deux grandes catégories de méthodes cryptographiques sont utilisées, à savoir la cryptographie symétrique et la cryptographie asymétrique.

2.2.4 La cryptographie symétrique

La cryptographie symétrique est fondée sur le partage d'une même clé, appelée clé secrète, entre deux entités engagées dans une communication. La même clé est utilisée pour le chiffrement et le déchiffrement d'un message. Le principe de fonctionnement de l'algorithme de chiffrement est présentée à la figure 2.3 et met en exergue deux personnes, Bob et $Alice$ désirant, s'échanger des messages. Ainsi $Alice$ souhaite envoyer un message à Bob , il utilise une fonction de chiffrement (E) et en paramètres d'entrée le message et la clé sécrète. À la réception du message, Bob applique au message chiffré l'algorithme de déchiffrement (E^{-1}) avec en paramètre la clé secrète partagée. Ces algorithmes symétriques sont caractérisés par leur solidité et des performances de

calculs et de traitements de gros volumes de données élevés. Cependant, ils présentent des limites, car ils nécessitent de gérer plusieurs clés (une pour chaque couple de communication) et surtout la problématique de l'échange des clés secrètes qui requiert que les parties engagées se mettent d'accord sur la clé secrète avant la communication. Data Encryption Standard (DES) et Advanced Encryption Standard (AES) [194] sont les protocoles symétriques les plus connus.

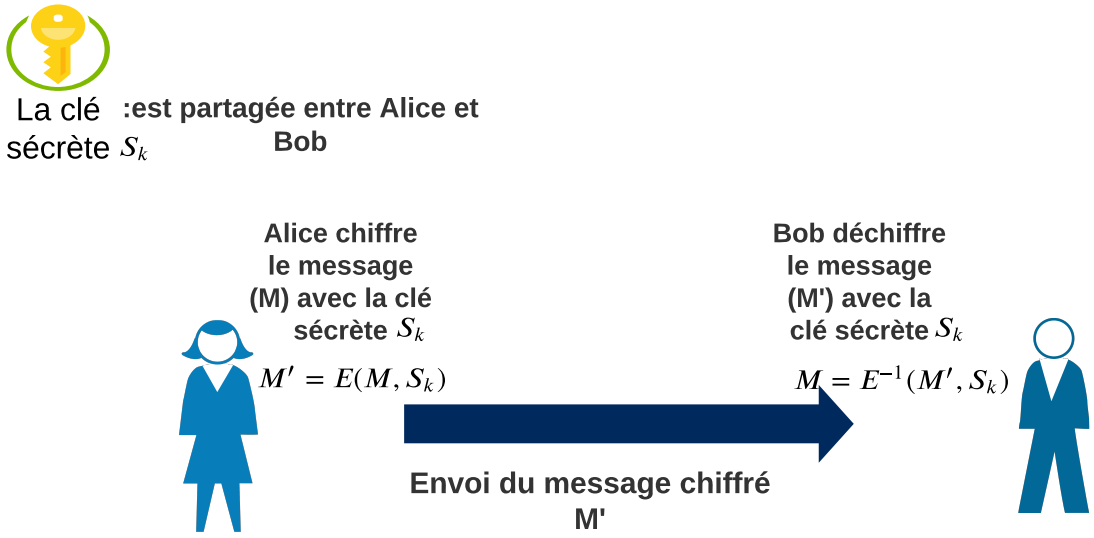


FIGURE 2.3 : Système de cryptographie symétrique

2.2.5 La cryptographie asymétrique

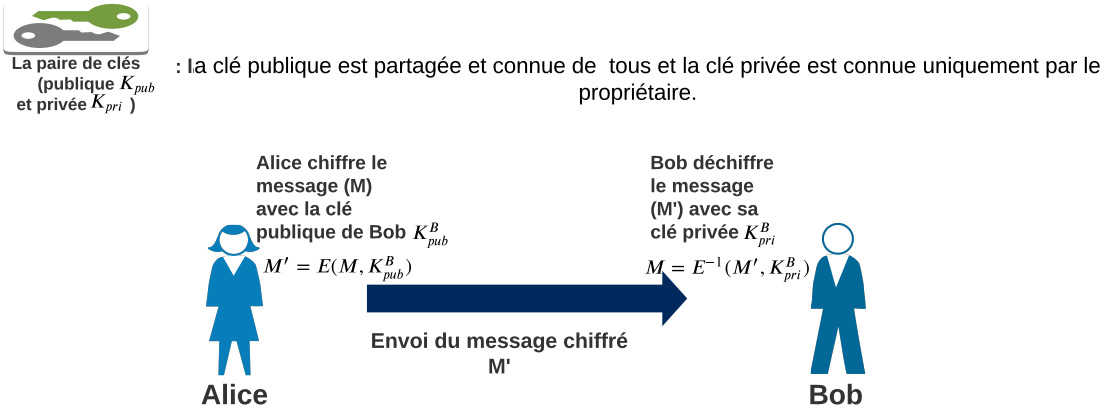


FIGURE 2.4 : Système de cryptographie asymétrique

La cryptographie asymétrique ou à clé publique utilise une paire de clés pour chaque entité. Une clé publique accessible à tous et l'autre privée qui ne doit être connue que par le détenteur légitime. Ces clés sont uniques et spécifiques à un algorithme. Si la clé privée est utilisée pour chiffrer un message, la clé publique servira au déchiffrement et vice versa. Ainsi, si $Alice$ désire envoyer un message chiffré à Bob , il chiffrera le message avec la clé publique de Bob, qui a la réception déchiffrera le message avec sa clé privé comme présenté à la figure 2.4. Bien que les questions de partage d'une même clé secrète et la gestion de plusieurs clés ne se posent plus, les performances des algorithmes asymétriques sont moins bonnes et ne sont pas adaptées au traitement de gros volumes de données. Par ailleurs, la nécessité de s'assurer qu'une entité est bien le

propriétaire légitime d'une clé publique dont il revendique la paternité a amené à combiner la cryptographie à clé publique PKI (Public key Infrstructures) et les certificats numériques par le biais des infrastructures à clés et les autorités de certifications.

2.2.6 Les signatures numériques

Considérée comme une version numérique des signatures manuscrites ordinaires avec un niveau de sécurité et de complexité plus élevé, une signature numérique est un mécanisme cryptographique qui permet de vérifier l'authenticité et l'intégrité des données numériques [7]. En d'autres termes, c'est un code rattaché à un message qui prouve que le message n'a subi aucune modification lors de sa transmission entre l'expéditeur et le destinataire. Cela est possible grâce aux fonctions de hachages. Une fonction de hachage est un algorithme à sens unique qui prend en entrée une donnée de taille arbitraire et fournit en sortie une donnée de longueur fixe appelée hache ou empreinte. La taille d'une valeur de hache varie en fonction de l'algorithme. À titre d'exemple, les algorithmes MD5 [175], SHA-1 [67], SHA-256 [67] ont des tailles d'empreintes respectives de 128, 160, 256 bits. Ces deux premiers algorithmes, bien qu'ayant longtemps été largement utilisé, sont déconseillés aujourd'hui car considéré comme cassés (possibilité de créer des collisions) ou fortement affaiblis [210][211]. Les fonctions de hachage peuvent être combinées à des systèmes cryptographiques en signant, par exemple, l'empreinte d'un message avec la clé privé d'une entité avant l'envoi afin d'assurer à la fois l'intégrité du message, l'authentification de l'émetteur et la non-répudiation du message. Ce processus est décrit dans la figure 2.5 ci-dessous. Ainsi, le message haché est signé avec la clé privé d'$Alice$ pour créer une signature S. Le message M est chiffré avec la clé publique de Bob pour produire un message M'. Le message M' et la signature S sont envoyés par Alice. À la réception du message, Bob déchiffre le message M' avec sa clé privée. À l'aide de la clé publique et la signature S, il extrait l'empreinte $H(M)$. Il calcule une nouvelle empreinte H_2 avec le message reçu M afin de comparer $H(M)$ et H_2. s'ils sont égaux alors le message n'a pas subi de modification, sinon il a été modifié.

FIGURE 2.5 : Signature numérique associé à la cryptographie asymétrique

2.2.7 Les algorithmes de signatures à clé publique

Dans cette section, nous décrivons le fonctionnement de trois des principaux algorithmes de chiffrement utilisés, à savoir l'algorithme Rivest-Shamir-Adleman (RSA), l'algorithme de signature numérique à courbe elliptique (ECDSA) et le système de signature numérique BLS.

2.2.7.1 L'algorithme RSA

Proposé en 1977 par les chercheurs Ron Rivest, Adi Shamir et Leonard Adleman du MIT, l'algorithme RSA [176] est un système cryptographique asymétrique. Il repose sur le chiffrement à clé publique, décrit plus haut, qui utilise une paire de clés (publique et privée). La popularité du RSA est due au fait qu'il est fondé sur le principe qu'il est beaucoup plus facile de faire le produit de deux nombres premiers que de factoriser un nombre en le produit de deux nombres premiers. Ce type d'opération est difficile, car il prendrait beaucoup de temps, même avec des ordinateurs très puissants. Cela a encouragé l'utilisation du RSA dans plusieurs systèmes d'authentification. Ce protocole fonctionne en trois principales phases : la génération des clés, le cryptage et le décryptage. Ci-dessous, un scénario dans lequel $Alice$ désire envoyer un message à Bob .

- **Étape 1 : Génération de la paire de clés (publique et privée) par** $Alice$
  1. choisir deux nombres premiers distincts p et q généralement très grand et de façon aléatoire ;
  2. calculer $n = p$ x q
  3. calculer $\phi(n) = (p-1)$ x $(q-1)$
  4. choisir un exposant et calculer son inverse :
     (a) Choisir e tel $pgcd(e, \phi(n)) = 1$
     (b) Calculer l'inverse d de e modulo $\phi(n)$ par l'algorithme d'Euclide étendu : d x $e \equiv 1(mod \phi(n))$
  5. la clé publique est constituée de n et e
  6. la clé privée est d
- **Étape 2 : Chiffrement du message**
  1. le message a envoyé, est transformé en un entier m tel que $0 \leq m < n$
  2. récupération de la clé publique et calcul du message chiffré x : $x \equiv m^e (mod\, n)$
  3. transmission du message x
- **Étape 3 : Déchiffrement du message**
  1. réception du message chiffré x
  2. déchiffrement à l'aide de la clé privé d en calculant $m \equiv x^d (mod\ n)$ à l'aide d'une exponentiation rapide

Une synthèse du fonctionnement de l'algorithme RSA est présentée à la figure 2.6 ci-dessous.

Plusieurs protocoles couramment utilisés dans nos systèmes informatiques tels que les protocoles SSL/TLS, SSH et bien d'autres sont établis à partir de l'algorithme RSA.

2.2.7.2 L'algorithme de signature numérique à courbe elliptique (ECDSA)

La force du RSA réside dans la difficulté que représente la factorisation de grands nombres entiers. Le traitement de grands nombres a une influence sur les performances de l'algorithme, même s'il renforce la puissance du chiffrement. C'est à ce niveau qu'intervient la cryptographie à courbe elliptique ou ECC (Elliptic Curve Cryptography) [127][151] de plus en plus adopté pour la mise en œuvre de chiffrement à clé publique. En effet, cette technologie, fondée sur les théories mathématiques des courbes ellip-

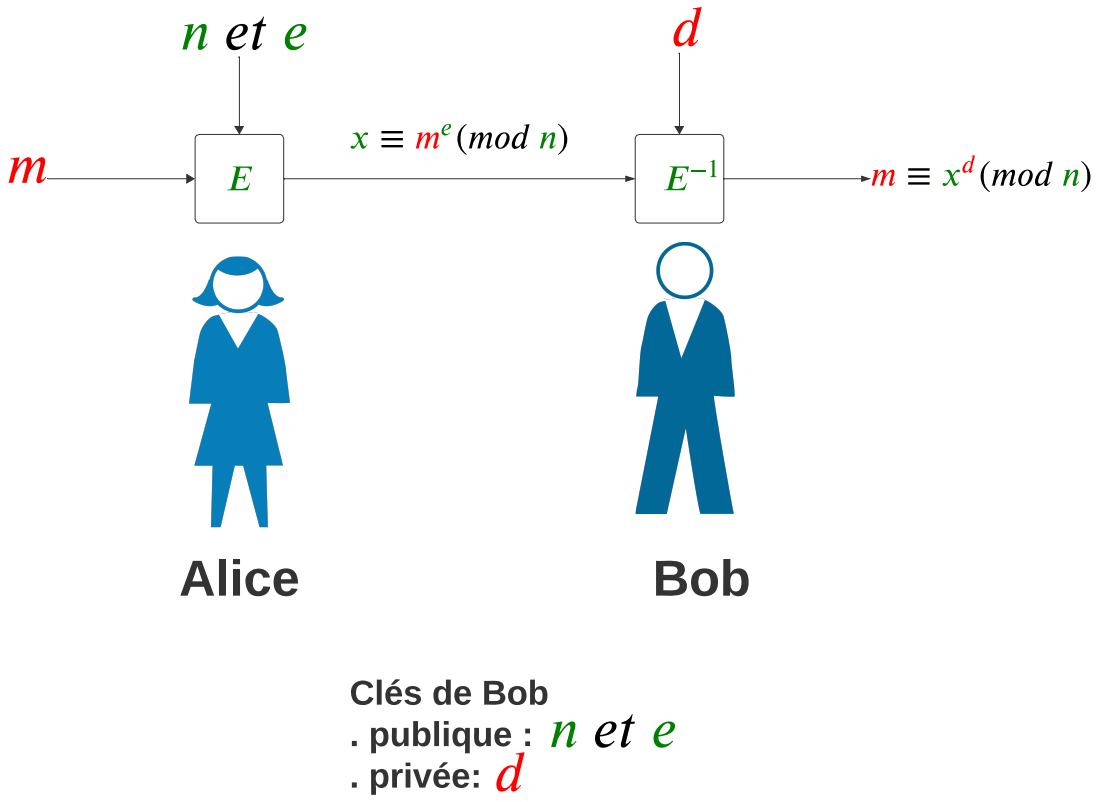


FIGURE 2.6 : Fonctionnement de l'algorithme RSA

tiques, permet de créer des clés de chiffrement à la fois petites, efficaces et rapides. La longueur des clés générées à travers ce système est alors plus courte que celle de la clé de l'algorithme RSA. À titre d'exemples déduits des directives du NIST pour une clé ECC de 512 bits, la taille de la clé RSA est de 15 360 bits pour une sécurité équivalente avec un traitement plus rapide et une consommation d'énergie moindre pour l'ECC [218]. Des travaux ont ainsi montré que l'ECC est plus performant que le protocole RSA [95][208]. La cryptographie à courbe elliptique a permis aux chercheurs de l'American National Standards Institute (ANSI) de proposer l'algorithme de signature numérique à courbe elliptique ou Elliptic Curve Digital Signature Algorithm (ECDSA). Cet algorithme est utilisé pour la cryptographie à clé publique et est fondé sur le problème du logarithme discret ou l'impossibilité de calculer le logarithme discret d'un élément de courbe elliptique aléatoire par rapport à un point de base connu de tous [218].

Dans un scénario dans lequel $Alice$ souhaite envoyer un message m à Bob, nous avons courbe elliptique E définie sur $\mathbb{F}_p$ avec un grand groupe $E(\mathbb{F}_p)$ d'ordre n et un générateur P. Les différentes étapes de l'algorithme sont les suivantes :

- **Génération des clés (opérations effectuées par Alice)** :
  1. choisir un nombre entier aléatoire $k_s \in [1; n-1]$
  2. calculer $k_p = k_s.P$
  3. partager ses paramètres publics $(E; P; n; K_p)$ et garder en secret sa clé privé k_s .
- **Génération d'une signature (par Alice)** :
  1. choisir un nombre entier aléatoire $k \in [1; n-1]$ tel que $PGCD(k; n) = 1$

2. calculer $k.P = (x_1; y_1)$ et $r = x_1 \ mod \ n$. Si $r = 0$, retourner choisir un nouveau k.
3. calculer $k^{-1} \ mod \ n$
4. calculer $\sigma = k^{-1}.(H(m) + k_s.r) \ mod \ n$. H est l'algorithme de hachage. Si $\sigma = 0$, recommencer la procédure de signature.
5. la signature du message m est $(r; \sigma)$

- **Vérification de la signature (effectuée par Bob)** :
  1. vérifier que σ et r sont des entiers $\in [1; n-1]$
  2. calculer $c = \sigma^{-1} \ mod \ n$ et $H(m)$
  3. calculer $u_1 = H(m).c \ mod \ n$ et $u_2 = r.c \ mod \ n$.
  4. calculer $u_1.P + u_2.k_p = (x_0; y_0)$ et $v = x_0 \ mod \ n$.
  5. la signature est approuvée si $v = r$

L'ECDSA est le protocole utilisé dans les technologies blockchain tel que le Bitcoin.

2.2.7.3 L'algorithme de signature numérique Boneh, Lynn and Shacham (BLS)

Le système BLS (Boneh, Lynn et Shacham) est un système de signature numérique introduit dans [38] par des chercheurs de l'université de Stanford. Il a la particularité de permettre l'agrégation de plusieurs signatures en une signature unique et fournit des moyens de vérification de cette signature. L'agrégation permet ainsi de réduire le temps de vérification des signatures et l'espace de stockage utilisé [177]. Par ailleurs, l'algorithme de signature BLS aide à générer des signatures de petites tailles et utilise la propriété d'appariement (bilinéaire) des courbes elliptiques [38] :

Soit G un générateur de groupes bilinéaires prenant en entrée un paramètre β et renvoyant un groupe bilinéaire $params = (q, G1, G2, G, g_1, g_2, e)$, où $G1$ et $G2$ sont des groupes cycliques d'ordre q.
g_1, g_2 les générateurs respectifs des groupes $G1$ et $G2$, e la fonction d'appariement bilinéaire telle que $e : G1 \times G2 \rightarrow G$.
La fonction d'appariement est efficacement calculable et a les propriétés suivantes :
$-\forall \ \beta \ \in \mathrm{Z}_q^*, \forall \ \lambda \ \in \mathrm{G1} \ , \forall \ \gamma \ \in \mathrm{G2} \ , \mathrm{e}(\beta\lambda, \gamma) = e(\lambda, \beta\gamma)$
$- \ e(\lambda, \gamma) \neq 1$

La fonction d'appariement bilinéaire ne permet pas de déterminer la valeur de β à partir des valeurs λ et γ. Ainsi, cette fonction est utilisée dans la construction d'une signature BLS en définissant comme clé secrète la valeur β. Trois principaux algorithmes interviennent dans le processus de création d'une signature numérique BLS [38] : la génération des clés, la signature et la vérification.
Soit H_{ash} la fonction de hachage cryptographique :

$H_{ash} : \{0,1\}^* \rightarrow G1$

- **Génération des clés** :
  1. choisir un nombre aléatoire $\beta \in \mathbb{Z}_q^*$
  2. définir $sk := (\beta), pk := (z)$
  3. la paire de clés est : (pk, sk) .
- **Signature** :
  1. sk représente la clé sécrète et pk ($pk \ \in \ G2$) la clé publique. La clé secrète sk est utilisée pour générer la signature sur le message haché à l'aide de la

fonction de hachage H_{ash}.

2. $\sigma \leftarrow skH_{ash}(msg)$, avec $\sigma, H_{ash}(msg) \in G1$
3. la signature est (σ)

- **Vérification** : La vérification des signatures est effectuée grâce aux appariements et les opérations associées[37][139]. Ainsi :

$$\begin{aligned} e(g_2, \sigma) &= e(g_2, skH_{ash}(msg)) \\ &= e(skg_2, H_{ash}(msg)) \\ &= e(pk, H_{ash}(msg)) \end{aligned} \tag{2.2.1}$$

  - si $e(g_2, \sigma) == e(pk, H_{ash}(msg))$ alors la signature est approuvée, sinon elle n'est pas approuvée.

L'un des principaux avantages de la signature BLS est la prise en charge de l'agrégation de signatures [139][37].

- **Agrégation de signatures** : l'algorithme BLS prend en entrée n signatures (σ_i) avec $i \in [1; n]$ et fournit en sortie une signature unique (σ_A). $\sigma_A \in G1, \sigma_A = \prod_{i=1}^{n} \sigma_i$
- **Vérification signature agrégée** : $i \in [1; n]$, pk_i la clé publique de l'ensemble des utilisateurs n, $\sigma_A \in G1$ la signature agrégée.
  - Si $e(g_2, \sigma_A) == \prod_{i=1}^{n} e(pk_i, H_{ash}(msg_i))$ alors la signature agrégée est approuvée, sinon elle ne l'est pas.

La preuve de la vérification de la signature agrégée est exprimée comme ci-dessous :

$$\begin{aligned} e(g_2, \sigma_A) &= e(pk_1, H_{ash}(msg_1))...e(pk_n, H_{ash}(msg_n)) \\ &= \prod_{i=1}^{n} e(g2, \sigma_i) \\ &= \prod_{i=1}^{n} e(g2, sk_i H_{ash}(msg_i)) \\ &= \prod_{i=1}^{n} e(sk_i g2, H_{ash}(msg_i)) \\ &= \prod_{i=1}^{n} e(pk_i, H_{ash}(msg_i)) \end{aligned} \tag{2.2.2}$$

Si $msg_1 = ...msg_n = msg$,

$$e(g_2, \sigma_A) = e(pk_1...pk_n, H_{ash}(msg))) \tag{2.2.3}$$

2.2.8 Enjeux de la gestion des identités dans le cloud

Selon une étude du CSA [54], une gestion efficace et sécurisé des identités dans le cloud constitue l'un des éléments clés du développement d'un environnement cloud sécurisé. Cependant, la nature complexe de cet environnement est source de plusieurs défis en termes de gestion des identités pour les différents acteurs (organisations, utilisateurs, fournisseurs de services cloud) [92][107]. Ces défis sont de plusieurs types et concernent des problèmes de conformité, de réglementation, de contrôle, de gestion de plusieurs

identités, ainsi que des enjeux de protection de la vie privée et des données sensibles. Face à ces défis, les systèmes de gestion d'identité traditionnels ont connu une évolution afin de répondre aux exigences de cet environnement. Ainsi, plusieurs propositions seront établies grâce à des architectures de fédérations d'identités plus compatibles avec le cloud [3][104]. Selvanathan *et al.*, ont proposé dans [185], une approche de gestion fédérée des identités dans le but d'assurer l'interopérabilité des informations d'identifications entre des plateformes cloud hétérogènes. Dans [163], les auteurs ont proposé un modèle fondé sur un fournisseur d'identité utilisant la norme OpenID Connect pour l'authentification et l'autorisation des utilisateurs cloud.

Bien que ces solutions aient contribué à améliorer la gestion de l'identité dans le cloud, elles présentent toutefois certaines limites (point de défaillance et dépendance unique, vulnérabilité aux attaques Man in the Middle, identités non persistantes et non vérifiables, etc.) à considérer pour des déploiements dans des environnements collaboratifs, dynamiques, complexes et distribués. Afin de répondre à ces préoccupations, des recommandations sur les identités décentralisées ont été faites par le W3C [69] [206]. L'identité décentralisée est une identité numérique vérifiable de façon cryptographique, portable, qui ne dépend pas d'une autorité centrale et dont l'objectif principal est de donner le contrôle total de sa gestion à son détenteur légitime. Ainsi, l'émergence de la technologie blockchain et ses applications vont favoriser la proposition de plusieurs systèmes de gestion d'identité à partir de ces identifiants décentralisés pour des infrastructures cloud et des systèmes distribués. Dans [149], les auteurs ont proposé un système de gestion des identités utilisant un contrat intelligent sur une blockchain. Ce système élimine le tiers de confiance lors de l'authentification des utilisateurs en fournissant une copie locale des attributs stockés dans une blockchain. Bien que ce système propose la possibilité à l'utilisateur de gérer ses attributs, elle ne garantit pas totalement leur autonomie dans la mesure où le système est géré de façon hiérarchique par une autorité qui valide les attributs. Un modèle de contrôle d'accès décentralisé appliqué dans un environnement d'internet des objets (IoT) a été présenté dans [199]. Ce modèle fondé sur des identifiants décentralisés permet d'exécuter des contrats intelligents pour réguler l'accès aux objets connectés. L'accès à l'objet est autorisé si un nombre défini d'oracles signe numériquement la demande d'accès. L'utilisation des oracles décentralisés permet d'éliminer le point de défaillance unique. Cependant, le besoin de signatures multiples augmente le temps de traitement de la requête et l'espace de stockage requis sur la blockchain. Dans [1], les auteurs ont également proposé un système décentralisé de contrôle d'accès aux données dans un environnement IoT. Ce système fournit un mécanisme de gestion de la réputation des oracles, aidant ainsi les utilisateurs à sélectionner l'oracle de confiance. Dans [162], un système contre la contrefaçon et le vol de smartphone reposant sur la blockchain et les spécifications d'identités décentralisés et vérifiables est exposé. Ce système décentralisé sans autorité centrale propose un mécanisme de traçabilité et de suivi du cycle de vie des smartphones. Par ailleurs, il offre au propriétaire du smartphone un contrôle sur la gestion des informations d'identifications de l'appareil. Les mêmes paradigmes d'identités décentralisées ont été utilisés pour l'authentification des patients, le stockage et le partage de documents médicaux électroniques dans [142].

2.2.9 Discussion

Dans cette section, nous avons traité de l'identité numérique, des systèmes de gestion d'identité, des protocoles d'authentification et des algorithmes de signature numériques utilisés pour contrôler et valider ces identités. Ces mécanismes de gestion ont évolué avec l'avènement du cloud computing pour répondre aux défis de perfor-

mances, de stockages et de sécurité soulevés par la nature distribuée, hétérogène et dynamique de cette infrastructure. L'un des principaux apports est l'émergence des identifiants décentralisés. Ces identités digitales, associées à la technologie blockchain, vont permettre d'apporter des réponses à des problématiques majeures telles que les points de défaillance unique, de stockage distribué, de contrôle et de validation des preuves d'identité des utilisateurs. Cependant, les modèles proposés présentent des limites en ce qui concerne la prise en compte des éléments essentiels pour la réussite des systèmes de gestion d'identité, tel qu'énoncé dans les lois de Cameron [42]. En effet, de nombreuses lois de Cameron, à savoir le consentement de l'utilisateur, l'identité dirigée, les parties justifiables, sont capitales pour des systèmes de gestion décentralisés d'identités. Par ailleurs, notre champ d'application de cloud communautaire présente certaines spécificités qu'il convient de considérer. La diversité des organisations, dans ce type d'environnement, nécessite des prises de décisions et des actions volontaires, communes et consensuelles entre les entités. Ces entités doivent donc être identifiées et la non-répudiation des actes posés et des contrats de collaboration doivent être assurés. L'autre facteur important considéré dans les solutions de gestion d'identité est la confiance entre les acteurs, comme c'est le cas des cercles de confiance définis dans les systèmes de gestion fédérés d'identités. Toutefois, ce cercle de confiance préétablie et fondée sur des accords commerciaux ne correspond pas aux relations de confiance dynamique et évolutive qui doivent exister entre les entités dans un environnement de collaboration, incertain et hétérogène comme le cloud. Comment identifier et choisir les entités de confiance avec lesquelles collaborer ? Comment suivre et évaluer confiance pour des relations durables et prospères ? Ces interrogations nous amènent à l'analyse de la gestion de la confiance dans le cloud dans la section suivante.

2.3 Mécanismes de gestion de la confiance dans le cloud computing

2.3.1 Définition de la confiance

La confiance a fait l'objet de plusieurs travaux de recherche dans de nombreux domaines et champs scientifiques. Il en découle plusieurs interprétations de ce concept. En économie, la confiance est utilisée pour renforcer la coopération entre les acteurs et gérer le risque pour maximiser les gains. Du côté social, elle permet d'améliorer les relations sociales au sein d'une communauté dont les membres agissent de leur propre volonté et dans l'intérêt de ladite communauté [62]. Du point de vue de l'Internet et ses applications, la confiance a été définie comme la compétence d'une entité à agir de manière fiable, sûre et de fournir des services de qualité dans un contexte donné [78]. Toutes ces approches soulignent le rôle majeur et central de la confiance et la préconisent comme moyen d'aide à la prise de décision et son intégration dans les environnements incertains ou risqués [80]. En considérant les interactions au sein d'un cloud communautaire, nous pouvons définir la confiance comme ci-dessous :

Une organisation A fait confiance à une organisation B si elle s'engage dans une action de partage de ressources basée sur la croyance que les actions futures de l'organisation B lui permettront de disposer de la ressource et d'obtenir les résultats escomptés.

En tenant compte des différentes disciplines dans lesquelles la confiance intervient et des différentes définitions, plusieurs propriétés permettent de la caractériser.

2.3.2 Propriété de la confiance

Il ressort des principales propriétés que la confiance est :

- **relationnelle** : le Larousse définit la confiance comme un « *sentiment de quelqu'un qui se fie entièrement à quelqu'un d'autre, à quelque chose*». Cette définition exprime le fait que la confiance implique deux entités. Ce caractère relationnel est étroitement lié à l'aspect dynamique de la confiance, dans la mesure où la confiance se construit au fil du temps suite à des interactions répétées entre les parties engagées. La confiance est ainsi décrite comme un phénomène social où des individus interagissent dans la société [157].
- **dynamique** : la confiance est dynamique, car elle évolue au fil du temps, s'acquiert, se maintient, se dégrade, peut se perdre et se regagner dans une relation [201]. Cette dynamicité résulte de plusieurs facteurs, à savoir le comportement des entités, l'observation, les expériences (anciennes et nouvelles) [193]. La majoration des nouvelles expériences dans l'évaluation de la confiance est très importante, car les anciennes peuvent devenir obsolètes et non pertinentes.
- **institutionnelle** : la confiance institutionnelle découle d'une organisation qui fournit un cadre, favorise, encourage la coopération entre les membres, récompense les bons comportements et sanctionne les mauvais [137]. Dans son livre, *"Trust : The Social Virtues and the Creation of Prosperity"*, paru en 1995, l'économiste Francis Kukuyama exprime la confiance institutionnelle en montrant que la société en général peut être divisée en des communautés de niveaux de confiance distincts. Il conclut que les communautés à fortes valeurs de confiance entre ses membres sont les plus prospères et les plus respectueuses des lois [84].
- **subjective** : un individu A, peut accorder un niveau de confiance à un individu B sur sa capacité à réaliser une action précise. Un individu C peut toutefois accorder une valeur de confiance différente à l'individu B pour sa disposition à réaliser la même action. La confiance dans ce cadre n'est donc pas objective, mais plutôt une « *probabilité subjective par laquelle un individu A s'attend à ce qu'un autre individu B accomplisse une action donnée de laquelle dépend son bien-être* » comme défini par Gambetta dans [85]. La nature subjective de la confiance conduit à la personnalisation du calcul de la confiance et du fait que la confiance dépend de la situation, du contexte, des préjugés et des préférences.
- **contextuelle** : le contexte désigne les conditions ou la situation dans laquelle la relation est établie et la confiance est évaluée [220][6]. En illustration, une entité A fait confiance à une entité B en tant que spécialiste des moteurs Mercedes, mais l'entité A n'a pas confiance en l'entité B concernant les moteurs Tesla. Ainsi, l'entité B est digne de confiance dans le contexte des moteurs Mercedes, et non dans le contexte des moteurs Tesla.
- **mesurable**. La confiance est le résultat d'un calcul effectué par la personne qui fait confiance [187]. Elle est une croyance quantifiée quant aux habilités de l'entité en qui l'on croît. Cette quantification peut être une échelle de valeurs, généralement dans l'intervalle [0 – 1] ou une simple classification [93].
- **Asymétrique** : la confiance est asymétrique en ce sens que le fait qu'une entité A fasse confiance à une entité B ne signifie pas nécessairement que l'entité B fait confiance à l'entité A [187]. Elle résulte des différences de perception, d'opinion, de croyances et d'attentes des entités.
- **propagatrice** : la confiance est propagatrice, en ce sens que si une entité A, fait confiance à une entité B, qui à son tour fait confiance à une entité C, que l'entité

A ne connaît pas C, l'entité A, peut accorder une certaine confiance à l'entité C en fonction de la confiance qu'elle accorde à l'entité B et de la confiance que l'entité B accorde à l'entité C. Toutefois, la confiance n'est pas transitive. En revanche, la nature propagatrice de la confiance fait que l'information sur la confiance peut être transmise d'une entité à une autre sans être directement liée [220]. Il est important de différencier la transitivité au système de recommandation fondé sur la propagation de la confiance dans la proposition de Jøsang et al. dans [115].

- **composable**. la propriété propagatrice de la confiance permet de collecter des informations de confiance à travers les différentes branches sociales entre des entités qui ne sont pas directement liées. Ainsi, si plusieurs branches recommandent différentes valeurs de confiance à une entité, elle doit composer les informations reçues pour en déduire la confiance à accorder. À titre d'exemple, si une entité B est recommandée à l'entité A par plusieurs chaines de son réseau, l'entité A doit composer les informations reçues des différentes branches pour décider de faire confiance à l'entité B ou pas [187].

2.3.3 Concepts clés associés à la confiance dans les systèmes d'information

Plusieurs concepts sont assimilés ou associés à la confiance en raison de sa complexité et de sa pluridisciplinarité. Dans cette section, nous aborderons les principales notions telles que la réputation, la recommandation, la sécurité et le risque.

2.3.3.1 La réputation

La confiance et la réputation sont des concepts très proches et parfois confondus, mais il est important de les différencier. Cette proximité est liée au fait qu'elles sont fondées sur une perception de l'autre dans un contexte (un moment, un endroit, etc.) bien précis [62]. En effet, La confiance est une notion qui consiste à se fier à l'authenticité des informations fournies par une entité en qui on a confiance, ce qui engendre de la réputation, car les informations provenant de cette dernière ont une valeur vis-a-vis d'autres entités. En conséquence, la réputation peut être considérée comme un moyen de renforcer et d'évaluer la confiance, on peut faire confiance à un individu s'il a bonne réputation [116]. Par ailleurs, la réputation est la vision qu'on a d'une entité en fonction des expériences passées sans aucun indice sur ces agissements futurs alors que la confiance fait une prévision sur ses comportements futurs sur la base de l'expérience ou les recommandations d'autres entités. La confiance est ainsi une relation et une perception locale entre deux entités. Là, où la réputation se présente comme un attribut et une perception globale de toutes les entités d'une organisation concernant les actions d'un de ses membres. Cela explique le fait qu'il est parfois bien plus facile de se fier d'abord sur la réputation plutôt que sur la confiance [200]. Dans le contexte d'une communauté collaborative, la réputation est alors une mesure collective de la confiance d'une entité établie à partir des évaluations des membres de la communauté sur les activités antérieures de cette dernière [116]. Les concepts de confiance et de réputation font généralement appel à une autre notion : la recommandation [116].

2.3.3.2 La recommandation

La recommandation est le processus par lequel le niveau de confiance d'une entité A en une entité B, sans interactions antérieures entre elles, s'évalue au travers des connaissances sur l'entité B communiquées par d'autres entités à l'entité A. Elle sert à combler le manque d'informations sur une entité inconnue. En général, dans la vie courante, on établit un avis sur une personne inconnue et la confiance à lui accorder en fonction des

recommandations positives ou négatives de notre entourage, au regard de leurs expériences personnelles avec cet inconnu [111]. La recommandation permet de construire la confiance sans interaction directe et de la propager à travers un réseau dans un domaine spécifique. Une entité A peut recommander de façon directe une entité C à une entité B ou indirectement en publiant et partageant son avis sur l'entité C sur l'ensemble du réseau. Comme la confiance, la recommandation peut être une valeur qualitative ou quantitative [116].

2.3.3.3 Sécurité

La confiance et la sécurité sont deux notions qui sont intrinsèquement liées et sont confondues dans plusieurs recherches. Les systèmes de gestion de la confiance ont longtemps traité la confiance et la sécurité de manière similaire [36][215][213]. En effet, les mécanismes de confiance déployés visaient à protéger les ressources contre les accès malveillants sans pour autant mettre l'accent sur la fiabilité et la confiance à accorder aux entités authentifiées. Il est important de faire la part entre techniques et outils de sécurisation, et les moyens à déployer pour évaluer la confiance des ressources et des utilisateurs du système d'information. Cette différence entre la sécurité et la confiance a été évoquée par Rasmussen et Jansson dans [173] au travers des notions de sécurité dure et de sécurité douce. Ils qualifiaient de sécurité dure les mécanismes traditionnels, à savoir l'authentification et le contrôle d'accès, et de sécurité douce ou sociale les techniques de gestion de confiance et de réputation.

2.3.3.4 Le risque

Le risque est lié à des évènements qui peuvent se réaliser ou pas. Faire confiance, c'est prendre un risque et coopérer sans avoir les éléments nécessaires pour prédire les résultats, ce qui entraîne une incertitude [116]. D'où le rapport étroit entre le risque et la confiance. La confiance est l'élément central de toute décision qui peut comprendre un risque, tandis que le risque renforce le lien de confiance dans une relation entre deux individus [56]. Comme la confiance, le risque intervient dans plusieurs disciplines avec plusieurs définitions et représentations. Ainsi, l'Organisation Internationale de Standardisation (ISO) [195] défini le risque comme *« la combinaison de la probabilité d'occurrence d'un évènement indésirable et de ses conséquences. »*. Le risque est ainsi formalisé comme ci :

$$Risque = Probabilité\ d'un\ évènement\ X\ Impact\ de\ l'évènement \tag{2.3.1}$$

Marsh a proposé une représentation du risque reposant sur un rapport entre les coûts et les bénéfices [143] :

$$Risque = \frac{Coûts}{Bénéfices} \tag{2.3.2}$$

Le secteur de la sécurité informatique propose une définition à travers le NIST qui décrit le risque comme le produit de la probabilité d'une menace sous forme d'attaque, en profitant d'une vulnérabilité potentielle et l'impact de cet événement sur l'organisation [91].

2.3.4 Modèles de gestion de la confiance

2.3.4.1 La gestion de la confiance

La première définition de la gestion de la confiance a été introduite par Blaze et al. et était axée sur une autorisation accordée à une entité en fonction d'un ensemble d'informations défini dans une politique de sécurité donnée. Ils ont ainsi défini la gestion de la confiance comme une méthode pour définir et exécuter des règles de politiques permettant d'autoriser ou non des actions [35][36]. Ainsi, une entité A ne peut engager une action vis-à-vis d'une entité B que si elle possède et présente les habilitations requises. L'entité B ne sera donc pas en mesure de lui accorder sa confiance que si les informations présentées sont valides et conformes à la politique de sécurité. La notion de gestion de la confiance va par la suite évoluer et être adoptée dans plusieurs domaines d'internet tels que les services web, le commerce électronique et plus récemment le cloud computing. De ce fait, une définition plus globale et consensuelle va émerger et présenter la gestion de la confiance comme « *l'activité de rassembler, de codifier, d'analyser et de présenter les preuves concernant la compétence, l'honnêteté, la sécurité et la fiabilité d'une entité en vue de prendre des décisions* » [179]. En d'autres termes, la gestion de la confiance est une démarche stratégique de résolution de problèmes de confiance dans le but de fournir les outils nécessaires à une entité pour déterminer (modéliser, calculer, mesurer, évaluer) le niveau de confiance à accorder à une autre entité.

2.3.4.2 Modéliser et mesurer la confiance

La confiance, malgré son caractère pluridisciplinaire, est fondamentalement orienté sur les relations sociales entre les individus [62]. En conséquence, l'application de la confiance dans les systèmes informatiques nécessite de la modéliser ainsi que les notions connexes afin d'atteindre les objectifs visés. Cette modélisation est généralement effectuée grâce à des théories mathématiques. L'une des principales approches est celle défendue par Abdul-Rahman et Hailesconsite [5], et consiste en une représentation du niveau de confiance par des valeurs discrètes. La valeur de confiance est un élément d'un ensemble fini de six éléments :

{Méfiance, Ignorance, Confiance minimale, Confiance moyenne, Bonne confiance, Confiance complète}

Ainsi, ils considèrent la confiance comme une croyance de l'expérience personnelle dans un contexte, et qui se propage dans le système sous forme de réputation. En dépit de la simplicité de cette approche, elle est trop rigide et offre peu d'options pour représenter certaines situations dynamiques. En effet, cette approche ne permet pas de représenter la confiance si une entité X accorde une « *très bonne confiance* » à Y. Par ailleurs, il est impossible d'exprimer le fait que l'entité X ait une « *confiance moyenne* » en Y et Z, mais préfère Z à Y [62]. Une alternative à cette proposition est la représentation du niveau de confiance par une valeur comprise dans un intervalle, généralement $[0\,;\,1]$ et qui peut être étendu à d'autres types d'intervalles. La transition de la forme discrète à une représentation continue a permis de prendre en comptes les préférences des entités et de déterminer plus finement les valeurs de confiance dans des environnements complexes comme le cloud. Ainsi, cette approche a été adoptée dans plusieurs travaux [200][145][122].

La confiance étant liée à l'incertitude, plusieurs méthodes fondées sur les théories de probabilités ont été proposées pour la représenter. Les principales sont : la théorie de Dempster-Shafer [222], la logique floue [77], la logique modale [70] et la logique subjective [110][111]. Cette dernière classe de logique probabiliste permet de spécifier des va-

leurs de probabilité avec des degrés d'incertitude. En prenant en compte l'incertitude, elle permet de raisonner avec des modèles dans des situations incertaines, d'absences de preuves ou d'informations incomplètes [110][47]. La logique subjective est utilisée dans le cas des évènements dont les estimations de probabilités sont incertaines. Le principal avantage de la logique subjective est d'aider à l'analyse et à la modélisation de manière plus réaliste de faits du monde réel, avec des résultats exprimant plus significativement l'ignorance et l'incertitude. Les valeurs de confiance ou opinions sont déterminées à partir de quatre paramètres dans la logique subjective : la croyance (b), l'incrédulité(d), l'incertitude (u) et le taux de base (α).

L'opinion de confiance d'une entité A à l'égard d'une entité B est formulée comme ci :

- Pour une interaction directe entre deux les deux entités :

$$\omega_B^A = b + (\alpha * u) \; avec \; b, d, u, \alpha \in [0,1] \; et \; b + d + u = 1 \tag{2.3.3}$$

$$\begin{cases} b = \frac{p_t}{p_t + n_t + 2} \\ d = \frac{n_t}{p_t + n_t + 2} \\ u = \frac{2}{p_t + n_t + 2} \end{cases} \iff \begin{cases} p_t = \frac{2b}{u} \\ n_t = \frac{2d}{u} \end{cases} \tag{2.3.4}$$

avec p_t le nombre d'échanges positifs précédents entre A et B, et n_t le nombre de transactions négatives. Une valeur de confiance de référence peut être accordée à toute entité en l'absence d'éléments spécifiques permettant de l'exprimer. Cette valeur représente le taux de base α. Elle varie selon que l'entité, soit digne de confiance ou non.

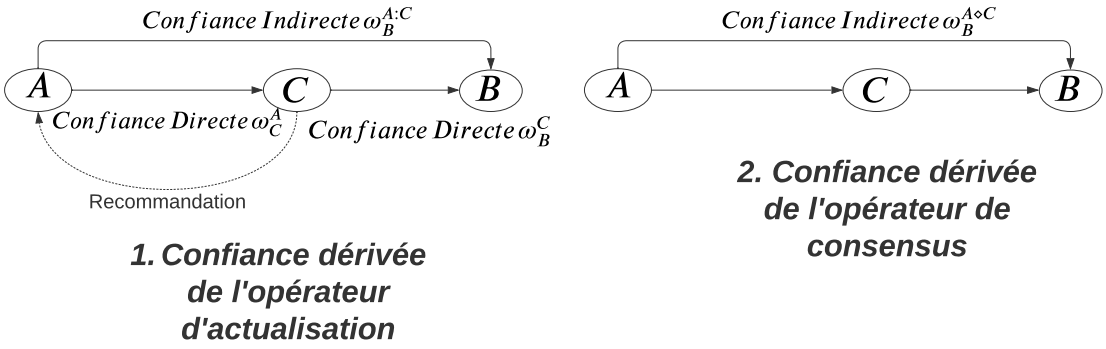


FIGURE 2.7 : Confiance dérivée d'interactions indirectes

- Dans les cas d'interactions indirectes ou recommandées :

  Pour inférer des valeurs de confiance, plusieurs opérateurs sont définis par la logique subjective [110]. Considérons trois entités A et B et C comme représentées sur la figure 2.7 ci-dessus. ω_C^A est la confiance de A en C et ω_B^C la confiance de C en B. La confiance indirecte entre A et B sera calculée comme l'opinion $\omega_B^{A:C}$ grâce à l'opérateur d'actualisation($\bigotimes$) :

$$\omega_B^{A:C} = \omega_C^A \bigotimes \omega_B^C \begin{cases} b_B^{A:C} = b_C^A b_B^C \\ d_B^{A:C} = b_C^A d_B^C \\ u_B^{A:C} = d_C^A + u_C^A + b_C^A u_B^C \\ \alpha_B^{A:C} = \alpha_B^C \end{cases} \tag{2.3.5}$$

  Par ailleurs, s'il existe deux opinions éventuellement contradictoires, telles que ω_B^A représente la confiance de A en B et ω_B^C est la confiance de C en B . La confiance

dérivée entre A et B est $\omega_B^{A\diamond C}$. Elle est exprimée ci-après grâce à la logique subjective et son opérateur de consensus ($\bigoplus$) [110][112] :

$$\omega_B^{A\diamond C} = \omega_B^A \bigoplus \omega_B^C \begin{cases} b_B^{A\diamond C} = \frac{b_B^A u_B^C + b_B^C u_B^A}{u_B^A + u_B^C - u_B^A u_B^C} \\ d_B^{A\diamond C} = \frac{d_B^A u_B^C + d_B^C u_B^A}{u_B^A + u_B^C - u_B^A u_B^C} \\ u_B^{A\diamond C} = \frac{u_B^A u_B^C}{u_B^A + u_B^C - u_B^A u_B^C} \\ \alpha_B^{A\diamond C} = \alpha_B^A \end{cases} \tag{2.3.6}$$

Avec $u_B^A + u_B^C - u_B^A u_B^C \neq 0$

2.3.4.3 Systèmes de la gestion de la confiance

Le système de gestion décrit les modalités de collectes d'informations et de détermination des valeurs de confiance. La valeur de confiance peut être obtenue à partir de résultats d'interactions directes, d'informations obtenues par recommandation ou par combinaison de ces deux valeurs [169]. Par ailleurs, la valeur de confiance peut être déduite dans certains cas à l'aide de la réputation. Elle est la résultante des expériences antérieures d'une entité [32]. Un système de gestion de confiance efficace doit prendre en compte les principales propriétés de la confiance mentionnées dans la section 2.3.2 cidessus [169]. Nous distinguons quatre principaux systèmes de gestion de la confiance fondés respectivement sur la politique, la réputation, la recommandation et la prédiction.

- **Système de gestion fondé sur la politique** : première technique de gestion de la confiance introduite par Blaze et al. [35]. Ce modèle utilise des politiques pour déterminer si une entité est autorisée à accéder à une ressource ou non. Ces autorisations sont formalisées grâce à des règles qui décrivent les exigences requises pour obtenir la confiance [160]. Ainsi, en fonction des politiques à respecter, une entité sera considérée comme digne de confiance ou non. Dans ce modèle, la valeur de confiance est généralement binaire et permet d'autoriser ou non l'accès à une ressource, d'approuver ou non un utilisateur. Plusieurs solutions ont été proposées par la communauté scientifique à partir de cette technique de gestion de la confiance dont PolicyMaker [35], KeyNote [34], The TrustBuilder [215], etc.
- **Système de gestion fondé sur la réputation** : particulièrement adaptés aux environnements collaboratifs comme les plateformes e-commerce, les systèmes de confiance fondés sur la réputation utilisent les interactions ou expériences directes entre entités et /ou l'expérience des autres, pour le choix de faire confiance à une autre entité. Le principe de ces systèmes consiste à utiliser des informations sur le comportement passé du digne de confiance et les recommandations d'autres entités pour évaluer la confiance que l'on peut accorder à cette entité [160]. La réputation est alors considérée comme la croyance de la communauté vis-à-vis d'une entité et sert à évaluer la confiance [224]. Des techniques spécifiques sont utilisées pour recueillir, rassembler et diffuser la réputation d'une entité dans le système. Par ailleurs, des mécanismes computationnels permettent de calculer la valeur de réputation [224][116]. Les plateformes e-commerce Amazon et eBay sont des cas pratiques de mise en œuvre de cette gestion de la confiance axée sur la réputation [160]. Ces systèmes permettent de mettre en exergue le caractère évolutif et dynamique de la confiance [99]. En effet, la confiance dans ce contexte est évaluée sur la base de l'historique des interactions et des comportements passés d'une entité qui peuvent varier. Toutefois, cette évaluation peut être corrompue par des

avis biaisés involontairement ou volontairement d'entités malveillantes, affectant ainsi la réputation d'une entité.

- **Système de gestion fondé sur la recommandation** : dans ces modèles de gestion, l'entité confiante détermine la valeur de confiance accordée au digne de confiance sur la base du partage d'expérience ou des recommandations d'autres entités confiantes [148][160]. Ces recommandations peuvent être directes (explicites) ou transitives. Cette technique de gestion de la confiance a été utilisée dans les modèles de référence EigenTrust [122] et PageRank de Google [134], ainsi que dans les technologies internet telles que les services web, les sites e-commerce, les réseaux sociaux et les infrastructures cloud [148]. À l'instar des systèmes fondés sur la réputation, les systèmes axés sur la recommandation sont confrontés à plusieurs types d'attaques (fausses évaluations, attaques Sybil) afin de corrompre les évaluations de la confiance [148].
- **Système de gestion fondé sur la prédiction** : dans les situations caractérisées par le manque d'informations préalables concernant une entité digne de confiance, le modèle de gestion fondé sur la prédiction se présente comme la solution adéquate pour évaluer la confiance [170][160]. Le principe de cette technique est de prédire le comportement d'une entité sur la base de mécanismes de similarité ou par analyse d'informations historiques [191]. Les mécanismes de similarité permettent de distinguer deux entités avec des profils identiques du fait que ces entités sont susceptibles de se faire confiance [160][159]. Cette technique a été utilisée dans les travaux présentés dans [159] pour déterminer des retours d'informations biaisées et dans les environnements cloud [96].

2.3.5 Gestion de la confiance dans le cloud

La confiance est considérée comme l'un des principaux obstacles à l'adoption du cloud computing. Par conséquent, différents modèles de confiance ont été proposés pour garantir la confiance dans le cloud et favoriser son adoption. Dans [125], un modèle de confiance à plusieurs niveaux (MTLTA) basé sur l'algorithme ABC (Artificial Bee Colony) a été proposé. Cette technique dynamique améliore la précision et la fiabilité de la gestion de la confiance entre les différentes entités. Cette contribution permet de déterminer les entités malveillantes à partir des évaluations des interactions précédentes et aide à choisir le fournisseur de service ayant la plus forte valeur de confiance. L. Guo et al. ont présenté dans [94], un modèle de gestion de la confiance fondé sur la confiance mutuelle avec un mécanisme de récompense avec punition. Le modèle permet d'identifier efficacement les utilisateurs et fournisseurs non fiables et d'augmenter le taux de réussite des transactions. La particularité de ce système est qu'il prend en compte les opinions de l'utilisateur et du fournisseur en exprimant explicitement la confiance mutuelle entre eux. Il tient également compte de l'impact du coût du service sur le choix du fournisseur et élimine les mauvais acteurs grâce au mécanisme de récompense avec punition. InterTrust, une technique de gestion de la confiance établie à partir de la logique subjective a été introduite dans [131]. Elle expose une amélioration de l'algorithme de gestion de la confiance Trust Network Analysis with Subjective Logic (TNA-SL) [111] en termes de réduction significative du temps d'exécution et d'évolutivité.

La diversité des offres de services et le taux croissant des besoins des utilisateurs nécessite une coopération entre fournisseurs de services. Une architecture de collaboration entre fournisseur de service appelé cloud fédéré peut être mise en place. Cette plateforme permettra aux fournisseurs de partager leurs ressources et leurs services excédentaires afin de fournir des services avec des qualités de service (QoS) conformes aux contrats de niveau de service (SLA) établis avec les utilisateurs [130]. Plusieurs

études pour garantir la confiance dans ce type environnement ont été menées par des chercheurs. Dans [165], K. Papadakis et al., ont proposé Reputation-based Trust Management (RTM), une plateforme collaborative de gestion des accords de niveau de service et de confiance pour les fournisseurs de services dans une fédération de cloud. Le système permet d'évaluer les services sur la base des SLA et des indicateurs clés de performance. Il est associé à un système de gestion de la confiance établi à partir de la réputation pour aider à la sélection des futurs fournisseurs. Performance based Risk driven Trust (PRTrust) a été présenté dans [130]. Ce modèle permet l'établissement d'une confiance fondée sur la performance et le risque pour le partage sécurisé de services. Il s'agit d'une extension du modèle EigenTrust [123]. Il fournit un mécanisme établi à partir de la réputation et évalue le risque afin de l'utiliser comme seuil de confiance pour la sélection des fournisseurs de services dans un environnement cloud fédéré en architecture pair à pair. Dans [171], les auteurs ont proposé un système de recommandation de service cloud utilisant un algorithme de calcul de degré de confiance fondé sur le clustering. Cet algorithme s'appuie sur des paramètres QoS, et offre un gain de temps dans le calcul du degré de confiance. Par ailleurs, il constitue un outil de recommandation efficace de services de confiance aux utilisateurs. Une étude dans [135] a présenté, Federated Cloud Trust Management Framework (FCTMF), un cadre de gestion de la confiance dans une fédération de cloud pour garantir la confiance entre les fournisseurs et les inciter à être actifs dans la fédération. Ils ont atteint leur objectif en se basant sur le SLA et les retours d'informations du client et du fournisseur pour déduire les valeurs de confiance. H. Kurdi et al., ont proposé dans [132], TrustyFeer, un système de gestion de la confiance pour améliorer la qualité de service en utilisant la logique subjective. Cette technique présente de meilleurs résultats en termes de réductions de services non conformes au SLA par rapport aux modèles TNA-SL et EigenTrust. WhatsTrust a été proposé dans [12]. C'est un modèle de gestion de la confiance pour le réseau social WhatsApp basée sur la logique subjective. Il permet de calculer les valeurs de réputation des utilisateurs et de détecter les utilisateurs malveillants. Dans [102], les auteurs ont présenté, un modèle d'organisation en domaine dans une fédération de cloud (ODTMF). Ce modèle étend la logique subjective grâce à un opérateur de fusion de poids et fournit une évaluation de la confiance entre les organisations au sein d'un domaine et entre des organisations de domaine distinct.

Les problèmes de confiance découlent de l'incertitude concernant la qualité des ressources et des entités engagées. La qualité pouvant être considérée en termes de fonctionnalités, de fiabilité et de sécurité des ressources. Par conséquent, sécuriser les ressources, c'est garantir un niveau de confiance élevé. Des infrastructures cloud digne de confiance doivent intégrer des mesures ou techniques de sécurité. Dans [75], un système sécurisé d'allocation de ressources (MSMC) entre plusieurs organisations au sein d'un cloud communautaire est proposé. Le système est composé de trois (3) algorithmes pour l'allocation des ressources et pour l'exécution du flux de travail. Le modèle offre des avantages en termes de gain de temps, de coûts et de respect des accords SLA. S. Garg et al., ont présenté SMICloud dans [87], un modèle d'évaluation de la qualité des services basé sur les indices de mesures de services (SMI) du CSMIC consortium. Le SMIcloud s'appuie sur des attributs tels le temps de réponse, la disponibilité, la fiabilité, la précision, la transparence, la sécurité et la disponibilité. Ce mécanisme basé sur le processus hiérarchique analytique (AHP) permet de classer les services sur la base des exigences de QoS.

2.3.6 Discussion

Cette section nous a servi de cadre pour présenter la confiance, ses principales propriétés, ainsi que les fondements mathématiques permettant de la modéliser et les principaux systèmes d'évaluation de la confiance. Ces modèles de gestion de la confiance proposés sont fondés sur la politique de sécurité, la réputation, la recommandation ou la prédiction. Par ailleurs, un état de l'art de la gestion de la confiance dans le cloud a été exposé. Il ressort de cette analyse bibliographique, que les modèles de gestion de la confiance dans le cloud proposés utilisent les retours d'informations des différents acteurs et des paramètres de qualité de service pour déterminer les valeurs de confiance. En outre, ces travaux ont été effectués dans des environnements de déploiement de cloud fédéré ou public. Bien que la fédération de cloud possède des caractéristiques d'un cloud communautaire, elle peut cependant être la combinaison de plusieurs types de déploiements (public, privé et communautaire), et donc ne répond pas exactement aux exigences et mode de gouvernance d'un cloud communautaire. En outre, il n'existe pas de travaux spécifiques sur l'évaluation de la confiance dans un cloud communautaire à notre connaissance dans la littérature. Enfin, l'intégration de mécanismes de sécurité aux modèles de confiance permet de maintenir un niveau de confiance élevé et durable entre les entités. Le fait que les premiers modèles de gestion de la confiance [35] soient fondés sur la gestion des accès et des autorisations, confirme cette dernière assertion. D'où, l'importance de la gestion des accès et des autorisations dans la sécurisation des systèmes d'information en général et en particulier dans les environnements de partage de ressources. Dans la section suivante, nous présentons les différents modèles de contrôle d'accès utilisés, et plus particulièrement ceux déployés dans les environnements cloud et les systèmes distribués de collaboration.

2.4 Modèle de contrôle d'accès dans le cloud computing

2.4.1 Politiques et modèles de contrôle d'accès

L'ensemble des procédures, lignes directrices ou règles de sécurité qui régissent le fonctionnement d'une organisation représente la politique de sécurité organisationnelle de cette organisation [60]. Cette politique peut être élaborée par l'organisation elle-même ou par des organismes législatifs ou réglementaires tiers. Elle a pour objet de mettre en place des objectifs de sécurité qui doivent être satisfaits, ainsi que des règles décrivant la vision globale et le plan d'évolution de l'organisation en matière de sécurité. La politique de sécurité est ainsi un axe important de la politique globale de l'organisation. Elle doit être en adéquation avec les objectifs, intégrer ou être associée à des mécanismes de détection de risques, de gestion de conflits et de vérifications de la conformité avec les mesures de base établies [24]. La politique de sécurité doit prévoir un plan de mise en œuvre précis et utiliser des techniques et des mécanismes de sécurité (dispositifs et critères d'authentification, liste de contrôle d'accès, règles de filtrage réseaux et applicatifs, algorithmes cryptographiques et de chiffrement, etc.) [97]. De façon générale, une politique de sécurité permet de gérer les autorisations et éventuellement les obligations au sein du système. Elle vise à permettre l'accès aux ressources aux utilisateurs authentifiés et légitimes tout en refusant l'accès aux non authentifiés, afin de prévenir et d'interdire les actions malveillantes. Ces politiques sont formalisées et déployées à travers des modèles de contrôle d'accès. Un modèle de contrôle permet de représenter la politique de sécurité et de réduire la complexité de celle-ci. Il permet de vérifier la complétude, la cohérence et la conformité d'une politique de sécurité en fonction de la vision globale de l'organisation [24]. De nombreux modèles de contrôle d'accès ont été proposés pour la sécurité des systèmes d'informations des organisations, mais éga-

lement pour des infrastructures informatiques récentes de plus en plus collaboratives, distribuées et multi-organisationnelles.

2.4.2 Modèles de contrôle d'accès classiques

Les modèles de contrôle d'accès ont longtemps fait l'objet d'une attention particulière de la part des chercheurs [17][188]. Nous présentons dans cette section les principaux modèles de références, à savoir le modèle discrétionnaire, le modèle obligatoire, le modèle fondé sur les rôles et le modèle axé sur l'organisation.

2.4.2.1 Contrôle d'accès discrétionnaire

Rendu populaire par son intégration dans les systèmes d'exploitation tels que Windows 2000 et Unix, le contrôle d'accès discrétionnaire ou Discretionary Access Control (DAC) permet d'attribuer des droits ou des privilèges d'accès sur les données ou les objets en fonction de l'identité ou des groupes des utilisateurs [97][133]. Les droits sont établis au moyen d'une matrice de contrôle d'accès dans laquelle un sujet est associé à une ligne et une colonne à un objet. Partant de ce principe, cette forme de gestion matricielle a un impact sur les performances de recherche et nécessite des espaces de stockage importants. En conséquence, l'autre option offerte par le DAC est l'utilisation des listes de contrôle d'accès (ACL) pour représenter les droits sous la forme d'un tableau de sujets associés à leurs droits individuels sur l'objet [133][188]. Les ACL sont efficaces, mais elles présentent des limites pour des systèmes avec un grand nombre d'utilisateurs ou d'objets [17]. Par ailleurs, la capacité de contrôle des droits sur les objets offerte aux utilisateurs, ainsi que l'absence de préservation de la confidentialité et de contraintes de copie de fichier, constituent des limites du système de contrôle d'accès discrétionnaire, le rendant non adapté à des environnements complexes comme le cloud computing [188].

2.4.2.2 Contrôle d'accès obligatoire

Contrairement au modèle d'accès discrétionnaire, dans le modèle d'accès obligatoire ou Mandatory Access Control (MAC), les droits d'accès sont exclusivement définis et gérés par un administrateur [188]. Le MAC propose une approche de sécurité à plusieurs niveaux, grâce au modèle de Bell et La Padula [29] qui permet à l'administrateur, d'attribuer différentes étiquettes de sécurité aux sujets et aux objets. Des travaux d'améliorations du modèle ont été proposées [31]. Malgré cela, ce modèle présente des inconvénients en termes de complexité de déploiement et de coûts de gestion. Par ailleurs, le MAC ne tient pas compte des principes de délégation, d'héritage et de moindres privilèges ainsi que de la séparation des tâches [17].

2.4.2.3 Contrôle d'accès fondé sur les rôles

Le modèle de contrôle d'accès fondé sur les rôles ou RBAC (pour Role-Based Acces Control [79][180] a été proposé afin d'apporter des solutions aux limites de ces prédécesseurs, à savoir DAC [97] et MAC. Dans RBAC, la politique de contrôle d'accès ne s'applique pas directement aux utilisateurs et les permissions ne sont plus liées de manière directe aux sujets, mais plutôt à travers des rôles, qui regroupent des sujets qui remplissent les mêmes fonctions. Un rôle est une abstraction d'une fonction exercée au sein de l'organisation. Des droits d'accès représentant des permissions ou des privilèges sont associés aux rôles. Quant à une permission, elle désigne les droits conformes aux tâches qui peuvent être exécutées par un rôle. En d'autres termes, le modèle RBAC

permet de spécifier en fonction des rôles assignés quels sujets a droit à accéder à une ressource donnée, et ne peut accéder à une ressource qu'un utilisateur ayant un rôle associé à cette ressource. Toutefois, un utilisateur peut avoir un ou plusieurs rôles et une ou plusieurs permissions peuvent être associés à chaque rôle. Il n'est donc pas nécessaire d'actualiser l'ensemble de la politique de contrôle d'accès en cas de création d'un nouveau sujet, mais plutôt d'attribuer le rôle à ce sujet, ce qui simplifie l'administration de la sécurité du système. Par ailleurs, ce modèle aide à maîtriser la complexité de la gestion des règles d'autorisation au travers du mécanisme d'héritage entre les rôles [24].

Malgré ces avantages, le modèle RBAC présente plusieurs limites. En effet, le modèle ne tient pas compte du contexte (temporel, spatial, etc.) dans l'attribution des droits, ainsi que de la nature dynamique et aléatoire du comportement des utilisateurs. De plus, il ne permet pas l'activation dynamique des droits accès et ne fournit pas des moyens de séparation des tâches des rôles [188]. Ces inconvénients ont pour conséquence de compliquer l'application du RBAC dans des systèmes dynamiques, distribués et dans des environnements dans lesquels plusieurs organisations collaborent.

2.4.2.4 Contrôle d'accès axé sur les organisations

Le modèle fondé sur l'organisation ou OrBAC (Organization-based Access Control) est un modèle de contrôle d'accès dérivé du modèle RBAC. Ce modèle a la particularité de permettre la définition de politique de contrôle d'accès en deux niveaux. Un niveau constitué d'entités abstraites (Rôle, Vue, Activité) et un niveau d'entités concrètes (Sujet, Objet, Action). Cette architecture permet d'exprimer des règles de politique de sécurité sur des entités abstraites indépendamment de leur implémentation [120]. Ce qui constitue le principal avantage de ce modèle. Ainsi, les entités concrètes exécutent des actions sur des objets grâce à des processus de contrôle fondés sur les règles de la politique de sécurité. À chaque entité abstraite est associée une entité concrète. De ce fait, un rôle est une abstraction d'un groupe d'utilisateurs exerçant une fonction dans l'organisation, une vue est un ensemble d'objets et l'ensemble des actions est représenté par une activité. La validité d'une règle peut dépendre de la situation d'une entité ou de conditions spécifiques dans lesquelles les privilèges sont accordés. OrBAC introduit dans ce cas la notion de contexte qui permet de modéliser les circonstances dans lesquelles les sujets sont autorisés à réaliser des actions sur des objets [120].

Le modèle OrBAC permet de spécifier les relations ci-dessous entre les entités de l'organisation :

- $Permission(org, r, v, a, c)$: l'organisation org autorise le rôle r à effectuer l'activité a sur la vue v dans un contexte c ;
- $Habilite(org, s, r)$: l'organisation org habilite un sujet s dans un rôle r ;
- $Utilise(org, o, v)$: l'organisation org utilise l'objet o dans la vue v ;
- $Considère(org, \alpha, a)$: l'organisation org considère l'action α comme faisant partie de l'activité a ;
- $Définit(org, s, \alpha, o, c)$: l'organisation org autorise l'action α du sujet s sur l'objet o si le contexte c est vrai.

OrBAC permet à travers des règles de sécurité de définir des obligations, des permissions, des interdictions et des recommandations. Ces règles sont formalisées comme ci-dessous :

$$Predicat(org, r, v, a, c) \tag{2.4.1}$$

où *org, r, v, a, c* représentent respectivement une organisation, un rôle, une vue, une activité et un contexte, et *Predicat* correspond soit à une permission, une obligation, une interdiction ou une recommandation. Les règles du modèle sont exprimées formellement à l'aide de la logique du premier ordre [120]. Une occurrence d'une permission d'un sujet autorisé à effectuer une action sur un objet est présentée dans le tableau 2.1 ci-dessous.

TABLE 2.1 : Spécification d'une permission avec OrBAC

$org \in Organisations, s \in Sujets, \alpha \in Actions, o \in Objets, a \in Activités, v \in Vues, c \in Contextes,$ *Permission*(org, r, v, a, c) $\wedge$ *Habilite*(org, s, r) $\wedge$ *Utilise*(org, o, v) $\wedge$ *Considère*(org, α, a)$\wedge$ *Définit*(org, s, α, o, c) $\rightarrow$ *Est_Permis*(s, α, o)

Cette règle signifie que si dans l'organisation org, le rôle r est autorisé à effectuer l'activité a sur la vue v quand le contexte c est vrai, et si le rôle r est assigné au sujet s, l'action α fait partie de l'activité a, l'objet o fait partie de la vue v, le contexte c est vrai pour les entités (org, s, α, o), alors le sujet s est autorisé à réaliser l'action α sur l'objet o.

On définit sur cette même base :

- $\rightarrow Est\_Obligé$ pour une obligation,
- $\rightarrow Est\_Interdit$ pour une interdiction,
- $\rightarrow Est\_Recommandé$ pour une recommandation

Le modèle OrBAC répond à la problématique de contexte souligné dans RBAC [63], et propose une représentation formelle des règles permettant de gérer de façon statique les conflits entre les règles, ce qui apporte de la souplesse dans l'administration des politiques. En outre, ce modèle est axé sur le concept d'organisation, qu'il définit comme un ensemble de sujets. Un sujet pouvant être soit un utilisateur ou une organisation. Il est ainsi possible avec OrBAC de définir une hiérarchie d'organisation pouvant collaborer entre elles [120]. Cette architecture suppose une organisation suprême au-dessus, imposant sa politique aux autres aux dépens du principe d'autonomie dans les systèmes collaboratifs et distribués. De ce fait, le modèle OrBAC n'est pas particulièrement adapté pour la gestion des accès dans le cloud et les systèmes collaboratifs autonomes. Les principales méthodes de contrôle d'accès proposées pour ce type d'infrastructure sont présentées dans la section suivante.

2.4.3 Modèles de contrôle d'accès pour le cloud et les systèmes collaboratifs

Les systèmes de collaboration permettent à des entités (utilisateurs ou à des organisations) de collaborer par le partage de données et de services. Ces systèmes peuvent être construits autour de deux types d'architectures : centralisée ou décentralisée. L'architecture centralisée permet de proposer des modèles de contrôle qui consistent à imposer

une politique de sécurité globale et centralisée aux acteurs. Elle requiert une autorité centrale qui peut être source de défaillance, de problèmes de confidentialité et de violation de l'autonomie des organisations [15]. Contrairement à la structure centralisée, l'architecture décentralisée est adaptée aux systèmes distribués et permet aux organisations de rester autonomes dans la définition de leur propre politique de sécurité. Plusieurs modèles vont être proposés pour ce type d'infrastructure de collaboration. Ainsi, F. Cuppens et al., ont présenté dans [64] le modèle O2O (Organization to Organization) permettant de gérer l'interopérabilité dans une collaboration entre des entités ayant défini leurs propres politiques de sécurité. Dans O2O, une organisation régule les permissions provenant d'autres organisations, via un VPO (Virtual Private Organisation), et permet à un sujet de garder le même rôle dans une autre organisation grâce à un RSSO (Role Single-Sign-On). Dans [119], les auteurs ont proposé une extension du modèle OrBAC à travers le concept de rôle dans l'organisation (RiO). Ce modèle appelé Multi-OrBAC permet de spécifier des politiques de sécurité dynamique et modulable pour chaque organisation, mais également définir des règles pour la gestion des interactions tout en étant compatible avec les règles internes à chaque organisation. Le PolyORBAC, introduit dans [71], est une approche qui utilise le modèle OrBAC pour spécifier la politique de sécurité locale à chaque organisation d'une part et, d'autre part, la technologie des services Web pour faciliter la collaboration et l'interopérabilité entre les organisations. Les modèles présentés ci-dessus proposent des techniques pour résoudre la question de l'autonomie des organisations dans la définition des règles de contrôle d'accès aux ressources lors d'une collaboration. Cependant, la problématique de la confiance entre ces entités autonomes pour l'établissement de relation durable demeure et doit être abordée.

2.4.4 Modèles de contrôle d'accès et gestion de la confiance

Comme souligné dans la section 2.3.1, la confiance entre les organisations est un facteur important pour inciter à la collaboration et garantir la sécurité des ressources partagées. Plusieurs travaux intégrant la confiance dans les modèles de contrôle d'accès ont été effectués. Dans [49], les auteurs ont proposé le TrustBAC, un modèle intégrant la confiance dans RBAC. Dans ce modèle, des niveaux de confiance sont affectés aux utilisateurs plutôt que des rôles. Plusieurs facteurs tels que les références de l'utilisateur, la recommandation et l'historique du comportement permettent de définir ces niveaux de confiance. Les niveaux de confiance sont par la suite associés aux rôles pour définir des permissions. K.Toumi and al., ont présenté dans [204] le modèle TRUST-OrBAC. Ce modèle étend OrBAC avec la notion de confiance. Sur la base de trois paramètres : la connaissance, la réputation et l'expérience, deux vecteurs de confiance sont associés aux organisations et aux utilisateurs. Ces vecteurs permettent d'attribuer des rôles dynamiques aux utilisateurs, et ainsi définir des règles de sécurité pour des environnements multi-organisationnels. Le modèle Trust Organization Based Access Control (TOrBAC) est exposé dans [21]. Ce modèle permet de calculer et d'ajouter un indice de confiance au modèle OrBAC dans la définition de politique de contrôle d'accès dans les infrastructures de cloud computing. Il introduit le module de TTP (Third Trust Party) qui permet à un utilisateur d'obtenir un indice de confiance après authentification, garantissant ainsi la confiance entre celui-ci et le fournisseur de services Cloud. Dans [22], M. Ben Saidi et A. Marzouk ont proposé le Multi-Trust_OrBAC qui est une extension du modèle TOrBAC adapté aux collaborations entre plusieurs organisations dans le cloud. Les auteurs de [8] ont présenté, Trust-PolyOrBAC, un modèle introduisant la confiance dans un modèle de contrôle d'accès PolyOrBAC pour des infrastructures critiques. Ce modèle intègre une couche de confiance entre l'étape d'authentification et l'étape de contrôle et d'autorisation d'accès aux ressources. Le modèle Tr-OrBAC est

proposé dans [2]. Il permet l'évaluation de la confiance entre les organisations sur la base de la logique floue. Les organisations prennent la décision de collaborer ou non en évaluant les pairs sur la base de la valeur de confiance calculée.

Outre la nécessité de garantir la confiance entre les acteurs, il est important de réduire l'intervention humaine, d'apporter plus de flexibilité et de réduire les conflits dans la définition des politiques de sécurité pour des systèmes distribués de plus en plus complexes, hétérogènes et dynamiques.

2.4.5 Contrôle d'accès, collaboration et systèmes multi-agents

La modélisation des interactions complexes entre diverses entités dans les environnements distribués de collaboration sans autorité centrale où les membres doivent communiquer et négocier directement entre eux est un réel défi. Des axes de résolution ont été proposés sur la base des systèmes Multi-Agents (MAS) [74]. Un agent est une entité capable de s'adapter et de prendre des décisions de manière indépendante et intelligente, d'exécuter des tâches complexes de manière autonome. Il est également à même d'interagir avec d'autres agents par le biais de la coopération, de la coordination et de la négociation dans le but d'atteindre un objectif [190]. L'intégration des agents dans les systèmes collaboratifs permet de déployer des infrastructures composées d'entités autonomes, proactives et des mécanismes de partage flexible, dynamique et intelligent conforme aux caractéristiques intrinsèques des agents [219] [23]. Plusieurs contributions associant les agents dans les modèles de contrôle d'accès ont ainsi été proposés. Dans [4], les auteurs ont présenté un modèle de contrôle d'accès aux ressources partagées dans une coalition dynamique. Ce modèle garantit plus de flexibilité dans la gestion des départs ou l'intégration de nouveaux acteurs dans une coalition. Par ailleurs, il ajoute un niveau « coalition » au modèle OrBAC et utilise une architecture composée d'agents pour améliorer la robustesse. H.Idrissi and al., ont proposé, dans [106], un modèle de contrôle d'accès établi à partir des agents mobiles et des principes du RBAC. Le modèle utilise les caractéristiques de mobilité et d'autonomie des agents mobiles pour combler les limites de communication. En outre, il fournit des techniques d'authentification des utilisateurs, de confidentialité et d'intégrité des données grâce à la cryptographie. Une architecture de contrôle d'accès fondée sur les agents dans une infrastructure de cloud computing a été proposé dans [15]. Ce modèle distribué garanti aux entités (agents), une gestion autonome, dynamique et partageable de leur politique de sécurité à travers des cellules de confiance. Dans [23], les auteurs ont proposé MA-MOrBAC, un modèle qui étend le Multi-OrBAC grâce à des agents mobiles pour des environnements collaboratifs distribués. Une architecture composée d'agents mobiles permet au modèle d'apporter des améliorations en termes de flexibilité et de robustesse. Une extension du modèle PriOrBAC à partir d'agents a été proposée dans [153]. Dans cette approche, les agents sont utilisés pour la négociation et l'établissement de contrat intelligent. Cette démarche a pour avantage de permettre une gestion automatique et dynamique dans la spécification des politiques de contrôle d'accès aux données et la protection de la vie privée. N. Hocine a proposé, dans [100], un système de gestion dynamique des politiques de sécurité. Ce système utilise les agents intelligents pour la prise en compte d'informations contextuelles liées aux dispositifs et aux utilisateurs dans l'élaboration des règles d'accès au sein d'une entreprise. Dans [203], les auteurs ont présenté un modèle théorique de contrôle d'accès dans le cloud. Ce modèle utilise des agents pour l'arbitrage des demandes d'accès, l'authentification des utilisateurs et la définition des règles de sécurité en fonction des exigences du cloud.

2.4.6 Discussion

Cette section a été consacrée à la gestion des accès et des autorisations. Nous avons d'abord défini les notions de politiques de sécurité et de contrôle d'accès dans les systèmes d'information. Ensuite, nous avons exposé une vue d'ensemble des principaux modèles de contrôle d'accès existants. Cette présentation a porté sur les principaux modèles classiques (DAC, MAC, RBAC), ainsi que sur les différents systèmes proposés sur la base de ces modèles de références, afin de répondre aux défis de contrôle d'accès posés par l'émergence des systèmes collaboratifs, distribués, complexes comme le cloud. La confiance étant un défi clé de ce type d'environnement hétérogène, une description des travaux intégrant la confiance dans les techniques de contrôle a été faite. Outre la confiance, les systèmes dynamiques et complexes nécessitent des moyens de définitions dynamiques, autonomes et intelligentes des règles de politique de sécurité. Ainsi, il a été réalisé une analyse de l'utilisation des systèmes multi-agents dans les environnements de collaboration et de leur intégration dans les mécanismes de contrôle d'accès. Le nombre important et la diversité des propositions témoignent de l'importance de la gestion des accès dans le cloud computing et environnements de collaborations. Toutefois, la littérature montre que les environnements de collaboration axés sur la communauté de type cloud communautaire n'ont pas fait l'objet de plusieurs travaux à notre connaissance. En effet, bien qu'ayant les propriétés d'une infrastructure cloud et de collaboration, le cloud communautaire présente des spécificités (relations sociales, interpersonnelles, autonomie, protection des intérêts et incitation des membres, gouvernance commune, etc.) qu'il convient de considérer dans l'élaboration des systèmes et politiques de contrôle d'accès. De plus, les systèmes proposés associent soit le contrôle d'accès à la confiance ou au système multi-agents. La mise en place d'un modèle qui intègre à la fois la gestion des accès, la confiance et les systèmes multi-agents dans un cloud communautaire apporterait une réponse à l'épineuse question de la sécurité et de la protection des ressources partagées pour ce type d'environnement.

2.5 Conclusion

Dans ce chapitre, nous avons abordé en premier lieu l'identité numérique et sa gestion dans le cloud computing. Il s'agissait pour nous de définir l'identité numérique et de présenter les différentes architectures, techniques, protocoles d'authentification et algorithmes de chiffrement utilisés pour gérer les identités dans les systèmes d'information. En outre, nous avons présenté une analyse des défis et des solutions proposées pour la gestion des identités dans le cloud. Malgré les efforts importants des chercheurs, il s'avère nécessaire de porter un regard plus approfondi sur la prise en compte des spécificités des environnements collaboratifs axés sur la communauté dans les systèmes proposés. Parmi les caractéristiques à considérer, la confiance entre les membres se présente comme un défi capital.

La deuxième partie de ce chapitre a donc été consacrée à cette question de gestion de la confiance. Il a été d'abord question de définir cette notion complexe et pluridisciplinaire qu'est la confiance, et de décrire les principales propriétés qui la caractérisent. En raison de sa nature initiale, sociale et relationnelle, plusieurs théories mathématiques sont utilisées pour la modéliser et la mesurer dans le cadre de son application dans la sécurité des systèmes d'information. Les principales théories ont donc été ensuite décrites ainsi que les différents systèmes de gestion de la confiance fondés sur la politique, la réputation, la recommandation et la prédiction. En outre, les solutions apportées de façon spécifique aux infrastructures cloud ont été présentées.

Depuis les premiers systèmes de gestion de la confiance, ceux-ci ont toujours été

liés, voire assimilés, à la gestion des accès et des autorisations. Il en est de même pour les systèmes de collaboration et de partage dont la gestion des accès aux ressources demeure un enjeu crucial. Fort de cela, la dernière partie de ce chapitre a été réservée aux politiques et modèles de contrôle d'accès. Dans cette partie, nous avons défini la politique de sécurité et le contrôle d'accès. De plus, nous avons décrit les principaux modèles de contrôle d'accès traditionnels et ceux proposés par la communauté scientifique en réponse à l'émergence de récents systèmes collaboratifs, distribués, hétérogènes, dynamiques et complexes. Des modèles de contrôle d'accès intégrant la confiance et utilisant les propriétés des systèmes multi-agents ont également été présentés.

En résumé, ce chapitre a permis de mettre en lumière trois thématiques principales de la sécurisation des systèmes informatiques en général et en particulier le cloud computing, telles que la gestion de la confiance, des identités et des accès.Il ressort de cette analyse des limites et des besoins d'amélioration des systèmes proposés concernant le cadre de cloud communautaire abordé dans cette thèse. Ces limites sont internes à chaque mécanisme et à la possibilité d'intégrer ces trois mécanismes à la fois dans une stratégie de sécurité dans un cloud communautaire. Un fait qui n'a pas encore été abordé dans la littérature à notre connaissance.

Le prochain chapitre servira de cadre pour proposer nos solutions d'amélioration de chaque mécanisme en fonction des exigences du cloud communautaire et le regroupement de ces techniques dans une stratégie Zero Trust pour la sécurité des ressources partagées dans la communauté.

Chapitre 3

Modélisation d'une stratégie de sécurité Zero Trust

«It is essential to know that no single specific technology is associated with Zero Trust architecture. The Zero Trust is a security model based on the principle of maintaining strict access controls and not trusting anyone by default ; a holistic approach to network security, that incorporates a number of different principles and technologies.»

Ludmila Morozova-Buss - Founder, Editor-In-Chief at Top Cyber News MAGAZINE, 2022 European 'Woman in Cyber' Trophy in Cybersecurity Supporting Professions.

Sommaire

3.1 Introduction

Après avoir exploré, dans les chapitres précédents, les mécanismes et stratégies de sécurité dans les systèmes cloud, ainsi que les défis de collaboration et de partage dans les environnements communautaires, nous présentons dans ce chapitre notre modèle de stratégie de sécurité Zero Trust. Cette démarche a pour but d'apporter une réponse à la question de la confiance, de la protection et du contrôle d'accès aux ressources partagées dans ce type d'infrastructure. En effet, dans les systèmes collaboratifs et plus spécifiquement ceux centrés sur la communauté, les interactions entre des parties prenantes fiables et dignes de confiance ont pour effet de stimuler les investissements, d'accroître l'innovation et leurs productivités [128]. Par ailleurs, la recrudescence des cyberattaques et la complexité de ces systèmes nécessitent l'adaptation des moyens de protection des données, services et des dispositifs. Ce chapitre est organisé de la manière suivante. Tout d'abord, nous abordons le principe de fonctionnement. Ensuite, chaque composant de la stratégie sera examiné de manière détaillée afin de présenter nos propositions d'améliorations et d'adaptations des mécanismes de sécurité étudiés en fonction des besoins du cloud communautaire.

3.2 Principe de fonctionnement et Architecture générale du modèle

Le Zero trust est une approche de cybersécurité qui vise la protection d'un système informatique (ressources, utilisateurs) au travers d'une évaluation permanente des entités du système, éliminant ainsi toute confiance implicite qui peut leur être accordée. En d'autres termes, elle considère toutes les entités (physiques et logicielles) du système comme potentiellement vulnérables en tout temps et en tout lieu. La mise en œuvre de cette stratégie varie en fonction du contexte du système, et exige des changements organisationnels et culturels. Les systèmes collaboratifs ont la particularité d'être constitués de différents acteurs, diverses ressources, pluridisciplinaires, avec des objectifs bien définis, fondés sur le partage et la coopération dans l'intérêt des entités engagées. Une démarche Zero Trust dans ce type d'infrastructure doit donc prendre en compte ces spécificités, et plus particulièrement pour des systèmes axés sur la communauté, tenir compte des caractéristiques décrites à la section 1.3.3.3 ainsi que des exigences sécuritaires présentées à la section 1.3.3.4. Parmi les éléments à considérer, la sécurité des ressources et la confiance sont capitales pour des organisations désireuses de collaborer et de partager des ressources afin de développer des relations durables, productives et bénéfiques. Toutefois, cela nécessite de proposer des mécanismes de sécurisation des ressources, de suivi de la confiance et des accords de collaboration. Par conséquent, nous proposons une stratégie de sécurité fondée sur une démarche Zero Trust pour une infrastructure de collaboration entre des organisations autonomes. Notre approche Zero Trust met en exergue une architecture constituée de différents composants dans le but de fournir les fonctions de sécurité suivantes : gestion d'identité (organisations, utilisateurs), définition de politique de contrôle d'accès, évaluation de niveau de confiance, de création et suivi de contrat de collaboration.

Cette architecture est représentée dans la figure 3.1 et les sections suivantes décrivent les différents composants.

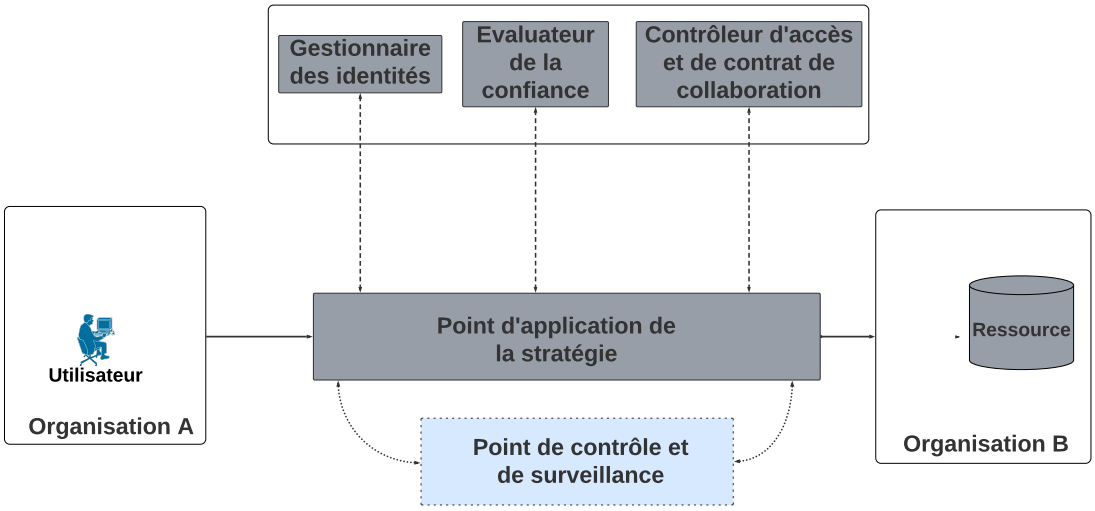


FIGURE 3.1 : Architecture du modèle Zero Trust

- **Organisations, utilisateurs et ressources** : les organisations sont des entreprises (grandes compagnies, PME, Startup, etc.) de tous types de domaines qui collaborent afin de partager des ressources informatiques. Chaque organisation dispose de ressources qui peuvent être mises à la disposition de ses utilisateurs et des utilisateurs d'autres organisations. Ces ressources peuvent être matérielles ou logicielles, à savoir des données, des machines virtuelles, des objets connectés, des applications, etc.
- **Gestionnaire des identités** : ce composant est responsable de l'identification et de l'authentification des organisations et des utilisateurs. Le gestionnaire d'identité utilise les identifiants décentralisés (DiD) [69] pour la gestion des identités des organisations. Chaque organisation dispose d'un DiD et d'un document DiD associé qu'elle crée après avoir généré une paire de clés cryptographiques (une clé publique et une clé privée). Des informations d'identifications vérifiables (VC) [206] sont attribuées par chaque organisation à ses utilisateurs. Ainsi, lors d'une collaboration, les utilisateurs sont authentifiés par leurs VC émises et signées de façon cryptographique par l'organisation à laquelle ils appartiennent. Les informations d'identifications sont enregistrées dans un registre distribué de type blockchain accessible aux organisations engagées et un contrat intelligent exécute l'algorithme d'authentification lors des collaborations.
- **Évaluateur de la confiance** : il est chargé de l'évaluation de la confiance entre les organisations. Sur la base de la réputation et de résultats antérieurs de collaboration, l'évaluateur de la confiance calcule, à l'aide de la logique subjective [110][111], la valeur de confiance de l'organisation fournisseur d'une ressource spécifique. Cette valeur constitue un critère de sélection et d'incitation pour une collaboration entre deux entités.

- **Contrôleur d'accès et de contrat de collaboration** : une collaboration est caractérisée par l'engagement des parties à mener des actions en vue de l'atteinte de l'objectif. Cet engagement des différentes parties est matérialisé par un accord de collaboration après une négociation. Le composant *Contrôleur d'accès et de contrat de collaboration* permet d'assurer la gestion de ces contrats de collaboration et de définir des règles de politiques d'accès aux ressources.
- **Point d'application de la stratégie** : ce composant sert d'interface entre tous les composants et est le point d'exécution de la stratégie. Il communique avec les autres composants afin d'activer, exécuter les mécanismes associés. Par ailleurs, il communique avec le *point de contrôle et de surveillance* afin d'effectuer une surveillance continue des différentes fonctions de sécurité et actualiser les niveaux de sécurité, les valeurs de confiance et les identités des organisations et des utilisateurs.

Dans les sections suivantes, nous présentons chaque mécanisme de sécurité proposé.

3.3 Gestion des identités

3.3.1 Vue d'ensemble du système

La gestion des identités permet d'assurer l'authentification des entités et de réguler l'accès aux ressources dans un système informatique. Pour des systèmes distribués et dynamiques comme le cloud communautaire, la transparence, la fiabilité et l'autonomie des entités dans la gestion des identités sont essentielles. Par conséquent, nous proposons un système décentralisé de gestion des identités établi à partir de contrats intelligents et des oracles de la blockchain. Notre modèle permet d'identifier les organisations et les utilisateurs de la communauté grâce aux identifiants décentralisés (DiD) et les informations d'identifications vérifiables (VC). Par ailleurs, l'utilisation des contrats intelligents permet d'exécuter différents mécanismes nécessaires au bon fonctionnement de notre environnement. Ces mécanismes sont relatifs à l'agrégation de signatures numériques lors de l'adhésion d'une organisation à la communauté et à l'authentification des organisations et des utilisateurs. En outre, notre infrastructure présente une architecture d'oracles distribués au sein de laquelle chaque organisation est représentée par un oracle permettant aux différents contrats intelligents de communiquer (fournir et recevoir des informations) avec le monde réel. Les sections suivantes décrivent l'architecture du système et son mode de fonctionnement.

3.3.2 Architecture et composants du système

L'architecture du système est présentée dans la figure 3.2 et est composée : d'un registre de données d'identités, de contrats intelligents d'enregistrement (CIE) et d'authentification (CIA), d'un réseau d'oracles distribués, des organisations et des utilisateurs de la communauté.

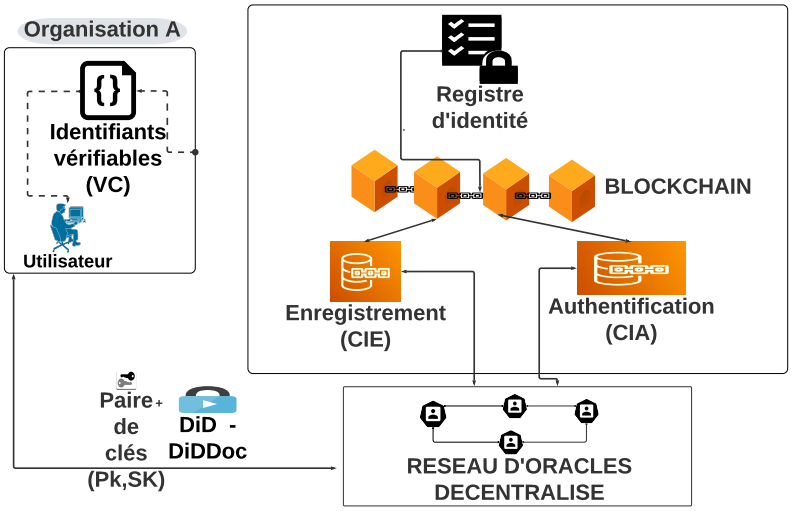


FIGURE 3.2 : Architecture du système de gestion décentralisée des identités

3.3.2.1 Les organisations de la communauté

Comme décrit précédemment, elles sont des fournisseurs ou des demandeurs de ressources. Ces entités collaborent par le partage de ressources de diverses natures et transmettent ou reçoivent des informations du réseau d'oracles. Ces organisations se distinguent par leur identifiant décentralisé (DiD) et divers attributs contenus dans le document DiD associé. Au sein de chaque organisation, un ou plusieurs utilisateurs émettent des requêtes de demande de ressources. Afin d'accéder à des ressources d'autres organisations, des informations d'identifications vérifiables (VC) sont attribuées aux utilisateurs. Ces VC sont émises et signées de façon cryptographique par l'organisation à laquelle l'utilisateur appartient. Chaque utilisateur génère ses clés cryptographiques, crée son DiD et son document DiD à l'intérieur de son organisation. Ces données de l'utilisateur sont stockées localement, gérées de manière fiable et transparente, et servent de moyen d'authentification de l'utilisateur au sein de l'organisation.

3.3.2.2 Le registre de données d'identités

La blockchain est un registre distribué, ouvert et sécurisé (utilisant des techniques cryptographiques) [182]. C'est une technologie de stockage et de transmission de l'information. Elle s'appuie sur un mécanisme de consensus qui garantit l'intégrité et la cohérence des transactions enregistrées dans les blocs et reparties de façon distribuée sur chaque nœud du réseau. Il existe deux grandes catégories de blockchains, à savoir les blockchains publiques (Bitcoin, Ethereum, etc.) et les blockchains privées ou de consortium (Corda, Hyperledger, etc.). Ces dernières sont destinées à un groupe d'entreprises ou d'acteurs réunies pour créer une blockchain accessible qu'aux membres de cette communauté. Cette catégorie va favoriser l'émergence de nouvelles blockchains dans différents domaines et des applications variées au travers de contrats intelligents [223]. Ainsi, dans notre approche, les différentes informations manipulées par les oracles et

les contrats intelligents, sont stockées dans des registres de type blockchain. Ce registre de données d'identités contient les documents DiD des organisations sauvegardés lors de leur intégration dans la communauté. Ces documents DiD permettent de faire la résolution des DiD présentés lors de la phase d'authentification.

3.3.2.3 Les contrats intelligents d'enregistrement et d'authentification

Un contrat intelligent est un algorithme (script informatique) exécuté sur une plateforme décentralisée, généralement une blockchain [209]. Ce programme est conçu sur la base de termes contractuels négociés entre des entités intervenants dans une transaction. Ces termes impliquent des dispositions commerciales, légales, des critères d'interactions, et différents types d'accord. Ainsi, il effectue des opérations algébriques et logiques si tous les critères ou règles prédéfinies sont respectés. Une fois les conditions définies réunies, l'algorithme est déclenché, exécuté automatiquement sans intervention humaine et signé de façon cryptographique par les différentes parties. Le contrat dit intelligent résultant est par la suite ajouté dans un bloc. Ce bloc est sauvegardé dans le registre et distribué à tous les nœuds [199]. Les contrats intelligents exécutent donc différents algorithmes permettant d'une part de stoker des informations dans la blockchain et, d'autre part, de fournir des données aux sources externes à la blockchain. Ces contrats sont auto-exécutables. Notre système de gestion des identités dispose de deux contrats intelligents : le contrat intelligent d'enregistrement (CIE) pour enregistrer les organisations dans le registre de la communauté et le contrat intelligent d'authentification (CIA) dédié à l'authentification.

3.3.2.4 Le réseau d'oracles distribué

Dans de nombreux scénarios d'applications, les éléments déclencheurs du contrat intelligent nécessitent de disposer de données non stockées dans la blockchain. Les contrats intelligents étant incapables d'échanger avec cet environnement extérieur, il convient de recourir à d'autres mécanismes afin d'étendre les champs d'utilisation des contrats intelligents. Les oracles de la blockchain ont pour but de combler l'incapacité des contrats intelligents à importer des informations externes à la blockchain. Un oracle est une interface facilitant la communication entre la blockchain et les sources de données externes du monde réel [26]. Les Oracles doivent être fiables et assurer la confiance entre les différentes entités (la blockchain et les sources de données externes). Ils permettent d'injecter des données dans les contrats intelligents (oracles entrants) et transmettent de données provenant de la blockchain (oracles sortants) aux sources externes [30]. Il existe différents types d'oracles : matériels (capteurs, etc.), logiciels (applications spécifiques au domaine) et humains. Les oracles sont déployés dans des architectures de type centralisé ou décentralisé. Dans une architecture centralisée, l'oracle peut être un point de défaillance, vulnérable aux attaques et surtout en opposition du principe distribué de la blockchain. L'approche décentralisée permet de fournir un réseau d'oracle décentralisé composé d'entités autonomes servants d'interface de communication entre le monde extérieur et les contrats intelligents [30][26]. Dans notre modèle, les oracles alimentent les contrats intelligents en données et leur permettent de communiquer avec le monde extérieur, en l'occurrence, les organisations et leurs utilisateurs. Le modèle propose un réseau d'oracles distribué constitué par des nœuds mis à la disposition par chaque entité membre de la communauté. Le bénéfice principal est de permettre à chaque organisation d'être représentatif et contribuer à fournir les informations fiables et nécessaires au bon fonctionnement des contrats intelligents. Chaque information provenant de la blockchain est diffusée à travers tout le réseau d'oracles. De même, une entrée nécessaire à l'exécution d'une fonction d'un contrat intelligent est fourni par tous les acteurs

engagés dans le processus. Les informations ainsi collectées sont agrégées et un consensus est trouvé pour ressortir la donnée attendue.

3.3.3 Principe de fonctionnement

Le fonctionnement général de notre système repose sur deux grandes phases. La première consiste en un processus de demande d'adhésion et d'enregistrement d'une organisation donnée au sein de la communauté. La seconde est une procédure d'authentification lors de la demande d'accès par un utilisateur à une ressource fournit par une organisation donnée différente de celle à laquelle il appartient.

3.3.3.1 Demande d'adhésion et enregistrement d'une organisation

Cette phase consiste pour une organisation à envoyer une requête de demande d'adhésion à la communauté dans le but de fournir ou solliciter des ressources. Cette requête doit être validée par toutes les organisations membres de la communauté. Un accord d'une entité à l'intégration d'une organisation donnée est matérialisé par sa signature numérique d'une convention d'adhésion. L'ensemble des signatures des organisations est agrégée en une signature unique grâce à la propriété d'agrégation de signatures de l'algorithme BLS [37]. Les étapes de l'enregistrement d'une organisation sont : la création de l'identifiant décentralisé de l'organisation, la collecte des réponses à la requête, l'agrégation des signatures et enfin l'enregistrement des informations dans le registre de gestion des identités. Ces étapes sont décrites dans les sections ci-dessous et présentées dans la figure 3.3.

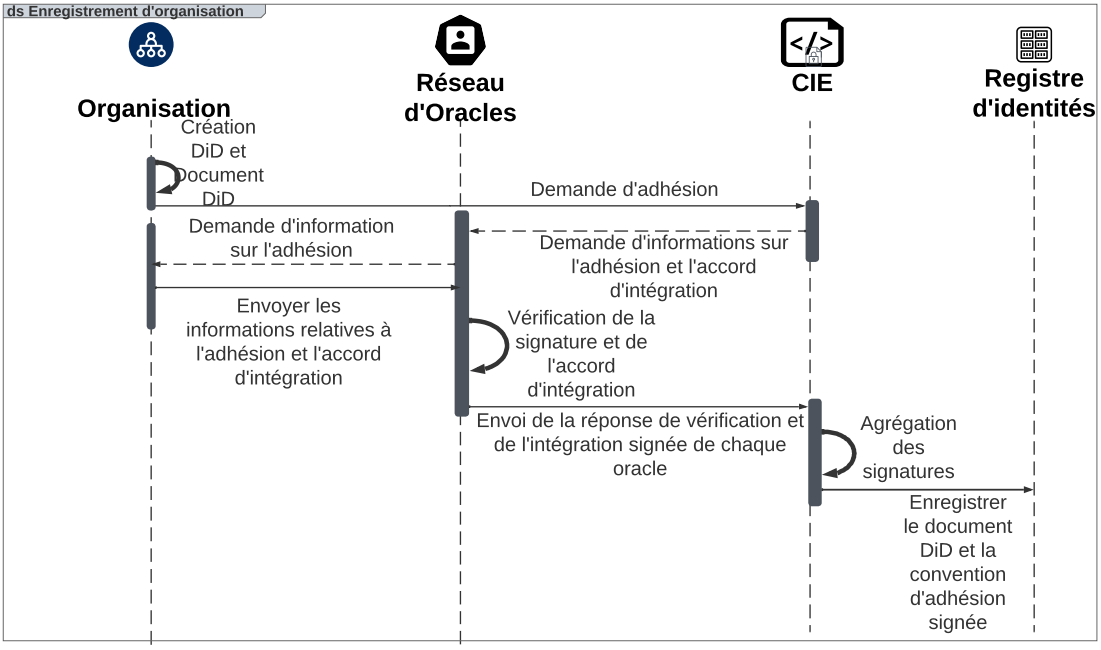


FIGURE 3.3 : Processus de demande d'adhésion et enregistrement d'une organisation

- **Création de l'identifiant décentralisé de l'organisation** : l'organisation sollicitant une adhésion génère une paire de clés cryptographiques : une clé publique pk_o et une clé privée sk_o. Puis, elle crée son DiD et le document DiD (DiD_Doc) associé. Le DiD_Doc est ensuite rattaché au message de demande d'adhésion msg_r. Une fonction de hachage est appliquée au résultat obtenu, signé avec la clé privée de

l'organisation et enfin transmis au contrat intelligent de gestion d'identité sous forme de requête $C_r = \{DiD, DiD\_Doc, \sigma_o, pk_o, msg_r\}$ avec

$\sigma_o = E(H_{ash}(msg_r||DID\_Doc), sk_o)$, E est l'algorithme de chiffrement.

- **Collecte des réponses :** dès réception de la demande d'adhésion, le contrat intelligent d'identité sollicite les informations de traitements de la requête auprès des oracles afin d'enclencher le processus de signature de la convention d'adhésion. Ainsi, chaque organisation vérifie la validité de la signature σ_o grâce à la clé publique pk_o du demandeur. Par ailleurs, l'algorithme de hachage est utilisé pour créer une nouvelle empreinte fondée sur le message et DiD document reçu, et ainsi le comparer au hash reçu pour s'assurer de l'intégrité des informations transmises. Après les différentes vérifications, chaque organisation O_i, par l'intermédiaire de son oracle associé, transmet au contrat intelligent d'identité sa décision $M_A = \{DiD_i, \sigma_i, pk_i, msg_i, C_r\}$ relative à la requête d'adhésion.
  msg_i est l'approbation ou la désapprobation de l'organisation (O_i) sur la demande d'intégration, $\sigma_i = E(H_{ash}(msg_i)), sk_i)$ est la réponse signée, sk_i, pk_i respectivement, la clé privée et la clé publique de l'organisation O_i et C_r la requête de demande d'adhésion associée. Les organisations O_i utilisent l'algorithme de signature BLS initialisée avec deux groupes cycliques $G1$ et $G2$ d'ordre q.
  Avec g_1, g_2 les générateurs respectifs des groupes $G1$ et $G2$.
  e la fonction d'appariement bilinéaire telle que $e : G1 \times G2 \rightarrow G$ avec $\sigma_i \in G2$, $pk_i = sk_i g_1 \in G1$ et $sk_i \in \mathbb{Z}_q^*$.

- **Agrégation des signatures et enregistrement de l'organisation :**

  Le contrat intelligent d'identité vérifie la validité des messages renvoyés par les oracles à l'aide de leurs clés publiques ainsi que les accords d'approbations reçus des oracles. L'adhésion n'est acceptée que si chaque organisation de la communauté donne un avis favorable. Les signatures renvoyées seront ainsi agrégées en une signature unique (σ_A) par le contrat intelligent afin de signer la convention d'adhésion.

$$\sigma_A = \sum_{i=1}^{n} \sigma i \tag{3.3.1}$$

  La convention signée est envoyée aux organisations et le Document DiD du demandeur est enregistré dans le registre de données d'identité. Ce processus d'enregistrement d'une organisation à la communauté sera également appliqué en cas de départ d'une organisation (fin d'existence de l'organisation, choix unilatéral de l'organisation de se retirer de la communauté, décision des membres de faire sortir une organisation de la communauté) dans le but de disposer d'une convention de départ signée et validée par les membres. L'organisation désirant quitter la communauté notifie son intention à la communauté et un accord est conclu et signé après approbation de la majorité des organisations. Il pourrait toutefois réintégrer en suivant la procédure d'intégration décrite ci-dessus appliquée à l'ensemble des organisations.

3.3.3.2 Authentification lors d'une demande d'accès à une ressource

Une organisation membre peut mettre à la disposition de la communauté ou demander l'accès à des ressources d'autres organisations pour ses utilisateurs. Ce processus, décrit dans la figure 3.4 ci-dessous, démarre avec la mise à disposition des utilisateurs de l'organisation demandeur des informations d'identifications vérifiables. Ensuite, l'authentification des organisations et des utilisateurs suivis de l'autorisation d'accès à la

ressource ou non grâce à l'évaluation de la confiance et la sélection du fournisseur idéal détaillé dans la section suivante.

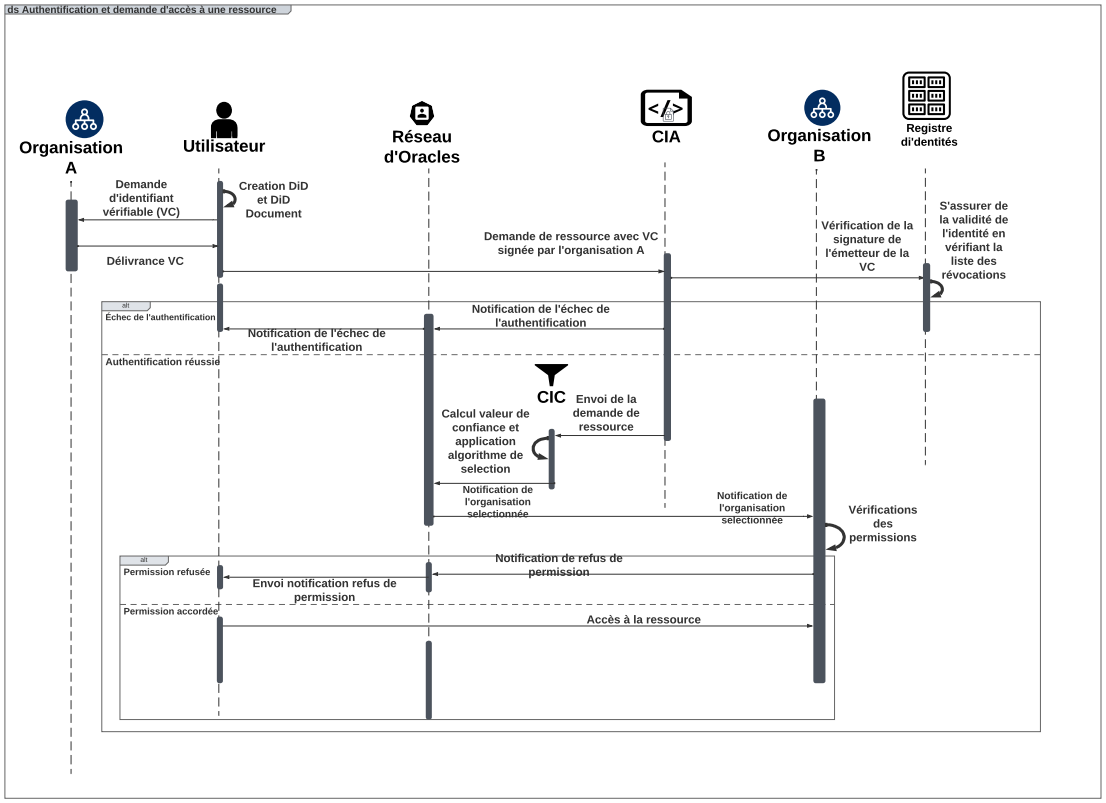


FIGURE 3.4 : Processus d'authentification et de demande d'accès à une ressource

- **Émission d'informations d'identifications vérifiables (VC)** : l'utilisateur sollicitant une ressource crée son identifiant décentralisé et le document DiD correspondant. Ensuite, l'organisation à laquelle appartient cet utilisateur émet à son endroit des informations d'identifications vérifiables. Ce VC est signé par l'organisation avec sa clé privée et contient des informations (DiD, objet de la demande, date de signature, etc) référençant l'utilisateur concerné [162].
- **Authentification et sélection du fournisseur** : la requête de demande de ressource est envoyée au contrat intelligent de gestion des identités avec le VC de l'utilisateur. Le contrat intelligent authentifie l'utilisateur à l'aide de la clé publique de l'organisation émettrice du VC et vérifie également la validité du VC dans la liste de révocation du registre. Après authentification de l'utilisateur, le contrat intelligent de confiance et de collaboration est exécuté et permet de sélectionner une organisation de confiance pour le partage de la ressource sollicitée. L'algorithme exécuté pour sélectionner le fournisseur est présenté dans la section suivante. Un accord de collaboration est négocié entre les deux organisations afin d'établir et de formaliser les termes de la coopération.
- **Accès à la ressource et mise à jour des informations :** sur la base du contrat de collaboration établi et des règles de politiques d'accès, l'utilisateur est autorisé à accéder à la ressource. À la fin de l'échange, les organisations fournissent aux oracles les données nécessaires à la mise à jour des valeurs de confiance par le contrat intelligent de confiance et de collaboration.

3.4 Gestion de la confiance

Un cloud communautaire (3C) a pour objectif de permettre à des organisations de partager des ressources afin de réduire les coûts d'investissement et de créer des opportunités commerciales sans pour autant faire fi de la qualité des ressources partagées. Il est caractérisé par des organisations ayant des besoins spécifiques ou des intérêts communs. Ainsi, la participation active des membres à la vie de la communauté et l'existence de relations durables constitue des atouts pour l'infrastructure. Par ailleurs, le caractère social dans les collaborations entre les organisations représente l'une des raisons fondamentales d'un cloud communautaire. Dans cette section, nous présentons le *SeComTrust*, un modèle pour l'évaluation et l'établissement de relations de confiance, de partage sécurisé de ressources entre les organisations d'un cloud communautaire. Notre approche consiste dans un premier temps à identifier et à sélectionner le fournisseur de confiance pour le partage d'une ressource donnée. Ensuite, effectuer un suivi de la transaction à travers des indicateurs de performance de services dérivés des attributs SMI du consortium CSMIC (Cloud Services Measurement Initiatives Consortium) [202], puis actualiser les valeurs de confiance et de réputation conformément au contrat de collaboration établi. La mise à jour des valeurs de confiance est réalisée grâce à un protocole de promotion et de relégation, qui permet de récompenser ou de sanctionner les acteurs de l'échange. Notre démarche subdivise le cloud communautaire en trois domaines de sécurité : le domaine de sécurité bas (L_{sd}), le domaine de sécurité intermédiaire (M_{sd}) et le domaine de sécurité avancé (H_{sd}).Un domaine de sécurité regroupe des organisations ayant un niveau d'assurance de sécurité spécifique (voir définition 3.4.5). Quant au niveau d'assurance (voir section 3.4.4), il représente la capacité d'une organisation à fournir des ressources d'un niveau de sensibilité donné (3.4.3). Des échanges peuvent être réalisés entre des organisations de domaines de sécurité identiques ou différents. Le choix du fournisseur de confiance repose sur l'opinion de confiance du demandeur vis-à-vis du fournisseur et de la réputation de ce dernier. Une opinion est une croyance subjective fondée sur la confiance et permet d'exprimer la valeur de confiance accordée à une organisation [47].

3.4.1 Hypothèse de recherche

Notre hypothèse repose sur un cloud communautaire, composé d'organisations regroupées dans différents domaines de sécurité, qui interagissent les unes avec les autres, en vue de collaborer et de partager des ressources. Ces échanges permettent de répondre aux demandes de ressources pour des organisations qui n'en possèdent pas, de proposer de nouveaux services et favoriser des relations commerciales. De ces interactions, peuvent être déduites des relations de confiance. Ces relations de confiance peuvent être décrites par des valeurs subjectives ou opinions, exprimant le niveau de confiance entre les organisations [48]. Nous représentons en conséquence, dans la figure 3.5 ci-dessous, un réseau de confiance superposé ou Trust overlay Network (TON) à notre cloud communautaire de partage de ressources en mode pair à pair à l'instar des propositions dans [130][132][226][225]. Les sommets ou nœuds de ce réseau illustrent les organisations et les arêtes, les transactions ou interactions entre elles. Une relation de confiance entre deux entités est représentée par une flèche dont la source est le demandeur et la pointe le fournisseur de la ressource. L'étiquette d'une arête exprime l'opinion de confiance du demandeur vis-à vis du fournisseur.

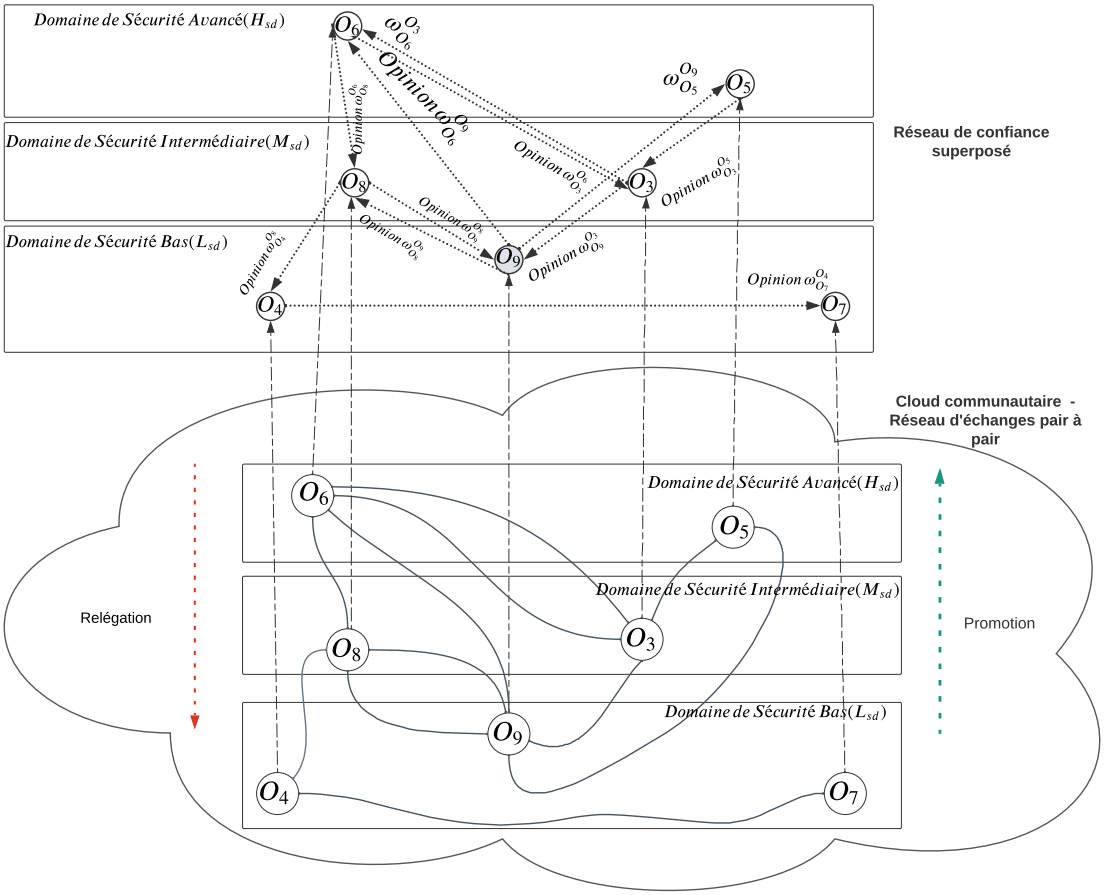


FIGURE 3.5 : Un réseau de confiance superposé pour un cloud communautaire multi-domaine

Dans la suite du document, nous nommerons *partenaire* ou *demandeur* l'organisation sollicitant une ressource et *fournisseur* le propriétaire de la ressource.

Definition 3.4.1. Soit O_i et O_j des organisations appartenant à un cloud Communautaire C. $\forall\ O_j, O_i \in C$, O_i est en relation avec O_j, signifie que O_j fournit une ressource à O_i et est noté $O_i \Re O_j$.

L'ensemble des relations entre les organisations permet de définir le cloud communautaire C comme un graphe dirigé G= (O, R), où O={O_1,O_2, ...,0_n} représente l'ensemble des organisations et R={R_1,R_2, ...,R_m} est l'ensemble des relations.

Definition 3.4.2. $O_i \Re O_j(r, g, q, t, \tau)$ est une relation de partage d'une ressource r de niveau de sensibilité g , de quantité q, à la date t pendant une période τ entre un fournisseur O_j et un partenaire O_i.

C le cloud communautaire représenté à la figure 3.5.

$$C = \{O_3, O_4, O_5, O_6, O_7, O_8, O_9\} \tag{3.4.1}$$

R l'ensemble des relations de partage : tel que :

$$\begin{aligned} R = \{&(O_4, 0_7), (O_8, 0_4), (O_3, 0_9), (O_3, 0_6), (O_9, 0_6), (O_9, 0_8), \\ &(O_9, 0_5), (O_8, 0_6), (O_8, 0_9), (O_5, 0_3)\} \end{aligned} \tag{3.4.2}$$

Nous représentons le cloud communautaire sous la forme d'une matrice de relations M_R(figure 3.6) mettant en exergue les relations entre les organisations. Les co-

lonnes de cette matrice représentent les fournisseurs et les lignes les demandeurs de ressources. La valeur 1 pour une relation existante et la valeur 0 pour l'absence de relation :

$$M_R = \begin{array}{c} Organisations \\ 0_3 \\ 0_4 \\ 0_5 \\ 0_6 \\ 0_7 \\ 0_8 \\ 0_9 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0_3 & 0_4 & 0_5 & 0_6 & 0_7 & 0_8 & 0_9 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

FIGURE 3.6 : Matrice des relations du cloud communautaire

Nous relevons les propriétés ci-dessous des relations au sein de la communauté :

- Réflexive : une organisation peut être à la fois fournisseur et demandeur d'une ressource ($O_3 \Re O_3$=1). La réflexivité des relations permet d'informer sur les différentes ressources disponibles ou susceptibles d'être partagées au sein de la communauté et d'en assurer un ravitaillement continu.
- Asymétrique :$O_3 \Re O_6$= 1 et $O_6 \Re O_3$= 0.

Des opinions de confiance sont déduites des différentes interactions entre organisation (figure 3.5). De ce fait, nous pouvons représenter l'ensemble des relations R (équation 3.4.2) de la communauté par un ensemble d'opinions de confiance R_O comme ci-dessous :

$$R_O = \{\omega_{O_7}^{O_4}, \omega_{O_4}^{O_8}, \omega_{O_9}^{O_3}, \omega_{O_3}^{O_5}, \omega_{O_5}^{O_9}, \omega_{O_9}^{O_8}, \omega_{O_6}^{O_9}, \omega_{O_8}^{O_6}, \omega_{O_8}^{O_9}, \omega_{O_3}^{O_6}, \omega_{O_6}^{O_3}\} \tag{3.4.3}$$

Nous exprimons cet ensemble par la matrice d'opinions M_{RO} ci-dessous :

$$M_{RO} = \begin{array}{c} Organisations \\ 0_3 \\ 0_4 \\ 0_5 \\ 0_6 \\ 0_7 \\ 0_8 \\ 0_9 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0_3 & 0_4 & 0_5 & 0_6 & 0_7 & 0_8 & 0_9 \end{array} \\ \begin{bmatrix} \omega_{O_3}^{O_3} & 0 & 0 & \omega_{O_6}^{O_3} & 0 & 0 & \omega_{O_9}^{O_3} \\ 0 & \omega_{O_4}^{O_4} & 0 & 0 & \omega_{O_7}^{O_4} & 0 & 0 \\ \omega_{O_3}^{O_5} & 0 & \omega_{O_5}^{O_5} & 0 & 0 & 0 & 0 \\ \omega_{O_3}^{O_6} & 0 & 0 & \omega_{O_6}^{O_6} & 0 & \omega_{O_8}^{O_6} & 0 \\ 0 & 0 & 0 & 0 & \omega_{O_7}^{O_7} & 0 & 0 \\ 0 & \omega_{O_4}^{O_8} & 0 & 0 & 0 & \omega_{O_8}^{O_8} & \omega_{O_9}^{O_8} \\ 0 & 0 & \omega_{O_5}^{O_9} & \omega_{O_6}^{O_9} & 0 & \omega_{O_8}^{O_9} & \omega_{O_9}^{O_9} \end{bmatrix} \end{array}$$

FIGURE 3.7 : Matrice d'opinions

Les organisations appartiennent à des domaines de sécurité (L_{sd},M_{sd},H_{sd},), nous désignons L le domaine de sécurité bas L_{sd}, M le domaine de sécurité intermédiaire M_{sd}, H le domaine de sécurité élevé H_{sd}.

Les domaines de sécurité sont formulés ci-dessous comme des sous-ensembles de la communauté :

$$\begin{aligned} L &= \{O_4, O_7, O_9\} \\ M &= \{O_3, O_8\} \\ H &= \{O_5, O_6\} \end{aligned} \tag{3.4.4}$$

Sur la base de ces sous ensembles ci-dessus (équation : 3.4.4, nous remplaçons chaque valeur d'interaction dans la matrice de relations par un rapport (domaine de sécurité partenaire/domaine de sécurité fournisseur) mettant en évidence les domaines de sécurité de chaque organisation impliquée dans un échange. Ainsi, nous obtenons la matrice de domaine de sécurité M_{sd} ci-après :

$$M_{sd} = \begin{array}{c} Organisations \\ O_3 \\ O_4 \\ O_5 \\ O_6 \\ O_7 \\ O_8 \\ O_9 \end{array} \begin{array}{c} \begin{array}{ccccccc} O_3 & O_4 & O_5 & O_6 & O_7 & O_8 & O_9 \end{array} \\ \begin{bmatrix} M/M & 0 & 0 & M/H & 0 & 0 & M/L \\ 0 & L/L & 0 & 0 & L/L & 0 & 0 \\ H/M & 0 & H/H & 0 & 0 & 0 & 0 \\ H/M & 0 & 0 & H/H & 0 & H/M & 0 \\ 0 & 0 & 0 & 0 & L/L & 0 & 0 \\ 0 & M/L & 0 & 0 & 0 & M/M & M/L \\ 0 & 0 & L/H & L/H & 0 & L/M & L/L \end{bmatrix} \end{array}$$

FIGURE 3.8 : Matrice de domaines de sécurité

Les rapports de domaines de sécurité de cette matrice permettront de fixer des seuils de valeurs d'opinions nécessaires à la régulation et à l'autorisation de partage de ressources entre organisations de domaines identiques ou différents (voir matrices de gouvernance 3.103.11).

Le processus d'évaluations de la confiance du *SeComTrust* se déroule en trois principales étapes :

- *Étape 1 - Identification des fournisseurs de la ressource sollicitée* : elle constitue la phase d'initialisation du processus suite à une requête de demande de ressources par une organisation. Les informations relatives à la ressource demandée sont le type de ressource, le degré de sensibilité, la quantité, la date de disposition souhaitée et la durée d'utilisation de la ressource. Les fournisseurs de la ressource sont identifiés parmi tous les fournisseurs de la communauté référencés dans le gestionnaire de ressources (3.4.2.1). Une vérification du stock de ressource disponible pour chaque fournisseur est effectuée afin d'établir une liste d'organisations capables de fournir la ressource dans les délais souhaités par le partenaire. Une même ressource peut être fournie par plusieurs fournisseurs pour combler un déficit en termes de quantité. Dans ce cas, deux processus distincts de partage sont effectués. La liste des fournisseurs identifiés est classée par ordre de priorité décroissante, de domaine de sécurité et de niveau d'assurance décroissant. Ce processus est décrit dans l'algorithme 1.
- *Étape 2 - Évaluation de la confiance et sélection du fournisseur* : sur la base de la liste établie à l'étape 1, un mécanisme d'inférence de valeur de confiance pour déterminer le fournisseur idéal pour le partage est amorcé. Dans un premier temps, il s'agit de vérifier dans la liste des transactions du demandeur la présence d'une interaction directe avec le premier fournisseur de la liste. En cas d'existence d'une

transaction antérieure, une valeur de confiance représentant l'opinion du demandeur vis-à-vis du fournisseur est calculée (voir algorithme 2). Dans le cas d'inexistence d'interaction antérieure avec le premier fournisseur de la liste, le processus est repris à l'identique avec le fournisseur suivant. Tant qu'un fournisseur n'est pas choisi, la même opération sera effectuée jusqu'au dernier élément de la liste. Si l'analyse de la liste de transactions directes ne permet pas d'identifier un fournisseur, l'option suivante sera d'effectuer le même type d'exploration dans la liste des transactions sur la base d'interactions indirectes selon les modèles FoF (Friend of Friend) et FoM (Friend of multiple friends)(Figure 3.12 et algorithme 3). En admettant que la liste des transactions antérieures du demandeur n'offre pas les résultats escomptés, le mécanisme se poursuivra à travers les listes de réputations spécifiques et globales (algorithme 4) jusqu'au choix d'un fournisseur de confiance. Enfin, la valeur de confiance du demandeur vis-à-vis du fournisseur sélectionné et celle du fournisseur à l'égard du demandeur sont comparées à des seuils d'opinions, afin de déterminer la faisabilité de l'échange entre les deux organisations. D'autres caractéristiques qualitatives et quantitatives rentre en ligne de compte dans la validation d'une autorisation de transaction (voir algorithme 5).

- *Étape 3 - Échange, suivi de contrat de collaboration et mise à jour des valeurs de confiance* : l'organisation demandeur de la ressource et le fournisseur sélectionné à l'étape 2 conviennent de paramètres contractuels quant à l'utilisation et à la qualité de la ressource fournie. Dès la mise à disposition de la ressource, une première vérification de la conformité de certains de ces paramètres permet de déduire le résultat de la transaction. Ce résultat initialise les actions de mise à jour des valeurs de réputation spécifiques et globales, de niveau d'assurance, de statut de disponibilité de la ressource dans le manager des ressources et de la liste de transaction du partenaire. Tout au long de la période d'utilisation de la ressource, un suivi est fait afin d'actualiser les valeurs de réputations du fournisseur en cas de violations des éléments contractuels établis auparavant par les deux entités. Le fournisseur est ainsi promu ou relégué d'un domaine de sécurité à un autre en fonction des scores confiance après chaque opération de mise à jour. Les sections 3.4.3.3 3.4.3.3 3.4.3.3 3.4.3.3 décrivent en détail toute cette étape 3.

3.4.2 Composants et architecture du système

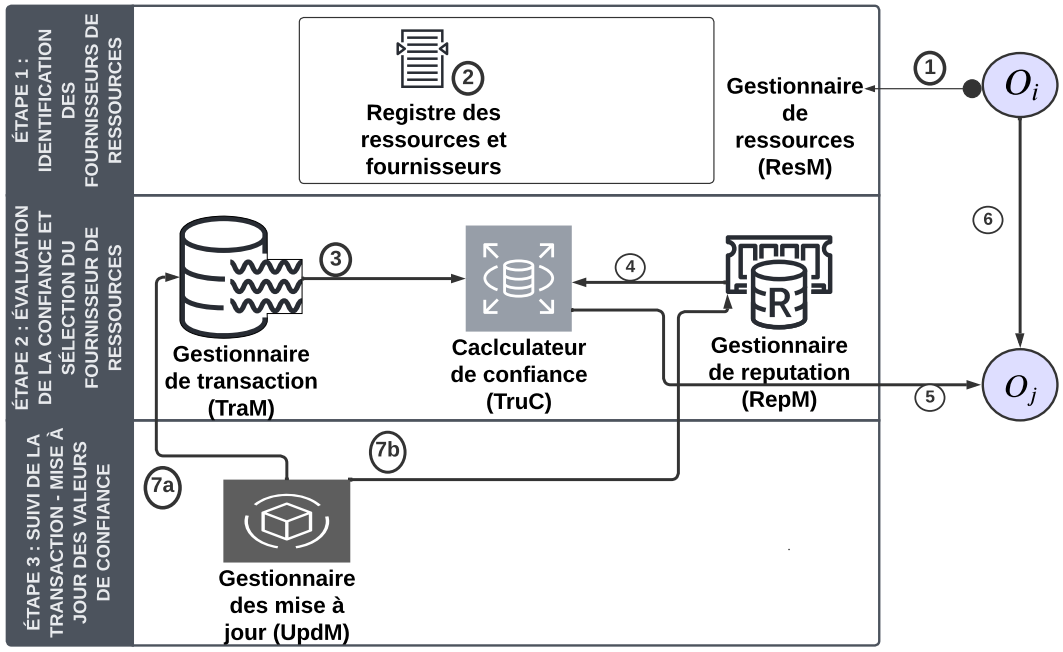


FIGURE 3.9 : Architecture du SeComTrust

L'architecture du *SeComTrust* est présentée à la figure 3.9 ci-dessus. Elle est composée des éléments suivants : le gestionnaire de Ressources (ResM), le manager de transaction (TraM), le calculateur de valeur de confiance (TruC), le gestionnaire de mise à jour de valeur de confiance et de réputation (UpdM), et le manager des valeurs de réputation (RepM). Nous décrivons chaque composant dans les sections ci-dessous.

3.4.2.1 Le gestionnaire de ressources (ResM)

Le gestionnaire de ressources est composé d'un registre qui contient la liste des organisations de la communauté et des ressources qu'elles offrent et d'un module de gestion des stocks. Les ressources sont de diverses natures. Elles peuvent être des infrastructures physiques virtualisées (espace de stockage, réseaux, serveurs, postes de travail), des applications, des services et des données. Chaque ressource est caractérisée par un niveau de sensibilité. Nous considérons que chaque ressource est affectée d'un niveau de sensibilité selon la norme CVSS (Common Vulnerability Scoring System) v2.0 [158]. Le module de gestion des stocks met à jour l'état de disponibilité des ressources au début et à la fin de chaque échange. Le répertoire des ressources est actualisé automatiquement en cas d'intégration d'un nouveau membre, d'ajout d'un nouveau service,

de départ d'une organisation ou de la fin de fourniture d'une ressource. Cette liste est exprimée sous la forme ci-dessous :

$$\begin{aligned} L_{resm} = \{&(O_{p1}, r_{p1}, g_{rp1}, Q_{rp1}, q_{a1}(t), s_{rp1}(t)), \\ &(O_{p2}, r_{p2}, g_{rp2}, Q_{rp2}, q_{a2}(t), s_{rp2}(t)), \ldots, \\ &(O_{pj}, r_{pj}, g_{rpj}, Q_{rpj}, q_{aj}(t), s_{rpj}(t))\} \end{aligned} \tag{3.4.5}$$

avec O_{pj} une organisation fournisseur de ressource de la communauté, r_{pj} la ressource, g_{rpj} le degré de sensibilité de la ressource, Q_{rpj} la quantité totale de cette ressource fournit par le fournisseur, $q_{aj}(t)$ la quantité totale de la ressource disponible à l'instant t et $s_{rpj}(t)$ l'état de disponibilité de la ressource.

Une ressource disponible est dans un état I ou B le cas contraire. Une ressource peut être fournie par une ou plusieurs organisations avec des niveaux de sensibilités identiques ou différents.

Comme dans [181], nous définissons la fonction $\gamma_{rj}(t)$ comme la fonction indicatrice de l'état de disponibilité d'une ressource à l'instant t. Ainsi :

$$\gamma_{rj}(t) = \begin{cases} 1\ if\ the\ resource\ is\ availlable\ then\ in\ a\ state\ I \\ 0\ else\ then\ in\ a\ state\ B \end{cases} \tag{3.4.6}$$

Pour notre modèle, nous exprimons la quantité totale de la ressource disponible à l'instant t :

$$q_{aj}(t) = \sum_{n=1}^{Q_{rpj}} r_n(t)\ with\ r_n(t) = 1\ if\ \gamma_{rn}(t) = 1 \tag{3.4.7}$$

Au début de tout nouvel échange, une opération de mise à jour de l'état de disponibilité des ressources est effectuée.

3.4.2.2 Le manager de transactions (TraM)

Le manager de transactions est le répertoire local des échanges d'une organisation. Il permet d'enregistrer et de référencer tous les partages effectués par un membre de la communauté. Le TraM contient les informations de confiance de tous les nœuds avec lesquels l'organisation a interagi en tant que demandeur de ressources. Le but du manager de transactions est de maintenir une liste de confiance locale pour chaque organisation et de mettre à disposition ces informations pour une détermination décentralisée, efficace et rapide des valeurs d'opinions de confiance. De ce fait, il est l'élément de consultation prioritaire dans notre processus de sélection du fournisseur de confiance.

Les informations du TraM se présentent comme ci-dessous :

$$\begin{aligned} L_{tram} = \{&(O_{p1}, r_{p1}, g_{rp1}, q_{rp1}, \omega_{O_{p1}}^{O_{ui}}, sr_{O_{p1}}, sd_{O_{p1}}, l_{a1}, b_{m1}, \theta_{s1}), \\ &(O_{p2}, r_{p2}, g_{rp2}, q_{rp2}, \omega_{O_{p2}}^{O_{ui}}, sr_{O_{p2}}, sd_{O_{p2}}, l_{a2}, b_{m2}, \theta_{s2}), \ldots, \\ &(O_{pj}, r_{pj}, g_{rpj}, q_{rpj}, \omega_{O_{pj}}^{O_{ui}}, sr_{O_{pj}}, sd_{O_{pj}}, l_{aj}, b_{mj}, \theta_{sj})\}. \end{aligned} \tag{3.4.8}$$

avec :

- O_{pj} le fournisseur de la ressource ;
- r_{pj} la ressource fournie ;

- g_{rpj} le degré de sensibilité de la ressource ;
- q_{rpj} la quantité de ressource fournie ;
- $\omega_{O_{pj}}^{O_{ui}}$ la valeur d'opinion de confiance du partenaire O_{ui} vis-à-vis du fournisseur O_{pj} ,
- $sr_{O_{pj}}$ la réputation spécifique du fournisseur ;
- $sd_{O_{pj}}$ le domaine de sécurité du fournisseur ;
- l_{a1} l'indicateur du respect de paramètres de qualité de la ressource ;
- b_{mj} le mode de facturation ;
- θ_{sj} le résultat du partage.

Comme dans [13][20] [19], nous définissons l'opinion de confiance globale du demandeur vis-à-vis du fournisseur comme la somme pondérée de la relation directe ou recommandée du fournisseur et de la réputation du fournisseur.

$$\omega_{O_{pj}}^{O_{ui}}(r,g,q,t,\tau) = \beta DRT_{O_{pj}}^{O_{ui}}(r,g,q,t,\tau) + (1-\beta) sr_{O_{pj}}(r,g) \tag{3.4.9}$$

$DRT_{O_{pj}}^{O_{u}i}(r,g,q,t,\tau)$ est l'opinion de confiance sur la base d'interactions directes entre le fournisseur et le partenaire. Par ailleurs, cette valeur peut être obtenue sur la base de recommandation d'organisations intermédiaires ayant déjà échangé indépendamment avec le fournisseur et le partenaire.

$sr_{O_{pj}}$ la réputation spécifique représente le comportement d'une organisation en tant que fournisseur d'une ressource donnée au sein de la communauté. Pour une organisation qui n'a pas encore fourni un type de ressource, la valeur de sa réputation spécifique liée à cette ressource est égale au taux de base sr_{init}, avec $sr_{init} = 0$. Cette valeur est mise à jour après chaque opération de partage de ressource (voir 3.4.3.3).

Une opinion de confiance représente un degré de confiance d'une organisation O_{ui} vis-à-vis d'une autre organisation O_{pj} dans une relation à une période donnée [47]. Ces valeurs d'opinions de confiance de notre système seront calculées en utilisant la logique subjective (SL) [110][113]. En effet, comme présenté à la section 2.3.4.2, la logique subjective est utilisée dans le cas des évènements dont les estimations de probabilités sont incertaines. C'est-à-dire lorsqu'on ignore la probabilité de réalisation. Le principal avantage de la logique subjective est d'aider à l'analyse et à la modélisation de manière plus réaliste de faits du monde réel, avec des résultats exprimant plus significativement l'ignorance et l'incertitude. Ainsi, la SL s'est avérée particulièrement efficace dans la caractérisation des situations incertaines, dans les outils d'aide à la prise de décision et les systèmes complexes comme le cloud communautaire. Par conséquent, la diversité des organisations et des ressources de notre communauté justifie l'incertitude sur la probabilité qu'une organisation fournisse une ressource dans les conditions souhaitées. Par ailleurs, la logique subjective nous permet de déterminer une valeur de confiance pour les nouveaux adhérents ou les membres inactifs de la communauté. Les valeurs de confiance sont calculées à partir de quatre paramètres : la croyance (b), l'incrédulité(d), l'incertitude (u) et le taux de base (α). Nous formulons l'opinion de confiance de l'organisation O_{ui} à l'égard de l'organisation O_{pj} (fournisseur de la ressource r_{pj} de degré de sensibilité g_{rpj}) comme l'opinion de O_{ui} à l'égard O_{pj}.

- Pour une interaction directe entre deux organisations :

$$DRT_{O_{pj}}^{O_{ui}}(r,g,q,t,\tau) = b + (\alpha * u)\ avec\ b,d,u,\alpha \in [0,1]\ et\ b+d+u = 1 \tag{3.4.10}$$

$$\begin{cases} b = \frac{p_t}{p_t+n_t+2} \\ d = \frac{n_t}{p_t+n_t+2} \\ u = \frac{2}{p_t+n_t+2} \end{cases} \iff \begin{cases} p_t = \frac{2b}{u} \\ n_t = \frac{2d}{u} \end{cases} \tag{3.4.11}$$

avec p_t le nombre d'échanges positifs précédents entre O_{ui} et O_{pj}, et n_t le nombre de transactions négatives. Une valeur de confiance de référence peut être accordée à tout acteur de la communauté en l'absence d'éléments spécifiques permettant de l'exprimer. Cette valeur représente le taux de base α et est primordiale pour les nouveaux adhérents ou les membres inactifs de la communauté. Elle varie selon que le membre soit digne de confiance ou non. Dans le cadre de communauté, le taux de base est défini comme ci-dessous :

$$\alpha = 0.5 \tag{3.4.12}$$

- Dans les cas d'interactions indirectes ou recommandées comme représentées sur la figure 2.7 où les entités A, B et C sont respectivement représentées par O_{ui}, O_{pj} et O_{tz} :

  La confiance dérivée entre O_{ui} et O_{pj} est $\omega_{O_{pj}}^{O_{ui}:O_{tz}}$ et est calculée grâce à l'opérateur d'actualisation($\bigotimes$) :

$$\omega_{O_{pj}}^{O_{ui}:O_{tz}} = \omega_{O_{tz}}^{O_{ui}} \bigotimes \omega_{O_{pj}}^{O_{tz}} \begin{cases} b_{O_{pj}}^{O_{ui}:O_{tz}} = b_{O_{tz}}^{O_{ui}} b_{O_{pj}}^{O_{tz}} \\ d_{O_{pj}}^{O_{ui}:O_{tz}} = b_{O_{tz}}^{O_{ui}} d_{O_{pj}}^{O_{tz}} \\ u_{O_{pj}}^{O_{ui}:O_{tz}} = d_{O_{tz}}^{O_{ui}} + u_{O_{tz}}^{O_{ui}} + b_{O_{tz}}^{O_{ui}} u_{O_{pj}}^{O_{tz}} \\ \alpha_{O_{pj}}^{O_{ui}:O_{tz}} = \alpha_{O_{pj}}^{O_{tz}} \end{cases} \tag{3.4.13}$$

  Par ailleurs, s'il existe deux opinions $\omega_{O_{pj}}^{O_{ui}}$ et $\omega_{O_{pj}}^{O_{tz}}$ respectivement, la confiance O_{ui} en O_{pj} et celle de O_{tz} en O_{pj}. La confiance dérivée entre O_{ui} et O_{pj} est une est représentée comme l'opinion $\omega_{O_{pj}}^{O_{ui} \diamond O_{tz}}$. Elle est exprimée ci-après grâce à la logique subjective et son opérateur de consensus ($\bigoplus$)[110] :

$$\omega_{O_{pj}}^{O_{ui} \diamond O_{tz}} = \omega_{O_{pj}}^{O_{ui}} \bigoplus \omega_{O_{pj}}^{O_{tz}} \begin{cases} b_{O_{pj}}^{O_{ui} \diamond O_{tz}} = \frac{b_{O_{pj}}^{O_{ui}} u_{O_{pj}}^{O_{tz}} + b_{O_{pj}}^{O_{tz}} u_{O_{pj}}^{O_{ui}}}{u_{O_{pj}}^{O_{ui}} + u_{O_{pj}}^{O_{tz}} - u_{O_{pj}}^{O_{ui}} u_{O_{pj}}^{O_{tz}}} \\ d_{O_{pj}}^{O_{ui} \diamond O_{tz}} = \frac{d_{O_{pj}}^{O_{ui}} u_{O_{pj}}^{O_{tz}} + d_{O_{pj}}^{O_{tz}} u_{O_{pj}}^{O_{ui}}}{u_{O_{pj}}^{O_{ui}} + u_{O_{pj}}^{O_{tz}} - u_{O_{pj}}^{O_{ui}} u_{O_{pj}}^{O_{tz}}} \\ u_{O_{pj}}^{O_{ui} \diamond O_{tz}} = \frac{u_{O_{pj}}^{O_{ui}} u_{O_{pj}}^{O_{tz}}}{u_{O_{pj}}^{O_{ui}} + u_{O_{pj}}^{O_{tz}} - u_{O_{pj}}^{O_{ui}} u_{O_{pj}}^{O_{tz}}} \\ \alpha_{O_{pj}}^{O_{ui} \diamond O_{tz}} = \alpha_{O_{pj}}^{O_{ui}} \end{cases} \tag{3.4.14}$$

3.4.2.3 Le calculateur de valeur de confiance (TruC)

Le TruC est le composant central de notre modèle. Il exécute l'algorithme principal du modèle et effectue les différents calculs de valeur de confiance afin de fournir une évaluation d'un fournisseur de ressources pour un partenaire. Les différents calculs sont portés sur les valeurs de confiance directe ou recommandée, d'opinion globale, mais également des tâches relatives à la faisabilité d'une transaction (comparaison de seuils de confiance, vérification, conformité de paramètres de qualité de service). Par ailleurs, il est responsable de l'exécution des différents algorithmes d'identification et de sélection du fournisseur.

3.4.2.4 Le Gestionnaire de mise à jour (UpdM)

Le gestionnaire de mise à jour intègre deux sous composants : le gestionnaire de paramètres de qualité de ressources (QoRM) et le Feedback Manager (FeeM). Il a pour rôle principal de procéder à l'actualisation des informations de confiance sur la base des résultats fournis par le Feedback Manager. Les valeurs mises à jour sont : la réputation spécifique du fournisseur, les réputations globales du partenaire et du fournisseur, et les différentes informations sur la transaction à enregistrer dans la TraM. Par ailleurs, les niveaux d'assurance et domaine de sécurité sont également actualisés grâce au mécanisme de promotion et relégation. Les différentes informations résultantes de ce processus permettront au gestionnaire de stock d'actualiser le stock et l'état de disponibilités des ressources. Les sous composants du gestionnaire de mise à jour sont décrits ci-dessous :

- **Le gestionnaire de paramètres de qualité de ressources (QoRM) :** c'est le composant qui gère les paramètres contractuels qualitatifs et quantitatifs liés à une ressource partagée. Il permet d'assurer le suivi et le contrôle du respect des engagements de chaque entité. Les résultats des analyses effectuées par ce composant permettent d'actualiser les valeurs de confiance durant tout le processus de partage.
- **Le Feedback Manager (FeeM) :** le Feedback manager recueil et consolide les résultats de l'analyse du QoRM, des avis de chaque participant individuellement dans le but de fournir une évaluation finale de la transaction. Le résultat d'un échange est exposé par le FeeM dès la réception et le déploiement de la ressource par le partenaire. Les conclusions du FeeM sont actualisées à chaque violation des paramètres contractuels de qualité durant la période d'utilisation. Le FeeM met ensuite ces informations à la disposition du gestionnaire de mise à jour en vue.

3.4.2.5 Le Manager de réputation(RepM)

Le RepM est le registre des réputations des organisations de la communauté. Nous distinguons deux types de réputations : la réputation de fournisseur spécifique d'une ressource donnée et la réputation globale d'une organisation découlant de son comportement général au sein de la communauté. Les informations de ce registre sont formulées comme ci-dessous :

$$\begin{aligned} L_{repm} = \{&(O_{p1}, r_{p1}, g_{rp1}, sr_{O_{p1}}, gr_{O_{p1}}, sd_{Op1}), \\ &(O_{p2}, r_{p2}, g_{rp2}, sr_{O_{p2}}, gr_{O_{p2}}, sd_{O_{p2}}), \ldots, \\ &(O_{pj}, r_{pj}, g_{rpj}, sr_{O_{pj}}, gr_{O_{pj}}, sd_{O_{pj}}\}. \end{aligned} \tag{3.4.15}$$

avec O_{pj} le fournisseur de la ressource, r_{pj} la ressource fournie, g_{rpj} le degré de sensibilité de la ressource fournie, $sr^{O_{pj}}$ la réputation de l'organisation en tant que fournisseur de r_{pj} de degré g_{rpj}, $gr_{O_{pj}}$ la valeur de réputation globale et $sd_{O_{pj}}$ le domaine de sécurité de l'organisation.

3.4.3 Évaluation de la confiance et mécanisme de promotion ou relégation

L'objectif de l'évaluation de la confiance est d'identifier un fournisseur de confiance pour une ressource donnée, de mettre à jour les valeurs de confiance et de réputation, et de récompenser ou sanctionner les acteurs d'une transaction à travers un protocole de promotion et de relégation.

Le système commun d'évaluation des vulnérabilités (CVSS) [61] définit un cadre permettant de spécifier les principales caractéristiques de vulnérabilités de ressources informatiques. Par ailleurs, il permet de mesurer la gravité de ces vulnérabilités et les conséquences de leurs exploitations sur des systèmes informatiques. Le CVSS fournit des indices de gravité qualitatifs (faible, moyen, élevé) et des scores qui représentent les caractéristiques de chaque vulnérabilité [158][183][192]. Le niveau de sensibilité des ressources du *SeComTrust* décrit le degré de vulnérabilité d'une ressource. Une ressource très sensible doit être moins vulnérable aux menaces et attaques. Nous définissons les niveaux de sensibilité des ressources de notre Cloud communautaire à partir de la gamme de score de base de la version CVSS v2.0 [158].

r_{pj} une ressource de degré de sensibilité g_{rpj} , L_g le niveau de sensibilité bas, M_g le niveau de sensibilité intermédiaire, H_g le niveau de sensibilité élevé.

Definition 3.4.3. r_{pj} est une ressource de niveau de sensibilité :

- L_g si $g_{rpj} \in [7, 10]$
- M_g si $g_{rpj} \in [4, 7[$
- H_g si $g_{rpj} \in [0, 4[$

Le niveau d'assurance exprime la capacité d'une organisation à fournir une ressource d'un niveau de sensibilité spécifique. Une organisation de niveau d'assurance élevé fournit des ressources peu vulnérables. Toutes les organisations intègrent la communauté avec un niveau d'assurance I_{l0}=0. La valeur du niveau d'assurance d'une organisation est mise à jour chaque fois qu'elle fournit une ressource. Ce processus est décrit dans 3.4.3.3

L_{il} le niveau d'assurance bas, M_{il} le niveau d'assurance intermédiaire, H_{il} le niveau d'assurance élevé.

Definition 3.4.4. I_l le niveau d'assurance d'une organisation O_{pj}. O_{pj} a un niveau d'assurance :

- L_{il} si $I_l \in [0, 4[$
- M_{il} si $I_l \in [4, 7[$
- H_{il} si $I_l \in [7, 10]$

Le domaine de sécurité est un regroupement des organisations de la communauté en fonction de leur niveau d'assurance. Une organisation de domaine de sécurité avancé à un niveau d'assurance élevé. L_{sd} le domaine de sécurité bas, M_{sd} le domaine de sécurité intermédiaire, H_{sd} le domaine de sécurité avancé.

Definition 3.4.5. I_l le niveau d'assurance d'une organisation O_{pj}. O_{pj} appartient au domaine de sécurité :

- L_{sd} si $I_l \in [0, 4[$
- M_{sd} si $I_l \in [4, 7[$
- H_{sd} si $I_l \in [7, 10]$

Le domaine de sécurité bas L_{sd} est le domaine initial de toutes les organisations de la communauté. Cependant, une organisation peut fournir des ressources de tout niveau de sensibilité, indépendamment de son domaine de sécurité. Le domaine de sécurité d'une organisation est actualisé à chaque transaction dans laquelle elle est impliquée comme fournisseur (3.4.3.33.4.3.3).

Les différents algorithmes intervenant dans l'évaluation de la confiance grâce au *SeComTrust* sont décrits ci-dessous.

3.4.3.1 L'identification des fournisseurs de la ressource demandée

Sur la base du registre des ressources, les fournisseurs disposant de la ressource demandée et dans un état I (disponible) à la date t souhaitée par le client, sont classés par ordre de priorité, du domaine de sécurité le plus élevé au plus bas. Au cas où nous distinguerions plusieurs organisations au sein du même domaine de sécurité, elles sont rangées du niveau d'assurance le plus élevé au plus bas.

Algorithme 1 : Identification des fournisseurs de ressources

Précondition : une organisation O_{ui} demande la ressource r_{ui} de degré de sensibilité g_{rui}

Entrée :O_{ui}, r_{ui}, g_{rui}, la liste des ressources L_{resm}

Sortie : La liste des fournisseurs de la ressource L_{rps}

Hypothèse : Toutes les ressources demandées existent et sont répertoriées dans la liste L_{resm} avec les fournisseurs associés

1: **Fonction** IDENTIFICATION(Liste $L_{resm}, r_{ui}, g_{rui}$)
2: L_{resm} *voir équation* 3.4.5
3: **pour** *chaque* $O_{pj} \in L_{resm}$ **faire**
4: **si** $r_{ui} == r_{pj}$ *et* $g_{rui} == g_{rpj}$ **alors**
5: $L_{rp} \leftarrow O_{pj}$
6: **fin si**
7: **fin pour**
8: **si** $L_{rp} == null$ **alors**
9: **pour** $each\ O_{pj} \in L_{resm}$ **faire**
10: **si** $r_{ui} == r_{pj}$ *et* $g_{rui} == g_{rpj}$ **alors**
11: $L_{rp} \leftarrow O_{pj}$
12: **fin si**
13: **fin pour**
14: **fin si**
15: Trier les organisations de la liste L_{rp} par domaine de sécurité et niveau d'assurance décroissants. En cas d'égalité des valeurs, la valeur la plus récente est considérée comme la plus importante.
16: $L_{rps} \leftarrow L_{rp}(DESC)$
17: **retourne** L_{rps}
18: **fin Fonction**

3.4.3.2 La sélection du fournisseur

Après la phase d'identification des fournisseurs de la ressource demandée, l'étape suivante du modèle consiste à rechercher et à sélectionner l'un des fournisseurs pour le partage de la ressource. Il s'agira de parcourir la liste des fournisseurs par ordre de priorité, de calculer la valeur de confiance du demandeur vis-à-vis du fournisseur, de déterminer celle du fournisseur vis-à-vis du partenaire et de comparer ces valeurs aux différents seuils d'opinions requis pour autoriser ou non une transaction. Ces opérations sont exécutées en différentes sous étapes selon un ordre chronologique bien précis. Tout d'abord, la recherche à partir de la liste de transactions directes du demandeur, ensuite sur la base de la liste de transactions indirectes ou de recommandations, suivra l'exploration de la liste de réputations spécifiques et enfin la sélection à partir de la liste de réputations globales. À chacune de ces phases, l'ensemble de la liste des fournisseurs est parcourue de la première à la dernière organisation. Le choix d'une organisation met fin au processus de sélection sinon l'on passe à l'étape suivante en

parcourant de nouveau la liste. Nous décrivons ci-dessous ces différentes ces phases.

- *La sélection à partir de la liste de transactions directes* : elle consiste à explorer la liste de transactions du demandeur afin de s'assurer de la présence de transactions antérieures directes avec le fournisseur identifié. La présence d'une transaction pour la même ressource, de même degré de sensibilité, permettra de sélectionner un fournisseur pour l'échange. Une interaction précédente avec un fournisseur pour une ressource distincte pourra éventuellement servir de base de sélection. S'il existe une interaction ou plusieurs interactions, la dernière transaction en date est retenue. Pour chaque fournisseur, nous calculons son opinion de confiance à l'égard du demandeur (représenté par la réputation globale du demandeur) et l'opinion du demandeur vis-vis du fournisseur calculer à partir des équations de 3.4.9 à 3.4.12. Ensuite, ces valeurs sont comparées aux valeurs seuils d'opinions requises en fonction des domaines de sécurité du partenaire et du fournisseur. L'autorisation pour un partage est obtenue en comparant les valeurs d'opinions du demandeur et du fournisseur aux valeurs seuils des matrices de gouvernance ci-dessous 3.103.11.
  Soit $O_{L_{sd}}$, $O_{M_{sd}}$, $O_{H_{sd}}$ des organisations de domaine de sécurité respectivement bas, intermédiaire et élevé. T_p la matrice de gouvernance du fournisseur qui exprime le seuil minimal de l'opinion du fournisseur vis-à-vis d'un demandeur (seuil minimal de réputation globale d'un demandeur) d'un domaine de sécurité donné et T_u la matrice de gouvernance du partenaire qui exprime le seuil minimal de l'opinion du demandeur à l'égard du fournisseur d'un domaine de sécurité donné. Haut (H), Intermédiaire (M), Bas (L) sont respectivement les degrés d'opinions requis dans chaque cas.

  Ainsi, nous considérons que pour un fournisseur de niveau de sécurité bas (L), son degré d'opinion minimal requis :

  - à l'égard d'un partenaire de niveau bas (L) doit être (H) ;
  - à l'égard d'un partenaire moyen (M) doit être (M) ;
  - à l'égard d'un partenaire de niveau élevé (H) doit être (L).

  Nous formulons les mêmes hypothèses pour des fournisseurs de domaine de sécurité respectivement moyen et élevé. Nous exprimons ces règles dans la matrice de gouvernance du fournisseur ci-dessous.

$$T_{O_{pj}} = \begin{array}{c} \\ O_{L_{sd}} \\ O_{M_{sd}} \\ O_{H_{sd}} \end{array} \begin{array}{c} \begin{array}{ccc} O_{L_{sd}} & O_{M_{sd}} & O_{H_{sd}} \end{array} \\ \begin{bmatrix} H & M & L \\ H & M & L \\ H & M & L \end{bmatrix} \end{array}$$

Nous faisons correspondre à ces seuils d'opinions des valeurs (λ_{max},λ_{med},λ_{min})

$$\text{comme illustré ci-après } T_{O_{pj}} = \begin{array}{c} \\ \mathrm{O}_{L_{sd}} \\ \mathrm{O}_{M_{sd}} \\ \mathrm{O}_{H_{sd}} \end{array} \begin{array}{c} \begin{array}{ccc} O_{L_{sd}} & O_{M_{sd}} & O_{H_{sd}} \end{array} \\ \begin{bmatrix} \lambda_{max} & \lambda_{med} & \lambda_{min} \\ \lambda_{max} & \lambda_{med} & \lambda_{min} \\ \lambda_{max} & \lambda_{med} & \lambda_{min} \end{bmatrix} \end{array}$$

FIGURE 3.10 : Matrice de gouvernance du fournisseur

Partant du même principe, nous établissons la matrice de gouvernance du partenaire ci-dessous :

$$T_{O_{ui}} = \begin{array}{c} \\ O_{L_{sd}} \\ O_{M_{sd}} \\ O_{H_{sd}} \end{array} \begin{array}{c} \begin{array}{ccc} O_{L_{sd}} & O_{M_{sd}} & O_{H_{sd}} \end{array} \\ \begin{bmatrix} H & M & L \\ H & M & L \\ H & M & L \end{bmatrix} \end{array}$$

$$T_{O_{ui}} = \begin{array}{c} \\ O_{L_{sd}} \\ O_{M_{sd}} \\ O_{H_{sd}} \end{array} \begin{array}{c} \begin{array}{ccc} O_{L_{sd}} & O_{M_{sd}} & O_{H_{sd}} \end{array} \\ \begin{bmatrix} \epsilon_{max} & \epsilon_{med} & \epsilon_{min} \\ \epsilon_{max} & \epsilon_{med} & \epsilon_{min} \\ \epsilon_{max} & \epsilon_{med} & \epsilon_{min} \end{bmatrix} \end{array}$$

FIGURE 3.11 : Matrice de gouvernance du partenaire

Un partage est autorisé entre un fournisseur O_{pj_H} de domaine de sécurité haut et un demandeur O_{ui_L} de domaine de sécurité bas, si :

$$\omega_{O_{pj_H}}^{O_{ui_L}} \geq \epsilon_{min} \; et \; \omega_{O_{ui_L}}^{O_{pj_H}} \geq \lambda_{max} \tag{3.4.16}$$

Le processus de sélection à partir d'interactions directe est présenté dans l'algorithme 2 ci-dessous.

Algorithme 2 : Sélection d'un fournisseur de ressources à partir de liste des transactions directes

Précondition : La liste des fournisseurs L_{rps} de la ressource g_{rui} de niveau de sensibilité g_{rui} demandée r_{ui} par l'organisation O_{ui}

Entrée : La liste des fournisseurs L_{rps}, la liste locale des transactions précédentes du demandeur L_{tram}, la liste des réputations des organisations L_{repm}

Sortie : Le fournisseur de ressources sélectionné O_{pjs}

Procédure SELECINDIRECTTRAM($L_{rps}, L_{tram}, L_{repm}, r_{ui}, g_{rui}$,$O_{ui}$) // avec $L_{rps} \leftarrow Identification(L_{resm}, r_{ui}, g_{rui})$ (voir algorithme 1)
  pour *chaque* $O_{pj} \in L_{rps}$ **faire**
    si $O_{pj} \in L_{tram}$ **alors**
      si $(r_{tram} == r_{ui} \; et \; g_{tram} == g_{rui}) \; ou \; (r_{tram} != r_{ui} \; et \; g_{tram} \geq g_{rui})$ **alors**
        $Récupérer \; les \; informations \; sur \; O_{pj}$
        $Calculer \; l'opinion(\omega_{O_{pj}}^{O_{ui}}) \; de \; confiance \; de \; O_{ui} \; envers \; O_{pj}$
        $grâce \; aux \; équations$ 3.4.10 $à$ 3.4.12
        $\omega_{O_{ui}}^{O_{pj}} \leftarrow gr_{O_{ui}}$ // $gr_{O_{pj}}$ réputation globale de O_{ui}
        $valInitTram(O_{pj}, \omega_{O_{ui}}^{O_{pj}}, \omega_{O_{pj}}^{O_{ui}}, r_{ui}, g_{rui}, O_{ui})$ (voir algorithme 5)
      fin si
    fin si
  fin pour
fin Procédure

- *La sélection à partir de la liste de transactions indirectes* : si la recherche dans la liste de transactions directes du demandeur ne permet pas d'identifier un fournisseur, l'étape suivante consiste à trouver un fournisseur sur la base d'organisations intermédiaires de la liste de transactions du demandeur ayant interagi auparavant avec un fournisseur de la liste identifié dans l'algorithme 1. Ce type d'interaction entre le demandeur et le fournisseur peut être présenté sous la forme d'une

relation Friend of a Friend (FoF) ou Friend of Multiple friends (FoM) [131]. Ces différents types de relations sont présentés à la figure 3.12 ci-dessus. Ce processus de calcul des valeurs de confiance est détaillé dans l'algorithme 3.

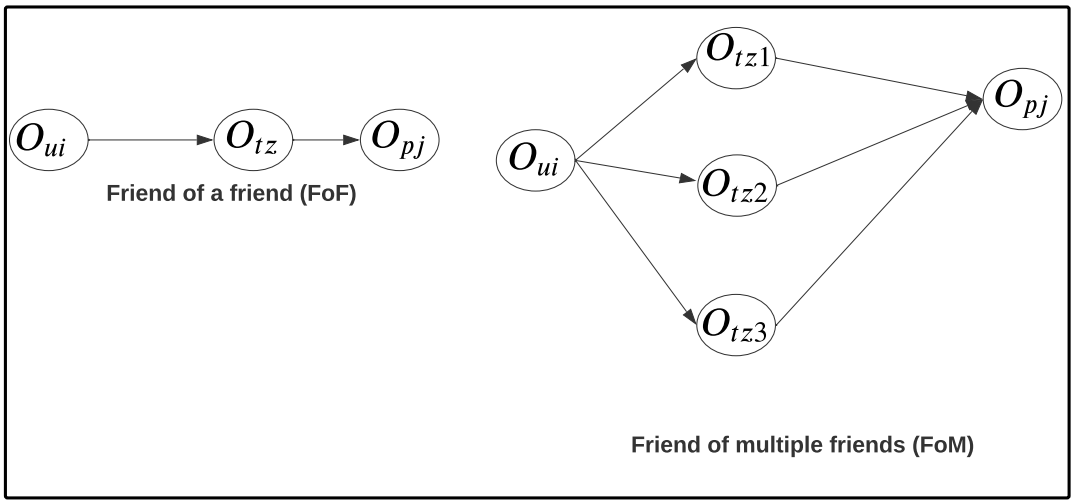


FIGURE 3.12 : Types de relations FoF et FoM

Algorithme 3 : Détermination de la valeur de confiance par recommandation

Précondition : La liste des fournisseurs L_{rps} de la ressource g_{rui} de niveau de sensibilité g_{rui} demandée r_{ui} par l'organisation O_{ui}

Entrée : La liste des fournisseurs L_{rps}, la liste locale des transactions précédentes du demandeur L_{tram}, la liste des réputations des organisations L_{repm}

Sortie : Le fournisseur de ressources sélectionné O_{pjs}

1: **Procédure** SELECTINDIRECTTRAM($L_{rps}, L_{tram}, L_{repm}, r_{ui}, g_{rui}$,$O_{ui}$) // Avec $L_{rps} \leftarrow Identification(L_{resm}, r_{ui}, g_{rui})$ (voir algorithme 1)
2: **pour** $chaque\ O_{pi} \in L_{rps}$ **faire**
3: **si** $O_{pj}\ est\ l'ami\ d'un\ seul\ ami\ (FoF)\ de\ O_{ui}\ dans\ L_{tram}$ **alors**
4: $Récupérer\ les\ informations\ sur\ O_{pj}$
5: $Calculer\ l'opinion(\omega_{O_{pj}}^{O_{ui}})\ de\ confiance\ de\ O_{ui}\ envers\ O_{pj}$
6: $grâce\ aux\ équations$ 3.4.10 à 3.4.13
7: $\omega_{O_{ui}}^{O_{pj}} \leftarrow gr_{O_{ui}}$ // $gr_{O_{pj}}$ réputation globale de O_{ui}
8: $valInitTram(O_{pj}, \omega_{O_{ui}}^{O_{pj}}, \omega_{O_{pj}}^{O_{ui}}, r_{ui}, g_{rui}, O_{ui})$ (voir algorithme 5)
9: **sinon**
10: $//O_{pj}\ est\ l'ami\ de\ plusieurs\ amis\ (FoM)\ de\ O_{ui}\ dans\ L_{tram}$
11: $Récupérer\ les\ informations\ sur\ O_{pj}$
12: $Calculer\ l'opinion(\omega_{O_{pj}}^{O_{ui}})\ de\ confiance\ de\ O_{ui}\ envers\ O_{pj}$
13: $grâce\ aux\ équations$ 3.4.10 à 3.4.14
14: $\omega_{O_{ui}}^{O_{pj}} \leftarrow gr_{O_{ui}}$ // $gr_{O_{pj}}$ réputation globale de O_{ui}
15: $valInitTram(O_{pj}, \omega_{O_{ui}}^{O_{pj}}, \omega_{O_{pj}}^{O_{ui}}, r_{ui}, g_{rui}, O_{ui})$ (voir algorithme 5)
16: **fin si**
17: **fin pour**
18: **fin Procédure**

- *La sélection à partir de la liste de réputation spécifique* : un recours à la base de réputations spécifiques sera nécessaire si aucun fournisseur n'est trouvé à la suite

des recherches basées sur la liste de transactions du demandeur (TraM). Une nouvelle liste de fournisseur avec des valeurs de réputations spécifiques non nulles ($sr! = 0$) est établie sur la base de la liste des fournisseurs de la ressource identifiée dans 1. Dans cette nouvelle liste, les organisations sont classées par ordre décroissant des valeurs de réputations spécifiques et de domaine de sécurité. Afin de vérifier la faisabilité de la transaction, la valeur de réputation globale du demandeur est comparé au seuil requis de la matrice de gouvernance du fournisseur courant. Si la condition est respectée, alors la transaction est autorisée. Sinon on passe à l'organisation suivante jusqu'à la dernière de la liste. Si cette option s'avère inefficace, l'on se référera aux réputations globales des fournisseurs. L'algorithme de sélection à partir de la liste de réputation est expliqué dans 4

- *La sélection à partir de la liste de réputation globale* : la liste de fournisseurs identifiés dans 1 est rangée par ordre décroissant de valeur de réputations globales et de domaine de sécurité. L'opinion du fournisseur vis-à-vis du partenaire servira de condition pour l'autorisation ou non de la transaction, comme dans le cas de la réputation spécifique. Ce processus est présenté dans l'algorithme 4.

Algorithme 4 : Sélection d'un fournisseur de ressources sur la base de sa réputation

Précondition : La liste des fournisseurs L_{rps} de la ressource g_{rui} de niveau de sensibilité g_{rui} demandée r_{ui} par l'organisation O_{ui}

Entrée : La liste des fournisseurs L_{rps}, la liste des réputations des organisations L_{repm}

Sortie : Le fournisseur de ressources sélectionné O_{pjs}

Fonction SELECTINREP($L_{rps}, L_{repm}, r_{pj}, g_{rpj}$) // Avec $L_{rps} \leftarrow Identification(L_{resm}, r_{ui}, g_{rui})$ (voir algorithme 1)
  pour $chaque\ O_{pj} \in L_{rps}$ **faire**
    si $sr_{O_{pj}}! = 0$ **alors**
      $L_{sr} \leftarrow O_{pj}$
      Classer les organisations par ordre décroissant des valeurs de réputation spécifiques
      $L_{srs} \leftarrow L_{sr}(DESC)$
    fin si
  fin pour
  si $L_{srs}! = null$ **alors**
    pour $chaque\ O_{pj} \in L_{srs}$ **faire**
      $valInitTram(O_{pj}, \omega_{O_{ui}}^{O_{pj}}, \omega_{O_{uj}}^{O_{ui}}, r_{ui}, g_{rui}, O_{ui})$ (voir algorithme 5)
    fin pour
  sinon
    Classer les organisations par ordre décroissant des valeurs de réputation spécifiques
    $L_{grs} \leftarrow L_{rps}(grDESC)$
    pour $chaque\ O_{pj} \in L_{grs}$ **faire**
      $valInitTram(O_{pj}, \omega_{O_{ui}}^{O_{pj}}, \omega_{O_{uj}}^{O_{ui}}, r_{ui}, g_{rui}, O_{ui})$ (voir algorithme 5)
    fin pour
  fin si
fin Fonction

Algorithme 5 : Validation et initialisation de la transaction

Précondition : La valeur de confiance du demandeur $\omega_{O_{ui}}^{O_{pj}}$, La valeur de confiance du fournisseur $\omega_{O_{pj}}^{O_{ui}}$

Entrée : L'organisation demandeur O_{ui}, l'organisation cliente O_{pj}, la valeur de confiance du demandeur $\omega_{O_{ui}}^{O_{pj}}$, la valeur de confiance du fournisseur $\omega_{O_{pj}}^{O_{ui}}$, la ressource r_{pj} de niveau de sensibilité g_{rpj}, q_{rpj} la quantité demandée, q_{rui} quantité fournie, $bm_{O_{ui}}$ le mode de facturation souhaité, $bm_{O_{pj}}$ le mode de facturation accepté par le prestataire, la date à laquelle le client souhaite disposer de la ressource t_{ui}, la date à laquelle le fournisseur s'engage à fournir la ressource t_{pj}, la date de livraison de la ressource t_d, Disponibilité initiale des ressources A_{rinit}, Retour d'information du fournisseur F_{Opj}, Retour d'information du demandeur F_{Oui}, la valeur du résultat du partage R_s, le type de résultat du partage T_{rs}. **Sortie** : Le fournisseur de ressources sélectionné O_{pjs}

Fonction valInitTram(O_{pj},$\omega_{O_{ui}}^{O_{pj}}$, $\omega_{O_{uj}}^{O_{ui}}$, $r_{pj}, g_{rpj}, q_{rpj}, q_{rui}, O_{ui}, t_{ui}, t_{pj}, t_d, t_{ui}, bm_{O_{ui}}, bm_{O_{pj}}$)
  T_{pj} *valeur seuil de confiance du fournisseur* Cette valeur est déduite de la matrice de gouvernance des fournisseurs voir dans 3.10
  T_{ui} *valeur seuil de confiance du demandeur* Cette valeur est déduite de la matrice de gouvernance des demandeurs 3.11
  si ($\omega_{O_{pj}}^{O_{ui}} \geq T_{ui}$ *et* $\omega_{O_{ui}}^{O_{pj}} \geq T_{pj}$) et ($q_{rui} == q_{rpj}$) et ($bm_{O_{ui}}$==$bm_{O_{pj}}$) **alors**
    si ($t_{pj} \geq t_d$) *et* ($t_{ui} \geq t_{pj}$)) || ($t_{pj} \geq t_{ui}$) *et* ($t_{pj} \geq t_d$)) **alors**
      si (A_{rinit}== 1) **alors**
        $F_{Opj} \leftarrow 1$, $F_{Oui} \leftarrow 1$, $R_s \leftarrow 1$, $T_{rs} \leftarrow 1$
        $updTrustValues(R_s, T_{rs})$ (voir algorithme 6)
      sinon
        $F_{Opj} \leftarrow 1$, $F_{Oui} \leftarrow 0$, $R_s \leftarrow 0$, $T_{rs} \leftarrow 0$
        $updTrustValues(R_s, T_{rs})$ (voir algorithme 6)
      fin si
    sinon si ($t_d \geq t_{pj}$) *et* ($t_{ui} \geq t_d$) **alors** // Violation mineure
      si (A_{rinit}== 1) **alors**
        $F_{Opj} \leftarrow 1$, $F_{Oui} \leftarrow 1$, $R_s \leftarrow 1$, $T_{rs} \leftarrow O.5$
        $updTrustValues(R_s, T_{rs})$ (voir algorithme 6)
      sinon
        $F_{Opj} \leftarrow 1$, $F_{Oui} \leftarrow 0$, $R_s \leftarrow 0$, $T_{rs} \leftarrow 0$
        $updTrustValues(R_s, T_{rs})$ (voir algorithme 6)
      fin si
    sinon// violation
      si (A_{rinit}== 1) **alors**
        $F_{Opj} \leftarrow 1$, $F_{Oui} \leftarrow 1$, $R_s \leftarrow 1$, $T_{rs} \leftarrow O.5$
        $updTrustValues(R_s, T_{rs})$ (voir algorithme 6)
      sinon
        $F_{Opj} \leftarrow 1$, $F_{Oui} \leftarrow 0$, $R_s \leftarrow 0$, $T_{rs} \leftarrow 0$
        $updTrustValues(R_s, T_{rs})$ (voir algorithme 6)
      fin si
    fin si
    $O_{pjs} \leftarrow O_{pj}$
  sinon
    $O_{pjs} \leftarrow null$
  fin si
  retourne O_{pjs}
fin Fonction

Après le choix de l'organisation et l'approvisionnement de la ressource, un retour de chaque acteur sur des propriétés qualitatives telles la date de mise à disposition, la disponibilité et la quantité de la ressource permettront de déduire le résultat de l'échange. Ce résultat déclenchera le processus de mise à jour des valeurs de confiance. Par ailleurs, un processus, de suivi de l'utilisation de la ressource permettra de garantir le respect des engagements de chaque partie et d'appliquer éventuellement des pénalités. Le résultat final R_s de la transaction est exprimé selon la matrice ci-dessous en fonction des évaluations des deux organisations O_{pj} et O_{ui} :

$$R_s = \begin{array}{c} \begin{array}{ccc} O_{pj} & O_{ui} & R \end{array} \\ \left[\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{array}\right] \end{array}$$

FIGURE 3.13 : Matrice de résultat de transaction

Les évaluations de chaque participant permettront de déclencher le mécanisme de mise à jour des informations de réputation spécifique et globale, de niveau d'assurance et de domaine de sécurité.

3.4.3.3 Mise à jour des valeurs de confiance

Algorithme 6 actualisation des valeurs de confiance

Précondition : Le résultat du partage de R_s ou de la violation des paramètres de qualité et de performances

Entrée : La valeur du résultat du partage R_s, Le type du résultat du partage T_{rs}.

Sortie :

Procédure UPDTRUSTVALUES(R_s, T_{rs})
  si $R_s == 1\ and\ T_{rs} == 1$ **alors** // Résultat positif sans violation
    $Mise\ à\ jour\ réputation\ spécifique\ avec\ équation\ 3.4.18(résultat\ positif)$
    $Mise\ à\ jour\ niveau\ d'assurance\ avec\ équation\ 3.4.19(résultat\ positif)$
    $Mise\ à\ jour\ reputation\ globale\ avec\ équation\ 4.4.1$
    $Promotion\ rélégation\ 3.4.3.3$
  sinon si $R_s == 1\ and\ T_{rs} == 0.5$ **alors** // Résultat positif avec violation
    $Mise\ à\ jour\ réputation\ spécifique\ avec\ équation\ 3.4.18(résultat\ positif\ avec\ violation)$
    $Mise\ à\ jour\ niveau\ d'assurance\ avec\ équation\ 3.4.19(résultat\ positif\ avec\ violation)$
    $Mise\ à\ jour\ reputation\ globale\ avec\ équation\ 4.4.1$
    $Promotion\ rélégation\ 3.4.3.3$
  sinon
    $Mise\ à\ jour\ réputation\ spécifique\ avec\ équation\ 3.4.18(résultat\ négatif)$
    $Mise\ à\ jour\ niveau\ d'assurance\ avec\ équation\ 3.4.19(résultat\ négatif)$
    $Mise\ à\ jour\ reputation\ globale\ avec\ équation\ 4.4.1$
    $Promotion\ rélégation\ 3.4.3.3$
  fin si
fin Procédure

- **Mise à jour de la réputation spécifique** : basé sur les normes de l'Organisation internationale de normalisation (ISO), les attributs SMI (Service Measurement In-

dex) ont été conçus et promus par Le consortium CSMIC (Cloud Services Measurement Initiatives Consortium). Ces attributs qualitatif et quantitatif représentent un ensemble d'indicateurs clés de performance(PKI) pour mesurer et comparer efficacement la qualité des services cloud. Le cadre SMI permet de caractériser une ressource du point de vue de l'utilisateur et du fournisseur en fonction de : la responsabilité, la facilité d'utilisation, l'assurance, l'agilité, la sécurité et la confidentialité, de l'aspect financier, la performance [202]. Plusieurs travaux fondés sur les SMI pour l'évaluation et la comparaison de services et fournisseurs de services ont été menés [189][197][18][87]. Nous abordons l'évaluation des ressources partagées au sein de notre communauté et des organisations sur la base des attributs SMI suivants : la disponibilité (3.3), le niveau de vulnérabilité (3.4), le temps de réponse (3.2) et le mode de facturation (3.1). Les attributs de disponibilité, de vulnérabilité et de temps de réponse permettent de mesurer et de garantir la participation active des membres et la sécurité des ressources. En outre, l'attribut du mode de facturation des ressources fait intervenir l'aspect social, en occurrence la gratuité dans les échanges.

Nous présentons dans les sections ci-dessous ces différents attributs.

Nom de la mesure	Mode de facturation
Attribut connexe	Processus de facturation
Contexte	Lors de la négociation pour le partage de ressource, il est nécessaire de préciser le mode de facturation (gratuit, partage en échange d'une ressource, échange par moyen fiduciaire traditionnel, échange par monnaie virtuelle). Le mode de facturation aura un impact sur la volonté de partager ou non, sur la quantité partagée, sur le temps accordé à l'utilisation de la ressource et sur les capacités d'extension de la ressource.
Audience de la mesure	Demandeur et fournisseur
Objectif :	Il s'agit d'une mesure de consentement mutuel des deux acteurs impliqués et qui permettra ou non la faisabilité d'une transaction. L'objectif commercial est la sélection d'un fournisseur qui répond aux besoins financiers d'un demandeur et vice - versa.
Définition de la mesure :	Attribuer une valeur à chaque mode de facturation. Les valeurs vont de 1 à 4 comme suit : 1 pour un mode fiduciaire traditionnel, 2 pour une monnaie virtuelle, 3 pour un échange contre une ressource et 4 gratuit. Des ressources pourront être acquises gratuitement en fonction de la réputation globale du demandeur ou en échange d'autres ressources dans le but d'inciter au partage au sein de la communauté.
Collecte de données :	le mode de facturation est collecté auprès de chaque acteur en phase de négociation de l'échange.

TABLE 3.1 : Attribut mode de facturation

Nom de la mesure	Temps de réponse
Attribut connexe	Service temps de réponse
Contexte	A une requête de demande d'une ressource, est associée la date à laquelle le partenaire souhaiterait accéder à la ressource. Le temps de réponse représente le temps pris par le fournisseur pour répondre à cette demande.
Audience de la mesure	Demandeur et fournisseur
Objectif :	S'assurer de l'efficacité et du respect du délai de mise à disposition d'une ressource par un fournisseur.
Définition de la mesure :	Définir comme éléments d'évaluation : la date souhaitée par le demandeur t_{ui}, la date de réponse promise par le fournisseur t_{pj} et la date de livraison effective t_d. Le temps de réponse sera évalué par trois scores différents : le score (1) pour une transaction se déroulant en respectant la date prévue, le score (0.5) pour une transaction étant prévu avant la date souhaitée, mais finalement fournit à une date supérieure à la période prévue, mais inférieure à la date souhaitée, le score (-1) pour une livraison au-delà de la date promise et avec une date souhaitée inférieure à la date promise.
Collecte de données :	Les dates (souhaitée et promise) sont définis respectivement par le partenaire et le fournisseur, et la date de livraison est déduite au moment de la livraison de la ressource.

TABLE 3.2 : Attribut temps de réponse

Nom de la mesure	Disponibilité
Attribut connexe	Disponibilité
Contexte	Une ressource est fournie pour période bien définie. Et elle doit avoir la capacité de garder un niveau de disponibilité jusqu'à la fin de cette période.
Audience de la mesure	Organisations (fournisseur/demandeur)
Objectif :	Maintenir un niveau de disponibilité efficient des ressources fournies au sein de la communauté.
Définition de la mesure :	Exprimée sous la forme d'une proportion de temps pendant laquelle les ressources sont disponibles par rapport au temps total pendant lequel elles devraient être. Elle peut être calculée comme ci-dessous : $$Disponibilité(r) = \frac{T_w}{T_f} \quad (3.4.17)$$ avec T_w le temps de disponibilité du service et T_f le temps total d'utilisation du service. Cette valeur sera comparée aux taux de disponibilité promis par le fournisseur afin d'évaluer la qualité de disponibilité de la ressource.
Collecte de données :	Le taux est disponibilité est obtenu grâce aux retours d'informations des deux acteurs.

TABLE 3.3 : Attribut Disponibilité

Nom de la mesure	Gestion des menaces et des vulnérabilités
Attribut connexe	Gestion proactive des menaces et des vulnérabilités
Contexte	Le niveau de vulnérabilité des ressources partagées a un impact sur la sécurité de l'infrastructure physique et logiciel de la communauté. Pour se prémunir des menaces et attaques, il est important de réduire le niveau de vulnérabilité des ressources partagées.
Audience de la mesure	Fournisseurs
Objectif :	Le but est de s'assurer que les ressources partagées au sein de la communauté sont sécurisées et respectent les normes et standard (comme énoncé dans 3.4.3).
Définition de la mesure :	Attribuer des niveaux de sensibilité à chaque ressource partagée. Ces niveaux sont définis selon la norme de degré de vulnérabilité CVSS (3.4.3). On a ainsi trois niveaux : élevé, moyen et bas.
Collecte de données :	Le niveau de sensibilité est défini par chaque fournisseur de ressources.

TABLE 3.4 : Attribut vulnérabilité

La réputation spécifique exprime le comportement d'une entité au sein de la communauté, en tant que fournisseur d'une ressource spécifique, à travers les résultats de ses interactions antérieures. Elle est mise à jour après la livraison d'une ressource au cours d'un échange et est actualisée à chaque violation des métriques de qualité de la ressource. Dans le but d'inciter au partage de ressources sécurisées (avec des niveaux de vulnérabilités réduits), un poids est affecté à chaque échange de ressource d'un niveau spécifique donné. Ainsi, un partage d'une ressource de niveau bas est coté à 20%, 35% pour un niveau moyen, et 45% pour un niveau élevé. Par ailleurs, un facteur d'impact du domaine de sécurité du fournisseur de l'échange est également établi et dépend des intervalles de valeur de niveau d'assurance (voir 3.4.4).

Nous exprimons la réputation spécifique comme ci-dessous :

$$sr_{O_{pj}} = \begin{cases} sr^{c}_{O_{pj}} + \Delta_i \; si \; résultat \; positif \\ sr^{c}_{O_{pj}} + \Delta_i/2 \; si \; résultat \; positif \; avec \; violation \\ sr^{c}_{O_{pj}} - \Delta_i \; si \; résultat \; négatif \\ Avec \; \Delta_i = \gamma_i \delta_i \; et \; \delta(j) = \frac{(I_{lmin(i)} + I_{lmax(i)})/2}{I_{lmax}} \end{cases} \tag{3.4.18}$$

$I_{lmin(i)}$ la valeur minimale du niveau d'assurance du domaine de sécurité i du fournisseur O_{pj} , $I_{lmax(i)}$ la valeur maximale du niveau d'assurance de O_{pj}, I_{lmax} la valeur maximale de niveau d'assurance (cette valeur est de 10, voir 3.4.4) et γ_i est le poids attribué pour la fourniture d'une ressource de domaine de sécurité donné et est déduit à partir de la matrice de mise à jour ci-dessous en fonction de la valeur i du domaine de sécurité du fournisseur : $i = 1$ pour L_{sd}, $i = 2$ pour M_{sd}, $i = 3$ pour H_{sd}

$$\gamma_i = \begin{array}{c} \begin{matrix} L_{sd} & M_{sd} & H_{sd} \end{matrix} \\ \begin{bmatrix} 0.2 & 0.35 & 0.45 \end{bmatrix} \end{array}$$

FIGURE 3.14 : Matrice de mise à jour réputation spécifique

À titre d'exemple, pour un fournisseur O_{p1} de domaine de sécurité 1 et un demandeur O_{u3} de domaine de sécurité 3 : $i = 1$ et $\gamma_i = 0.2$

- **Mise à jour du niveau d'assurance**
  La mise à jour du niveau d'assurance d'une organisation correspondant à l'actualisation de sa capacité à fournir des ressources avec un niveau de sensibilité donné. i le domaine de sécurité du fournisseur tel que : $i = 1$ pour L_{sd}, $i = 2$ pour M_{sd}, $i = 3$ pour H_{sd} .

$$\gamma(i) = \begin{array}{c} \begin{matrix} L_{sd} & M_{sd} & H_{sd} \end{matrix} \\ \begin{bmatrix} 0.2 & 0.35 & 0.45 \end{bmatrix} \end{array}$$

FIGURE 3.15 : Matrice de mise à jour de niveau d'assurance

La valeur maximale du niveau d'assurance est 10 (voir 3.4.4). Il est donc important de s'assurer qu'elle ne croît pas indéfiniment. Ainsi, le niveau d'assurance $I_{lO_{pj}}$ de l'organisation O_{pj} peut être exprimé comme ci-dessous :

$$I_{lO_{pj}} = \begin{cases} I^c_{lO_{pj}} + \gamma_1(i) \; si \; résultat \; positif \; et \; I^c_{lO_{pj}} \leq 9.9 \\ I^c_{lO_{pj}} + \gamma_1(i)/2 \; si \; résultat \; positif \; avec \; violation \; et \; I^c_{lO_{pj}} \leq 9.9 \\ I^c_{lO_{pj}} + \gamma_2(i) \; si \; résultat \; positif \; et \; I^c_{lO_{pj}} > 9.9 \\ I^c_{lO_{pj}} + \gamma_2(i)/2 \; si \; résultat \; positif \; avec \; violation \; et \; I^c_{lO_{pj}} > 9.9 \\ Avec \; \gamma_1(i) = \gamma_(i) \; et \; \gamma_2(i) = (10 - I^c_{lO_{pj}}) \; \times \; \gamma_(i) \end{cases} \tag{3.4.19}$$

$$I_{lO_{pj}} = \begin{cases} I^c_{lO_{pj}} - \gamma(i) \; si \; résultat \; négatif \end{cases} \tag{3.4.20}$$

- **Mise à jour de la réputation globale**
  La réputation globale est fondée sur l'ensemble des résultats des interactions d'une organisation en tant que fournisseur au sein de la communauté. Ainsi la réputation globale est formulée ci-après :

$$gr_{O_{pj}} = \alpha + \rho \sum_{k=1}^{n} sr_{Opj}(k), \rho = \frac{ST_{O_{pj}}}{ST_C} \tag{3.4.21}$$

  avec α le taux de base (α=0.5), n le nombre de réputations spécifiques de l'organisation O_{pj}, $ST_{O_{pj}}$ le nombre total d'échanges pour un fournisseur de ressources donné, ST_C le nombre total de partages au sein de la communauté, et ρ le poids des échanges de l'organisation.

- **La promotion ou la relégation dans les domaines de sécurité**
  Après chaque opération de mise à jour, outre les valeurs de confiance, le niveau d'assurance de l'organisation fournisseur de la ressource est également actualisé. Cette valeur de niveau d'assurance va permettre la promotion ou la relégation dans un domaine de sécurité selon la définition 3.4.5 .

3.5 Gestion des accès et des contrats de collaboration

Les systèmes collaboratifs centrés sur la communauté présentent des spécificités particulières en plus de celle des systèmes collaboratifs classiques. En effet, ces systèmes sont définis par des relations transactionnelles, durables et évolutives. Ces relations représentent des connexions sociales contextuelles entre les entités. Par ailleurs, les systèmes axés sur la communauté sont hétérogènes et fondamentalement orientés sur les besoins et intérêts des membres de la communauté [164]. Il convient donc prendre en comptes ces caractéristiques dans les propositions de techniques de contrôle d'accès pour cette catégorie de système collaboratif. Ce modèle permettra la définition dynamique et autonome des politiques de contrôle d'accès aux ressources et de formaliser l'engagement mutuel de chaque entité dans les processus de collaboration. En conséquence, nous proposons le *Community-OrBAC*, un modèle de contrôle d'accès utilisant des agents autonomes. Notre modèle vise à fournir des moyens pour définir des politiques de sécurité fiables, dynamiques, tenant compte des paramètres contextuels décrits dans la figure 3.16 ci-dessous.

3.5.1 Contexte dans les systèmes collaboratifs centrés sur la communauté

Une collaboration entre des entités dépend de différents paramètres contextuels liés à ces entités ou aux ressources partagées. Il est essentiel de considérer ces conditions dans la définition des règles de politiques de sécurité des entités engagées. Nous étendons le contexte dans *OrBAC* décrit dans [63] avec deux nouveaux concepts : le contexte de sécurité et le contexte social comme représenté dans la figure 3.16.

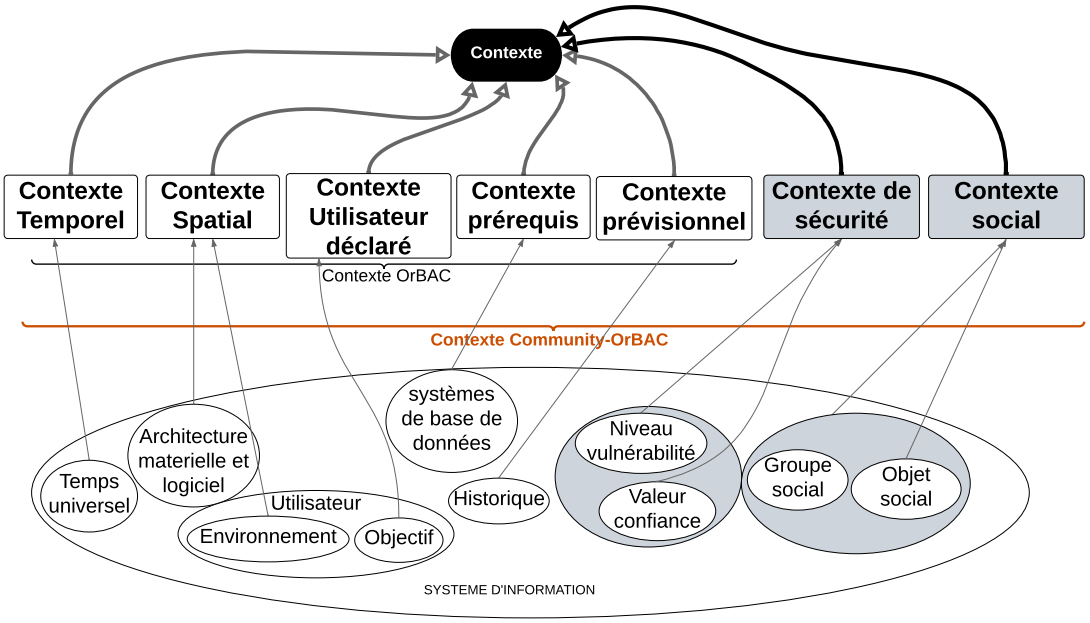


FIGURE 3.16 : Paramètres contextuels Community-OrBAC

3.5.1.1 Le contexte de sécurité

Le contexte de sécurité est un ensemble d'informations contextuelles permettant de caractériser le niveau de sécurité d'une entité (utilisateurs, ressources) et adapter son comportement en fonction de celui-ci. Ces informations contextuelles peuvent être de divers types, notamment les valeurs de niveau de sécurité, la robustesse des protocoles et des mécanismes de sécurité[118].

- **Principe** : le contexte de sécurité permet de spécifier qu'une action donnée d'un sujet sur un objet n'est autorisée qu'en fonction du niveau de sécurité de cet objet et de la confiance accordée à ce sujet. À titre d'exemple, dans une communauté d'organisations, une organisation peut être autorisée à utiliser une ressource de niveau de vulnérabilité bas si cette dernière présente un niveau de confiance élevé. Les exigences sont représentées par le niveau de vulnérabilité de la ressource et la valeur de confiance accordée à l'organisation. Ainsi, la validation d'un accès requiert l'identification des niveaux de vulnérabilité des ressources et l'évaluation de la confiance entre les organisations engagées dans les interactions. À chaque niveau de vulnérabilité sera associé un seuil de valeur de confiance. Dans [63] le contexte de sécurité a été introduit dans les contextes spatiaux logiques à travers des prédicats de modélisation de la sécurité des applications préconisés dans [214]. Ils ont souligné par ailleurs la nécessité de travaux supplémentaires afin de définir un ensemble de contextes qui spécifie un niveau de confiance nécessaire à l'exécution d'une action.

  Nous désignons le contexte de sécurité par $Contexte\_sécurité$ et ses deux compo-

santes : $Niveau\_vulnérabilité$ et $Valeur\_confiance$. Les conditions requises pour un contexte donné sont exprimées formellement par des règles logiques et une algèbre de contexte dans des cas de contextes composites [63]. Le contexte de sécurité est formulé dans le tableau 3.5 ci-dessous :

TABLE 3.5 : Règle de contexte de sécurité

$org \in Organisations, s \in Sujets, \alpha \in Actions, o \in Objets,$ *Définit*$(org, s, \alpha, o,$ *Niveau_vulnérabilité* $\&$*Valeur_confiance*$)$ $\rightarrow$ *Définit*$(org, s, \alpha, o,$ *Contexte_sécurité*$)$

Cette formalisation traduit que dans l'organisation org, un sujet s est autorisé à effectuer une action α sur un objet o donné si $Contexte\_sécurité$ composé de $Niveau\_vulnérabilité$ de l'objet et $Valeur\_confiance$ du sujet est vrai.

- **Exemple de permission utilisant le contexte de sécurité** :

  À titre d'illustration, considérons un laboratoire médical $Lab1$ au sein duquel, le Directeur est autorisé à consulter la base de données d'essais cliniques $cov.db$. Cette action n'est possible que dans un contexte de sécurité où le niveau de vulnérabilité des informations consultées est nv_2 et la valeur de confiance du Directeur est vc_4. Ce privilège est exprimé comme ci-dessous :

  - $Permission(Lab1, Directeur, consulter, cov.db, Contexte\_sécurité)$

  où le contexte de sécurité $Contexte\_sécurité$ est formulé dans le tableau 3.6 :

TABLE 3.6 : Règle de contexte de sécurité laboratoire médical

$s \in Sujets, \alpha \in Actions, o \in Objets, consulter \in Activités$ $Habilite(Lab1, s, Directeur) \wedge$ Utilise (Lab1, o, cov.db) $\wedge$ Considère(Lab1, $\alpha, consulter) \wedge$ Niveau_vulnérabilité(o, nv_2) $\wedge$ $Valeur\_confiance(s, vc_4)$ $\rightarrow Définit(Lab1, s, \alpha, o, Contexte\_sécurité)$

Cette règle signifie que dans l'organisation $Lab1$ le sujet s effectue une action α sur objet o dans le contexte $Contexte\_sécurité$ si le sujet s est habilité dans le rôle $Directeur$, l'objet o est utilisé dans une vue $cov.db$, le niveau de vulnérabilité de l'objet est nv_2 ($Niveau\_vulnrabilit(o, nv_2)$) et la valeur de confiance du sujet s est vc_4 ($Valeur\_confiance(s, vc_4)$).

3.5.1.2 Le contexte social

Dans « Communauté », Encyclopédie de la philosophie (2002) de Vattimo, la communauté est définie comme « un ensemble de sujets liés par un ou plusieurs facteurs de différente nature qui les amènent à avoir plus de relations entre eux ». Par ailleurs, selon le dictionnaire Le Robert (1980) une communauté est « un groupe social caractérisé par le fait de vivre ensemble, de posséder des biens communs, d'avoir des intérêts, un but commun ». Il ressort de ces deux définitions de la communauté, un engagement mutuel de chaque entité dans l'atteinte des objectifs, la protection des intérêts et les liens sociaux qui peuvent exister entre les membres. Une communauté requiert donc la mise en place de stratégies et d'actions communes au profit de ses membres. Par conséquent, nous décrivons le contexte social comme l'intérêt d'une action, d'un sujet ou d'une res-

source pour la communauté. Cette perception permet de scinder la communauté en différents groupes sociaux comme dans [118].

- **Principe** : le contexte social permet d'exprimer une règle qui accorde un privilège pour une action d'un sujet sur un objet en fonction de la portée communautaire de l'objet et du centre d'intérêt du groupe social auquel appartient le sujet. Nous exprimons le contexte social $Contexte\_social$ au travers de deux attributs : $Objet\_social$ et $Groupe\_social$. Le tableau 3.7 présente la définition d'une règle de contexte social.

TABLE 3.7 : Règle de contexte social

$org \in Organisations, s \in Sujets, \alpha \in Actions, o \in Objets,$ *Définit* (org, s, α, o, *Objet_social* &*Group_social*) $\rightarrow$ *Définit*($org, s, \alpha, o,$ *Contexte_social*)

Elle signifie que dans l'organisation org, un sujet s peut exécuter une action α sur un objet o donné si le contexte social $Contexte\_social$ est vrai. Le contexte social est constitué de la portée sociale de l'objet $Objet\_social$ et du centre d'intérêt du groupe social du sujet $Group\_social$.

- **Exemple de permission utilisant le contexte social** :

  À titre d'illustration, considérons la startup λ repartie en différents groupes sociaux. Un utilisateur u appartenant au groupe social gs est autorisée à consulter la plateforme intranet app ayant pour portée sociale os. Cette permission est exprimée comme ci :

  - $Permission(\lambda, u, consulter, app, Contexte\_social)$

  Le tableau 3.8 décrit la règle de contexte social.

TABLE 3.8 : Règle de contexte social Startup λ

Habilite(λ, s, u) $\wedge$ *Utilise*($\lambda, o,$ *app*)$\wedge$ *Considère*($\lambda, \alpha, consulter$) $\wedge$ *Objet_social*(o, os) $\wedge$ *Groupe_social*(s, gs) $\rightarrow$ *Définit*($\lambda, s, \alpha, o, Contexte\_social$)

Cette expression explique que dans l'organisation λ le sujet s effectue une action α sur l'objet o dans le contexte $Contexte\_social$ si le sujet s est habilité dans le rôle u, l'objet o est utilisé dans une vue app, l'objet social de la ressource est os représenté par ($Objet\_social(o, os)$) et le centre d'intérêt du groupe social du sujet s est gs ($Groupe\_social(s, gs)$).

3.5.2 Fonctionnement Community-OrBAC

La collaboration entre les membres de la communauté doit garantir leur autonomie et un accès régulé aux ressources partagées. Des techniques d'interactions et des mécanismes de contrôle d'accès aux ressources doivent être déployés. Les entités engagées dans une collaboration sont autonomes, cependant coopérer revient à renoncer à une partie de son autonomie [216]. Cette situation peut être source de conflits et des problèmes de coopération. Nous apportons une réponse à cette problématique d'autonomie des organisations grâce aux systèmes multi-agents. En effet, les agents autonomes sont capables de s'engager dans divers types d'interactions sociales et de coopération avec d'autres agents. Le modèle de résolution de problèmes de coopération proposé dans [216] par M. Wooldridge constitue le fondement des phases du processus de collaboration entre les entités de notre système. Ces différentes étapes sont : l'expression

du besoin, l'engagement collectif, la négociation d'un contrat intelligent de coopération et l'action collective. Les entités ou sujets intervenants dans une collaboration sont représentés par des agents.

3.5.2.1 L'expression du besoin

L'atteinte d'un objectif est conditionnée par l'identification des différentes actions à mener. Une entité s'engage dans une collaboration si elle reconnait le besoin de collaboration et croit en l'existence d'une entité ou groupe d'entités pouvant lui permettre d'atteindre son but [216]. Par conséquent, le processus de collaboration démarre avec l'expression explicite du besoin par l'agent demandeur de la ressource. Toutefois, une demande ne sera acceptée que si la ressource sollicitée est disponible à la période désirée et son accès est autorisé par la politique de sécurité de l'entité propriétaire. Nous pouvons alors introduire une nouvelle relation $Disponible$ entre les entités $organisation$ et $objet$ dans un contexte temporel. Cette relation sera associée aux relations $Demande(org, s, \alpha, o)$ et $Est\_Accepté(s, \alpha, o)$ exposées dans [63]. L'expression explicite d'un besoin présente plusieurs avantages. Elle constitue un moyen de suivi du respect des engagements et de gestion des conflits. Le tableau 3.9 ci-dessous présente la formalisation d'une règle d'acceptation d'une action d'un sujet sur un objet.

TABLE 3.9 : Règle d'acceptation d'une action sur un objet

$org \in Organisations, s \in Sujets, \alpha \in Actions, o \in Objets, contexte\_temporel \in Contextes,$ *Demande*(org, s, α, o)$\wedge$ *Disponible*(org, o, contexte_temporel) $\wedge$ *Est_Permis*(s, α, o) $\rightarrow$ *Est_Accepté*(s, α, o)

3.5.2.2 L'engagement collectif

Après l'expression du besoin, l'étape suivante consiste à trouver une entité partenaire pour la collaboration. Dans une communauté composée de plusieurs sujets, il existe diverses entités capables d'aider à la réalisation de l'objectif visé. Ce processus commence par l'identification des sujets potentiels pour une collaboration donnée, ensuite l'évaluation de la confiance des entités et enfin la sélection du partenaire idéal.

- **L'identification des potentiels partenaires** : les membres de la communauté exposent dans le registre des objets de la communauté les ressources dont ils disposent. Les objets sont déclarés sur la base de règles de contrôle d'accès établis dans les politiques locales de chaque entité. La prise en compte des contextes social et de sécurité est obligatoire dans le choix du partenaire. Ainsi, une matrice de gouvernance des objets doit définir les exigences de ces contextes. Cette matrice met en exergue le niveau de confiance requis pour un niveau de vulnérabilité d'un objet donné d'une part et d'autre part, le groupe social du sujet exigé pour une ressource de portée sociale donnée. Outre le contexte social et le contexte de sécurité, le contexte peut être étendu à d'autres aspects (spatial, temporel, etc.) tels que définis dans [65].
- **L'évaluation de la confiance et la sélection du fournisseur** : la confiance entre les entités est un élément clé favorisant le partage et la collaboration. Cette confiance sera déterminée à partir d'un modèle d'évaluation de la confiance. Ce modèle exposé à la section 3.4 permet de déterminer la valeur de confiance des potentiels partenaires et d'en sélectionner un sur la base de l'algorithme de sélection intégré

à ce modèle. La sélection d'une entité ayant exposé volontairement sa capacité à collaborer en vue de contribuer à satisfaire un besoin explicitement exprimé par une entité paire constitue l'engagement collectif des deux sujets [216].

3.5.2.3 Négociation et création d'un contrat dynamique de collaboration

Lors de cette étape, les agents engagés doivent être d'accord sur les différentes actions à mener dans le but d'atteindre l'objectif de la collaboration. En effet, l'exigence d'autonomie des organisations et l'éventualité de conflits dans les actions nécessitent de parvenir à un accord entre les entités sur la conduite à tenir [216]. Une négociation pourra permettre d'aboutir à cet accord. La négociation se traduit généralement par des propositions, des contre-propositions et des suggestions pour aboutir à un consensus sur le résultat final. Les actions à effectuer et le cadre de suivi de cette collaboration seront consolidés dans un contrat dynamique et intelligent. Ce processus de négociation est crucial et peut s'avérer complexe. D'où l'utilisation des agents intelligents, autonomes, capables de rendre dynamique la définition, le suivi des politiques et d'éviter ou réduire l'intervention humaine [216]. La mise en place du contrat sera effectuée par des agents représentant les organisations et chargés de négocier, de définir et d'actualiser éventuellement les termes de cet accord. Ainsi, un contrat électronique se définit comme un accord formel entre les entités concernées dans une collaboration. Les clauses du contrat sont automatiquement spécifiées et appliquées sur la base des règles de la politique de sécurité [153]. Plusieurs travaux ont mis en exergue la négociation, la définition et la gestion de contrat électronique dans les collaborations entre entités d'organisations distribuées [184][153].

Nous proposons une approche fondée sur le *Web Services Agreement* (*WS-Agreement*) [105], un standard de spécification des accords de niveaux de service intégrant un protocole de négociation et de renégociation de contrat. Cette technique s'appuie sur un langage : WS-Agreement Specification et un protocole de négociation (WS-Agreement Negotiation Protocol) [153]. WS-Agreement Specification permet d'exprimer les interactions entre les entités sur la base du langage XML. Le contrat est matérialisé grâce à un fichier XML dont la structure est composée des sections suivantes : le nom, le contexte et les termes de l'offre [27]. Le protocole de négociation WS-Agreement Negotiation Protocol comporte trois couches : la couche de négociation, la couche d'accord et la couche de service. La couche de négociation expose les dispositions et un langage pour négocier des offres, créer des contrats à partir des offres négociées. La couche accord est consacrée à la création et à la surveillance des contrats. La couche service permet de mettre à disposition le service définit dans un accord. Ce protocole est ainsi adapté à différents types d'environnements, dont les infrastructures utilisant les systèmes multi-agents [153][27]. Par ailleurs, le *WS-Agreement* a été associé à des règles de sécurité *OrBAC* afin de permettre à des utilisateurs et des fournisseurs de services cloud de négocier, créer et surveiller des accords de niveau de service (*SLA*) dans [138].

Pour illustrer le fonctionnement de ce protocole, considérons un agent $orgA$ demandeur d'une ressource et un agent $orgB$ fournisseur. La négociation commence par l'envoi d'une requête de demande d'une ressource exposée par l'agent $orgB$ dans le registre des objets. À la réception de la requête, $orgB$ répond en transmettant la structure de base d'un contrat *WS-Agreement*. Sur la base de ce modèle et de ses besoins, $orgA$ construit une offre puis l'envoie à $orgB$. Cette offre peut être validée directement ou faire l'objet d'une contre-proposition en cas de non-conformité avec les contraintes prédéfinies par $orgB$. Cette opération est répétée jusqu'à ce qu'un accord soit trouvé ou non. Une fois l'offre validée, l'agent $orgB$ crée un contrat qu'il signe et le soumet à $orgA$. Ce dernier à son tour marque son approbation en signant l'accord et le partage

avec l'agent $orgB$. Ce scénario de négociation est présenté à la figure 3.17.

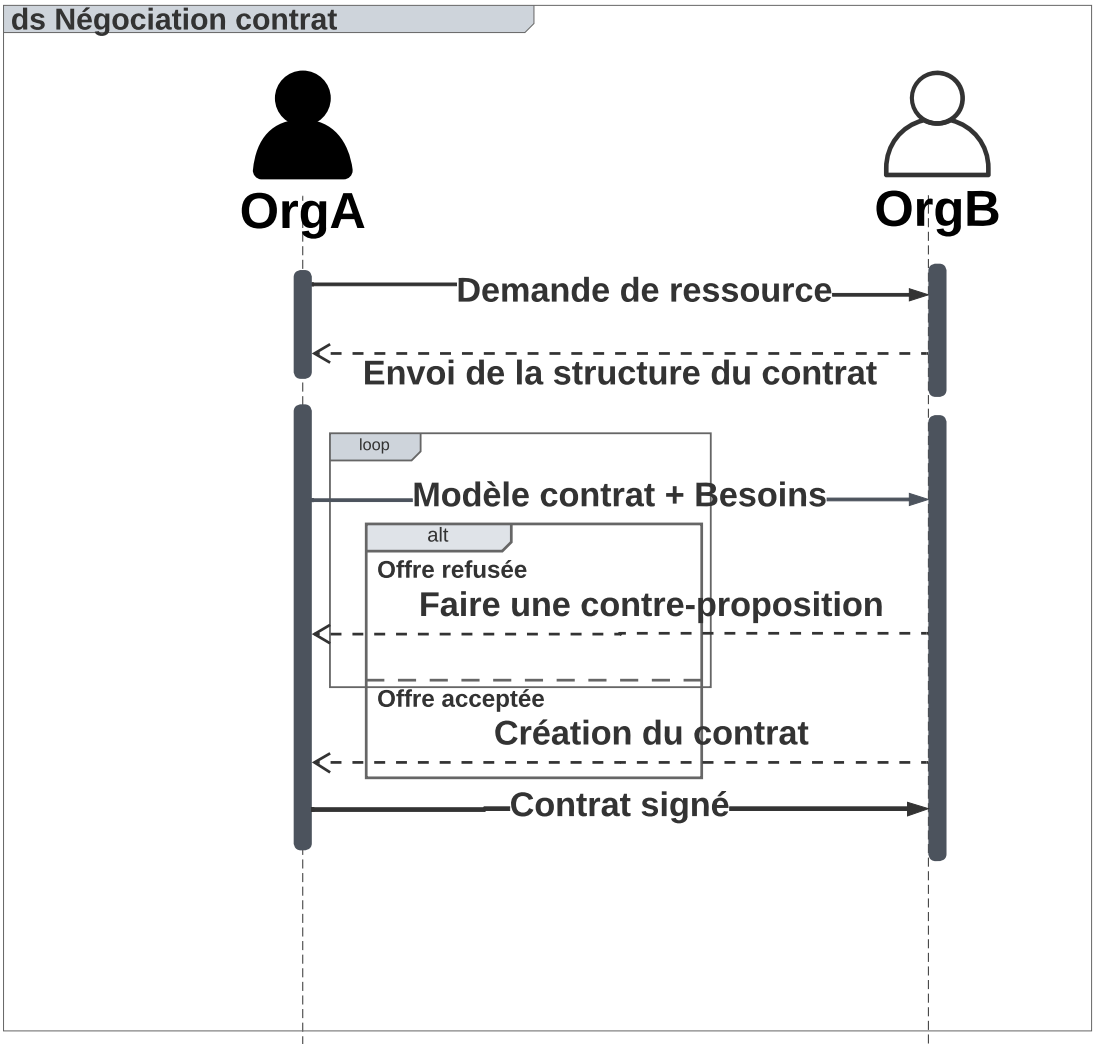


FIGURE 3.17 : Négociation de contrat de coopération entre deux organisations

3.5.2.4 L'action collective

Les négociations effectuées, les entités ont donc un accord sur l'action collective à réaliser et un contrat pour suivre le processus en vue de l'atteinte de l'objectif. En partant du scenario présenté lors de la phase de négociation, le but de l'action collective est de permettre à un utilisateur u_A de l'organisation $orgA$ d'accéder à une ressource Res_B de l'organisation $orgB$. Afin de préserver l'autonomie des entités dans la définition des règles de sécurité, l'approche adoptée est la procédure d'invocation et de partage de services présentée dans [71] en introduisant les notions d'objet agent virtuel (VOA) et de sujet agent virtuel(VUA). Ces éléments représentent respectivement l'objet distant invoqué et le sujet dans l'organisation fournisseur de l'objet.

De ce fait, un objet VOA_Res_B est créé dans la politique locale de $orgA$ et lié à une action $invoquer$. Une permission autorisant le rôle associé au sujet u_A d'exécuter l'activité correspondant à l'action $invoquer$ sur la vue représentant l'objet VOA_Res_B est également définie dans la politique locale de $orgA$. Cette règle est exprimée dans le tableau 3.10 ci-dessous.

TABLE 3.10 : Permission au niveau de l'organisation demandeur

$orgA \in Organisations, u_A \in Sujets, invoquer \in Actions, VOA\_Res_B \in$ $Objets, consulter \in Activités, c \in Contexte,$ *Permission*$(orgA, r, consulter, vue\_VOA\_Res_B, c) \wedge$ *Habilite* (orgA, $u_A, r) \wedge$ *Utilise* (orgA, VOA_Res$_B, vue_VOA_Res_B) \wedge$ *Considère* (orgA, invoquer, consulter) $\wedge$ *Définit* (orgA, $u_A, invoquer, VOA\_Res_B, c)$ $\rightarrow$ *Est_Permis*$(u_A, invoquer, VOA\_Res_B)$

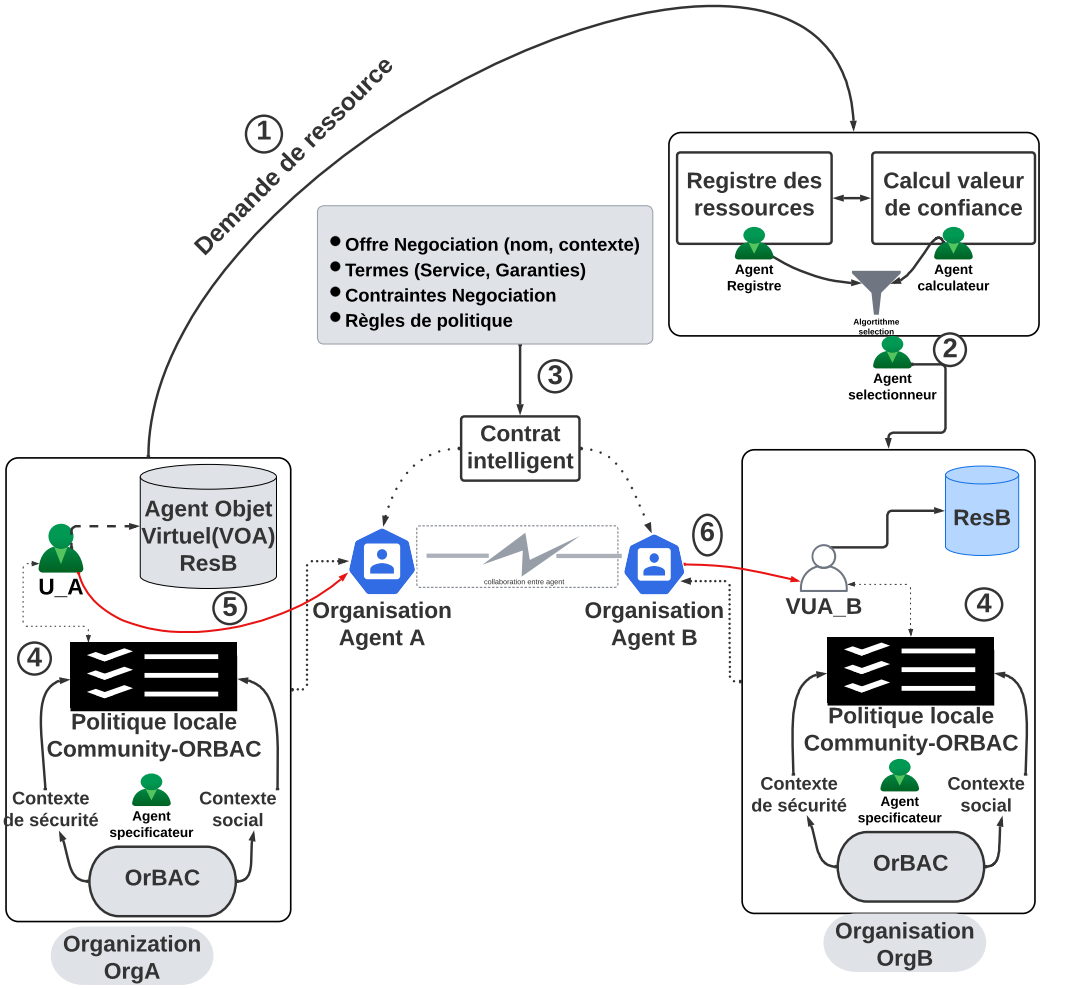
Par ailleurs, dans la politique locale de $OrgB$, un utilisateur virtuel vua_B est créé et associé à un rôle disposant d'une permission permettant d'exécuter une activité sur la vue de l'objet Res_B. L'action $invoquer$ va déclencher une communication entre l'agent associé à l'objet virtuel de $OrgA$ et celui de l'organisation $OrgB$. Cette communication se fait conformément aux dispositions du contrat établi entre les deux entités. À la réception du message de l'agent de l'organisation $OrgA$ suite à l'invocation, les actions liées au sujet vua_B sur l'objet Res_B seront exécutées comme illustré dans la figure 3.18 ci-dessous.

Le tableau 3.11 ci-dessous présente la règle dans la politique locale de $OrgB$.

TABLE 3.11 : Permission au niveau de l'organisation fournisseur

$orgB \in Organisations, vua_B \in Sujets, exécuter \in Actions, Res_B \in$ $Objets, Afficher \in Activités, c \in Contexte,$ *Permission*$(orgB, r, Afficher, vue\_Res_B, c) \wedge$ *Habilite* (orgB, vua$_B, r) \wedge$ *Utilise* (orgB, Res$_B, vue_Res_B) \wedge$ *Considère* (orgB, excuter, Afficher) $\wedge$ *Définit*(orgB, vua$_B, exécuter, Res_B, c)$ $\rightarrow$ *Est_Permis*$(vua_B, exécuter, Res_B)$

Notons que toute action de toute entité de la collaboration est conditionnée par une authentification. Ce processus d'authentification a été exposé dans la section 3.3 relative à notre modèle de gestion des identités.



① **Demande de ressource.**

② **Sélection des ressources sur la base des ressources exposées et du système d'évaluation de la confiance.**

③ **Negociation et création d'un contrat intelligent de collaboration.**

④ **Définition de règles de politique de sécurité locales pour chaque organisation.**

⑤ **Invocation de l'objet et initialisation de la communication entre l'organisation de l'agent.**

⑥ **Réception de la demande d'invocation et validation de la permission.**

FIGURE 3.18 : Architecture Community-OrBAC

3.6 Conclusion

Dans ce chapitre, nous avons présenté les fondements de notre stratégie de sécurité Zero Trust dans un cloud communautaire. Le modèle a été conçu pour répondre à la complexité, à l'hétérogénéité, à la nécessité de sécuriser et aux caractéristiques particulières de ce type de système centré sur la communauté. Nous avons d'abord abordé le fonctionnement de la stratégie et de l'architecture générale associée, ainsi qu'une description des principaux composants. Par la suite, nous avons présenté dans des sections spécifiques et de façon détaillée chaque mécanisme de sécurité intervenant dans notre démarche Zero Trust.

Le premier mécanisme décrit concerne la gestion des identités. Nous avons ainsi présenté une vue d'ensemble de notre système de gestion décentralisée des identités établi à partir des identifiants décentralisés, la technologie blockchain et les techniques associées telles que les contrats intelligents et les Oracles. Cette gestion des identités a pour but principal d'enregistrer les organisations dans la communauté de manière sécurisée et consensuelle grâce à un système d'agrégation des signatures numériques d'accord d'adhésion et un stockage des identités dans un registre distribué. Par ailleurs, le modèle intègre un algorithme exécuté par un contrat intelligent pour l'authentification des utilisateurs et des organisations.

La deuxième section a porté sur l'évaluation de la confiance des organisations au sein de la communauté. Ainsi, après l'identification et l'enregistrement des organisations dans la communauté grâce au système proposé dans la section précédente, nous évaluons la confiance de ces dernières lors des processus de partage de ressources. Notre approche consiste à diviser le cloud communautaire en trois domaines de sécurité logique (bas, intermédiaire, avancé) où chaque domaine de sécurité regroupe des organisations ayant la capacité de fournir des ressources d'un niveau de sécurité bien précis. Des valeurs de confiance sont ensuite calculées sur la base des interactions directes ou recommandés et la réputation d'organisation désirant collaborer. Puis ces valeurs sont utilisées dans un algorithme de sélection afin de déterminer le fournisseur idéal pour un échange. Des indicateurs de performances et un mécanisme de relégation/promotion permettent également d'actualiser les valeurs de confiance et de garantir son caractère dynamique et évolutif.

La dernière partie de ce chapitre a été consacrée à la gestion des accès et des contrats de collaboration. Nous avons proposé un modèle de contrôle d'accès considérant le contexte social et le contexte de sécurité dans la définition des règles de politique de sécurité. Outre ces paramètres contextuels importants pour les environnements de collaboration axés sur la communauté, notre modèle utilise les systèmes multi-agents afin d'apporter de la dynamique et de l'autonomie à la spécification des règles. Par ailleurs, le modèle intègre un protocole de négociation permettant aux organisations d'établir et de suivre des engagements de collaboration.

En définitive, nous avons présenté trois mécanismes liés et complémentaires qui permettent d'apporter un contrôle de sécurité permanent durant tout le processus de collaboration comme suggérer par les principes de base de la stratégie Zero Trust. Ces mécanismes permettent ainsi d'assurer l'identification, l'authentification, le choix du partenaire de collaboration et le suivi des accords préétablis. Le chapitre suivant porte sur les expérimentations des mécanismes proposés et la démonstration de l'efficacité de notre stratégie.

Chapitre 4

Implémentation et Simulations

«Que la stratégie soit belle est un fait, mais n'oubliez pas de regarder le résultat.»

Winston CHURCHILL

Sommaire

4.1 Introduction

Dans le chapitre précédent, nous avons présenté l'architecture globale de notre stratégie ainsi qu'une description des différents mécanismes de sécurité retenus pour la mise en place de notre stratégie. Nous souhaitons à présent valider l'utilisation de ces mesures, leur efficacité et leur fiabilité dans un cadre de sécurisation d'un cloud communautaire. Afin d'atteindre cet objectif, nous allons d'abord décrire les enjeux de la collaboration entre des organisations dans un cloud communautaire et un scénario mettant en évidence l'application de notre stratégie dans cette infrastructure. Nous examinerons ensuite les trois mécanismes (gestion de l'identité, confiance et contrôle d'accès) impliqués dans notre stratégie à travers les outils utilisés pour leur mise en œuvre ainsi que les tests et les résultats des expérimentations de chaque mécanisme. Enfin, nous concluons par une discussion sur les résultats obtenus dans l'application de notre stratégie Zero Trust.

4.2 Cadre expérimental

4.2.1 Capacités du cloud communautaire

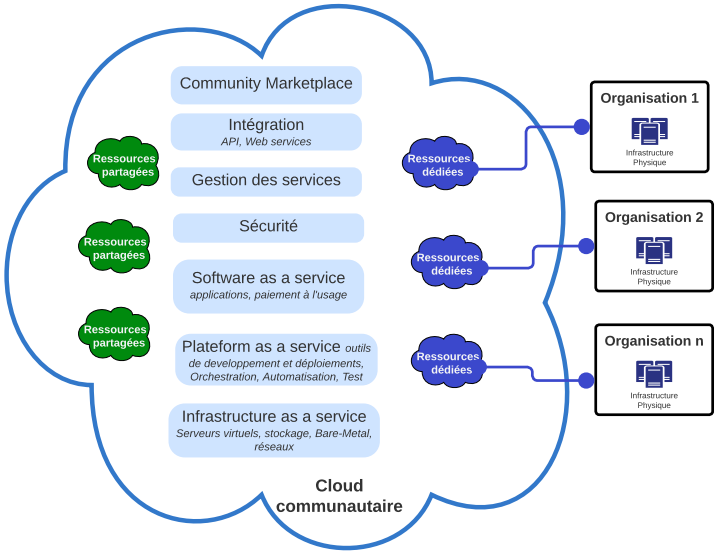


FIGURE 4.1 : Capacité cloud communautaire d'expérimentation

Comme il est décrit dans la section 1.3.3, un cloud communautaire est principalement axé sur la collaboration entre des organisations autonomes. En fonction des objectifs visés et des motivations de sa mise en place, le cloud communautaire propose plusieurs modèles d'engagement, qui conditionne ses capacités et les services qu'il offre [144]. Ainsi, dans notre scénario, nous nous appuyons sur un modèle proposant les différents services cloud (IaaS, PaaS, SaaS). Les membres de la communauté peuvent ainsi échanger plusieurs solutions, données et diverses formes de collaboration. La figure 4.1 montre les capacités offertes par notre cloud communautaire.

4.2.2 Architecture Zero Trust dans un Cloud Communautaire

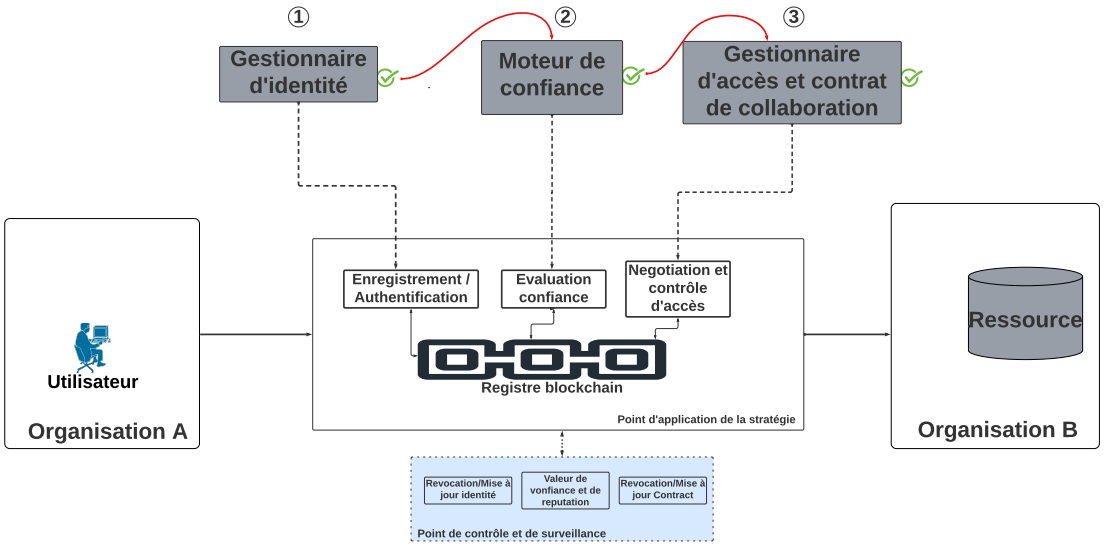


FIGURE 4.2 : Architecture stratégie Zero Trust du cloud communautaire

L'architecture proposée dans la figure 4.2 est établie à partir de notre modèle Zero Trust dans un contexte de collaboration décrit dans le chapitre précédent. Elle représente les différentes phases et les fonctions associées de notre démarche permettant à un utilisateur d'une organisation donnée d'accéder à une ressource d'une organisation paire. La première étape porte sur les mesures d'identification et d'authentification des organisations, des utilisateurs et des ressources. La deuxième phase consiste à évaluer la confiance entre les organisations à travers une fonction d'inférence de valeur de confiance suite à une demande de ressources. L'étape 3 permet d'établir un contrat de collaboration et de définir les règles d'accès aux ressources grâce à un système de gestion et de contrôle d'accès. Enfin, la dernière phase consiste à surveiller le partage, le respect des termes de collaboration et tenir à jour les différents registres de données de sécurité. Les sections suivantes décrivent la mise en œuvre de ces phases et les différentes technologies associées.

4.3 Identification, Enregistrement, Authentification

4.3.1 Objectifs

Dans le but de mettre en œuvre notre système de gestion des identités, nous nous intéressons à l'identification, à l'enregistrement et à l'authentification des organisations et des utilisateurs au sein de la communauté. Il sera question de montrer comment connecter les entités entre elles, répondre à des requêtes, envoyer des messages, gérer l'émission, le stockage sécurisé des informations d'identification et leur vérification dans le cadre d'accès à une ressource. L'atteinte de ces objectifs passe par le choix du registre de stockage décentralisé, la mise en place du cadre de coordination des interactions entre les entités et la conception des contrôleurs exécutant la logique métier qui définit une fonctionnalité spécifique du système. Par ailleurs, différents tests pour évaluer l'efficacité ainsi que les performances du système seront menés.

4.3.2 Scénario

Le scénario d'implémentation présenté dans la figure 4.3 fait intervenir trois entités. Il s'agit de deux organisations (A et B) et un utilisateur appartenant à l'organisation A souhaitant accéder à une ressource sécurisée de l'organisation B. Pour accéder à cette ressource de l'organisation B, l'utilisateur doit disposer d'un certificat d'identification vérifiable émis par l'organisation A et qu'il présentera à l'organisation B afin d'accéder à la ressource.

La démonstration part du principe que vous obtenez d'abord un justificatif d'identité vérifiable auprès d'une autorité appropriée, ensuite, vous utilisez ce justificatif d'identité pour accéder à une ressource protégée. Dans ce cas, une autorité suffisante est un service qui vous permet de prouver que vous contrôlez votre adresse électronique, tandis que le service protégé est un faux site web du gouvernement de la Colombie-Britannique.

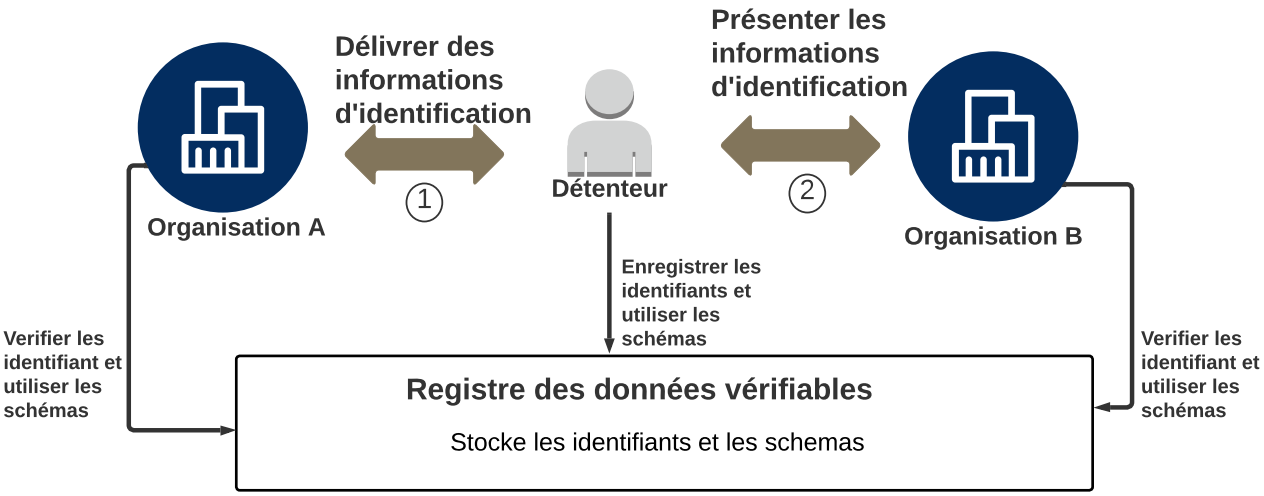


FIGURE 4.3 : Scénario d'enregistrement et d'authentification d'identité

4.3.3 Environnement d'expérimentation

Le système de gestion des identités a été mis en place à partir d'un ensemble de solutions de la plateforme open-source $Hyperledger$, qui propose différents outils et technologies de blockchain. Les projets utilisés dans notre approche sont présentés dans la figure 4.4 et décrits ci-dessous.

- **Hyperledger Indy** :

  Premier projet de la fondation $Hyperledger$ centré sur l'identité, $Hyperledger\ Indy$ est un registre distribué qui fournit des outils, des librairies réutilisables. Ces composants permettent la création, la publication et la gestion des identifiants décentralisés sans autorité centrale, ainsi que des informations d'identification vérifiables dans un format interopérable. Conçu initialement dans un esprit de package de gestion complète des identités souveraines, $Hyperledger\ Indy$ a par la suite été à l'origine d'autres solutions permettant ainsi une gestion plus souple des identités décentralisées. L'un des projets issus de $Indy$ est $Hyperledger\ Ursa$.
- **Hyperledger Ursa** : dérivé de la fonction « indy-crypto » du projet $Indy$, il a été proposé afin de rendre les fonctionnalités cryptographiques de ce projet réutilisable dans d'autres initiatives et apporter des améliorations grâce au soutien

d'une large communauté et d'experts de la cryptographie. $Hyperledger\ Ursa$ est une bibliothèque cryptographique partagée, intégrant différents protocoles cryptographiques (signatures BLS, ED25519, etc.) pour améliorer la sécurité, éviter la duplication et les problèmes d'implémentation des fonctions cryptographiques dans les projets. Ainsi, $Ursa$ propose des fonctionnalités facilement utilisables par $Hyperledger\ Indy$, $Aries$ et toute autre application nécessitant une fonction cryptographique efficace, solide et vérifiée.

- **Hyperledger Aries** : les agents utilisés dans $Hyperledger\ Indy$ ne pouvant communiquer qu'entre eux, le projet $Aries$ [82] a été proposé afin d'assurer l'interopérabilité entre des agents de différents projets. Ainsi, il est le module « agent » des projets $Hyperledger$ axés sur les identités décentralisées. $Hyperledger\ Aries$ fournit des outils partagés, réutilisables, et interopérables qui permettent la création, la transmission, le stockage et la vérification d'identifiants numériques à travers des interactions pair à pair sur la blockchain. Pour cela, il intègre un ensemble de spécifications ($DIDComm$) pour permettre une communication sécurisée entre les agents. Les agents $Aries$ sont des composants logiciels qui représentent des entités telles que des personnes, des organisations et des objets. $Hyperledger\ Aries$ garantit la compatibilité récente et future des projets Hyperledger avec les autres solutions du monde des identités souveraines. Différents frameworks permettent de déployer $Hyperledger\ Aries$ tels que *Aries cloud Agent-Python (ACA-Py), Aries Framework.NET, Aries VCX (for Verifiable Credential eXchange), Aries Framework JavaScript (AFJ), Aries Framework Go (AF-Go)*. Nous utilisons dans nos travaux ACA-Py.

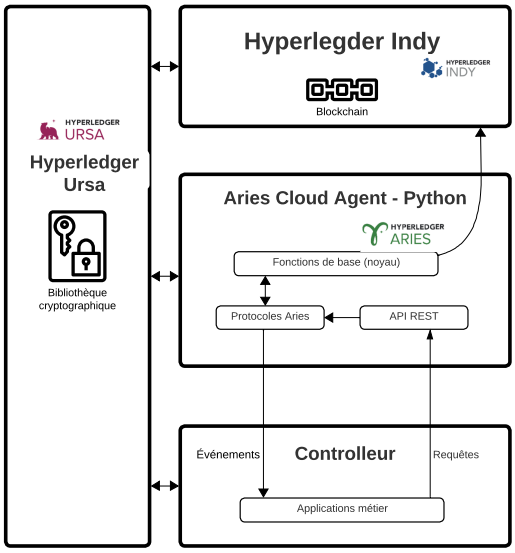


FIGURE 4.4 : Outils d'expérimentations du modèle de gestion d'identité

Ces projets proposent un écosystème composé d'agents $Aries$ représentant les entités (organisations et utilisateurs) échangeant des justificatifs d'identité vérifiables qui sont émis, détenus, prouvés et vérifiés. Ainsi, ces agents se connectent à un registre blockchain de type $Hyperledger\ Indy$ pour lire et écrire les informations nécessaires au partage des références et des présentations vérifiables. Pour nos expérimentations, nous simulons un registre $Hyperledger\ Indy$ local fondé sur un réseau *VON-Network* (Verifiable Organizations Network) [59], qui est un registre distribué proposé par le gouvernement de la Colombie-Britannique (BC). Il permet ainsi de faire fonctionner grâce à des conteneurs Docker, à des fins de test et de développement, un registre blo-

ckchain Indy à quatre nœuds avec différentes fonctionnalités (interface web pour visualiser les transactions, un formulaire Web pour l'enregistrement de DiD, l'accès au fichier *genesis* grâce à une API). Le fichier *genesis* contient les informations nécessaires (adresses IP et ports, protocoles cryptographiques) pour la connexion d'un agent au registre. Par ailleurs, la coordination des interactions entre les agents et le stockage des identifiants dans le registre blockchain est assuré grâce au framework *Aries Cloud Agent-Python (ACA-Py)*. ACA-Py fournit une interface *OpenAPI/Swagger* permettant de tester le fonctionnement des API lors du développement des contrôleurs.

Les différents composants de notre système sont installés sur un serveur avec *processeur x86 (Intel/AMD), 4VCPU, 16 Go RAM, 160 Go de stockage et un système d'exploitation Ubuntu 20.0*. Le langage de programmation des contrôleurs est *Python* et l'environnement de développement est *Pycharm*.

4.3.4 Expérimentations

4.3.4.1 Déploiement du réseau VON-Network

Le déploiement du VON-Network consiste à cloner le repository du VON-Network sur *GitHub* et ensuite construire le réseau grâce à des images *Docker*. Enfin, lancer le réseau *Indy* qui sera accessible à l'adresse à partir d'un serveur Web à l'adresse : *@IP-serveur :9000*. Cette interface (voir figure 4.5 permet de consulter le fichier *genesis* du réseau, créer un DiD, parcourir les trois registres du réseau *Indy* (domaine, pool, configuration) et consulter les différentes transactions.

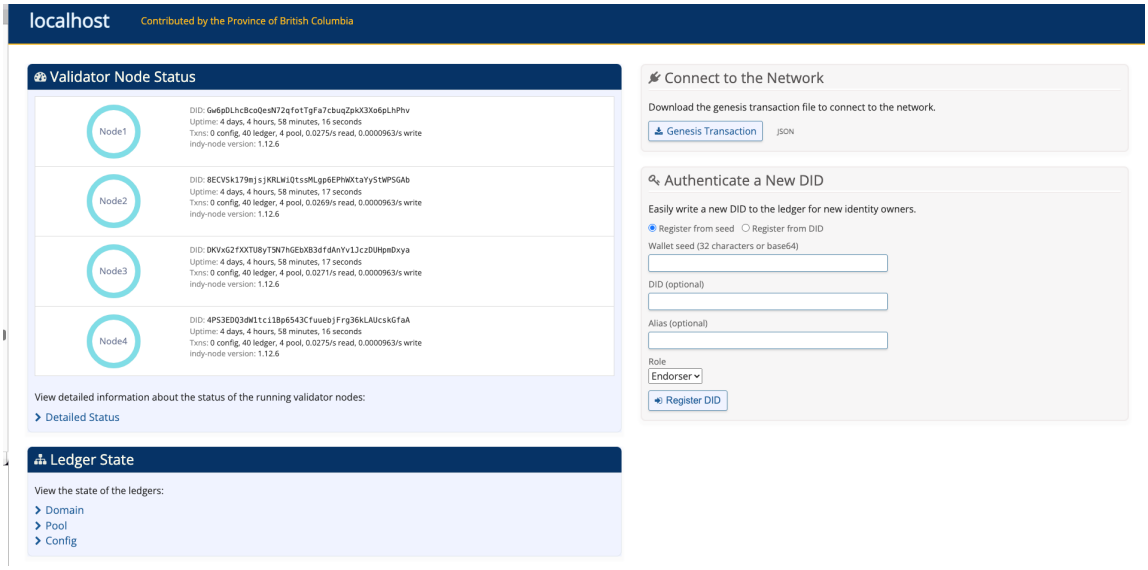


FIGURE 4.5 : Interface d'administration du réseau VON-Network

4.3.4.2 Établissement de connexion

L'objectif de cette phase est de pouvoir établir une connexion entre les agents représentant les organisations et l'utilisateur. Les principales étapes sont les suivantes :

- utiliser l'agent représentant *l'organisation A* pour créer une invitation ;
- réception et acceptation de l'invitation par l'utilisateur appartenant à *l'organisation A* ;
- l'utilisateur envoi une demande connexion à *l'organisation A* ;

- *l'organisation A* reçoit la demande, accepte la connexion et finalise le processus de connexion ;

Une fois la connexion établie entre les deux agents, nous disposons d'un canal pour échanger des messages sécurisés et cryptés. Nous effectuons des tests d'envoi de message texte pour vérifier le bon fonctionnement de la connexion. Ces différents tests sont effectués à partir de l'interface *OpenAPI/Swagger* de chaque agent (voir figure 4.6 et 4.7).

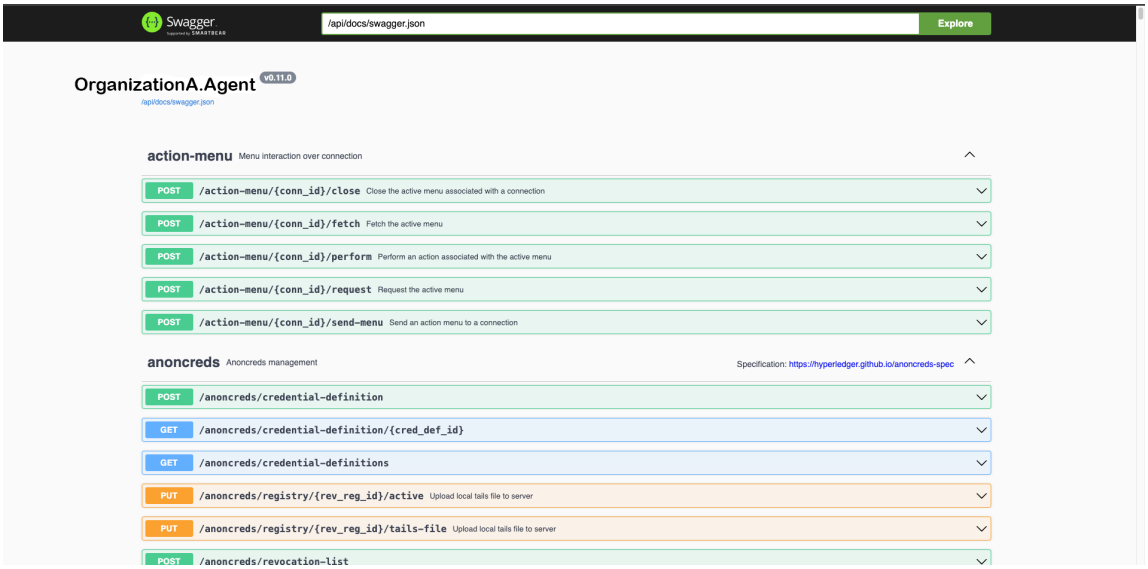


FIGURE 4.6 : Interface OpenAPI/Swagger de l'organisation A

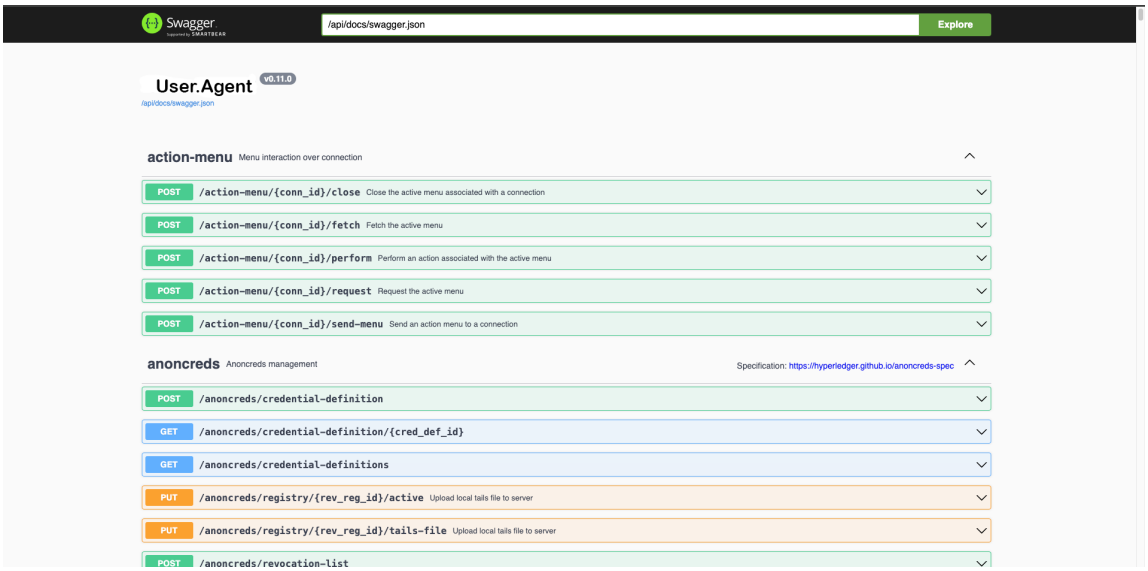


FIGURE 4.7 : Interface OpenAPI/Swagger de l'utilisateur

4.3.4.3 Délivrance de titre d'identification

L'étape représente la délivrance d'un titre justificatif/certificat à l'utilisateur par *l'organisation A*. Ce processus commence par l'enregistrement du DiD de *l'organisation A* dans le registre *Indy*. Ensuite, les autres phases consistent de manière chronologique en :

- la création et au stockage d'un schéma ;

- la création d'une définition de justificatif d'identité et son enregistrement dans le registre ;
- l'initialisation de la connexion entre *l'organisation A* et l'utilisateur ;
- la délivrance du titre par *l'organisation A* ;
- la réception et l'enregistrement du titre par l'utilisateur ;
- la réception d'un accusé de réception par *l'organisation A*.

4.3.4.4 Demande et présentation d'une preuve

Après la délivrance du titre, l'utilisateur dispose désormais de son titre d'identification. À partir de l'agent de *l'organisation A*, nous envoyons une demande de preuve à l'utilisateur. L'utilisateur reçoit la demande de preuve, sélectionne le justificatif et répond à la preuve.

4.3.4.5 Accès à une ressource

Dans le cadre d'une demande d'accès à une ressource appartenant à une *organisation B* par l'utilisateur, il doit prouver son identité (son organisation d'origine, et qu'il dispose d'un titre fourni par ce dernier). Nous développons donc le contrôleur de *l'organisation B*, déployons son agent, puis présentons les différentes étapes que l'utilisateur doit suivre pour prouver qu'il est autorisé à accéder à la ressource. Les différentes fonctions à ajouter au contrôleur de *l'organisation B* sont relatifs :

- à une demande à l'utilisateur afin de fournir des preuves de son affiliation à l'organisation parente (*organisation A*) ;
- à la validation de la preuve reçue de l'utilisateur ;
- à l'autorisation ou au refus d'accès à la ressource.

4.3.4.6 Test et vérification

L'interface *OpenAPI/Swagger* (Figures 4.7 et 4.6) offerte par ACA-Py dispose d'un espace d'administration permettant d'exécuter différents types de requêtes afin de tester les fonctionnalités des contrôleurs. Plusieurs points de terminaisons sont ainsi exposés par cette API REST. Le tableau 4.1 ci-dessous met en exergue quelques points de terminaison utilisés dans notre scénario pour chaque agent (Organisation A et utilisateur).

Action	Émetteur (Organisation A)	Détenteur (utilisateur)
Envoi d'une demande		POST/issuecredential-2.0/records/{cred_ex_id}/send-request
Délivrance de titre	POST/issue-credential-2.0/records/{cred_ex_id}/issue	
Stockage du titre		POST/issue−credential-2.0/records/{cred_ex_id}/store
Envoyer une demande de preuve	POST/present-proof-2.0/send-request	
Envoi de la preuve		POST/present-proof-2.0/records/{pres_ex_id}/send-presentation
Validation de la preuve	POST/present-proof-2.0/records/{pres_ex_id}/verify-presentation	

TABLE 4.1 : Points de terminaisons OPenAPI/Swagger

4.3.5 Résultats

Le scénario présenté dans cette section vise à valider les fonctions d'identification, d'enregistrement des identités décentralisées et d'authentification des utilisateurs et des organisations. Afin de tester la performance des agents en interaction, nous mettons en

place un script qui initialise les agents (*Organisation A* et utilisateur), puis exécute une série d'actions d'émission et de validation d'informations d'identification. Ainsi, nous exécutons, une délivrance de 100, 200, 300 justificatifs d'identité à l'utilisateur par *l'organisation A*. Les temps d'exécution de chaque opération du processus sont présentés dans le tableau 4.2 ci-dessous.

Opération	**Temps d'exécution (s)**
Connexion des agents	0.43
Création schéma, définition et publication	4.92
Initialisation de l'échange de 100 justificatifs d'identification	8.36
Initialisation de l'échange de 200 justificatifs d'identification	17.47
Initialisation de l'échange de 300 justificatifs d'identification	42.56
Durée totale d'envoi, réception et validation de 300 justificatifs d'identification	49.29
Temps moyen par titre	0.16

TABLE 4.2 : Durée d'exécution du processus d'émission et validation de justificatifs d'identification

Nous avons ainsi montré à travers un processus conduit de bout en bout comment enregistrer les organisations dans un registre distribué. Par ailleurs, l'émission d'informations d'identifications vérifiables à l'endroit d'un utilisateur et sa validation par une organisation a été démontrée.

4.4 Evaluation de la confiance

4.4.1 Environnement d'expérimentation

Nous proposons un environnement d'expérimentation de cloud communautaire établi en deux phases. Lors de la première phase, nous initialisons l'architecture de notre 3C. Il s'agit essentiellement de générer des fichiers de jeux de données décrivant les organisations, les ressources fournies et des requêtes d'expression de besoins de ressources. Ensuite, dans la seconde phase, nous produisons des données statistiques à travers des simulations de partage de ressources entre les organisations. Les informations déduites de ces expériences permettent d'évaluer les performances de notre modèle de confiance. Les expérimentations sont menées sur un *MacBook Pro (Retina, 15 pouces, mi-2015), processeur 2,2 GHz Intel Core i7 quatre cœurs, mémoire 16 Go 1600 MHz DDR3*. La programmation est effectuée dans un environnement de développement (IDE) *Pycharm* et le langage *Python version 3.9*. Chaque organisation au sein de la communauté peut être demandeur et/ou fournisseur de ressources. Nous distinguons deux types d'organisations fournisseurs de ressources. D'une part, des organisations fournissant des ressources conforment aux contrats de niveau de service (SLA) établi à la base entre les acteurs impliqués dans une transaction. Celles-ci sont qualifiées de bons fournisseurs ou organisation G. D'autre part, celles mettant à dispositions des ressources non fiables sont dites malicieuses ou organisation M. Le nombre d'organisations étant une caractéristique essentielle dans la mise en place d'une communauté perenne et prospère, nous effectuons nos expérimentations sur des groupes d'organisations de la plage [80;250] membres. Le taux d'organisations malicieuses est également variée de 20 à 80%. Des tours constitués de 500 demandes de ressources sont effectués à chaque jeu d'expérimentation. Les paramètres d'expérimentation sont résumés dans tableau 4.3.

Paramètres de l'expérimentation	Valeurs
Nombre de fournisseurs de ressources	80, 120, 150, 180, 200, 220, 250
Nombre de types de ressources	10
Nombre de niveaux de sensibilité	3
Nombre de tours	15, 20
Pourcentages de fournisseurs malicieux	20%, 40%, 60%, 80%
Nombre de transactions par tours	500

TABLE 4.3 : Les paramètres d'expérimentations

Les principales métriques utilisées pour mesurer la performance de notre modèle sont les suivantes :

- $SRTG$: taux de succès de transactions d'organisations fiables (organisations G).

$$SRTG = \frac{Nombres\ de\ bonnes\ ressources\ fournies\ par\ les\ organisations\ G}{Nombre\ total\ de\ ressources\ fournies} \tag{4.4.1}$$

- $RPOT$: taux de participations des organisations G aux transactions. Ce taux permet d'évaluer le nombre d'organisations différentes participant aux différents jeux d'expérimentations.
- Les valeurs de réputation spécifique et de niveau d'assurance déduite grâce à notre mécanisme de promotion et de relégation.
- Le temps d'exécution de notre algorithme en fonction de tailles variables de groupe de fournisseurs de ressources.

Les performances de notre modèle sont comparées à l'algorithme de gestion de confiance *Intertrust* [131] et au modèle *TNA-SL* [111], [113].

4.4.2 Paramètres et seuil de sélection

La valeur de confiance de sélection d'un fournisseur à partir du *SeComTrust* est calculée grâce à l'équation équation 3.4.9. Afin de déterminer la valeur de β, représentant le poids de la valeur de confiance directe ou recommandée (DRT) dans cette équation, nous examinons le taux de participation d'organisations différentes aux transactions (RPOT) et le taux de succès des fournisseurs G (SRTG). Le RPOT permet d'évaluer le nombre de fournisseurs participant activement aux transactions, limitant ainsi la possibilité de sélectionner toujours les mêmes organisations dans l'optique d'augmenter le SRTG. Le SRTG quant à lui est un indicateur de performance important des modèles de confiance. Il exprime la capacité du modèle de confiance à résister aux attaques malveillantes. Nos expérimentations portent sur une communauté de 80 fournisseurs dont 20% de malveillants. Un cycle d'expérimentation se compose de 20 tours. Dans un tour, nous simulons le traitement de 500 demandes de ressources. L'une des particularités du *SeComTrust* est de tenir compte des interactions directes entre les organisations et de leur comportement dans le temps au sein de la communauté. Ainsi, nous estimons que le poids de la recommandation directe ne doit pas être trop grand ou trop petit. Par conséquent, nous effectuons des simulations en fixant la valeur de β entre 3 et 7. Les résultats des expérimentations présentés à la figure 4.8 montrent que nous avons les valeurs de RPOT et SRTG conjointement plus élevés (RPOT= 0.21, SRTG= 0.98) lorsque β est égal 0.6 et le seuil est égal 0.3. En définitive, nous maintenons β à 0.6 et le seuil de sélection à 0.3 afin de fournir un modèle avec un taux de réussite de transaction de fournisseurs G élevé et une forte participation des organisations.

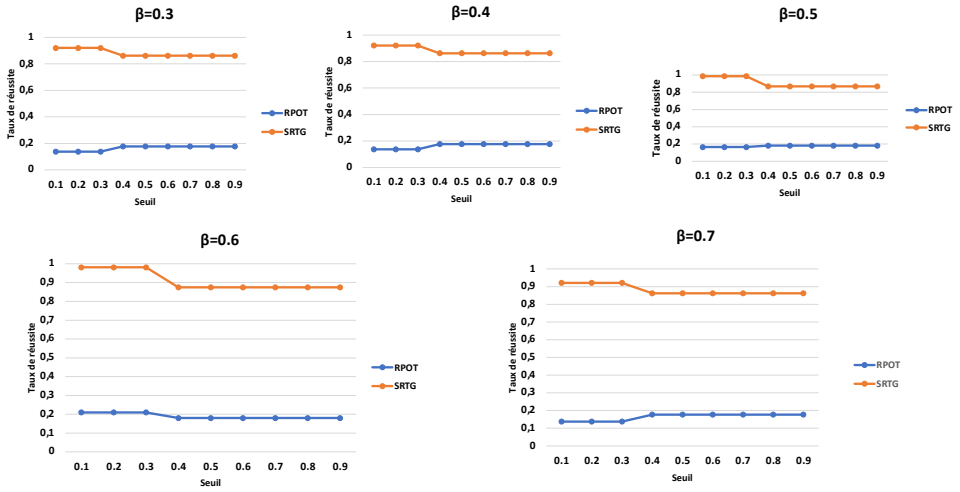


FIGURE 4.8 : sélection de β et du seuil

4.4.3 Résultats et discussions

Dans le but d'analyser les performances du *SeComTrust*, nous avons effectué quatre types d'expérience. Ces expérimentations permettent de comparer notre modèle au modèle TNA-SL [111][113] et à l'algorithme *Intertrust* [131]. La première simulation consiste à évaluer l'évolutivité de notre modèle en augmentant le nombre d'organisations au sein de la communauté, dont 20% de fournisseurs malveillants. Nous constituons ainsi des 3C de 80, 100, 120, 150, 180, 200, 220 et 250 membres. Nous comparons les taux de réussite de fournisseurs G de notre modèle au deux autres modèles suscités. Par ailleurs, la seconde expérience consiste à faire varier le nombre d'organisations malveillantes (organisations M) de 20% à 80% et prouver la résistance de notre modèle aux attaques. L'objectif de la troisième expérimentation est d'observer le changement des valeurs de réputation et de niveau d'assurance afin d'évaluer la performance de notre mécanisme de promotion et de relégation. Enfin, le quatrième type de simulation permet de comparer le temps d'exécution de notre algorithme à ceux de TNA-SL [111][113] et *Intertrust* [131].

4.4.3.1 L'évolutivité

L'évolutivité est une des caractéristiques majeures d'un environnement cloud [72]. Nous modélisons notre cadre de partage de ressources autour d'ensembles de tailles variées d'organisations. Les communautés d'organisations varient de 80 à 250 membres. Pour chaque groupe d'organisations, nous intégrons 20% de malicieux. Les échanges entre organisations sont représentés par des fichiers de données de traces des échanges. Les résultats présentés dans la figure 4.9 ci-dessus montrent les taux de réussite des trois modèles (*SeComTrust, InterTrust, TNA-SL*). Chaque modèle est exécuté en 15 tours de 500 requêtes de transactions par groupe d'organisations. L'on déduit de ces résultats que le taux de réussite du *SeComTrust* est largement supérieur au taux de réussite des algorithmes *Intertrust* et TNA-SL pour tous les groupes d'utilisateurs expérimentés. Cette situation s'explique par le fait que la valeur de confiance du *SeComTrust* est obtenue grâce à la somme pondérée de la confiance directe ou recommandée et de la valeur de réputation spécifique. Alors que *Intertrust* et TNA-SL calculent la confiance sans tenir compte de la réputation. Par ailleurs, le mécanisme de mise à jour des valeurs de

réputation proposé et la sélection du fournisseur à partir de différentes listes de transactions selon un ordre bien précis justifient les taux de réussite du *SeComTrust*. En conclusion, nous pouvons affirmer que notre modèle permet de déployer des systèmes cloud évolutifs.

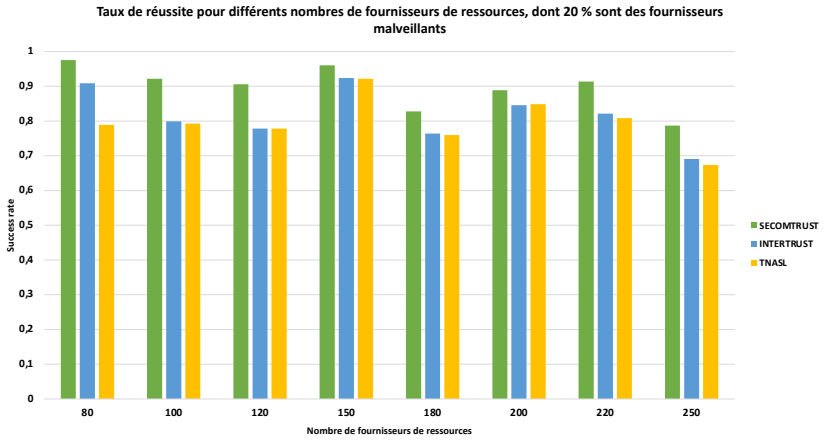


FIGURE 4.9 : Taux de réussite pour différents nombres de fournisseurs de ressources dont 20 % sont des fournisseurs malveillants

4.4.3.2 Résistances aux attaques

Dans l'otique d'évaluer la capacité de résistance aux attaques de notre modèle, nous faisons varier le taux de fournisseurs M dans un pool de 80 organisations. Le taux d'organisations malveillantes est varié de 20%, 40%, 60% et 80%. Quinze (15) tours de 500 transactions ont permis d'avoir les résultats présentés dans les figure 4.10, figure 4.11, figure 4.12 et figure 4.13. Les différents graphes présentent l'évolution des valeurs SRTG pour les différentes proportions d'entités malveillantes. Le SRTG du *SeComTrust* est en perpétuelle croissance et significativement plus élevé que ceux des algorithmes *InterTrust* et TNA-SL jusqu'à atteindre le maximum pour un taux de 20% de malveillants. Ce constat s'explique par le fait que notre approche propose le calcul de la valeur de confiance du fournisseur en combinant les interactions antérieures directes ou recommandées et la réputation. En outre, la gestion dynamique de la confiance, à travers la mise à jour des valeurs de confiance sur la base du respect des attributs de performances, permet d'accroître les valeurs de réputation des organisations, contrairement aux deux autres modèles qui n'intègrent pas cet aspect. Les SRTG des modèles *Intertrust* et TNA-SL connaissent également une évolution relativement plus faible pour des taux de 20%, 40% et 60% de malveillants illustrés par les figure 4.10, figure 4.11et figure 4.12. Cependant, avec un taux 80% de malicieux sur la figure 4.13, nous constatons une baisse du SRTG pour ces deux algorithmes jusqu'à atteindre la valeur nulle pour le TNA-SL. Par ailleurs, les figure 4.10, figure 4.11, figure 4.12 et figure 4.13 mettent en évidence la variation du nombre d'organisations malveillantes en fonction du taux d'organisations malveillantes injecté. Il ressort que notre modèle permet de réduire, voire éliminer les organisations malveillantes au sein de la communauté. Le suivi de la qualité des ressources à travers les attributs SMI en cas de violation des engagements proposé par notre modèle permet d'identifier les ressources de qualité et classifier les bons fournisseurs. Contrairement aux contributions TNA-SL et *InterTrust*, notre tech-

nique fait croître plus rapidement à chaque tour de transaction la valeur de confiance et la réputation des bons fournisseurs et réduit considérablement celle des malicieux. La probabilité de sélectionner des organisations malveillantes pour des échanges sur le long terme est ainsi limitée.

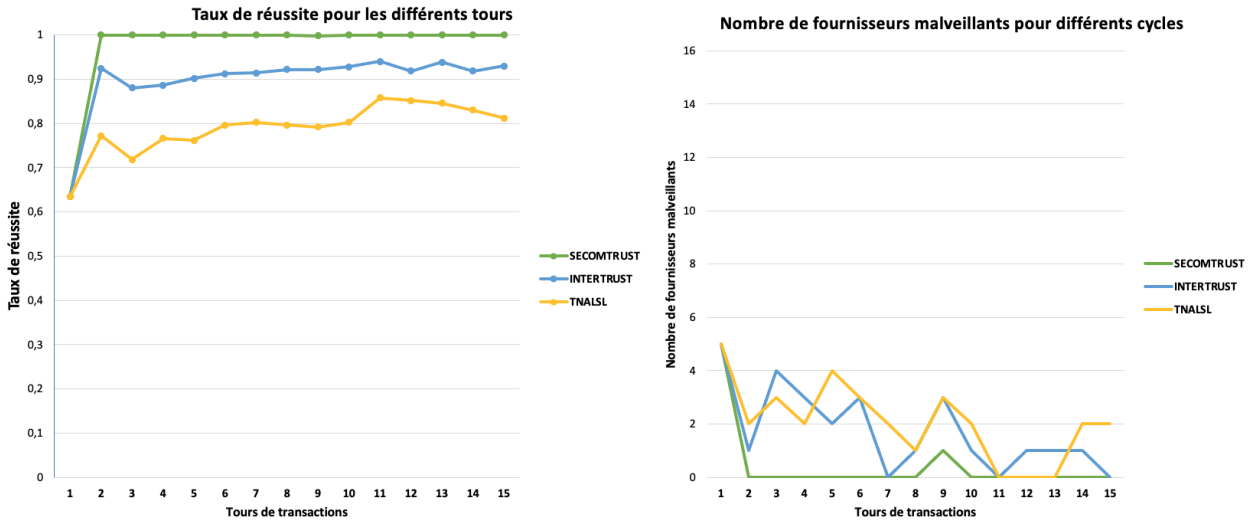


FIGURE 4.10 : Taux de réussite des échanges pour différents cycles d'échanges (20 % fournisseurs M)

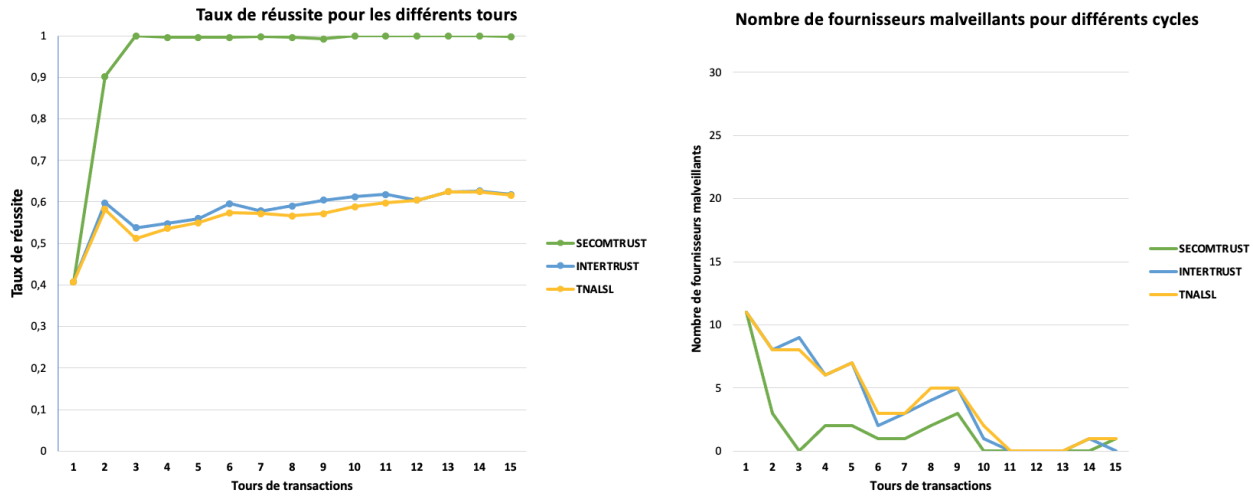


FIGURE 4.11 : Taux de réussite des échanges pour différents cycles d'échanges (40 % fournisseurs M)

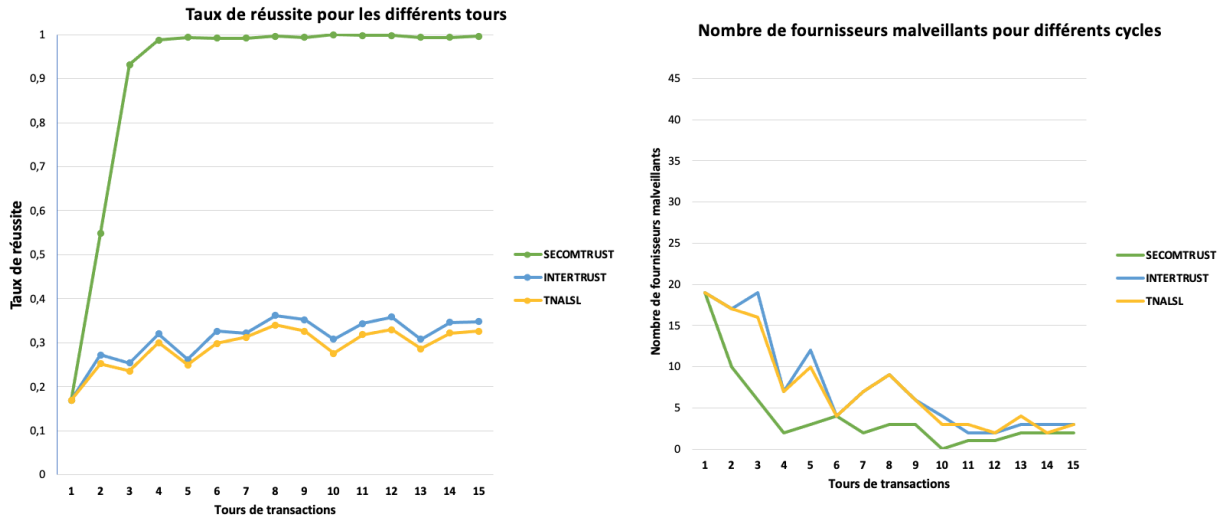


FIGURE 4.12 : Taux de réussite des échanges pour différents cycles d'échanges (60 % fournisseurs M)

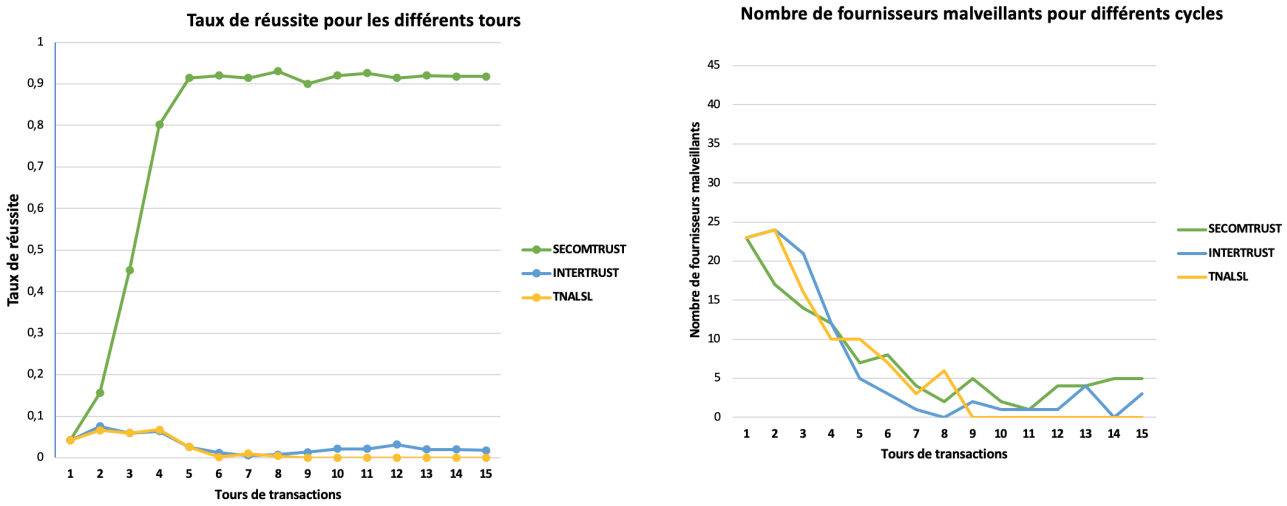


FIGURE 4.13 : Taux de réussite des échanges pour différents cycles d'échanges (80 % fournisseurs M)

4.4.3.3 Variation de la valeur de réputation spécifique et du niveau d'assurance

Ce volet d'expérimentation consiste à étudier le comportement de deux types organisations. Une organisation de type G et une autre de type M. La figure 4.14 montre l'évolution du niveau d'assurance. Le niveau d'assurance est la capacité d'une organisation à fournir une ressource d'un niveau de sensibilité spécifique et permet aux organisations de migrer d'un domaine de sécurité à un autre. Le mécanisme de promotion et de relégation permet à l'organisation G de passer du domaine de sécurité du niveau 1 au domaine supérieure 2 (niveau Intermédiaire) à partir du tour 13 comme le montre la figure 4.16. En outre, la figure 4.15 montre la variation de la réputation spécifique des deux types d'organisations. La réputation spécifique est un critère de sélection du fournisseur de confiance. Les organisations avec des valeurs de réputation spécifique élevées sont privilégiées dans l'algorithme de sélection des fournisseurs. Avec l'augmentation du nombre de tours, nous constatons sur la figure 4.15 que la valeur de réputation spécifique du fournisseur G est en constante progression. Le fournisseur malveillant à quant à lui une valeur réputation spécifique qui décroît. Par conséquent,

nous pouvons conclure que le *SeComTrust* permet de distinguer efficacement les bons fournisseurs des fournisseurs malveillants au fur et à mesure que les transactions augmentent.

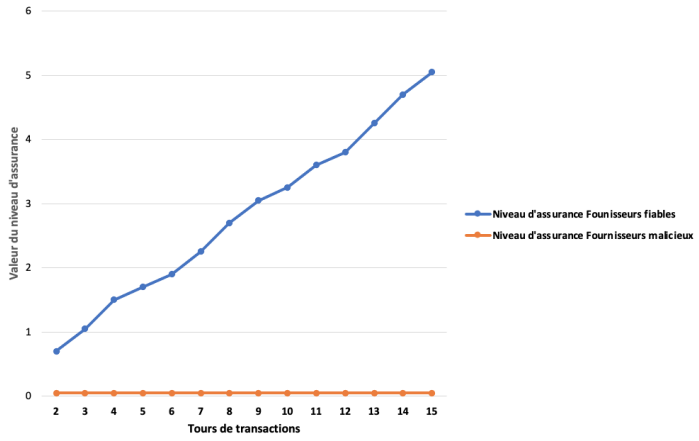


FIGURE 4.14 : Valeur niveau d'assurance

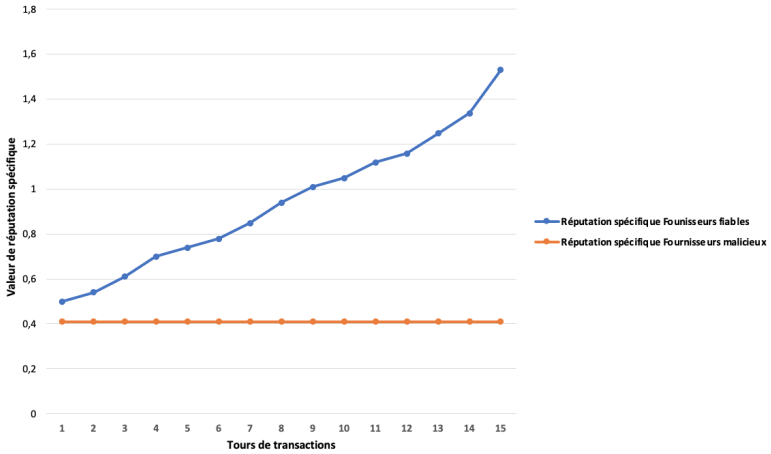


FIGURE 4.15 : Valeur réputation spécifique

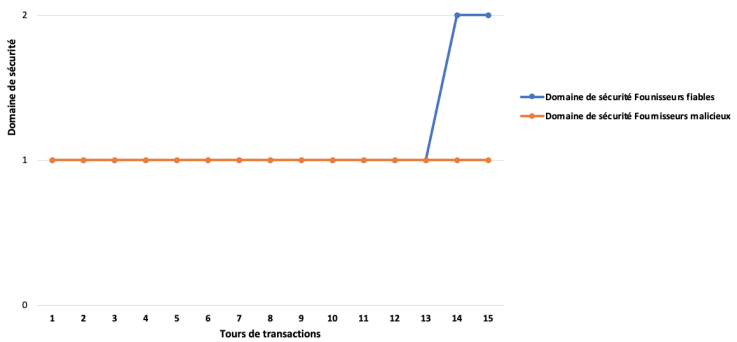


FIGURE 4.16 : Variation domaine de sécurité

4.4.3.4 Temps d'exécution

La figure 4.17 montre le temps d'exécution des modèles *SeComTrust*, *Intertrust* et TNA-SL. Ces expérimentations ont été effectuées pour chaque tour de 500 transactions avec différents groupes constitués 80, 120, 180, 220, 250 membres. Les résultats montrent que le temps d'exécution de notre modèle est largement plus bas que ceux des deux autres modèles. Notre modèle garantie un SRTG élevé tout en maintenant un taux d'exécution bas. Les résultats montrent que le temps d'exécution de notre modèle est largement plus bas que ceux des deux autres modèles. La sélection du fournisseur de la ressource de notre modèle se fait tout d'abord sur la base de la liste de transactions antérieures du demandeur, puis sur la base de la liste de réputation. Ce mécanisme permet d'accélérer le processus de sélection. Notre modèle garantie un SRTG élevé tout en maintenant un faible temps d'exécution.

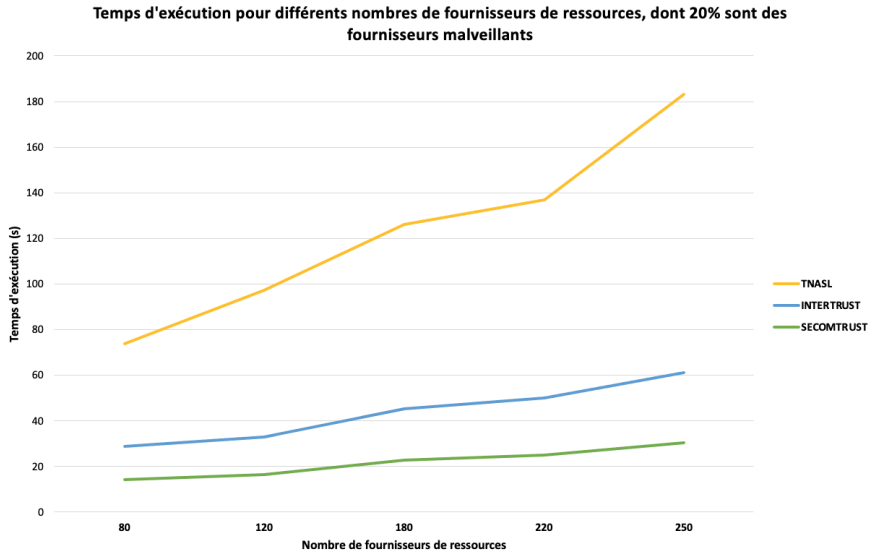


FIGURE 4.17 : Temps d'exécution pour différents nombres de fournisseurs de services, dont 20 % sont des fournisseurs malveillants

4.5 Contrat de collaboration et contrôle d'accès

Les actions à mener par chaque organisation lors du partage de la ressource doivent explicitement être identifiés et définis dans un contrat de collaboration pour garantir l'autonomie des entités et éviter les conflits. Par ailleurs, cela permet d'assurer le suivi de la qualité des ressources tout au long de la collaboration. Après l'établissement du contrat de collaboration, les utilisateurs de l'organisation sollicitant la ressource sont autorisés à accéder à la ressource selon les règles de politiques d'accès définies. Toutes ces opérations sont réalisées grâce au composant *gestionnaire d'accès et contrat de collaboration* de notre architecture Zero Trust.

4.5.1 Scénario de collaboration

Nous présentons un scénario d'application du modèle **Community-OrBAC** présenté à la section 3.5.2 dans un cloud communautaire. Le scénario repose sur une architecture présentée dans la figure 4.18. Elle est composée de startups regroupées dans une communauté d'entreprise *Com_Startup*. Chaque startup représente une organisation. Ces organisations sont réunies dans l'optique de partager des ressources de type : *Software*

as a Service(SaaS), *Platform as a Service(PaaS)* et *Infrastructure as a Service(IaaS)*. Ces ressources sont référencées dans un registre de ressources. Chaque organisation membre est soit fournisseur et/ou demandeur de ressources. Ainsi, dans notre scénario, la startup $DevCorpo$ sollicite un cluster de serveurs pour la mise en place d'infrastructures de développement d'applications métiers. La ressource correspondante à ce besoin dans le registre est le $Clusterkub$ fourni par la startup $InfraGroup$. Les deux organisations négocient et mettent en place un contrat de collaboration dynamique et évolutif durant toute la période de partage. Le processus de négociation entre les organisations $InfraGroup$ et $DevCorpo$ est conforme à la procédure représentée dans la figure 3.17. Dans ce contexte, les organisations $InfraGroup$ et $DevCorpo$ sont représentées respectivement par $OrgB$ (agent fournisseur) et $OrgA$ (agent demandeur).

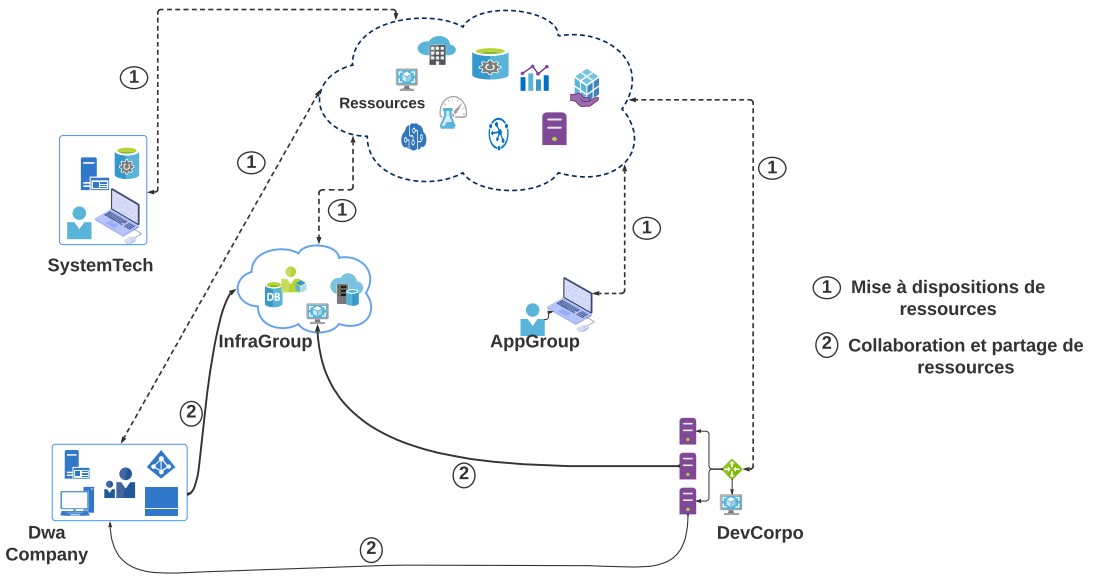


FIGURE 4.18 : Architecture cloud communautaire Com_Startup

4.5.2 Architecture d'expérimentation

L'architecture d'expérimentation du *Community-OrBAC* adoptée utilise les solutions du projet $Hyperledger$, particulièrement les agents $Hyperledger\ Aries$ qui proposent un cadre d'interactions sécurisées entre des agents. Cette architecture est constituée par plusieurs agents représentés dans la figure 4.19 et décrits ci-dessous.

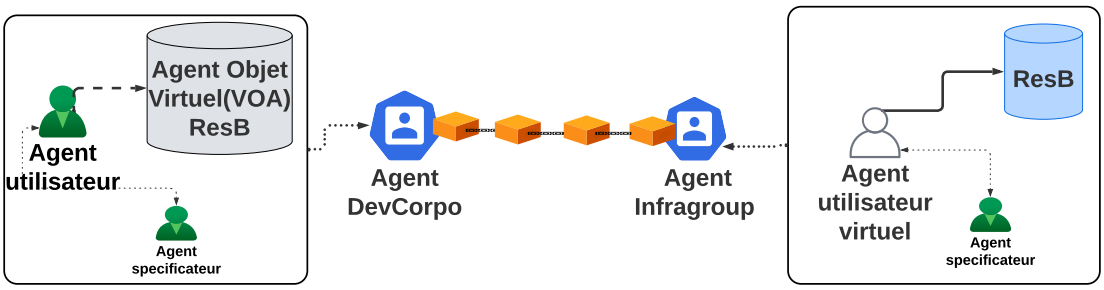


FIGURE 4.19 : Architecture d'expérimentation Com_Startup

- *Les agents spécificateurs* : ils représentent au sein de chaque organisation les agents responsables de l'exécution des fonctions des contrôleurs implémentant les règles

de politiques de sécurité locales à chaque organisation.

- *L'agent utilisateur* : il représente l'utilisateur désirant accéder à la ressource.
- *L'agent objet virtuel* représente la ressource dans l'organisation du demandeur. Cet agent exécute les fonctions d'*invocation* permettant à l'utilisateur d'accéder à la ressource distante grâce à une règle de la politique locale de son organisation.
- Les agents *DevCorpo* et *Infragroup* représentent les oracles de chaque organisation, permettant aux organisations d'interagir avec le registre blockchain.
- *L'agent utilisateur virtuel* représente l'agent sollicitant la ressource dans l'organisation fournisseur.

4.5.3 Spécification de règles Community-OrBAC

Le contrat de collaboration établi, nous présentons ci-dessous les règles *Community-OrBAC* pour le partage de la ressource $Clusterkub$. Comme présenté dans le fonctionnement du *Community-OrBAC* (section 3.5.2), l'accès à une ressource distante nécessite la création de l'agent objet virtuel $VOA\_clusterkub$, représentant la ressource désirée $clusterkub$ dans l'organisation demandeur, et de l'agent utilisateur virtuel vua_B dans la politique de sécurité du propriétaire de la ressource (voir figure 3.18).

La permission dans la politique locale $DevCorpo$ est présentée dans le tableau 4.4 ci-dessous. Cette permission est accordée dans un contexte c considérant le niveau de vulnérabilité et la portée sociale de la ressource $VOA\_clusterkub$.

TABLE 4.4 : Règle dans la politique locale du demandeur $DevCorpo$

$DevCorpo \in Com\_Startup, s \in Sujets, invoquer \in Actions, VOA\_clusterkub \in Objets, consulter \in Activités, c \in Contexte, r \in Roles$
Permission(DevCorpo, r, consulter, vue_VOA_clusterkub, c) $\wedge$ *Habilite* (DevCorpo, s, r) $\wedge$ *Utilise*(DevCorpo, VOA_clusterkub, vue_VOA_clusterkub) $\wedge$ *Considère* (DevCorpo, invoquer, consulter) $\wedge$ *Définit* (DevCorpo, s, invoquer, VOA_clusterkub, c) $\rightarrow$ *Est_Permis*$(s, invoquer, VOA\_clusterkub)$

Le tableau 4.5 décrit la règle d'accès dans la politique du propriétaire $InfraGroup$ dans un contexte évalué sur la base de la valeur de confiance et du groupe social du sujet vua_B.

TABLE 4.5 : Règle dans la politique locale du fournisseur $Infragroup$

$InfraGroup \in Com\_Startup, vua_B \in Sujets, exécuter \in Actions, Clusterkub \in Objets, Afficher \in Activités, c \in Contexte, r \in Roles,$
Permission (InfraGroup, r, Afficher, Vue_ clusterkub, c) $\wedge$ *Habilite* (InfraGroup, vua$_B$, r)$\wedge$ *Utilise* (InfraGroup, Clusterkub, Vue_clusterkub) $\wedge$ *Considère* (InfraGroup, exécuter, Afficher) $\wedge$ *Définit* (InfraGroup, vua$_B$, $excuter, Clusterkub, c$) $\rightarrow$ *Est_Permis*$(vua_B, excuter, Clusterkub)$

4.5.4 Discussion

L'étude de cas présente différents avantages apportés par notre modèle dans une collaboration entre deux entités de façon générale et spécifiquement entre membres d'une même communauté. En effet, l'utilisation des agents autonomes et la démarche de négociation proposée exposent des interactions de type pair à pair, consensuelles, garantissant une souplesse et une indépendance de chaque entité dans la gestion de ses utilisateurs et du contrôle des accès à ses ressources. Par ailleurs, au regard des apports significatifs apportés par la combinaison des systèmes multi-agents et des technologies blockchain [41][25], la négociation et la création de contrats dynamiques peuvent être déployées grâce à des contrats intelligents auto-exécutables. Les agents serviront de sources de données (modifications des clauses du contrat, pénalités, etc.) pour des algorithmes représentant les contrats intelligents. En outre, l'identification des niveaux de sécurité des ressources partagées et l'évaluation de la confiance est fortement recommandée dans la mise en place de stratégie de cybersécurité dans le cloud computing [39]. De façon spécifique pour des organisations centrées sur la communauté, les membres peuvent mettre à la disposition de leurs pairs des ressources avec des exigences d'accessibilité réduites (niveau de confiance, sans contrepartie financière, etc.). Cette action visant à enrichir la communauté et dans l'intérêt de ses membres peut être une prérogative à l'adhésion. Un tel scénario serait difficilement envisageable pour des systèmes non communautaires. Le contexte de sécurité et le contexte social introduits par notre modèle constituent par ailleurs des critères supplémentaires et fiables pour définir des règles de sécurité robustes et personnalisées.

4.6 Conclusion

Dans ce chapitre, nous avons présenté les scénarios d'expérimentations et de validation des mesures de sécurité de notre stratégie Zero Trust dans un cloud communautaire.

Nous avons d'abord exposé le cadre expérimental à travers la description des capacités de notre cloud communautaire et de l'architecture générale de la stratégie Zero Trust adoptée.

Ensuite, nous proposons une implémentation de notre système de gestion décentralisée des identités. Ensuite, nous proposons une implémentation de notre système de gestion décentralisée des identités. La mise en œuvre de notre mécanisme de gestion des identités a été effectuée grâce aux projets open source $Indy$, $Aries$, et $Ursa$ de la fondation Hyperledger. Ces solutions proposent des outils de stockage des informations d'identité dans un registre blockchain, de développement des applications métiers et des agents permettant d'assurer l'interopérabilité de notre système avec des systèmes tiers.

Après le système de gestion d'identité, l'étape suivante a consisté à présenter une implémentation et une validation des performances de notre modèle d'évaluation et de sélection d'organisation de confiance (*SeComTrust*). Nous avons ainsi montré que le *SeComtrust* garantit l'évolutivité d'un cloud communautaire, ainsi qu'une résistance aux attaques de fournisseurs malveillants. Par ailleurs, le *SeComtrust* permet, grâce à la variation des valeurs de réputation et de niveau d'assurance, de distinguer les bons fournisseurs des malveillants et d'éliminer ou réduire la participation des malicieux aux échanges de la communauté. Ces performances ont été validées en comparant notre modèle à d'autres modèles de référence (TNA-SL et *Intertrust*).

Enfin, nous avons exposé une étude de cas de notre modèle de contrôle d'accès *Community-OrBAC* et une architecture d'expérimentation fondée sur les agents du pro-

jet Hyperledger Aries. Nous avons montré qu'à travers l'utilisation des agents et d'un protocole de négociation, ce modèle permet aux organisations de définir des règles de sécurité de façon dynamique et autonome, et d'établir des accords de collaboration de manière consensuelle.

Chapitre 5

Conclusion et Perspectives

« La routine structure. La structure ouvre une perspective. La perspective un horizon. »

Peter James, Comme une tombe (2005)

Sommaire

5.1 Conclusion

Les technologies émergentes, dites de $4^{\grave{e}}$ génération (Cloud computing, IoT, IA, etc.) et les innovations majeures qu'elles apportent, affectent de diverses manières les habitudes des populations ainsi que les pratiques au sein des entreprises. Ainsi, de gros volumes de données de nature diverse et sensible transitent sur des infrastructures informatiques distribuées, constituées d'entités hétérogènes et exposées à différents types de menaces. Cette thèse s'inscrit dans la droite ligne des efforts de proposition de mécanismes et techniques de protection des ressources partagées (données et services) pour des systèmes de collaboration sécurisés, fiables et de confiance. Plus particulièrement, elle est axée sur un partage sécurisé de ressources entre des acteurs réunis au sein d'une communauté. En effet, l'établissement de relations au sein d'une communauté dans le but de partager des ressources requiert un cadre de confiance et des moyens de protection des données échangées. En outre, la diversité des menaces et le niveau élevé et sophistiqué des récentes cyberattaques impliquent d'adopter de nouvelles approches dans la sécurisation de ce type d'infrastructure. Par conséquent, nous avons proposé un modèle de sécurité fondé sur la stratégie de cybersécurité Zero Trust. Le modèle proposé s'appuie sur un processus de sécurité hiérarchique à travers une gestion décentralisée des identités, un modèle de spécification de politique de contrôle d'accès et de contrat de collaboration et une technique d'évaluation et de suivi de la confiance entre les différentes parties.

Les deux premiers chapitres nous ont permis de faire un état de l'art sur le cloud computing en général, en particulier le cloud communautaire, ainsi que les défis de collaboration et sécuritaires rencontrés dans ces systèmes. Ainsi, dans le premier chapitre, nous avons présenté le cloud computing, ses caractéristiques, son fonctionnement et les services qu'il offre. Par ailleurs, les besoins et solutions de collaboration offerts, ainsi que les défis sécuritaires auxquels sont confrontés les acteurs du cloud, ont permis d'explorer les stratégies et moyens de sécurisation des infrastructures cloud. Le deuxième chapitre a été consacré aux mécanismes de sécurité, notamment la gestion des identités, les modèles de contrôle d'accès et les systèmes d'évaluation de la confiance. Les spécificités d'un environnement communautaire nous ont permis de montrer les limites de l'application de ces solutions existantes dans un cloud communautaire.

Le troisième chapitre présente nos différentes propositions d'amélioration des mécanismes de sécurité dans un cloud communautaire. En effet, la communauté étant constituée d'organisations autonomes et hétérogènes, il est important de disposer de moyens d'identification et d'authentification des acteurs. Nous avons alors proposé un système de gestion décentralisée des identités fondé sur la blockchain et le système de signature numérique BLS. L'approche des identités décentralisées permet de garantir l'autonomie de chaque organisation dans la gestion de l'identité de ses utilisateurs et de sa propre identité au sein de la communauté. En outre, le système d'agrégation des signatures utilisé permet d'améliorer la sécurité à travers la signature et l'accord de chaque organisation lors de l'intégration ou du départ d'un membre. Un système d'authentification des utilisateurs et de stockage des informations de transactions a également été proposé grâce aux contrats intelligents et à la technologie blockchain. Des tests d'expérimentation de notre système de gestion d'identité ont été effectués dans un environnement de simulation avec la blockchain $Hyperledger$ et les résultats ont montré son efficacité.
L'identification et l'authentification des utilisateurs et des organisations étant assurées, il est important, pour une collaboration donnée, de sélectionner le fournisseur idéal de confiance parmi toutes les organisations engagées dans la communauté. Ainsi, dans la deuxième partie de ce chapitre, nous avons proposé un système d'évaluation et de

suivi de la confiance des organisations. Ce système subdivise la communauté en trois groupes de domaines de sécurité. Chaque domaine est composé d'organisation avec un niveau de confiance bien défini. Cette valeur de confiance est calculée grâce à la logique subjective sur la base des résultats d'interactions directes ou recommandées et de la réputation des organisations. La valeur de confiance constitue l'un des paramètres de l'algorithme de sélection pour déterminer le fournisseur idéal de confiance. Par ailleurs, des attributs de mesure de qualité de ressources (disponibilité, vulnérabilité, etc.) ont été définis afin de suivre la qualité des ressources fournies. Cette action permet de suivre et de garantir la nature dynamique de la confiance à travers un mécanisme de récompense et de punition qui fait croitre ou décroitre le niveau de confiance. Notre système d'évaluation de la confiance a été expérimenté et comparé avec des modèles précédents. Cette opération a permis de valider le modèle grâce aux bonnes performances obtenues.
Le fournisseur idéal de confiance authentifié et sélectionné, dans la dernière partie de ce chapitre, nous avons proposé un modèle de spécification de politique de sécurité et de contrôle d'accès pour la collaboration entre les organisations. Le modèle appelé *Community-OrBAC*, fondé sur le modèle OrBAC, permet de définir des règles de sécurité en considérant le contexte de sécurité et le contexte social. Par ailleurs, il permet aux entités d'être autonomes dans la spécification de leur politique et de négocier des accords de collaboration afin d'éviter les éventuels conflits et le non-respect des engagements de chaque partie.

Dans le dernier chapitre, nous avons proposé une stratégie de cybersécurité Zero Trust dans un cloud communautaire fondé sur les différents mécanismes présentés dans le chapitre précédent. Cette stratégie permet d'assurer un contrôle et une protection constante, à travers l'identification et l'authentification des organisations et des ressources, l'évaluation de la confiance, le contrôle d'accès aux ressources et le suivi des accords de collaboration.

Pour conclure, cette thèse nous a permis d'examiner un large éventail de concepts, de modèles et de technologies dans les domaines du cloud, des environnements de collaboration et de partage, en particulier ceux liés à la communauté. Par ailleurs, nous avons exploré les défis, mécanismes et stratégies de sécurité de ces infrastructures. Notre but d'étudier la problématique de la sécurité des ressources partagées et de la confiance entre les membres d'une communauté. Nous avons fourni une architecture fondée sur une stratégie de cybersécurité Zero Trust pour répondre à cet objectif. Nous avons également montré que le travail proposé s'intègre dans une thématique riche, d'actualité et encourageante pour les défis futurs de sécurité des infrastructures cloud.

Les principales contributions de ce travail sont résumées dans la figure 5.1.

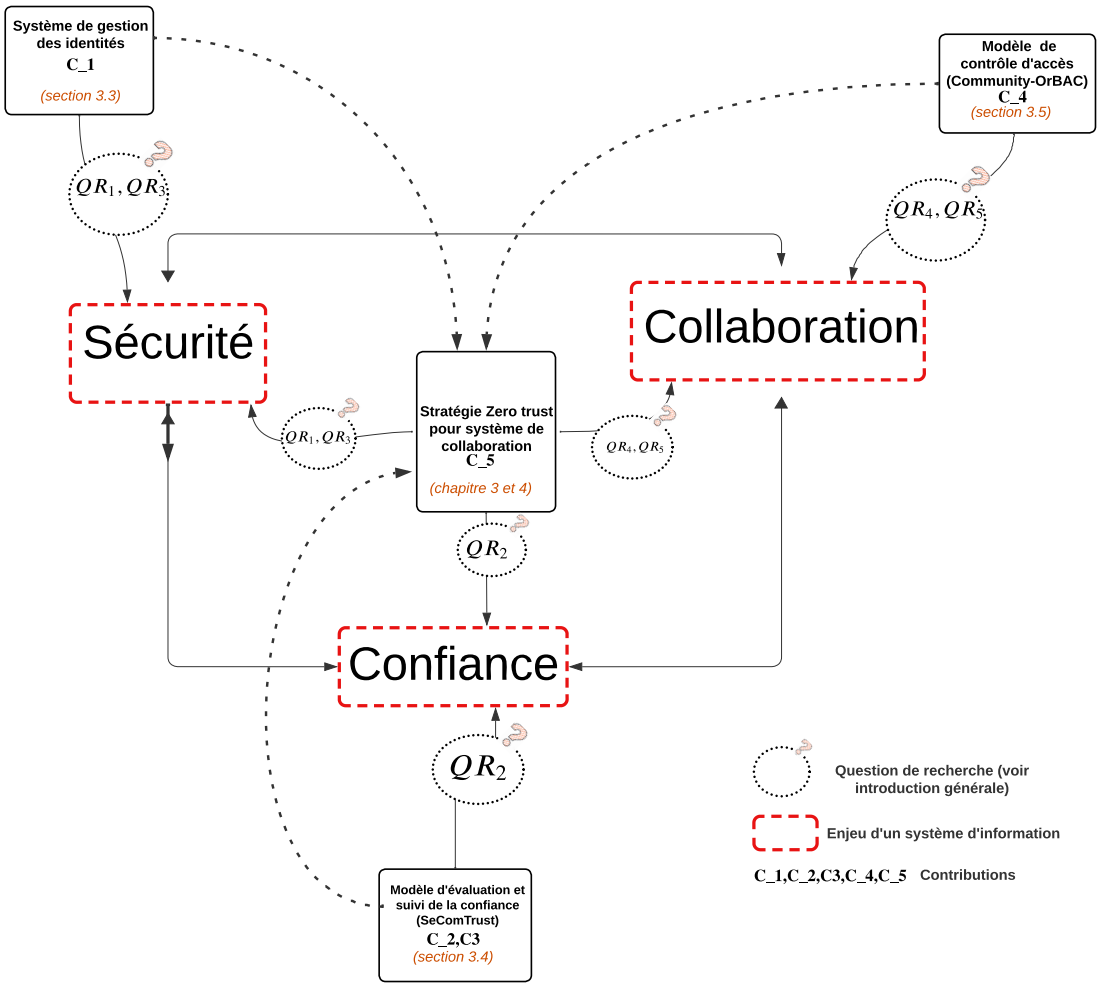


FIGURE 5.1 : Principaux résultats de cette thèse

5.2 Perspectives

Ce projet de thèse nous a permis d'apporter notre contribution à la sécurité des infrastructures informatiques en proposant une stratégie de sécurité Zero Trust dans le cloud communautaire. Ainsi, différents mécanismes de sécurité ont été mis en œuvre et évalués à travers des expérimentations et des cas d'étude. Cependant, plusieurs améliorations sont à envisager du point de vue de la stratégie et des mécanismes concernés. Comme axes d'améliorations, nous pouvons énumérer les points ci-dessous :

- Les mesures de sécurité de notre stratégie ont été évaluées et testées dans des scénarios indépendants. Une première amélioration de la démarche serait de proposer une implémentation du modèle de contrôle d'accès *Community-OrBAC* et de l'évaluer par rapport à d'autres modèles. Cette perspective pourrait être accompagnée d'une mise en œuvre de la stratégie dans un environnement concret de cloud communautaire réunissant des organisations (des PME, Startups) en situation réelle de collaboration, mettant en exergue les trois modèles de sécurité proposés.
- La présence de concurrents dans la communauté pourrait être étudiée dans la phase de définition du seuil de confiance et de sélection du partenaire de confiance. Cette démarche pourrait permettre d'anticiper ou de prédire d'éventuels comportements malveillants ou menaces de sécurité de la part des acteurs de la commu-

nauté.

- La stratégie proposée stocke les identifiants décentralisés dans un unique registre blockchain. La proposition d'un résolveur communautaire des identifiants décentralisés compatible avec différents types de registres blockchain permettrait une interopérabilité du système avec d'autres registres internes aux organisations. Le composant de surveillance mentionné dans l'architecture et non étudié pourrait être associé. La proposition de ce mécanisme de supervision des valeurs de confiance et des identifiants décentralisés répondrait à l'un des principes importants d'une stratégie de sécurité Zero Trust.

Bibliographie

[1] H. A. BREIKI, L. A. QASSEM, K. SALAH, M. H. U. REHMAN et D. SEVTINOVIC. "Decentralized access control for IoT data using blockchain and trusted oracles". In : *IEEE International Conference on Industrial Internet* (2019), p. 248-257. DOI : 10.1109/ICII.2019.00051.

[2] N. A. AALI, A. BAINA et L. ECHABBI. "Tr-OrBAC : Towards a Trust Framework for Collaborative Systems in Critical Information Infrastructures". In : *Journal of Network and Innovative Computing* 4 (2016), p. 106-115.

[3] Temidayo ABAYOMI-ZANNU et Isaac ODUN-AYO. "Cloud identity management - A critical analysis". In : *International MultiConference of Engineers and Computer Scientists* 2239 (2019), p. 170-175. ISSN : 20780958.

[4] B. I. ABDELKRIM, A. BAINA, C. FELTUS, J. AUBERT, M. BELLAFKIH et D. KHADRAOUI. "Coalition-OrBAC : An agent-based access control model for dynamic coalitions". In : *Advances in Intelligent Systems and Computing* 16 (2018), p. 1060-1070.

[5] A ABDUL-RAHMAN et S HAILES. "Using Recommendations for Managing Trust in Distributed Systems". In : *IEEE Malaysia International Conference on Communication* 97 (1997).

[6] Alfarez ABDUL-RAHMAN et Stephen HAILES. "Supporting trust in virtual communities". In : *Proceedings of the Annual Hawaii International Conference on System Sciences* 2000-Janua.c (2000), p. 1-9. ISSN : 15301605.

[7] Binance ACADEMY. "Les Fonctions de Hachage Cryptographie à Clé Publique (PKC)". URL : https://academy.binance.com/fr/articles/what-is-a-digital-signature.

[8] Nawal AIT AALI, Amine BAINA et Loubna ECHABBI. "Trust integration in collaborative access control model for Critical Infrastructures". In : *2015 10th International Conference on Intelligent Systems : Theories and Applications, SITA 2015* (2015). DOI : 10.1109/SITA.2015.7358427.

[9] Ziyad R. ALASHHAB, Mohammed ANBAR, Manmeet Mahinderjit SINGH, Yu-Beng LEAU, Zaher Ali AL-SAI et Sami ABU ALHAYJA'A. "Impact of coronavirus pandemic crisis on technologies and cloud computing applications". In : *Journal of Electronic Science and Technology* 19.1 (mars 2021), p. 100059. ISSN : 1674862X. DOI : 10.1016/j.jnlest.2020.100059.

[10] Mazhar ALI, Samee U. KHAN et Athanasios V. VASILAKOS. "Security in cloud computing : Opportunities and challenges". In : *Information Sciences* (2015). ISSN : 00200255. DOI : 10.1016/j.ins.2015.01.025.

[11] L ALLIANCE. “Introduction to the liberty alliance identity architecture”. In : *March, available online : http ://www. projectliberty. org* (2003), p. 1-14.

[12] Fatimah ALMUZAINI, Sarah ALROMAIH, Alhanoof ALTHNIAN et Heba KURDI. “Whatstrust : A trust management system for whatsapp”. In : *Electronics (Switzerland)* 9.12 (2020), p. 1-17. ISSN : 20799292. DOI : 10.3390/electronics9122190.

[13] BEULAH KURIAN ALUNKAL. “GRID EIGEN TRUST : A Framework for computing reputation in grids”. In : *Zitteliana* 18.1 (2003), p. 22-27.

[14] ANSSI. “Le modèle Zero Trust”. URL : https://www.ssi.gouv.fr/agence/publication/le-modele-zero-trust. *Consulté le 25/11/2022*.

[15] Nick ANTONOPOULOS, Kyriakos KOUKOUMPETSOS et Alex SHAFARENKO. “Access control for agent-based computing : A distributed approach”. In : *Internet Research* 11.1 (2001), p. 55-64. ISSN : 10662243. DOI : 10.1108/10662240110365724.

[16] Michael ARMBRUST, Armando FOX, Rean GRIFFITH, Anthony D. JOSEPH, Randy KATZ, Andy KONWINSKI, Gunho LEE, David PATTERSON, Ariel RABKIN, Ion STOICA et Matei ZAHARIA. “A view of cloud computing”. In : *Communications of the ACM* 53.4 (2010), p. 50-58. ISSN : 00010782. DOI : 10.1145/1721654.1721672.

[17] R. AUSANKA-CRUES. “Methods for access control : Advances and limitations”. In : *Harvey Mudd College* (2001), p. 1-5.

[18] Majid AZADI, Ali EMROUZNEJAD, Fahimeh RAMEZANI et Farookh K. HUSSAIN. “Efficiency measurement of cloud service providers using network data envelopment analysis”. In : *IEEE Transactions on Cloud Computing* 7161.c (2019). ISSN : 21687161. DOI : 10.1109/TCC.2019.2927340.

[19] F. AZZEDIN et M. MAHESWARAN. “Integrating trust into grid resource management systems”. In : *Proceedings of the International Conference on Parallel Processing* 2002-Janua (2002), p. 47-54. ISSN : 01903918. DOI : 10.1109/ICPP.2002.1040858.

[20] Farag AZZEDIN et Muthucumaru MAHESWARAN. “Evolving and managing trust in grid computing systems”. In : *Canadian Conference on Electrical and Computer Engineering* 3 (2002), p. 1424-1429. ISSN : 08407789. DOI : 10.1109/CCECE.2002.1012962.

[21] M. B. SAIDI, A. A. ELKALAM et A. MARZOUK. “TOrBAC : A Trust Organization Based Access Control Model for Cloud Computing Systems”. In : *International Journal of Soft Computing and Engineering* 24 (2012), p. 2231-2307.

[22] M. B. SAIDI et A. MARZOUK. “Multi-Trust_OrBAC : Access Control Model for Multi-Organizational Critical Systems Migrated To the Cloud”. In : *International Journal of Soft Computing and Engineering* 3 (2013), p. 2231-2307.

[23] Z. B. YAHYA, F. B. KTATA et K. GHEDIRA. “MA-MOrBAC : A distributed access control model based on mobile agent for multi-organizational, collaborative and heterogeneous systems”. In : *Risks and Security of Internet and Systems : 12th International Conference, CRiSIS 2017, Dinard, France, September 19-21, 2017, Revised Selected Papers 12* (2018), p. 101-114.

[24] Amine BAINA. “Contrôl d’Accès pour les Grandes Infrastructures Critiques Application au réseau d’énergie électrique”. In : (2009), p. 1-151.

[25] Ricardo BARBOSA, Ricardo SANTOS et Paulo NOVAIS. "Smart Contracts Based on Multi-agent Negotiation". In : *In : International Conference on Practical Applications of Agents and Multi-Agent Systems. Cham : Springer International Publishing*. Cham, 2021, p. 104-114.

[26] Davide BASILE, Valerio GORETTI, Claudio DI CICCIO et Sabrina KIRRANE. "Enhancing Blockchain-Based Processes with Decentralized Oracles". In : *In : International Conference on Business Process Management. Cham : Springer International Publishing*. 2021, p. 102-118.

[27] D. BATTR, F. M. T. BRAZIER, K. P CLARK, M. OEY, A. PAPASPYROU, W. OLIVER, P. WIEDER et W. ZIEGLER. "A Proposal for WS-Agreement Negotiation". In : (2010), p. 233-241.

[28] Bouziane BELDJILALI, Belabbas YAGOUBI, Bouamrane KARIM, Chikhi SALIM et Chourfia ABDELLAH. "Gestion de Confiance dans le Cloud Computing". In : (2016).

[29] La Padula L. J. BELL D. E. "Secure computer system : Unified exposition and multics interpretation". In : March (1976).

[30] Abdeljalil BENIICHE. "A Study of Blockchain Oracles". In : *arXiv :2004.07140* (mars 2020), p. 1-9.

[31] K BIBA. "Integrity considerations for secure computer systems, MTR-3153". In : *Mitre Corporation* (1975).

[32] Mahantesh BIRJE, Praveen S CHALLAGIDAD, Vani S RESHMI et Mahantesh N BIRJE. "Reputation Based Trust Model in Cloud Computing". In : *Internet Things Cloud Comput* 5.5-1 (2017), p. 5-12.

[33] Eleanor BIRRELL et Fred B. SCHNEIDER. "Federated identity management systems : A privacy-based characterization". In : *IEEE Security and Privacy* 11.5 (2013), p. 36-48. ISSN : 15407993. DOI : 10.1109/MSP.2013.114.

[34] Matt BLAZE, Joan FEIGENBAUM et Angelos D. KEROMYTIS. "KeyNote : Trust Management for Public-Key Infrastructures : Position Paper". In : *Security Protocols : 6th International Workshop Cambridge, UK, April 15–17, 1998 Proceedings 6. Springer Berlin Heidelberg* (1998), p. 59-63.

[35] Matt BLAZE, Joan FEIGENBAUM et Jack LACY. "Decentralized trust management". In : *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy* (1996), p. 164-173.

[36] Matt BLAZE, Joan FEIGENBAUM et Martin STRAUSS. "Compliance checking in the policymaker trust management system". In : *Financial Cryptography : Second International Conference, FC'98 Anguilla, British West Indies February 23–25, 1998 Proceedings 2. Springer Berlin Heidelberg* (1998), p. 254-274. DOI : 10.1007/BFb0055488.

[37] D. BONEH, M. DRIJVERS et G. NEVEN. "Compact Multi-signatures for Smaller Blockchains". In : *International Conference on the Theory and Application of Cryptology and Information Security. Cham : Springer International Publishing* (2018), p. 435-464.

[38] D. BONEH, B. LYNN et H. SHACHAM. "Short signatures from the weil pairing". In : *International conference on the theory and application of cryptology and information security. Berlin, Heidelberg : Springer Berlin Heidelberg* (2001), p. 514-532.

[39] Oliver BORCHERT et Allen TAN. “Implementing a Zero Trust”. In : *national insutute of standard and technology (NIST)* March (2020). URL : https://www.nccoe.nist.gov/sites/default/files/legacy-files/zt-arch-project-description-draft.pdf.

[40] R. BUYYA, C. S. YEO, S. VENUGOPAL, J. BROBERG et I. BRANDIC. “Cloud computing and emerging IT platforms : Vision, hype, and reality for delivering computing as the 5th utility”. In : *Future Generation Computer Systems* 25.6 (2009), p. 599-616. ISSN : 0167739X. DOI : 10.1016/j.future.2008.12.001. URL : http://dx.doi.org/10.1016/j.future.2008.12.001.

[41] Davide CALVARESI, Alevtina DUBOVITSKAYA, Jean Paul CALBIMONTE, Kuldar TAVETER et Michael SCHUMACHER. “Multi-agent systems and blockchain : Results from a systematic literature review”. In : *Advances in Practical Applications of Agents, Multi-Agent Systems, and Complexity : The PAAMS Collection : 16th International Conference, PAAMS 2018, Toledo, Spain, June 20–22, 2018, Proceedings 16. Springer International Publishing* (2018), p. 110-126.

[42] K. CAMERON. “The Laws of Identity”. In : *Microsoft Corporation* (2005), p. 8-11. ISSN : 0036-8075.

[43] L. Jean CAMP. “Digital identity”. In : *IEEE Technology and Society Magazine* 23.3 (2004), p. 34-41. ISSN : 02780097. DOI : 10.1109/MTAS.2004.1337889.

[44] Scott CANTOR, John KEMP et OTHERS. “Liberty ID-FF Protocols and Schema Specification”. In : *Version* 183 (2003), p. 1-2.

[45] Scott CANTOR et Tom SCAVO. “Shibboleth architecture.” In : *Protocols and Profiles* 10.16 (2005), p. 29.

[46] “Capgemini et Orange annoncent le projet « Bleu »”. URL : https://www.capgemini.com/fr-fr/news/capgemini-et-orange-annoncent-le-projet-de-creer-bleu-une-societe-qui-fournira-un-âĂL’cloud-de-confianceâĂL’-en-france/.

[47] Rui Costa CARDOSO, Abel J.P. GOMES et Mario M. FREIRE. “A User Trust System for Online Games-Part I : An Activity Theory Approach for Trust Representation”. In : *IEEE Transactions on Computational Intelligence and AI in Games* 9.3 (2017), p. 305-320. ISSN : 1943068X. DOI : 10.1109/TCIAIG.2016.2592965.

[48] Rui Costa CARDOSO, Abel J.P. GOMES et Mário M. FREIRE. “A User trust system for online games-part II : A subjective logic approach for trust inference”. In : *IEEE Transactions on Computational Intelligence and AI in Games* 9.4 (2017), p. 354-368. ISSN : 1943068X. DOI : 10.1109/TCIAIG.2016.2593000.

[49] Sudip CHAKRABORTY et Indrajit RAY. “TrustBAC - Integrating trust relationships into the RBAC model for access control in open systems”. In : *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT* 2006 (2006), p. 49-58.

[50] David C. CHOU. “Cloud computing : A value creation model”. In : *Computer Standards and Interfaces* 38 (2015), p. 72-77. ISSN : 09205489. DOI : 10.1016/j.csi.2014.10.001. URL : http://dx.doi.org/10.1016/j.csi.2014.10.001.

[51] CISA. “Zero Trust Maturity Model”. URL : https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf.

[52] “Cloud Security alliance”. URL : https://cloudsecurityalliance.org.

[53] CLOUD SECURITY ALLIANCE. “State of Cloud Security 2016”. In : (2016).

[54] CLOUD SECURITY ALLIANCE. “Top Threats to Cloud Computing - Pandemic Eleven”. In : *Cloud Security Alliance* 6.August (2022), p. 128. ISSN : 2252-3405.

[55] “Cloud strategies to fuel innovation across Africa”. URL : http://www.worldwideworx.com/cloud2020/. *Consulté le 03/01/2021*.

[56] Piotr COFTA. “Trust, Complexity and Control : Confidence in a Convergent World”. In : *Trust, Complexity and Control : Confidence in a Convergent World* (2007), p. 1-294. DOI : 10.1002/9780470517857.

[57] Angela L. COLETTI, Karen L. SEDATOLE et Kristy L. TOWRY. “The Effect of Control Systems on Trust and Cooperation in Collaborative Environments”. In : *The Accounting Review* 80.2 (avr. 2005), p. 477-500. ISSN : 0001-4826. DOI : 10.2308/accr.2005.80.2.477.

[58] “Collaboration sur le cloud : de quoi s’agit-il et comment cela peut-il aider votre organisation ?” URL : https://fr-fr.workplace.com/blog/cloud-collaboration. *Consulté le 01/07/2023*.

[59] Province of British COLUMBIA. “Digital Credential Services”. URL : https://digital.gov.bc.ca/digital-trust/. *Consulté le 04/06/2023*.

[60] COMMON CRITERIA. “Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model September 2012 Revision 4”. In : *International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15408 Common Criteria, Part 1 :2012* September (2012), p. 93.

[61] “Common Vulnerability Scoring System SIG”. URL : https://www.first.org/cvss/. *Consulté le 05/03/2022*.

[62] Benjamin COSTE et Benjamin COSTE. “Détection contextuelle de cyberattaques par gestion de confiance à bord d ’ un navire”. In : (2019).

[63] F. CUPPENS et N. CUPPENS-BOULAHIA. “Modeling contextual security policies”. In : *International Journal of Information Security* 7.4 (2008), p. 285-305. ISSN : 16155262. DOI : 10.1007/s10207-007-0051-9.

[64] F. CUPPENS, N. CUPPENS-BOULAHIA et C. COMA. “O2O : Virtual private organizations to manage security policy interoperability”. In : *In Information Systems Security : Second International Conference, ICISS 2006, Kolkata, India, December 19-21* Proceeding (2006), p. 101-115.

[65] Frédéric CUPPENS et Alexandre MIÈGE. “Modelling contexts in the Or-BAC model”. In : *Proceedings - Annual Computer Security Applications Conference, ACSAC* 2003-Janua.Acsac (2003), p. 416-425. ISSN : 10639527. DOI : 10.1109/CSAC.2003.1254346.

[66] CYBERARK. “Healthfirst applies an identity security-first approach to implement Zero Trust”. URL : https://www.cyberark.com/customer-stories/healthfirst/?utm_medium=paid_search&utm_source=google&utm_campaign=identity_security&utm_content=identity_security_nov_2022_is_lp_id_71&utm_term=id_71. *Consulté le 10/04/2023*.

[67] Quynh H. DANG. “Secure Hash Standard”. In : (2015).

[68] DCSSI. “La défense en profondeur appliquée aux systèmes d ’ information”. In : (2004), p. 1-51. URL : https://www.ssi.gouv.fr/guide/la-defense-en-profondeur-appliquee-aux-systemes-dinformation/.

[69] “Decentralized Identifiers (DIDs) v1.0”. URL : https://www.w3.org/TR/did-core/.

[70] Robert DEMOLOMBE. "To Trust Information Sources : A Proposal for a Modal Logical Framework". In : *Trust and Deception in Virtual Societies*. Sous la dir. de Cristiano CASTELFRANCHI et Yao-Hua TAN. Dordrecht : Springer Netherlands, 2001, p. 111-124.

[71] Y. DESWARTE et A. A. E. KALAM. "PolyOrBAC : An Access Control Model for Inter-Organizational Web Services". In : *IGI Global* (2009), p. 901-923.

[72] V. P. DINA. "Implementing Community Cloud to Overcome the Problems of Complexity and Security in Business Environment". In : *Indian Journal of Applied Research* 2 (2011), p. 1-3.

[73] Mickael DORIGNY. "Qu'est ce que la défense en profondeur ?" URL : https://www.it-connect.fr/cybersecurite-defense-en-profondeur/#google_vignette. *Consulté le 13/06/2023*.

[74] A. DORRI, S. S. KANHERE et R. JURDAK. "Multi-Agent Systems : A Survey". In : *IEEE Access* 6 (2018), p. 28573-28593. ISSN : 21693536. DOI : 10.1109/ACCESS.2018.2831228.

[75] Kalka DUBEY, Mahmoud Y. SHAMS, S. C. SHARMA, Abdulaziz ALARIFI, Mohammed AMOON et Aida A. NASR. "A Management System for Servicing Multi-Organizations on Community Cloud Model in Secure Cloud Environment". In : *IEEE Access* 7 (2019), p. 159535-159546. ISSN : 2169-3536. DOI : 10.1109/ACCESS.2019.2950110. URL : https://ieeexplore.ieee.org/document/8886574/.

[76] Gary ELLISON, Sun MICROSYSTEMS, John KEMP, Thomas WASON et Peter THOMPSON. "Liberty ID-WSF Web Services Framework Overview". In : (), p. 1-26.

[77] Rino FALCONE, Giovanni PEZZULO et Cristiano CASTELFRANCHI. "A fuzzy approach to a belief-based trust computation". In : *Trust, Reputation, and Security : Theories and Practice : AAMAS 2002 International Workshop, Bologna, Italy, July 15, 2002. Selected and Invited Papers 5. Springer Berlin Heidelberg* (2003), p. 73-86.

[78] Wenjuan FAN, Shanlin YANG, Jun PEI et He LUO. "Building trust into cloud". In : *International Journal of Cloud Computing and Services Science* (2012).

[79] David F. FERRAIOLO et D. Richard KUHN. "Role-Based Access Controls". In : *15th National Computer Security Conference* (1992), p. 554-563.

[80] Mohamed FIRDHOUS, Osman GHAZALI et Suhaidi HASSAN. "Trust Management in Cloud Computing : A Critical Review". In : *International Journal on Advances in ICT for Emerging Regions (ICTer)* 4.2 (sept. 2012), p. 24. ISSN : 1800-4156. DOI : 10.4038/icter.v4i2.4674. URL : https://icter.sljol.info/article/10.4038/icter.v4i2.4674/.

[81] The Jericho FORUM et Hostile WORLD. *Jericho Forum ™ Commandments*. Rapp. tech. May. 2007. URL : https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf.

[82] Hyperledger FOUNDATION. "Hyperledger Aries". URL : https://www.hyperledger.org/projects/aries. *Consulté le 05/07/2023*.

[83] Willem FOURIE. "Cloud computing could be key to speeding up Africa's development." URL : https://theconversation.com/cloud-computing-could-be-key-to-speeding-up-africas-development-121344. *Consulté le 06/03/2020*.

[84] F FUKUYAMA. "Trust : The Social Virtues and the Creation of Prosperity". In : *Free, New York* (1995).

[85] Diego GAMBETTA. "Can We Trust Trust ?" In : *Trust : Making and breaking cooperative relations* 13 (2000), p. 213-237.

[86] Emmanuel GARBOLINO et Franck GUARNIERI. "Concept de défense en profondeur : contribution à la sécurité des ICPE". In : *Techniques de l'Ingénieur*. Référence SE2065. Editions T.I., 2012, Référence SE2065 -14 pages. URL : https://minesparis-psl.hal.science/hal-00720761.

[87] Saurabh Kumar GARG, Steve VERSTEEG et Rajkumar BUYYA. "A framework for ranking of cloud computing services". In : *Future Generation Computer Systems* 29.4 (juin 2013), p. 1012-1023. ISSN : 0167739X. DOI : 10.1016/j.future.2012.06.006. URL : http://dx.doi.org/10.1016/j.future.2012.06.006https://linkinghub.elsevier.com/retrieve/pii/S0167739X12001422.

[88] GARTNER. "5 technologies influentes présentées dans le rapport Impact Radar de Gartner sur les technologies et tendances émergentes pour l'année 2022". URL : https://www.gartner.fr/fr/articles/5-technologies-influentes-presentees-dans-le-rapport-impact-radar-de-gartner-sur-les-technologies-et-tendances-emergentes-pour-2022. *Consulté le 01/07/2023*.

[89] GARTNER. "Gartner Identifies Three Factors Influencing Growth in Security Spending". URL : https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i. *Consulté le 10/02/2023*.

[90] GARTNER. "Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025". URL : https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending. *Consulté le 28/04/2023*.

[91] Alexis Feringa GARY STONEBURNER Alice Goguen. "Risk Management Guide for Information Technology Systems". In : *NIST Special Publication 800-30* (2002), p. 800-300.

[92] Anu GOPALAKRISHNAN. "Cloud Computing Identity Management". In : *SETLabs Briefings, InfoSys* 7.7 (2009), p. 45-55.

[93] Tyrone GRANDISON et Morri SLOMAN. "A survey of trust in internet applications". In : *IEEE Communications Surveys & Tutorials* 3.4 (2009), p. 2-16. ISSN : 1553-877X. DOI : 10.1109/comst.2000.5340804.

[94] Liangmin GUO, Hao YANG, Kaixuan LUAN, Yonglong LUO, Liping SUN et Xiaoyao ZHENG. "A trust management model based on mutual trust and a reward-with-punishment mechanism for cloud environments". In : *Concurrency and Computation : Practice and Experience* 33.16 (2021), p. 1-20. ISSN : 15320634. DOI : 10.1002/cpe.6283.

[95] Nils GURA, Arun PATEL, Arvinderpal WANDER, Hans EBERLE et Sheueling Chang SHANTZ. "Comparing elliptic curve cryptography and RSA on 8-Bit CPUs". In : *Cryptographic Hardware and Embedded Systems-CHES 2004 : 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings 6. Springer Berlin Heidelberg* (2004), p. 119-132.

[96] Sheikh Mahbub HABIB, Sebastian RIES et Max MUHLHAUSER. "Towards a trust management system for cloud computing". In : *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011* (2011), p. 933-939. DOI : 10.1109/TrustCom.2011.129.

[97] Michael A. HARRISON, Walter L. RUZZO et Jeffrey D. ULLMAN. "Protection in Operating Systems". In : *Communications of the ACM* 19.8 (1976), p. 461-471. ISSN : 15577317. DOI : 10.1145/360303.360333.

[98] Yuanhang HE, Daochao HUANG, Lei CHEN, Yi NI et Xiangjie MA. "A Survey on Zero Trust Architecture : Challenges and Future Trends". In : *Wireless Communications and Mobile Computing* 2022 (juin 2022). Sous la dir. d'Yan HUO, p. 1-13. ISSN : 1530-8677. DOI : 10.1155/2022/6476274.

[99] Ferry HENDRIKX, Kris BUBENDORFER et Ryan CHARD. "Reputation systems : A survey and taxonomy". In : *Journal of Parallel and Distributed Computing* 75 (2015), p. 184-197. ISSN : 07437315. DOI : 10.1016/j.jpdc.2014.08.004.

[100] Nadia HOCINE. "Agent-based access control framework for enterprise content management". In : *Multiagent and Grid Systems* 17.2 (2021), p. 129-143. ISSN : 18759076. DOI : 10.3233/MGS-210346.

[101] The White HOUSE. "Executive Order on Improving the Nation's Cybersecurity". URL : https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/?utm_source=link%5C. *Consulté le 23/05/2023*.

[102] Zhengyu HU, Lianzhong LIU et Chen WANG. "Organization domain trust evaluation model in federa environment based on subjective logic". In : *Proceedings - 2011 International Conference of Information Technology, Computer Engineering and Management Sciences, ICM 2011* 1 (2011), p. 380-384. DOI : 10.1109/ICM.2011.62.

[103] John HUGHES et Eve MALER. "SAML v2.0 Technical Overview". In : *OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08* 13 (2005), p. 12.

[104] Phil HUNT, K GRIZZLE, E WAHLSTROEM et C MORTIMORE. "System for cross-domain identity management : core schema". In : (2016), p. 1-23.

[105] John Rofrano IBM. "Web Services Agreement Specification (WS-Agreement)". In : (2007), p. 1-81.

[106] H. IDRISSI, M. ENNAHBAOUI, E. M. SOUIDI, A. REVEL et S. ELHAJJI. "Access control using mobile agents". In : *International Conference on Multimedia Computing and Systems* (2014), p. 1216-1221. DOI : 10.1109/ICMCS.2014.6911154.

[107] I. INDU, P. M.Rubesh ANAND et Vidhyacharan BHASKAR. "Identity and access management in cloud environment : Mechanisms and challenges". In : *Engineering Science and Technology, an International Journal* 21.4 (2018), p. 574-588. ISSN : 22150986. DOI : 10.1016/j.jestch.2018.05.010. URL : https://doi.org/10.1016/j.jestch.2018.05.010.

[108] ISO. "ISO/IEC 24760-3 :2016 Information technology — Security techniques — A framework for identity management — Part 3 : Practice". In : 1 (2016), p. 1-31.

[109] Gouvernement du Canada ITSP.50.104. "Guide sur la défense en profondeur pour les services fondés sur l'infonuagique". In : (2020).

[110] A. JØSANG. "Subjective Logic". In : *Cham : Springer* 3 (2016).

[111] A. JØSANG, S. POPE et R. HAYWARD. "Trust Network Analysis with Subjective Logic". In : *Conferences in Research and Practice in Information Technology Series (2006)* 48 (2006), p. 85-94.

[112] Audun JOSANG. "The consensus operator for combining beliefs". In : *Artificial Intelligence* 141.1-2 (2002), p. 157-170. ISSN : 00043702. DOI : 10.1016/S0004-3702(02)00259-X.

[113] Audun JØSANG et Touhid BHUIYAN. "Optimal trust network analysis with subjective logic". In : *Proceedings - 2nd Int. Conf. Emerging Security Inf., Systems and Technologies, SECURWARE 2008, Includes DEPEND 2008 : 1st Int. Workshop on Dependability and Security in Complex and Critical Inf. Sys.* (2008), p. 179-184. DOI : 10.1109/SECURWARE.2008.64.

[114] Audun JØSANG, John FABRE, Brian HAY, James DALZIEL et Simon POPE. "Trust requirements in identity management". In : *Conferences in Research and Practice in Information Technology Series* 44 (2005), p. 99-108. ISSN : 14451336.

[115] Audun JØSANG, Elizabeth GRAY et Michael KINATEDER. "Analysing Topologies of Transitive Trust". In : *Proceedings of the First International Workshop on Formal Aspects in Security & Trust (FAST2003). Pisa, Italy* (2003), p. 9-22.

[116] Audun JØSANG, Roslan ISMAIL et Colin BOYD. "A survey of trust and reputation systems for online service provision". In : *Decision Support Systems* 43.2 (2007), p. 618-644. ISSN : 01679236. DOI : 10.1016/j.dss.2005.05.019.

[117] Audun JØSANG et Simon POPE. "User Centric Identity Management". In : *In AusCERT Asia Pacific information technology security conference* 22 (2005), p. 2005. ISSN : 00121096.

[118] V. JOVANOVIKJ, D. GABRIJELČIČ et T. KLOBUČAR. "A conceptual model of security context". In : *International Journal of Information Security* 13.6 (2014), p. 571-581. ISSN : 16155270. DOI : 10.1007/s10207-014-0229-x.

[119] A. A. El KALAM et Y. DESWARTE. "Multi-OrBAC : A New Access Control Model for Distributed, Heterogeneous and Collaborative Systems". In : *8th IEEE International Symposium on Systems and Information Security* 1 (2006).

[120] A. A.E. KALAM, R. E. BAIDA, P. BALBIANI, S. BENFERHAT, F. CUPPENS, Y. DESWARTE, A. MIEGE, C. SAUREL et G. TROUESSIN. "Organization based access control". In : *IEEE 4th International Workshop on Policies for Distributed Systems and Networks* May 2014 (2003), p. 120-131. DOI : 10.1109/POLICY.2003.1206966.

[121] Jyri KALLELA. "Federated Identity Management Solutions". In : *In TKK T-110.5190 Seminar on Internetworking* (déc. 2008), p. 1-8. ISSN : 0018-9162. DOI : 10.1109/MC.2005.408. URL : http://ieeexplore.ieee.org/document/1556498/.

[122] Sepandar D. KAMVAR, Mario T. SCHLOSSER et Hector GARCIA-MOLINA. "The EigenTrust algorithm for reputation management in P2P networks". In : *Proceedings of the 12th International Conference on World Wide Web, WWW 2003* (2003), p. 640-651. DOI : 10.1145/775152.775242.

[123] Sepandar D. KAMVAR, Mario T. SCHLOSSER et Hector GARCIA-MOLINA. "The Eigentrust algorithm for reputation management in P2P networks". In : (2003), p. 640. DOI : 10.1145/775240.775242.

[124] Collins KARIUKI. "Comment utiliser la défense en profondeur pour protéger vos données". URL : https://geekflare.com/fr/defense-in-depth/. *Consulté le 03/12/2022*.

[125] Shweta KAUSHIK et Charu GANDHI. "Multi-level Trust Agreement in Cloud Environment". In : *2019 12th International Conference on Contemporary Computing, IC3 2019* (2019), p. 1-5. DOI : 10.1109/IC3.2019.8844933.

[126] John KINDERVAG. "Applying zero trust to the extended enterprise." In : *Forrester Research, Cambridge, MA, Rep. E-RES60253* (2011), p. 1-8.

[127] By Neal KOBLITZ. "Elliptic Curve Cryptosystems". In : 4.177 (1987), p. 203-209.

[128] Jiro KONDO, Danielle LI et Dimitris PAPANIKOLAOU. "Trust, Collaboration, and Economic Growth". In : *Management Science* 67.3 (mars 2021), p. 1825-1850. ISSN : 0025-1909. DOI : 10.1287/mnsc.2019.3545.

[129] Mourad KRIM. "Le cloud souverain favoriserait la collaboration et le développement d'un écosystème de partage des données". URL : https://itsocial.fr/enjeux-it/enjeux-strategie/dsi/le-cloud-souverain-favoriserait-la-collaboration-et-accelererait-le-developpement-dun-ecosysteme-de-partage-des-donnees/. *Consulté le 08/01/2023*.

[130] Rakesh KUMAR et Rinkaj GOYAL. "Performance based Risk driven Trust (PRTrust) : On modeling of secured service sharing in peer-to-peer federated cloud". In : *Computer Communications* 183.June 2021 (fév. 2022), p. 136-160. DOI : 10.1016/j.comcom.2021.11.013.

[131] Heba KURDI, Auhood ALFARIES, Abeer AL-ANAZI, Sara ALKHARJI, Maimona ADDEGAITHER, Lina ALTOAIMY et Syed Hassan AHMED. "A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments". In : *Journal of Supercomputing* 75.7 (2019), p. 3534-3554. ISSN : 15730484. DOI : 10.1007/s11227-018-2669-y. URL : https://doi.org/10.1007/s11227-018-2669-y.

[132] Heba KURDI, Bushra ALSHAYBAN, Lina ALTOAIMY et Shada ALSALAMAH. "TrustyFeer : A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds". In : *Wireless Communications and Mobile Computing* 2018 (2018). ISSN : 15308677. DOI : 10.1155/2018/1073216.

[133] Butler W LAMPSON. "The following paper by Butler Lampson has been frequently refer- Because the original is not widely available , we are re- printing it here . If the paper is referenced in published work , the citation should read : " Lampson , B . W ., " Protection , " i". In : *Information Sciences* (1974), p. 18-24. DOI : 10.1145/775265.775268.

[134] Amy N LANGVILLE et Carl D MEYER. *Google's PageRank and beyond : The science of search engine rankings*. Princeton university press, 2006.

[135] Rabia LATIF, Syeda Hadia AFZAAL et Seemab LATIF. "A novel cloud management framework for trust establishment and evaluation in a federated cloud environment". In : *Journal of Supercomputing* 77.11 (2021), p. 12537-12560. ISSN : 15730484. DOI : 10.1007/s11227-021-03775-8. URL : https://doi.org/10.1007/s11227-021-03775-8.

[136] M. LAURENT et S. BOUZEFRANE. *La gestion des identités numériques*. ISTE. 2015, p. 284. ISBN : 978-1-78405-056-6.

[137] J. David LEWIS et Andrew WEIGERT. "Trust as a social reality". In : *Social Forces* 63.4 (1985), p. 967-985. ISSN : 15347605. DOI : 10.1093/sf/63.4.967.

[138] Y. LI, N. CUPPENS-BOULAHIA, J. M. CROM, F. CUPPENS et V. FREY. "Expression and enforcement of security policy for virtual resource allocation in IaaS cloud". In : *ICT Systems Security and Privacy Protection : 31st IFIP TC 11 International Conference, SEC 2016, Ghent, Belgium, May 30-June 1, 2016, Proceedings 31. Springer International Publishing* (2016), p. 105-118.

[139] X. LIU et J. FENG. "Trusted Blockchain Oracle Scheme Based on Aggregate Signature". In : *Journal of Computer and Communications* 09.03 (2021), p. 95-109. ISSN : 2327-5219. DOI : 10.4236/jcc.2021.93007.

[140] Luis F. LUNA-REYES. "Trust and Collaboration in Interagency Information Technology Projects". In : *SSRN Electronic Journal* (2006), p. 1-32. ISSN : 1556-5068. DOI : 10.2139/ssrn.2122102.

[141] E MALER et D REED. "The Venn of Identity : Options and Issues in Federated Identity Management". In : *IEEE Security and Privacy* 6.2 (2008), p. 16 -23. DOI : 10.1109/MSP.2008.50.

[142] T. MANOJ, K. MAKKITHAYA et V. G. NARENDRA. "A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records". In : *Cogent Engineering* 9.1 (2022). ISSN : 23311916. DOI : 10.1080/23311916.2022.2035134.

[143] S. P. MARSH. "Formalising trust as a computational concept." Thèse de doct. 1994.

[144] Karolina MARZANTOWICZ et Lukasz PACIORKOWSKI. "Community cloud : Closing the gap between public and private". In : *Handbook of Research on End-to-End Cloud Computing Architecture Design* (2016), p. 39-55. DOI : 10.4018/978-1-5225-0759-8.ch003.

[145] Paolo MASSA et Paolo AVESANI. "Trust metrics on controversial users : Balancing between tyranny of the majority and echo chambers". In : *International Journal on Semantic Web and Information Systems* 3.1 (2007), p. 39-64. ISSN : 15526291. DOI : 10.4018/jswis.2007010103.

[146] Ulf MATTSSON. "Zero Trust Architecture". In : *Controlling Privacy and the Use of Data Assets*. June. Boca Raton : CRC Press, mai 2021, p. 127-134. DOI : 10.1201/9781003189664-11.

[147] Stuart MCCLURE, Shanit GUPTA, Carric DOOLEY, Vitaly ZAYTSEV, Xiao Bo CHEN, Kris KASPERSKY, M SPOHN et R PERMEH. "Protecting your critical assets-lessons learned from operation aurora". 2010. URL : http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

[148] Adis MEDIĆ. "Survey of Computer Trust and Reputation Models – The Literature Overview". In : *International Journal of Information and Communication Technology Research* 2.3 (2012).

[149] Peter MELL, Jim DRAY et James SHOOK. "Smart Contract Federated Identity Management without Third Party Authentication Services". In : *LNI,Gesellschaft für Informatik* (juin 2019), p. 37-48. ISSN : 16175468.

[150] Peter MELL et Timothy GRANCE. "The NIST Definition of Cloud Computing". In : *National Institute of Science and Technology, Special Publication* 800.2011 (2011), p. 145.

[151] Victor S. MILLER. "Use of Elliptic Curves in Cryptography". In : *Conference on the theory and application of cryptographic techniques. Berlin, Heidelberg : Springer Berlin Heidelberg* (1985), p. 417-426.

[152] KONICA MINOLTA. "L'informatique, une source de frustration pour les PME". URL : https://www.konicaminolta.fr/fr-fr/news/une-nouvelle-enquete-de-konica-minolta-revele-que-les-pme-se-contentent-dâĂŹune-informatique-sous-perf. *Consulté le 08/01/2022*.

[153] J. E. MOKHTARI, A. A. E. KALAM, S. BENHADDOU et J. P. LEROY. "Dynamic Management of Security Policies in PrivOrBAC". In : *International Journal of Advanced Computer Science and Applications* 12.6 (2021), p. 693-701. ISSN : 21565570. DOI : 10.14569/IJACSA.2021.0120681.

[154] Simnikiwe MZEKANDABA. "Africa embraces cloud even as security fears persist". URL : https://www.itweb.co.za/content/Kjlyrvw1P3DMk6am. *Consulté le 03/01/2021*.

[155] Louis NAUGES. "Cloud communautaire : la troisième voie - Louis Naugès". URL : https://nauges.typepad.com/my_weblog/2011/04/cloud-communautaire-la-troisiÃÍme-voie-.html. *Consulté le 09/01/2022*.

[156] NETAPP. "2023 Cloud Complexity Report". In : March (2023). URL : https://www.netapp.com/company/cloud-complexity-report/.

[157] L NIKLAS. "Trust and power". In : *Trans. Howard Davis, John Raffan, and Kathryn Rooney. Chichester, UK : John Wiley & Sons.* (1979).

[158] NIST. "National Vulnerabilitity Database". URL : https://nvd.nist.gov/vuln-metrics/cvss. *Nist.gov*.

[159] Talal H. NOOR et Quan Z. SHENG. "Trust as a service : A framework for trust management in cloud environments". In : *Web Information System Engineering–WISE 2011 : 12th International Conference, Sydney, Australia, October 13-14, 2011. Proceedings 12. Springer Berlin Heidelberg* (2011), p. 314-321.

[160] Talal H. NOOR, Quan Z. SHENG, Sherali ZEADALLY et Jian YU. "Trust management of services in cloud environments : Obstacles and solutions". In : *ACM Computing Surveys* 46.1 (2013), p. 1-30. ISSN : 03600300. DOI : 10.1145/2522968.2522980.

[161] "OAuth 2.0". URL : https://oauth.net/2/.

[162] A. S. OMAR et O. BASIR. "Decentralized Identifiers and Verifiable Credentials for Smartphone Anticounterfeiting and Decentralized IMEI Database". In : *Canadian Journal of Electrical and Computer Engineering* 43.3 (2020), p. 174-180. ISSN : 08408688. DOI : 10.1109/CJECE.2020.2970737.

[163] S. P. OTTA et S. PANDA. "Decentralized Identity and Access Management of Cloud for Security as a Service". In : *14th International Conference on Communication Systems and Networks* (2022), p. 299-303. DOI : 10.1109/COMSNETS53615.2022.9668529.

[164] F. PACI, A. SQUICCIARINI et N. ZANNONE. "Survey on access control for community-centered collaborative systems". In : *ACM Computing Surveys* 51.1 (2018). ISSN : 15577341. DOI : 10.1145/3146025.

[165] Konstantinos PAPADAKIS-VLACHOPAPADOPOULOS, Román Sosa GONZÁLEZ, Ioannis DIMOLITSAS, Dimitrios DECHOUNIOTIS, Ana Juan FERRER et Symeon PAPAVASSILIOU. "Collaborative SLA and reputation-based trust management in cloud federations". In : *Future Generation Computer Systems* 100 (2019), p. 498-512. ISSN : 0167739X. DOI : 10.1016/j.future.2019.05.030. URL : https://doi.org/10.1016/j.future.2019.05.030.

[166] Nathan PARDE. "Zero-trust architecture may hold the answer to cybersecurity insider threats | MIT News | Massachusetts Institute of Technology". URL : https://news.mit.edu/2022/zero-trust-architecture-may-hold-answer-cybersecurity-insider-threats-0517. *Consulté le 01/01/2023*.

[167] S. PEARSON. "Privacy, Security and Trust in Cloud Computing". In : *Springer London*. 2013, p. 3-42.

[168] Milan PETKOVIC et Willem JONKER. *Security, Privacy and Trust in Modern Data Management (Data-Centric Systems and Applications)*. 2007, p. vi-471. ISBN : 9783540698609. URL : http://portal.acm.org/citation.cfm?id=1296121.

[169] POOJAGOYAL et Sukhvinder Singh DEORA. *A Review : Trust Management Techniques Used for Cloud Computing*. T. 1. 2022, p. 117-132.

[170] Uthpala Subodhani PREMARATHNE, Ibrahim KHALIL, Zahir TARI et Albert ZOMAYA. "Cloud-Based Utility Service Framework for Trust Negotiations Using Federated Identity Management". In : *IEEE Transactions on Cloud Computing* 5.2 (2017), p. 290-302. ISSN : 21687161. DOI : 10.1109/TCC.2015.2404816.

[171] A. Shenbaga Bharatha PRIYA et R. S. BHUVANESWARAN. "Cloud service recommendation system based on clustering trust measures in multi-cloud environment". In : *Journal of Ambient Intelligence and Humanized Computing* 12 (2020), p. 7029-7038.

[172] David PUZAS. "Modèle de responsabilité partagée". URL : https://www.crowdstrike.fr/cybersecurity-101/cloud-security/shared-responsibility-model/. *Consulté le 2605/2023*.

[173] Lais RASMUSSON et Sverker JANSSON. "Simulated social control for secure internet commerce". In : *Proceedings New Security Paradigms Workshop* Part F1294 (1996), p. 18-25. DOI : 10.1145/304851.304857.

[174] David RECORDON et Drummond REED. "OpenID 2.0 : A platform for user-centric identity management". In : *Proceedings of the Second ACM Workshop on Digital Identity Management, DIM 2006. Co-located with the 13th ACM Conference on Computer and Communications Security, CCS'06* (2006), p. 11-16. DOI : 10.1145/1179529.1179532.

[175] R. RIVEST. "The MD5 message-digest algorithm". In : *rfc1321* (1992).

[176] R. L. RIVEST, A. SHAMIR et L. ADLEMAN. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In : *Communications of the ACM* 21.2 (1978), p. 120-126. ISSN : 15577317. DOI : 10.1145/359340.359342.

[177] A. RONDELET. "A note on anonymous credentials using BLS signatures". In : *arXiv :2006.05201* (2020), p. 1-19.

[178] Scott ROSE, Oliver BORCHERT, Stu MITCHELL et Sean CONNELLY. *Zero Trust Architecture*. Rapp. tech. Gaithersburg, MD : National Institute of Standards et Technology, août 2020, p. 49. DOI : 10.6028/NIST.SP.800-207.

[179] Sini RUOHOMAA et Lea KUTVONEN. "Trust management survey". In : *International Conference on Trust Management* (2005), p. 77-92.

[180] Ravi S SANDHU, Hal L FEINSTEIN, Charles E YOUMAN et Edward J COYNE. "RolemBased Access Control Models m". In : 29.2 (1996), p. 38-47.

[181] Boonyarith SAOVAPAKHIRAN et Michael DEVETSIKIOTIS. "Enhancing computing power by exploiting underutilized resources in the community cloud". In : *IEEE International Conference on Communications* (2011). ISSN : 05361486. DOI : 10.1109/icc.2011.5962544.

[182] N. SATOSHI. "Bitcoin : A Peer-to-Peer Electronic Cash System". 2020.

[183] Karen SCARFONE et Peter MELL. "An analysis of CVSS version 2 vulnerability scoring". In : *2009 3rd International Symposium on Empirical Software Engineering and Measurement, ESEM 2009* (2009), p. 516-525. DOI : 10.1109/ESEM.2009.5314220.

[184] V. SCOCA, R. B. URIARTE et R. D. NICOLA. "Smart Contract Negotiation in Cloud Computing". In : *IEEE International Conference on Cloud Computing* 2017-June (2017), p. 592-599. ISSN : 21596190. DOI : 10.1109/CLOUD.2017.81.

[185] N. SELVANATHAN, D. JAYAKODY et V. DAMJANOVIC-BEHRENDT. "Federated identity management and interoperability for heterogeneous cloud platform ecosystems". In : *ACM International Conference Proceeding Series* (2019). DOI : 10.1145/3339252.3341492.

[186] Business SFR. "Top 5 des cyberattaques les plus emblématiques depuis 3 ans". URL : https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html. *Consulté le 03/12/2022*.

[187] Wanita SHERCHAN, Surya NEPAL et Cecile PARIS. "A survey of trust in social networks". In : *ACM Computing Surveys* 45.4 (2013), p. 1-33. ISSN : 03600300. DOI : 10.1145/2501654.2501661.

[188] P. G. SHYNU et K. JOHN SINGH. "A comprehensive survey and analysis on access control schemes in cloud environment". In : *Cybernetics and Information Technologies* 16.1 (2016), p. 19-38. ISSN : 13144081. DOI : 10.1515/cait-2016-0002.

[189] Jane SIEGEL et Jeff PERDUE. "Cloud services measures for global use : The Service Measurement Index (SMI)". In : *Annual SRII Global Conference, SRII* (2012), p. 411-415. ISSN : 21660778. DOI : 10.1109/SRII.2012.51.

[190] Kwang Mong SIM. "Agent-based approaches for intelligent intercloud resource allocation". In : *IEEE Transactions on Cloud Computing* 7.2 (2019), p. 442-455. ISSN : 21687161. DOI : 10.1109/TCC.2016.2628375.

[191] Florian SKOPIK, Daniel SCHALL et Schahram DUSTDAR. "Start trusting strangers ? Bootstrapping and prediction of trust". In : *International conference on web information systems engineering. Berlin, Heidelberg : Springer Berlin Heidelberg* (2009), p. 275-289.

[192] Georgios SPANOS, Angeliki SIOZIOU et Lefteris ANGELIS. "WIVSS : A new methodology for scoring information systems vulnerabilities". In : *ACM International Conference Proceeding Series* (2013), p. 83-90. DOI : 10.1145/2491845.2491871.

[193] Steffen STAAB, Bharat BHARGAVA, Leszek LILIEN, Arnon ROSENTHAL, Marianne WINSLETT, Morris SLOMAN, Tharam S. DILLON, Elizabeth CHANG, Farookh Khadeer HUSSAIN, Wolfgang NEJDL, Daniel OLMEDILLA et Vipul KASHYAP. "The pudding of trust". In : *IEEE Intelligent Systems* 19.5 (2004), p. 74-88. ISSN : 15411672. DOI : 10.1109/MIS.2004.52.

[194] William STALLINGS et Mohit P TAHILIANI. "Cryptography and network security : principles and practice, vol. 6". In : *editor : Pearson London* (2014).

[195] International Organization for STANDARDIZATION. "Risk management—Vocabulary". In : *ISO guide 73 : 2009* (2009).

[196] Ecole SUPERIEURE et D E Genie INFORMATIQUE. "Systemes De Protection Contre". In : (2008).

[197] Thasni T, C KALAIARASAN et K A VENKATESH. "Cloud Service Selection using DEA based on SMI Attributes". In : *International Journal of Engineering and Advanced Technology* 9.4 (2020), p. 850-855. DOI : 10.35940/ijeat.d7908.049420.

[198] Hamed TABRIZCHI et Marjan KUCHAKI RAFSANJANI. "A survey on security challenges in cloud computing : issues, threats, and solutions". In : *The Journal of Supercomputing* 76.12 (déc. 2020), p. 9493-9532. DOI : 10.1007/s11227-020-03213-1.

[199] Erzhena TCYDENOVA, Byoungjin SEOK, Minjeong CHO et Changhoon LEE. "Decentralized Access Control for Internet of Things Using Decentralized Identifiers and Multi-signature Smart Contracts". In : *International Conference on Platform Technology and Service*. IEEE, août 2022, p. 66-70. ISBN : 978-1-6654-5957-0. DOI : 10.1109/PlatCon55845.2022.9932120.

[200] W. T.Luke TEACY, Jigar PATEL, Nicholas R. JENNINGS et Michael LUCK. "TRAVOS : Trust and reputation in the context of inaccurate information sources". In : *Autonomous Agents and Multi-Agent Systems* 12.2 (2006), p. 183-198. ISSN : 13872532. DOI : 10.1007/s10458-006-5952-x.

[201] Source THE, Management REVIEW, No JUL, Denise M ROUSSEAU et Ronald S BURT. "Introduction to Special Topic Forum : Not so Different after All : A Cross-Discipline View of Trust". In : 23.3 (1998), p. 393-404.

[202] THE CLOUD SERVICE MEASUREMENT INITIATIVE CONSORTIUM (CSMIC). "Service Measurement Index Framework Version 2.1". In : July (2014).

[203] Manoj V. THOMAS et K. CHANDRA SEKARAN. "Agent-based approach for distributed access control in cloud environments". In : *Proceedings of the 2013 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2013* (2013), p. 1628-1633. DOI : 10.1109/ICACCI.2013.6637425.

[204] K. TOUMI, C. ANDRÉS et A. CAVALLI. "Trust-OrBac : A trust access control model in multi-organization environments". In : *International Conference on Information Systems Security. Berlin, Heidelberg : Springer Berlin Heidelberg* (2012), p. 89-103.

[205] UIT-T. "Recommandation UIT-T Y.2720 : Cadre de gestion d'identité des réseaux NGN". In : (2009).

[206] "Verifiable Credentials Data Model v1.1". URL : https://www.w3.org/TR/vc-data-model/.

[207] David WALDEN. "50th Anniversary of MIT's Compatible Time-Sharing System". In : *IEEE Annals of the History of Computing* 33.4 (2011), p. 84-85.

[208] Qingxian WANG. "The application of elliptic curves cryptography in embedded systems". In : *ICESS 2005 - Second International Conference on Embedded Software and Systems* 2005 (2005), p. 527-598. DOI : 10.1109/ICESS.2005.90.

[209] Shuai WANG, Liwei OUYANG, Yong YUAN, Xiaochun NI, Xuan HAN et Fei-Yue WANG. "Blockchain-Enabled Smart Contracts : Architecture, Applications, and Future Trends". In : *IEEE Transactions on Systems, Man, and Cybernetics : Systems* 49.11 (nov. 2019), p. 2266-2277. ISSN : 2168-2216. DOI : 10.1109/TSMC.2019.2895123.

[210] Xiaoyun WANG et Hongbo YU. "Finding collisions in the full SHA-1". In : *CRYPTO 2005* (2005).

[211] Xiaoyun WANG et Hongbo YU. "How to break MD5 and other hash functions". In : *Annual international conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg : Springer Berlin Heidelberg* (2005), p. 19-35.

[212] Rory WARD et Betsy BEYER. "Beyondcorp : A new approach to enterprise security". In : Apress, 2014.

[213] Ahmad Samer WAZAN, Romain LABORDE, David W. CHADWICK, Francois BARRERE, Abdelmalek BENZEKRI, Mustafa KAIIALI et Adib HABBAL. "Trust management for public key infrastructures : Implementing the X.509 trust broker". In : *Security and Communication Networks* 2017 (2017). ISSN : 19390122. DOI : 10.1155/2017/6907146.

[214] Horst F. WEDDE et Mario LISCHKA. "Role-based access control in ambient and remote space". In : *Proceedings of ACM Symposium on Access Control Models and Technologies (SACMAT 2002)* 9 (2004), p. 21-30. DOI : 10.1145/990036.990040.

[215] Marianne WINSLETT, Ting YU, Kent E. SEAMONS, Adam HESS, Jared JACOBSON, Ryan JARVIS, Bryan SMITH et Lina YU. "Negotiating trust on the web". In : *IEEE Internet Computing* 6.6 (2002), p. 30-37. ISSN : 10897801. DOI : 10.1109/MIC.2002.1067734.

[216] M. WOOLDRIDGE. *Reasoning about Rational Agents*. The MIT Press, 2003, p. 241. ISBN : 9780262515566.

[217] Recommandation UIT-T X.811. "TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS CADRES DE SÉCURITÉ POUR SYSTÈMES OUVERTS : CADRE D'AUTHENTIFICATION". In : 811 ().

[218] ANSI X9.62. "Public Key Cryptography for the Financial Services Industry : The Elliptic Curve Digital Signature Algorithm (ECDSA)". In : (1999).

[219] Zeineb Ben YAHYA, Farah Barika KTATA et Khaled GHEDIRA. "Multi-organizational Access Control Model Based on Mobile Agents for Cloud Computing". In : *International Conference on Web Intelligence, WI 2016* (2017), p. 656-659. DOI : 10.1109/WI.2016.0116.

[220] Reda YAICH. "Trust management systems : A retrospective study on digital trust". In : *Cyber-Vigilance and Digital Trust : Cyber Security in the Era of Cloud Computing and IoT* (2019), p. 51-103. DOI : 10.1002/9781119618393.ch2.

[221] Shalanda D. YOUNG. "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles". In : *Executive Office of the President* 26633.January (2022), p. 1-29. URL : https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[222] Bin YU et Munindar P. SINGH. "An evidential model of distributed reputation management". In : *Proceedings of the International Conference on Autonomous Agents* 2 (2002), p. 294-301. DOI : 10.1145/544741.544809.

[223] Y. YUAN et F. Y. WANG. "Blockchain and Cryptocurrencies : Model, Techniques, and Applications". In : *IEEE Transactions on Systems, Man, and Cybernetics : Systems* 48.9 (2018), p. 1421-1428. ISSN : 21682232. DOI : 10.1109/TSMC.2018.2854904.

[224] Giorgos ZACHARIA et Pattie MAES. "Trust management through reputation mechanisms". In : *Applied Artificial Intelligence* 14.9 (2000), p. 881-907. ISSN : 10876545. DOI : 10.1080/08839510050144868.

[225] Runfang ZHOU et Kai HWANG. "PowerTrust : A robust and scalable reputation system for trusted peer-to-peer computing". In : *IEEE Transactions on Parallel and Distributed Systems* 18.4 (2007), p. 460-473. ISSN : 10459219. DOI : 10.1109/TPDS.2007.1021.

[226] Runfang ZHOU et Kai HWANG. "Trust overlay networks for global reputation aggregation in P2P grid computing". In : *20th International Parallel and Distributed Processing Symposium, IPDPS 2006* 2006 (2006). DOI : 10.1109/IPDPS.2006.1639268.

Titre : Stratégie de sécurité Zero Trust dans un environnement de cloud communautaire

Mots clés : Zero Trust, Confiance, identités décentralisées, Blockchain, Contrôle d'accès, Cloud communautaire

Résumé : De nos jours, la société est caractérisée par une mobilité importante des populations et des besoins croissants en termes de partage de gros volumes de données sensibles au sein des entreprises et de collaboration avec des organisations partenaires ou concurrentes. Ces collaborations procurent de nombreux avantages aux entreprises en termes d'évolutivité et de croissance économique. Cependant, les systèmes informatiques de ces organisations sont exposés à divers types de menaces et cyberattaques de plus en plus sophistiquées. Les stratégies traditionnelles de sécurisation des infrastructures fondées sur le périmètre ne sont plus suffisantes. Le modèle de sécurité Zero Trust est une approche de cybersécurité qui considère toutes les entités d'une infrastructure comme potentiellement vulnérables en tout temps et en tout lieu. Cette stratégie se positionne comme une réponse à la problématique de sécurisation de ces systèmes hétérogènes, complexes, dynamiques et distribués. Cependant, sa mise en œuvre varie en fonction du contexte du système, et exige des changements organisationnels et culturels. En effet, les systèmes de collaboration sont caractérisés par la nécessité de garantir l'autonomie des entités engagées, la confiance entre elles et le besoin de protection des informations sensibles de diverses natures échangées.

Dans cette thèse, nous proposons, une stratégie de sécurité Zero Trust dans un contexte de collaboration entre des organisations au sein d'un cloud communautaire. Le modèle présente une architecture hiérarchique pour sécuriser les échanges au sein et entre des organisations. Il fournit un système de gestion décentralisée des identités des utilisateurs et des organisations grâce aux identifiants décentralisés et aux informations d'identifications vérifiables. Cette méthode expose un moyen d'authentification continue des entités et de stockage des données dans un registre distribué de type blockchain. Par ailleurs, la démarche propose une technique d'évaluation de la confiance entre les organisations. En outre, la stratégie inclut un mécanisme de spécification de règles de politique d'accès et de suivi de contrat de collaboration. Des expérimentations ont été menées afin de prouver l'efficacité et la fiabilité des mécanismes proposés, fournissant ainsi une architecture et des mesures de sécurité associées pour le déploiement d'une stratégie Zero Trust dans un environnement de collaboration.

Title : Zero Trust security strategy in a community cloud environment

Keywords : Zero Trust, Trust, Decentralized identities, Blockchain, Access control, Community cloud

Abstract : Today's society is characterized by a highly mobile population and growing needs in terms of sharing large volumes of sensitive data within companies and collaborating with partner or competitor organizations. These collaborations bring many benefits to companies in terms of scalability and economic growth. However, the IT systems of these organizations are exposed to various types of increasingly sophisticated threats and cyberattacks. Traditional perimeter-based infrastructure security strategies are no longer sufficient. The Zero Trust security model is a cybersecurity approach that considers all entities in an infrastructure as potentially vulnerable at all times and everywhere. This strategy is positioned as a response to the problem of securing these heterogeneous, complex, dynamic, and distributed systems. However, its implementation varies according to the system context, and requires organizational and cultural changes.
Indeed, collaborative systems are characterized by the need to guarantee the autonomy of the entities involved, the trust between them and the need to protect sensitive information of various kinds exchanged.

In this thesis, we propose a Zero Trust security strategy in the context of collaboration between organizations within a community cloud. The model presents a hierarchical architecture for securing exchanges within and between organizations. It provides a decentralized management system for user and organizational identities using decentralized identifiers and verifiable credentials. This method exposes a means of continuous authentication of entities and storage of data in a blockchain-type distributed ledger. Furthermore, the approach offers a technique for assessing trust between organizations. The strategy also includes a mechanism for specifying access policy rules and monitoring collaboration contracts. Experiments have been carried out to prove the effectiveness and reliability of the proposed mechanisms, providing an architecture and associated security measures for deploying a Zero Trust strategy in a collaborative environment.